Cisco IOS IPS에서 라우터 및 SDM 및 Cisco IOS CLI 구성

목차

소개

Cisco 라우터 및 SDM(Security Device Manager) 2.2에서 Cisco IOS® IPS 컨피그레이션은 SDM 애플리케이션 내에 통합됩니다. Cisco IOS IPS를 구성하려면 별도의 창을 실행할 필요가 없습니다.

Cisco SDM 2.2에서 새로운 IPS 컨피그레이션 마법사는 라우터에서 Cisco IOS IPS를 활성화하는 데 필요한 단계를 안내합니다. 또한 고급 구성 옵션을 사용하여 Cisco SDM 2.2와 함께 Cisco IOS IPS를 활성화, 비활성화 및 조정할 수 있습니다.

Cisco에서는 사전 조정된 SDF(signature definition file)와 함께 Cisco IOS IPS를 실행할 것을 권장합니다. attack-drop.sdf, 128MB.sdf 및 256MB.sdf 이러한 파일은 메모리 양이 다른 라우터에 대해 생성됩니다. 이 파일은 Cisco SDM과 함께 번들로 제공되며, 이는 라우터에서 Cisco IOS IPS를 처음 활성화할 때 SDF를 권장합니다. 이러한 파일은 http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup에서 다운로드할 수도 있습니다(등록된 고객만 해당).

기본 SDF를 활성화하는 프로세스는 Enable Cisco IOS IPS with a Factory Default SDF에 자세히 설명되어 있습니다. 기본 SDF가 충분하지 않거나 새 서명을 추가하려는 경우 기본 SDF를 활성화한 후 Append Additional Signatures에 설명된 절차를 사용할 수 있습니다.

사전 요구 사항

요구 사항

Cisco SDM 2.2를 사용하려면 JRE(Java Runtime Environment) 버전 1.4.2 이상이 필요합니다. DRAM을 기반으로 하는 Cisco에서 권장하고 조정된 서명 파일은 Cisco SDM과 함께 번들로 제공됩니다(Cisco SDM과 함께 라우터 플래시 메모리에 로드됨).

사용되는 구성 요소

이 문서의 정보는 Cisco 라우터 및 SDM 2.2를 기반으로 합니다.

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

공장 기본 SDF로 Cisco IOS IPS 활성화

CLI 절차

CLI를 사용하여 Cisco 1800 Series 라우터와 Cisco IOS IPS를 구성하여 라우터 플래시에 128MB.sdf를 로드하려면 이 절차를 완료합니다.

1. SDEE(Security Device Event Exchange) 이벤트 알림을 사용하도록 라우터를 구성합니다.
   ```
   yourname#conf t
   ```

2. 구성 명령(한 줄에 하나씩)을 입력한 다음 Cntl+Z를 눌러 종료합니다.
   ```
   yourname(config)#ip ips notify sdee
   ```

3. 인터페이스에 연결하는 데 사용되는 IPS 규칙 이름을 생성합니다.
   ```
   yourname(config)#ip ips name myips
   ```

4. Cisco IOS IPS 시스템에서 서명을 읽을 파일을 지정하도록 IPS location 명령을 구성합니다.이 예에서는 flash에서 파일을 사용합니다. 128MB.sdf 이 명령의 위치 URL 부분은 파일을 가리키도록 FTP, HTTP, HTTPS, RTP, SCP 및 TFTP를 통해 플래시, 디스크 또는 프로토콜을 사용하는 유효한 URL일 수 있습니다.
   ```
   yourname(config)#ip ips sdf location flash:128MB.sdf
   ```

   참고: 텔넷 세션을 통해 라우터를 구성하는 경우 **terminal monitor** 명령을 활성화해야 합니다. 그렇지 않으면 시그니처 엔진이 빌드될 때 SDEE 메시지가 표시되지 않습니다.
5. Cisco IOS IPS가 트래픽을 스캔하도록 활성화하려는 인터페이스에서 IPS를 활성화합니다. 이 경우 인터페이스 fastEthernet 0에서 양방향으로 활성화했습니다.
   ```
   yourname(config)#interface fastEthernet 0
   yourname(config-if)#ip ips myips in
   *Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS:
           SDF loaded successfully from opacl
   *Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS:
           SDF loaded successfully from flash:128MB.sdf
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
           OTHER - 4 signatures - 1 of 15 engines
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_READY:
           OTHER - 0 ms - packets for this engines will be scanned
   *Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
           MULTI-STRING - 0 signatures - 2 of 15 engines
   ```

```
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED:
        MULTI-STRING - there are no new signature definitions for this engine
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
        STRING.ICMP - 1 signatures - 3 of 15 engines
*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
        STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-ENGINE_BUILDING:
        STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-ENGINE_READY:
        STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26 00:32:31.393: %IPS-6-ENGINE_BUILDING:
        STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26 00:32:33.641: %IPS-6-ENGINE_READY:
        STRING.TCP - 2248 ms - packets for this engine will be scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING:
        SERVICE.FTP - 3 signatures - 6 of 15 engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY:
        SERVICE.FTP - 16 ms - packets for this engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING:
        SERVICE.SMTP - 2 signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY:
        SERVICE.SMTP - 28 ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
        SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
        SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-ENGINE_BUILDING:
        SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-6-ENGINE_READY:
        SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:33.801: %IPS-6-ENGINE_BUILDING:
        SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct 26 00:32:44.505: %IPS-6-ENGINE_READY:
        SERVICE.HTTP - 10704 ms - packets for this engine will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING:
        ATOMIC.TCP - 11 signatures - 11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY:
        ATOMIC.TCP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING:
        ATOMIC.UDP - 9 signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.UDP - 4 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILD_SKIPPED:
        ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.IPOPTIONS - 0 ms - packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
        ATOMIC.L3.IP - 5 signatures - 15 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY:
        ATOMIC.L3.IP - 0 ms - packets for this engine will be scanned
yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```

IPS 규칙이 인터페이스에 처음 적용될 때 Cisco IOS IPS는 SDF locations 명령으로 지정한 파일에서 빌드 서명을 시작합니다. SDEE 메시지는 콘솔에 로깅되며 구성된 경우 syslog 서버로 전송됩니다. <*number*>개 엔진의 SDEE 메시지는 시그니처 엔진 구축 프로세스를 나타냅니다. 마지막으로, 두 숫자가 동일하면 모든 엔진이 구축됩니다.**참고:** IP 가상 리어셈블리는 (켜지면) 해당 인터페이스를 통해 라우터로 들어오는 조각화된 패킷을 자동으로 리어셈블하는 인터

페이스 기능입니다. Cisco에서는 트래픽이 라우터로 들어오는 모든 인터페이스에서 ip virtual-assembly를 활성화할 것을 권장합니다. 위의 예에서는 인터페이스 fastEthernet 0에서 "ip virtual-assembly"를 켜는 것 외에도 내부 인터페이스 VLAN 1에서도 이를 구성합니다.

```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

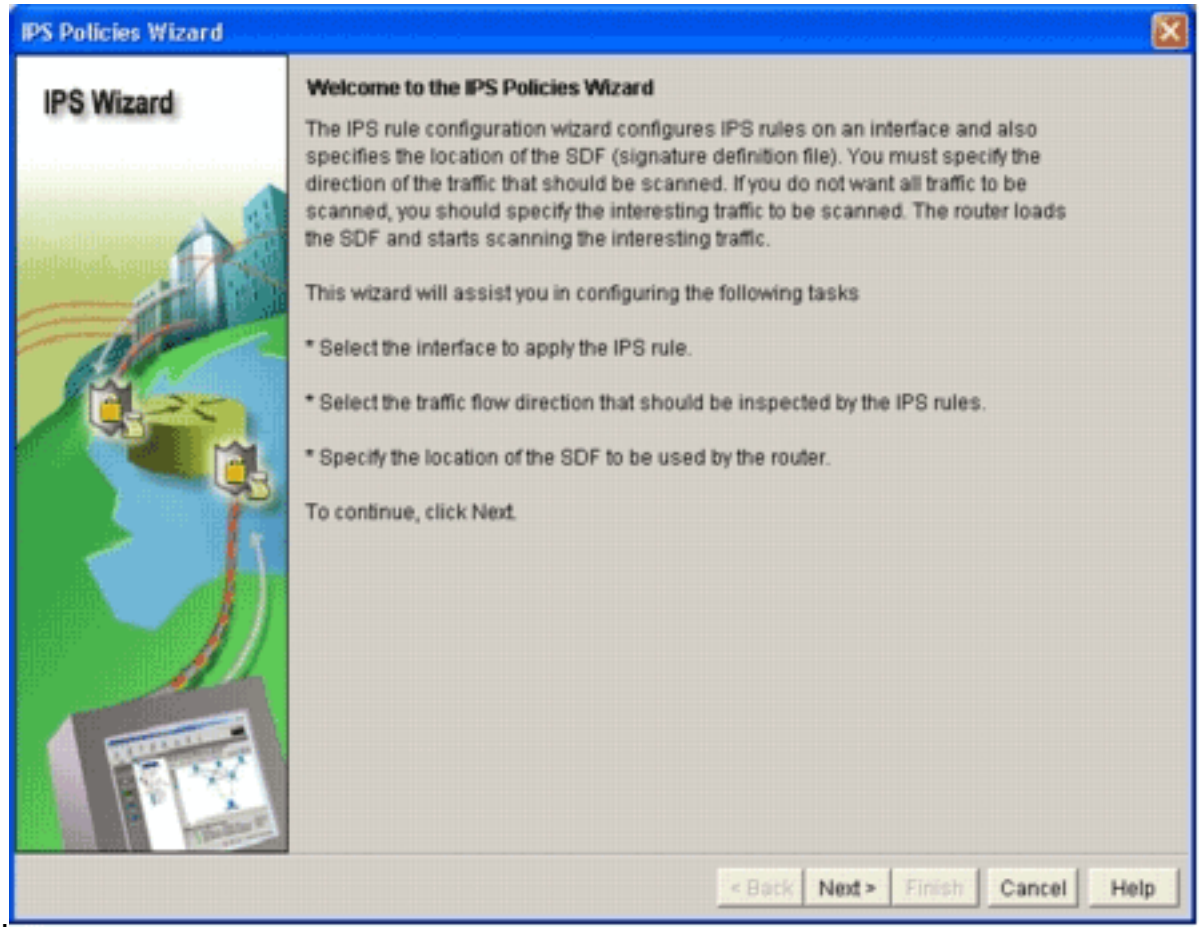
SDM 2.2 절차

Cisco SDM 2.2를 사용하여 Cisco 1800 Series 라우터와 Cisco IOS IPS를 구성하려면 이 절차를 완료합니다.

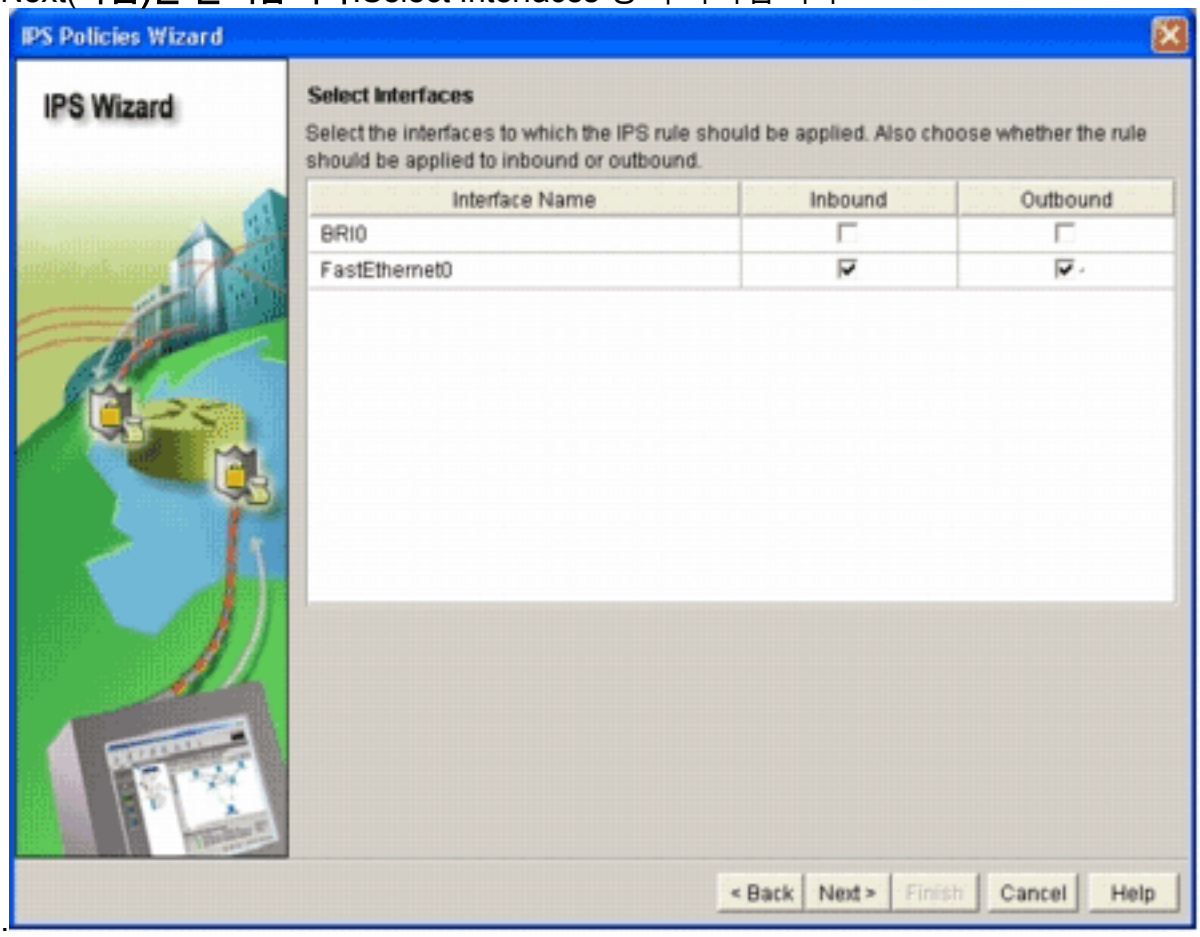
1. SDM 애플리케이션에서 Configure를 클릭한 다음 **Intrusion Prevention**을 클릭합니다

2. Create **IPS** 탭을 클릭한 다음 **Launch IPS Rule Wizard를 클릭합니다**.Cisco SDM은 Cisco IOS IPS 기능을 구성하려면 SDEE를 통한 IPS 이벤트 알림이 필요합니다. 기본적으로 SDEE 알림은 활성화되지 않습니다. Cisco SDM은 다음 이미지에 표시된 대로 SDEE를 통해 IPS 이벤트 알림을 활성화하라는 메시지를 표시합니다

3. **확인**을 **클릭합니다**.IPS Policies Wizard 대화 상자의 Welcome to the IPS Policies Wizard 창이 나타납니다

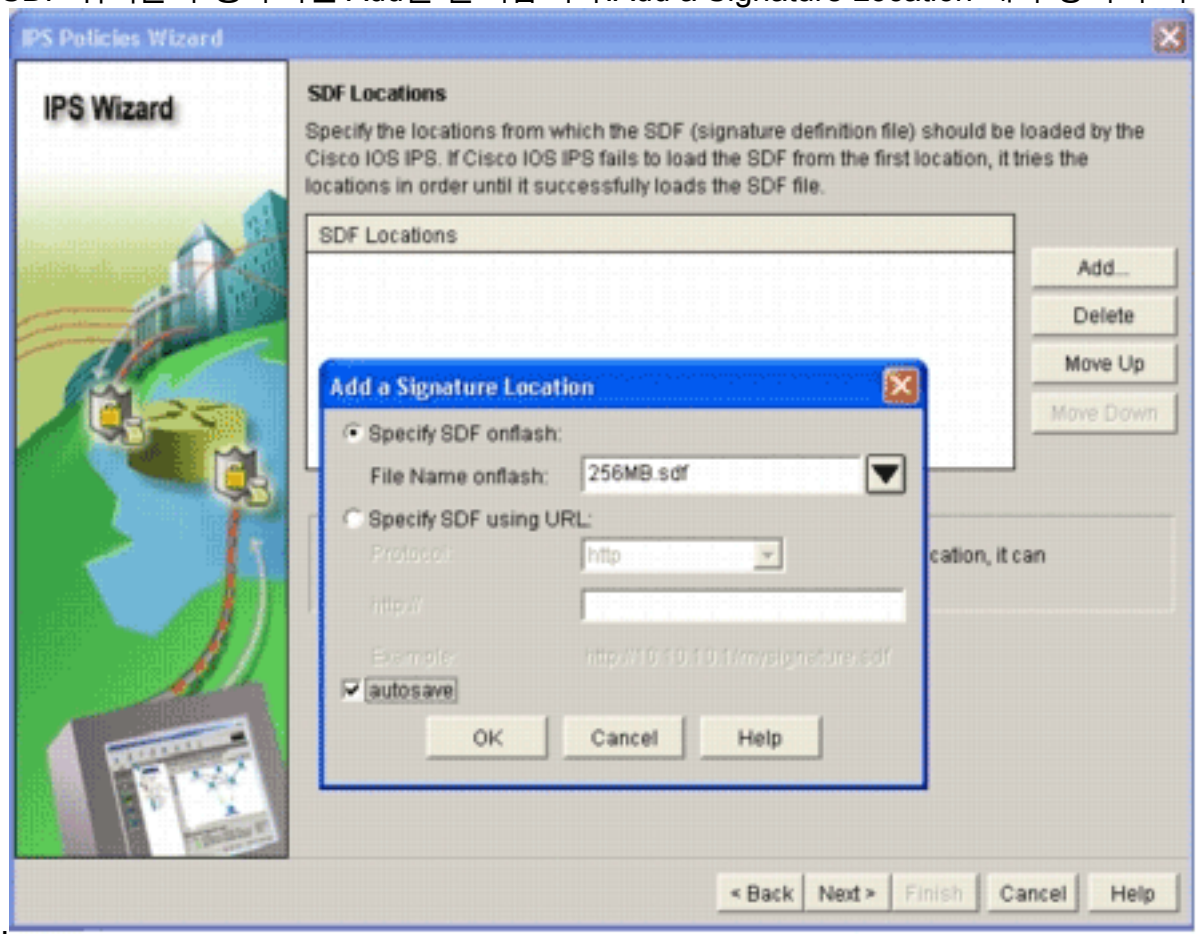


4. Next(**다음)를 클릭합니다**.Select Interfaces 창이 나타납니다

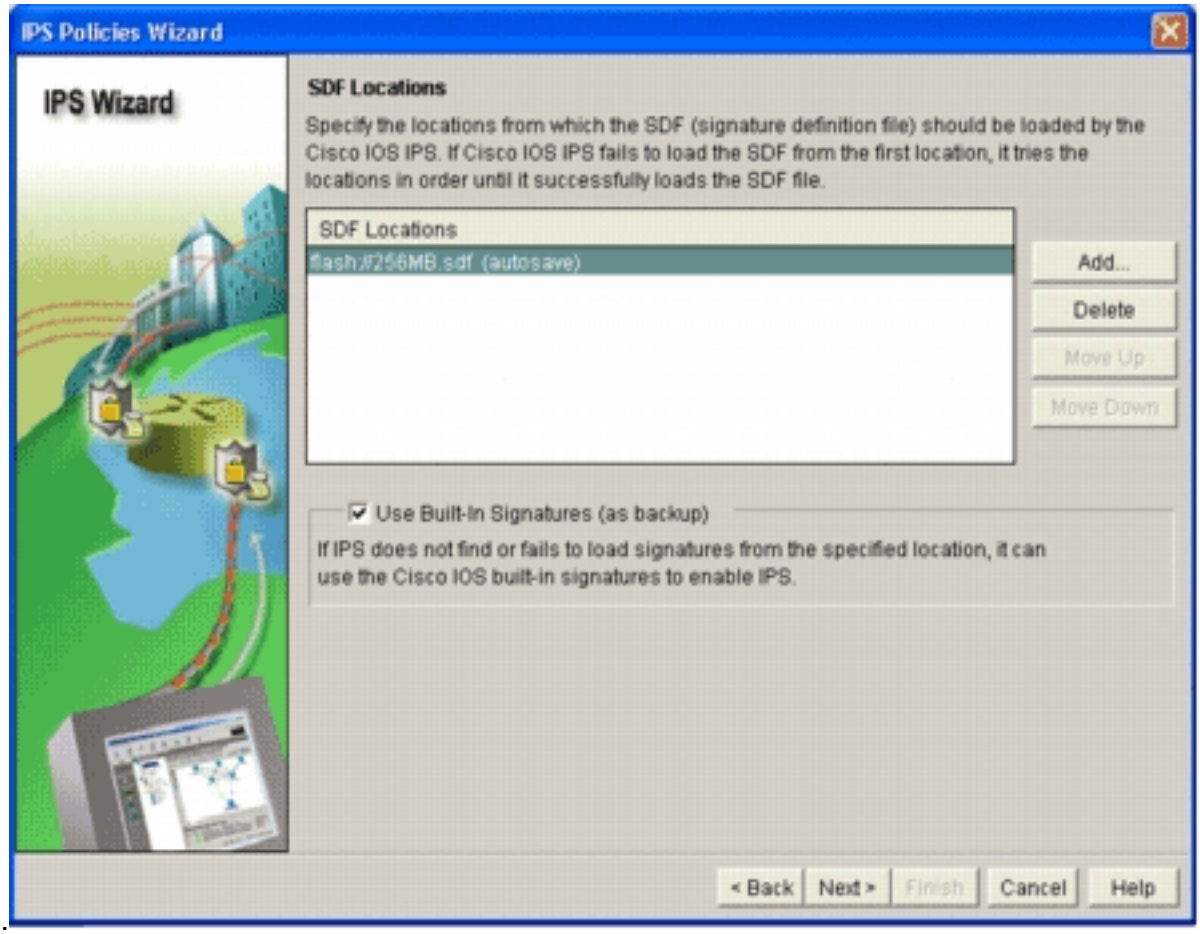


5. IPS를 활성화할 인터페이스를 선택하고 해당 인터페이스의 방향을 나타내려면 **Inbound** 또는 **Outbound** 확인란을 클릭합니다.**참고:** 인터페이스에서 IPS를 활성화할 경우 인바운드 및 아웃바운드 방향을 모두 활성화하는 것이 좋습니다.

6. Next(**다음)를 클릭합니다**.SDF Locations(SDF 위치) 창이 나타납니다.
7. SDF 위치를 구성하려면 Add를 클릭합니다.Add a Signature Location 대화 상자가 나타납니다

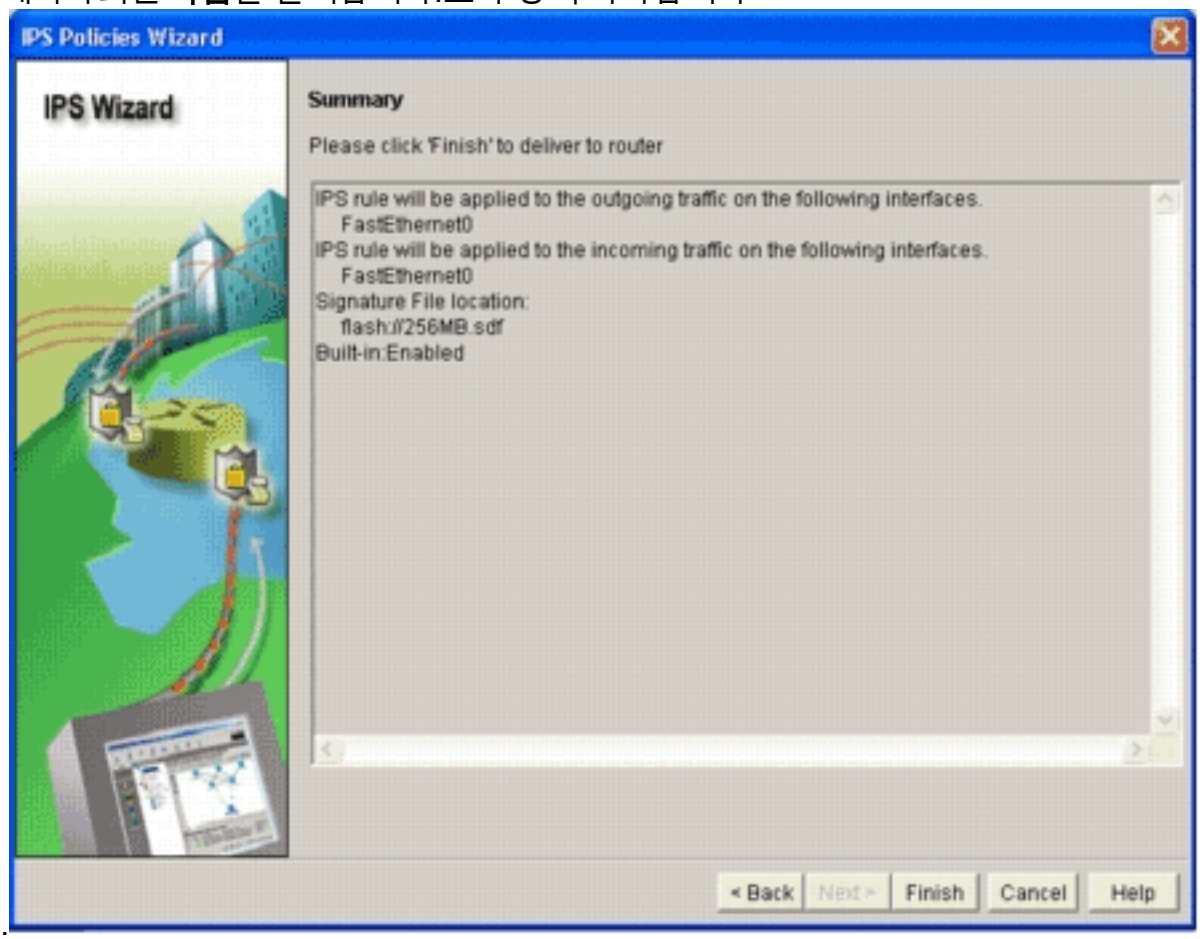


8. **Specify SDF on flash** 라디오 버튼을 클릭하고 **File Name on flash** 드롭다운 목록에서 256MB.sdf**를** 선택합니다.
9. 자동 **저장** 확인란을 클릭하고 **확인**을 클릭합니다.**참고:** 서명이 변경되면 자동 저장 옵션은 서명 파일을 자동으로 저장합니다.SDF 위치 창에 새 SDF 위치가 표시됩니다

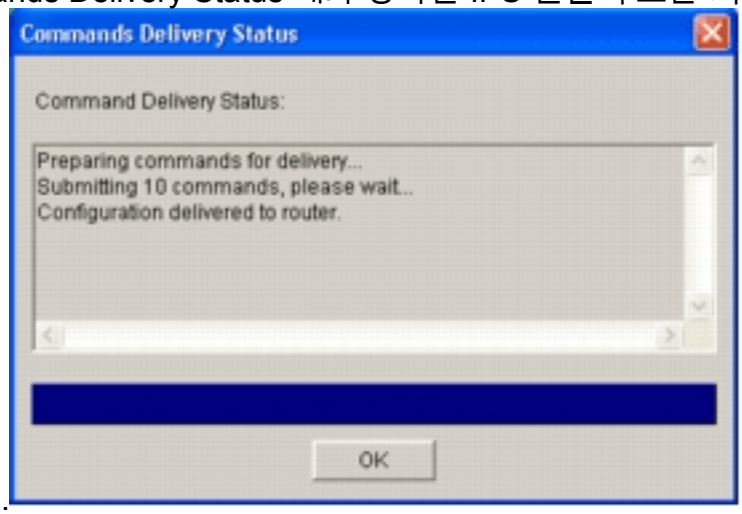


참고: 백업을 지정하기 위해 서명 위치를 추가할 수 있습니다.

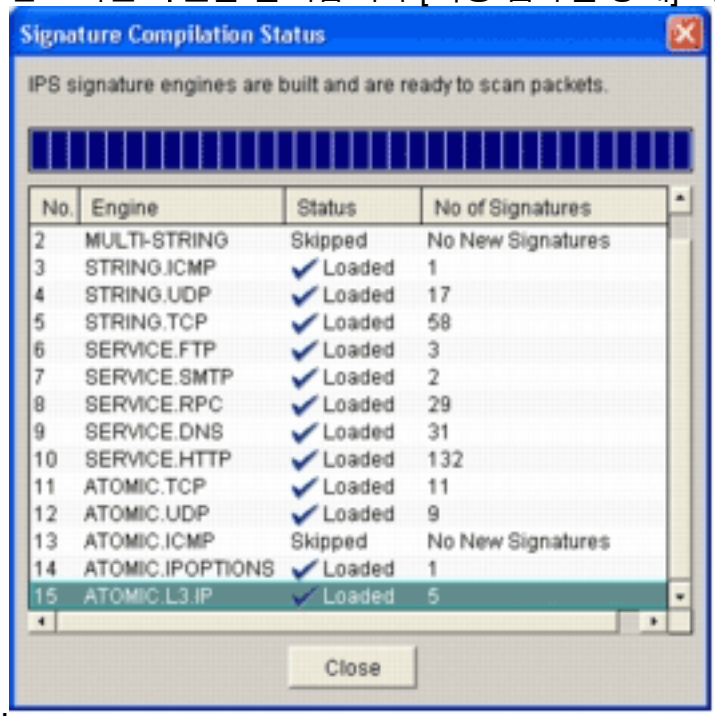
10. Use **Built-In Signatures (as backup)(기본 서명(백업으로 사용)** 확인란을 클릭합니다.**참고:** 하나 이상의 위치를 지정하지 않는 한 내장 서명 옵션을 사용하지 않는 것이 좋습니다.
11. 계속하려면 **다음**을 클릭합니다.요약 창이 나타납니다



12. **마침**을 **클릭합니다**.Commands Delivery Status 대화 상자는 IPS 엔진이 모든 서명을 컴파일 할 때의 상태를 표시합니다.

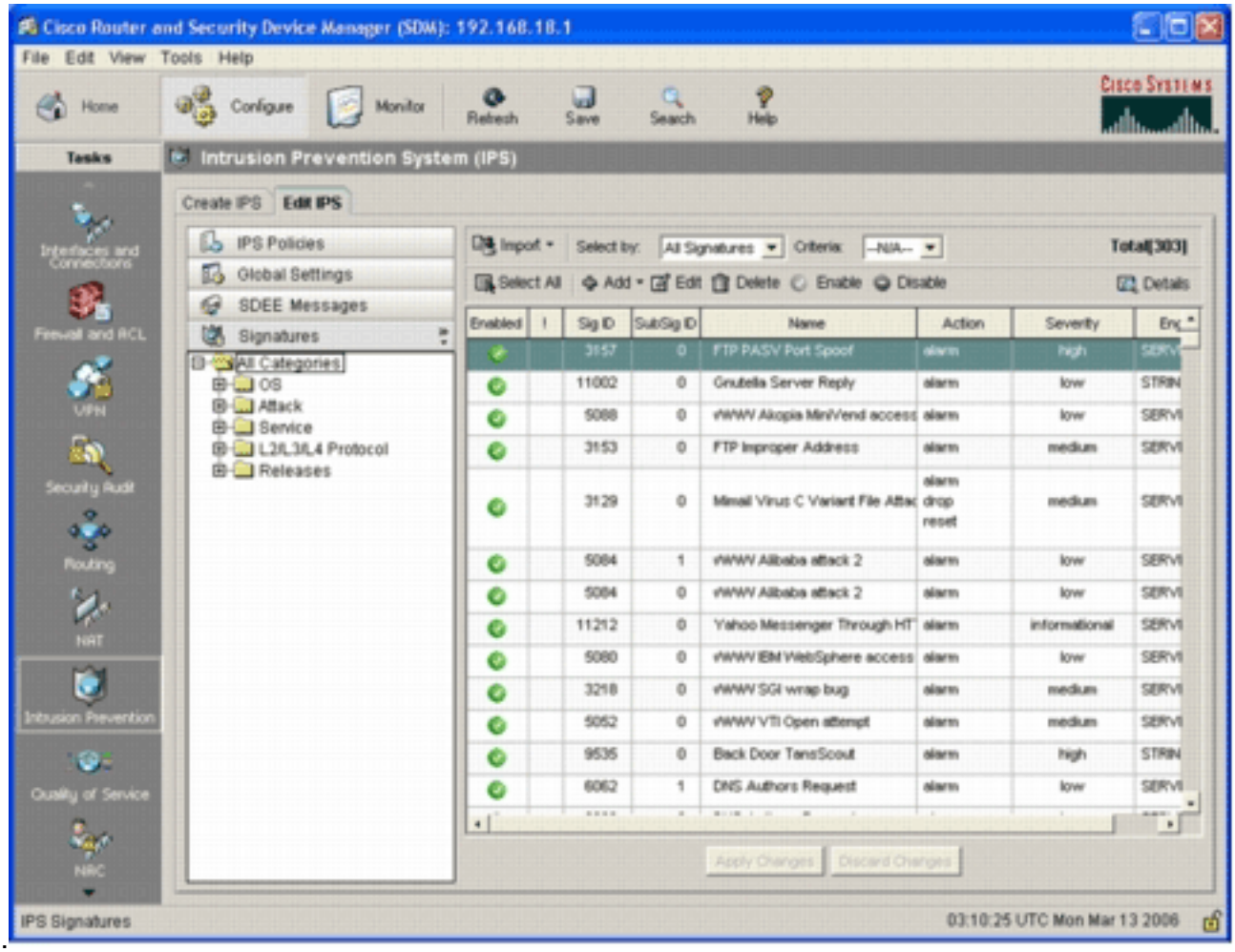


13. 프로세스가 완료되면 **확인**을 클릭합니다.[서명 컴파일 상태] 대화 상자에 서명 컴파일 정보가 표시됩니다.



이 정보는 컴파일된 엔진 및 해당 엔진의 서명 수를 보여줍니다. 상태 열에 *Skipped*를 표시하는 엔진의 경우 해당 엔진에 대한 시그니처가 로드되지 않습니다.

14. Signature **Compilation** Status 대화 상자를 닫으려면 Close를 클릭합니다.
15. 라우터에 현재 로드되어 있는 시그니처를 확인하려면 Configure(구성)**를** 클릭한 다음 **Intrusion Prevention(침입 방지)을** 클릭합니다.
16. Edit **IPS(IPS 편집**) 탭을 클릭한 다음 Signatures(서명)를 **클릭합니다**.IPS 서명 목록이 Signatures 창에 나타납니다



기본 SDF 활성화 후 추가 서명 추가

CLI 절차

분산 IOS-Sxxx.zip 파일에서 시그니처를 생성하거나 시그니처 정보를 읽는 데 사용할 수 있는 CLI 명령이 없습니다. Cisco에서는 SDM 또는 Management Center for IPS Sensor를 사용하여 Cisco IOS IPS 시스템의 서명을 관리하는 것이 좋습니다.

이미 서명 파일이 준비되었으며 Cisco IOS IPS 시스템에서 실행되는 SDF와 이 파일을 병합하려는 고객의 경우 다음 명령을 사용할 수 있습니다.

```
yourname#show running-config | include ip ips sdf
ip ips sdf location flash:128MB.sdf
yourname#
```

signature location 명령으로 정의된 서명 파일은 라우터가 재로드할 때 또는 라우터 IOS IPS가 재구성된 경우 시그니처 파일을 로드하는 파일입니다. 병합 프로세스가 성공하려면 signature file location 명령으로 정의된 파일도 업데이트해야 합니다.

1. 현재 구성된 서명 위치를 확인하려면 **show** 명령을 사용합니다.출력에는 구성된 서명 위치가 표시됩니다. 이 명령은 현재 실행 중인 시그니처가 로드되는 위치를 보여줍니다.
   ```
   yourname#show ip ips signatures
   Builtin signatures are configured
   ```
   플래시에서 서명이 마지막으로 로드됨:128MB.sdfCisco SDF 릴리스 버전 S128.0트렌드 SDF 릴리스 버전 V0.0
2. 서명 파일을 병합하려면 **copy <*url*> ips-sdf** 명령을 이전 단계의 정보와 함께 사용합니다.

```
yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf
Loading mysignatures.xml from 10.10.10.5 (via Vlan1): !
[OK - 1612 bytes]
*Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport
4715
*Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from
        tftp://10.10.10.5/mysignatures.xml
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature
        definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures -
        2 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures -
        3 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures -
        4 of 15 engines
*Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are
        no new signature definitions for this engine
*Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures -
        5 of 15 engines
*Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False -
        This parameter is not supported
*Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this
        engine will be scanned
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures -
        6 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures -
        7 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures -
        8 of 15 engines
*Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures -
        9 of 15 engines
*Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures -
        10 of 15 engines
*Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
        11 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures -
        12 of 15 engines
*Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures -
        13 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures -
        14 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are
```

```
        no new signature definitions for this engine
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures -
        15 of 15 engines
*Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are
        no new signature definitions for this engine
yourname#
```

copy 명령을 실행하면 라우터가 서명 파일을 메모리에 로드한 다음 서명 엔진을 구축합니다. 콘솔 SDEE 메시지 출력에서 각 서명 엔진의 빌드 상태가 표시됩니다.%IPS-6-ENGINE_BUILD_SKIPPED는 이 엔진에 대한 새 서명이 없음을 나타냅니다.%IPS-6-ENGINE_READY는 새 시그니처가 있으며 엔진이 준비되었음을 나타냅니다. 이전과 같이 "15/15 엔진" 메시지는 모든 엔진이 구축되었음을 나타냅니다.IPS-7-UNSUPPORTED_PARAM은 특정 매개변수가 Cisco IOS IPS에서 지원되지 않음을 나타냅니다. 예를 들어, CapturePacket 및 ResetAfterIdle입니다.**참고:** 이러한 메시지는 정보 전용이며 Cisco IOS IPS 서명 기능 또는 성능에 영향을 미치지 않습니다. 디버깅(수준 7)보다 높은 로깅 수준을 설정하여 이러한 로깅 메시지를 끌 수 있습니다.

3. 라우터가 다시 로드될 때 병합된 시그니처 세트가 업데이트된 시그니처와 함께 있도록 signature location 명령으로 정의된 SDF를 업데이트합니다. 이 예에서는 병합된 서명이 128MB.sdf 플래시 파일에 저장된 후의 파일 크기 차이를 보여 줍니다.

```
yourname#show flash:
-#- --length-- -----date/time------ path
4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf
yourname#copy ips-sdf flash:128MB.sdf
yourname#show flash:
-#- --length-- -----date/time------ path
4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf
```

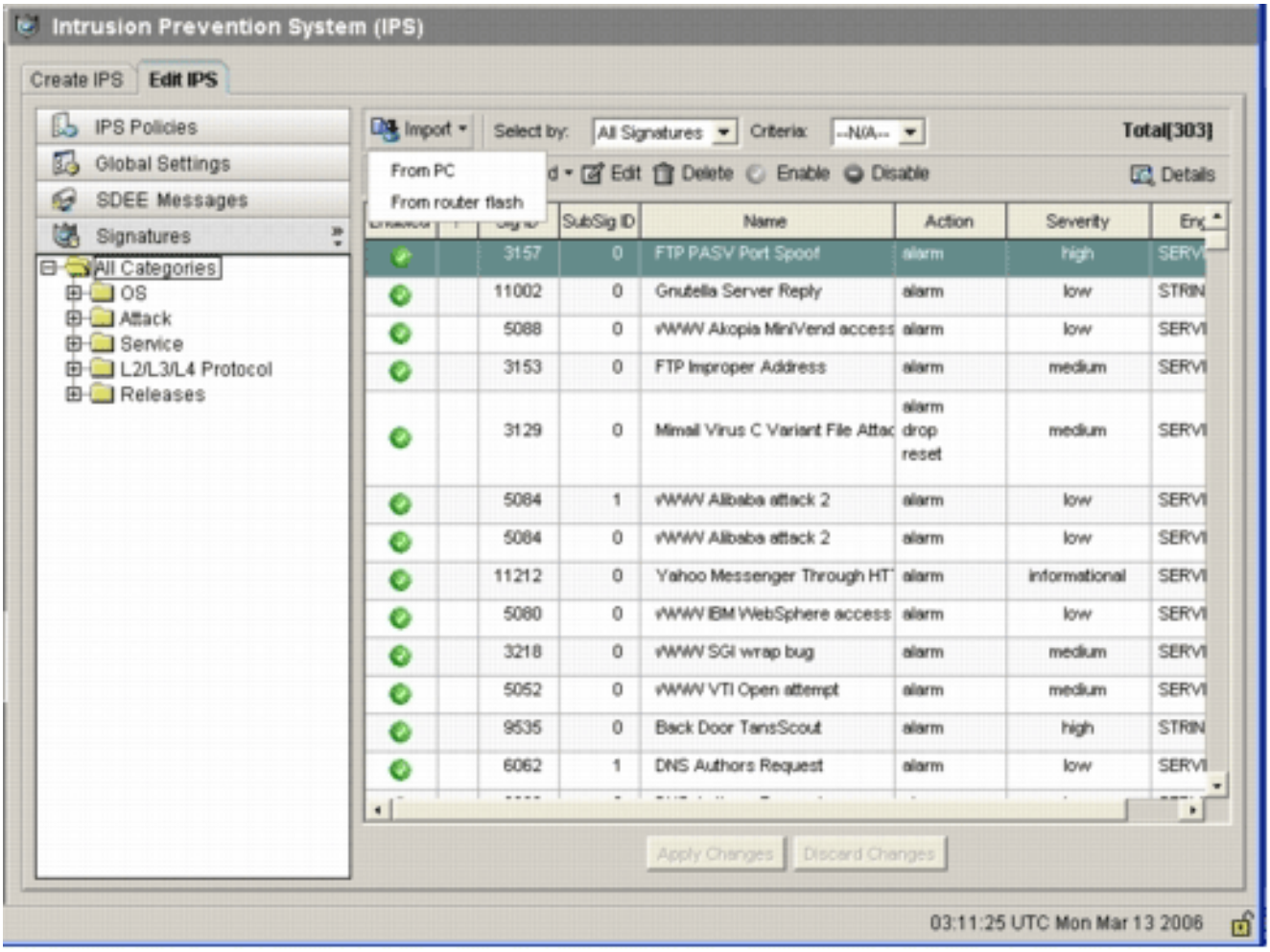
경고: 이제 새로운 128MB.sdf에 고객이 병합한 서명이 포함되어 있습니다. 내용은 Cisco 기본 128MB.sdf 파일과 다릅니다. 혼동을 방지하기 위해 이 파일을 다른 이름으로 변경하는 것이 좋습니다. 이름이 변경되면 signature location 명령도 변경해야 합니다.

SDM 2.2 절차

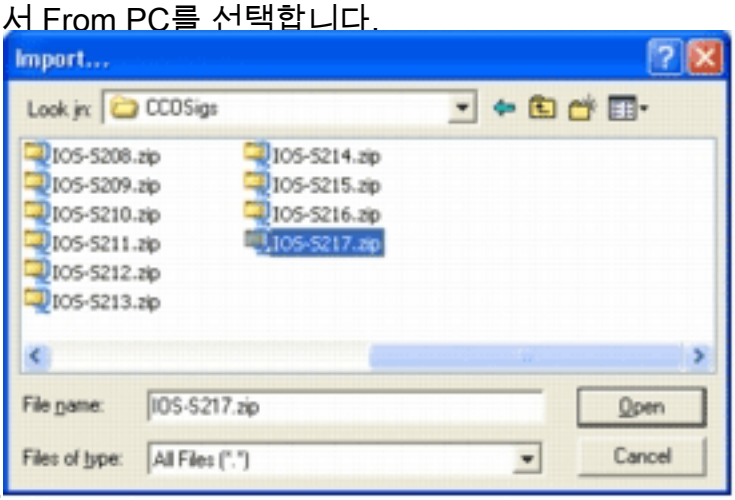
Cisco IOS IPS가 활성화되면 Cisco SDM 가져오기 기능으로 서명 세트를 실행하는 라우터에 새 서명을 추가할 수 있습니다. 새 서명을 가져오려면 다음 단계를 완료합니다.

1. 기본 SDF 또는 IOS-Sxxx.zip 업데이트 파일을 선택하여 추가 서명을 가져옵니다.
2. Configure(**구성**)를 클릭한 다음 **Intrusion Prevention(침입 방지)을 클릭합니다**.
3. Edit **IPS** 탭을 클릭한 다음 Import를 **클릭합니다**

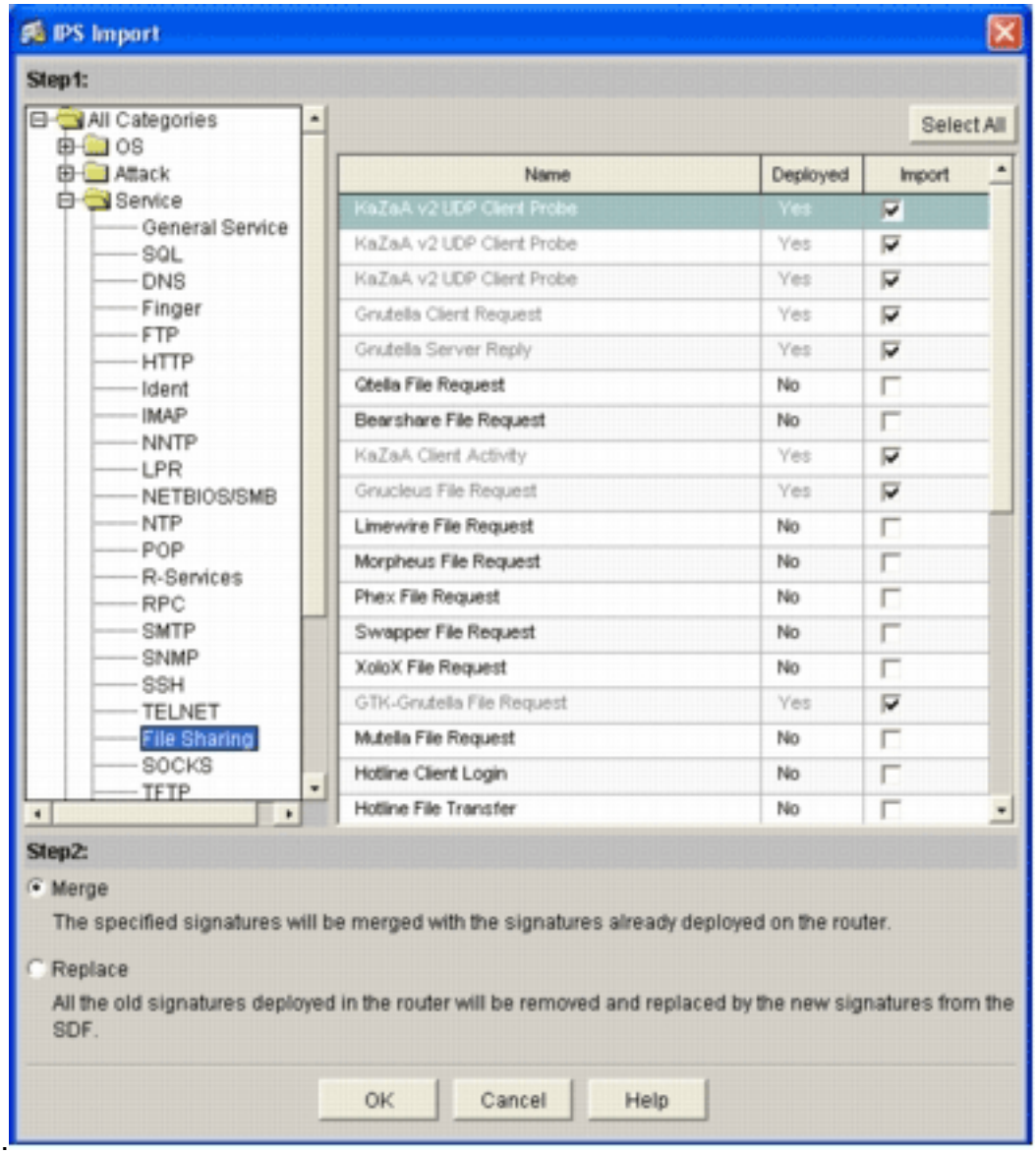
.



4. Import(**가져오기**) 드롭다운 목록에서 From PC를 선택합니다.

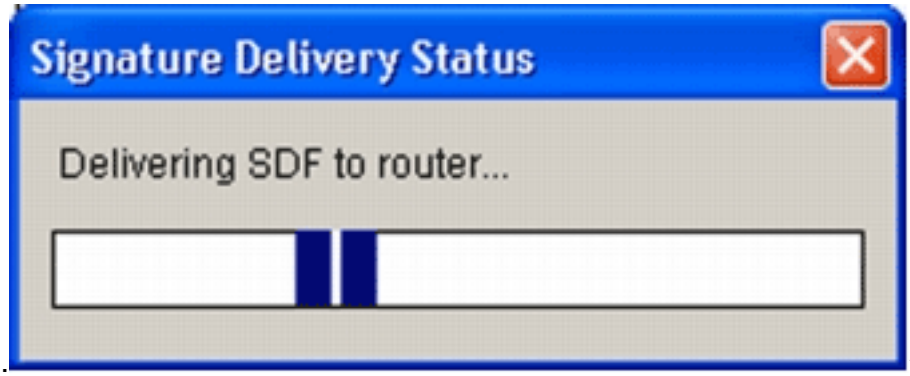


5. 서명을 가져올 파일을 선택합니다. 이 예에서는 Cisco.com에서 다운로드되고 로컬 PC 하드 디스크에 저장된 최신 업데이트를 사용합니다.
6. **열기**를 **클릭합니다.경고:** 메모리 제약 조건 때문에 이미 배포된 서명 위에 제한된 수의 새 서명만 추가할 수 있습니다. 너무 많은 서명을 선택한 경우, 메모리가 부족하여 라우터가 모든 새 서명을 로드하지 못할 수 있습니다.시그니처 파일 로드가 완료되면 IPS Import 대화 상자가 나



타납니다.

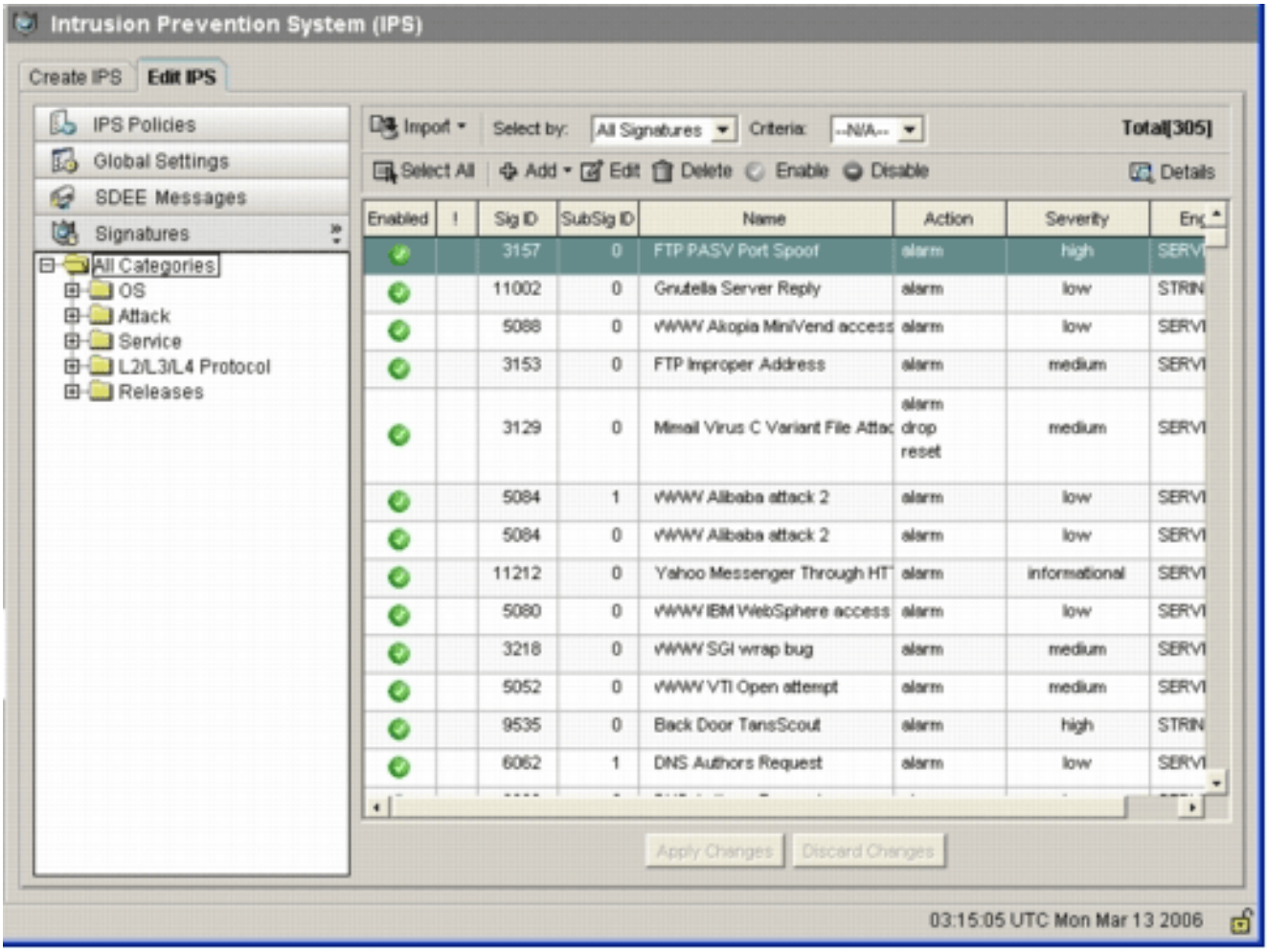
7. 왼쪽 트리 보기를 탐색하고 가져올 서명 옆에 있는 **Import** 확인란을 클릭합니다.
8. **병합** 라디오 버튼을 클릭한 다음 **확인**을 클릭합니다.**참고:** Replace 옵션은 라우터의 현재 시그니처 세트를 가져오도록 선택한 서명으로 대체합니다.확인을 클릭하면 Cisco SDM 애플리케이션이 라우터에 서명을 전달합니다



참고: 서명을 컴파일하고 로드하는 동안 CPU 사용률이 높습니다. 인터페이스에서 Cisco IOS IPS가 활성화되면 서명 파일이 로드되기 시작합니다. 라우터가 SDF를 로드하는 데 약 5분이 걸립니다. Cisco IOS 소프트웨어 CLI에서 CPU 사용률을 보려면 **show process cpu** 명령을 사용할 수 있습니다. 그러나 라우터가 SDF를 로드하는 동안에는 추가 명령을 사용하거나 다른 SDF를 로드하지 마십시오. 이렇게 하면 서명 컴파일 프로세스가 완료하는 데 더 오래 걸릴 수 있습니다. SDF를 로드할 때 CPU 사용률이 100%에 근접하기 때문입니다. 서명 목록이 *활성화됨* 상태가 아닌 경우 해당 서명 목록을 찾아보고 서명을 활성화해야 할 수 있습니다.총 서명 번호가 519로 증가했습니다. 이 숫자는 파일 공유 하위 범주에 속하는 IOS-S193.zip 파일에서 사용 가능한 모든 서명을 포

함합니다

.



Cisco SDM을 사용하여 Cisco IOS IPS 기능을 관리하는 방법에 대한 자세한 내용은 다음 URL에서 Cisco SDM 설명서를 참조하십시오.

서명 선택 및 서명 범주 작업

네트워크에 대한 올바른 서명을 효과적으로 선택하는 방법을 결정하려면 보호 중인 네트워크에 대한 몇 가지 사항을 알아야 합니다. Cisco SDM 2.2 이상에서 업데이트된 서명 범주 정보를 통해 고객이 네트워크를 보호할 올바른 서명 집합을 선택할 수 있도록 지원합니다.

범주는 서명을 그룹화하는 방법입니다. 서명과 관련된 서명의 하위 집합으로 시그니처 선택을 좁히는 데 도움이 됩니다. 하나의 시그니처는 하나의 카테고리에만 속할 수 있거나 여러 카테고리에 속할 수 있습니다.

다음은 5가지 최상위 범주입니다.

- OS—운영 시스템 기반 시그니처 분류
- 공격 - 공격 기반 시그니처 분류
- 서비스—서비스 기반 시그니처 분류
- Layer 2-4 Protocol—프로토콜 레벨 기반 시그니처 분류
- 릴리스—릴리스 기반 시그니처 분류

이러한 각 범주는 하위 범주로 구분됩니다.

예를 들어, 인터넷에 광대역 연결을 사용하는 홈 네트워크와 기업 네트워크에 대한 VPN 터널을 고려하십시오. 광대역 라우터는 인터넷에 대한 개방형(비 VPN) 연결에서 Cisco IOS Firewall을 활성

화하여 인터넷에서 시작된 연결이 홈 네트워크에 연결되는 것을 방지합니다. 홈 네트워크에서 인터넷으로 시작되는 모든 트래픽이 허용됩니다. 사용자가 Windows 기반 PC를 사용하고 HTTP(웹 브라우징) 및 전자 메일과 같은 애플리케이션을 사용한다고 가정합니다.

사용자가 필요로 하는 애플리케이션만 라우터를 통과할 수 있도록 방화벽을 구성할 수 있습니다. 이렇게 하면 네트워크 전체에 퍼질 수 있는 원치 않는 트래픽과 잠재적 악성 트래픽의 흐름을 제어할 수 있습니다. 홈 사용자가 특정 서비스를 필요로 하거나 사용하지 않는 것을 고려하십시오. 해당 서비스가 방화벽을 통과할 수 있도록 허용되면, 공격이 네트워크 전체에서 흐름에 사용할 수 있는 잠재적인 구멍이 있습니다. 모범 사례에서는 필요한 서비스만 허용합니다. 이제 활성화할 서명을 선택하는 것이 더 쉽습니다. 방화벽을 통과하도록 허용하는 서비스에 대해서만 서명을 활성화해야 합니다. 이 예에서 서비스는 이메일 및 HTTP를 포함합니다. Cisco SDM은 이 구성을 간소화합니다.

범주를 사용하여 필수 서명을 선택하려면 **Service(서비스) > HTTP**를 선택하고 모든 서명을 활성화합니다. 이 선택 프로세스는 모든 HTTP 서명을 선택하여 라우터로 가져올 수 있는 서명 가져오기 대화 상자에서도 작동합니다.

DNS, NETBIOS/SMB, HTTPS 및 SMTP를 선택해야 하는 추가 범주가 있습니다.

기본 SDF 파일에 대한 서명 업데이트

빌트당 3개의 SDF(attack-drop.dsf, 128MB.sdf 및 256MB.sdf)는 현재 Cisco.com의 http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup에 게시되어 있습니다(등록된 고객만 해당). 이러한 파일의 최신 버전은 사용 가능한 즉시 게시됩니다. 이러한 기본 SDF로 Cisco IOS IPS를 실행하는 라우터를 업데이트하려면 웹 사이트로 이동하여 이러한 파일의 최신 버전을 다운로드하십시오.

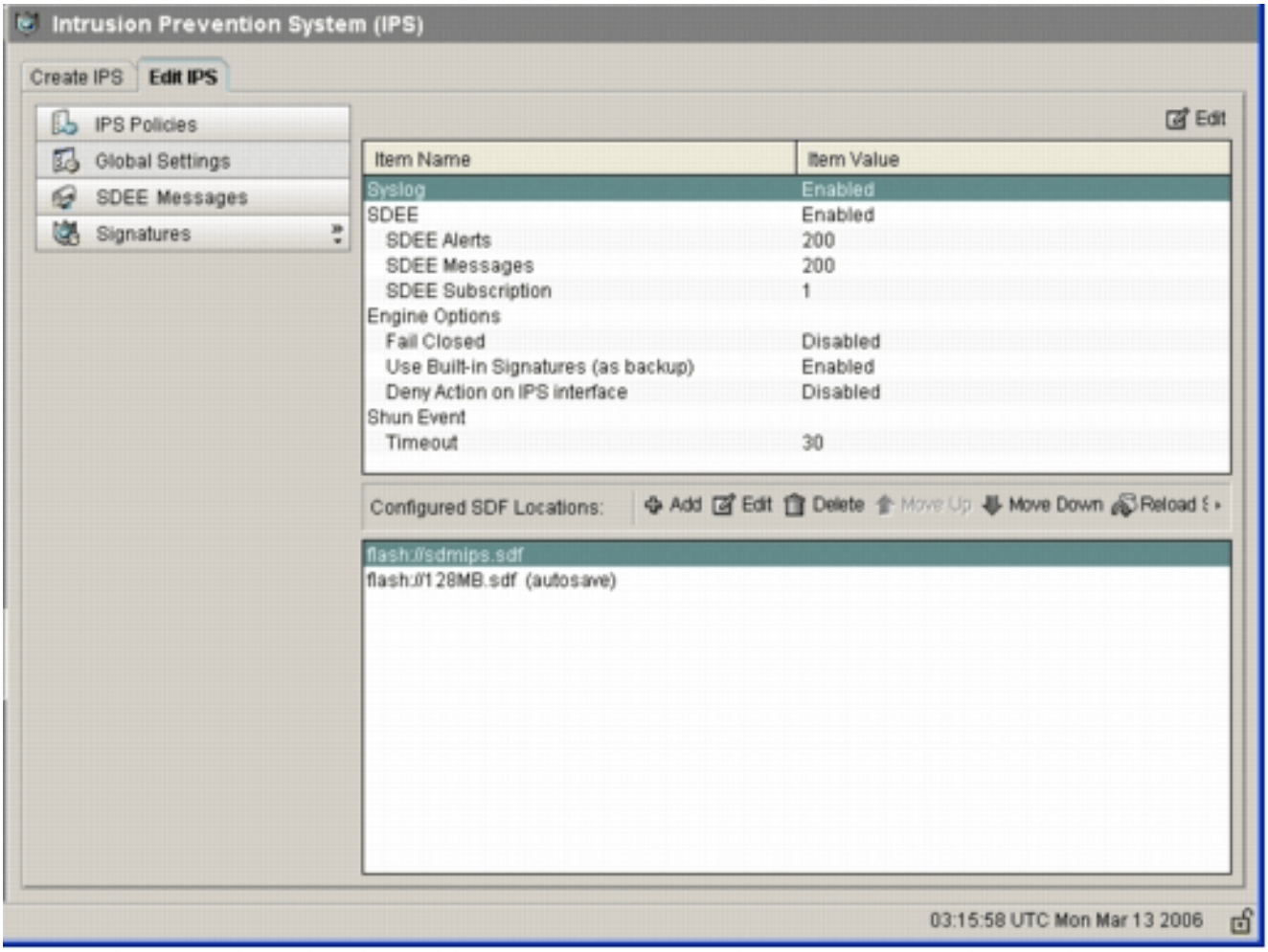
CLI 절차

1. 다운로드한 파일을 라우터에서 이러한 파일을 로드하도록 구성된 위치에 복사합니다. 라우터가 현재 구성된 위치를 확인하려면 show running-**config를** 사용합니다. **ip ips sdf** 명령**에서**|.
   ```
   Router#show running-config | in ip ips sdf
   ip ips sdf location flash://256MB.sdf autosave
   ```
   이 예에서 라우터는 플래시에 256MB.sdf를 사용합니다. 다운로드한 새 256MB.sdf를 라우터 플래시에 복사할 때 파일이 업데이트됩니다.
2. Cisco IOS IPS 하위 시스템을 다시 로드하여 새 파일을 실행합니다.Cisco IOS IPS를 다시 로드하는 방법에는 두 가지가 있습니다. 라우터를 다시 로드하거나 Cisco IOS IPS를 재구성하여 서명을 다시 로드하기 위해 IOS IPS 하위 시스템을 트리거합니다. Cisco IOS IPS를 재구성하려면 구성된 인터페이스에서 모든 IPS 규칙을 제거한 다음 다시 인터페이스에 IPS 규칙을 다시 적용합니다. 그러면 Cisco IOS IPS 시스템이 다시 로드됩니다.

SDM 2.2 절차

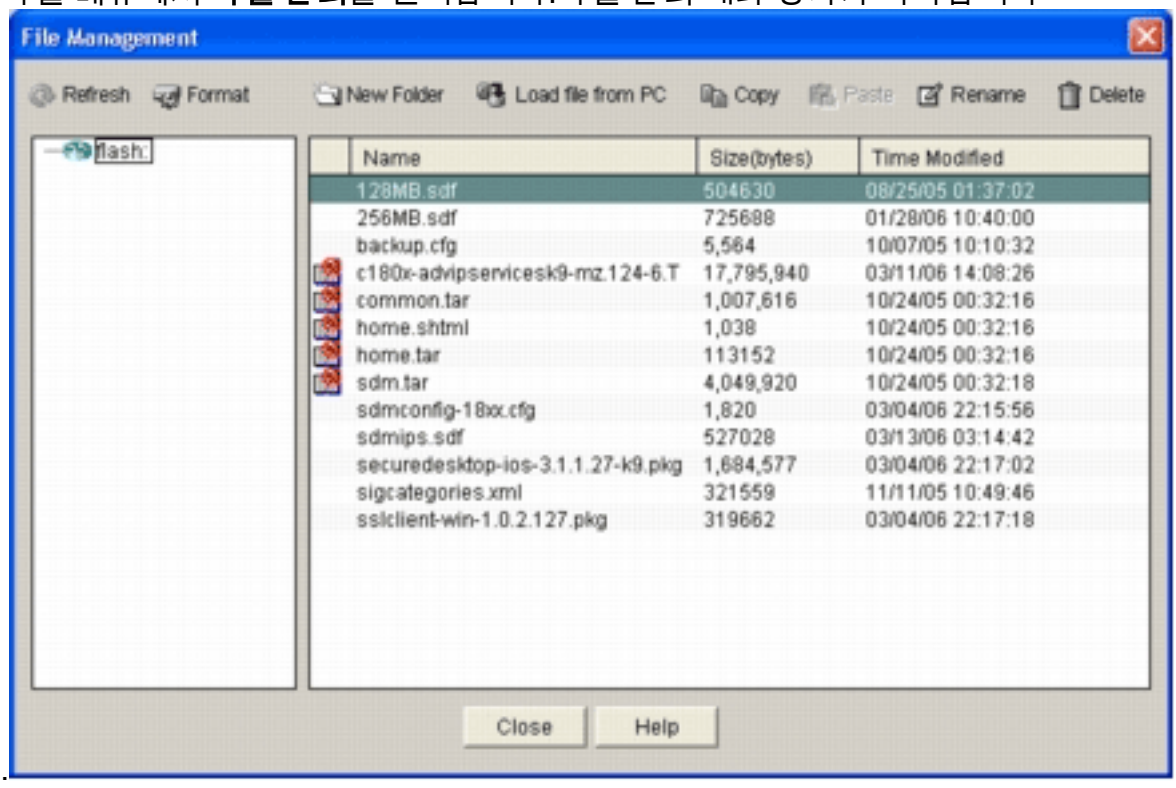
라우터에서 기본 SDF를 업데이트하려면 다음 단계를 완료하십시오.

1. Configure**(구성)**를 클릭한 다음 **Intrusion Prevention(침입 방지)을 클릭합니다**.
2. Edit **IPS(IPS 편집)** 탭을 클릭한 다음 **Global Settings(전역 설정)**를 클릭합니다
   .



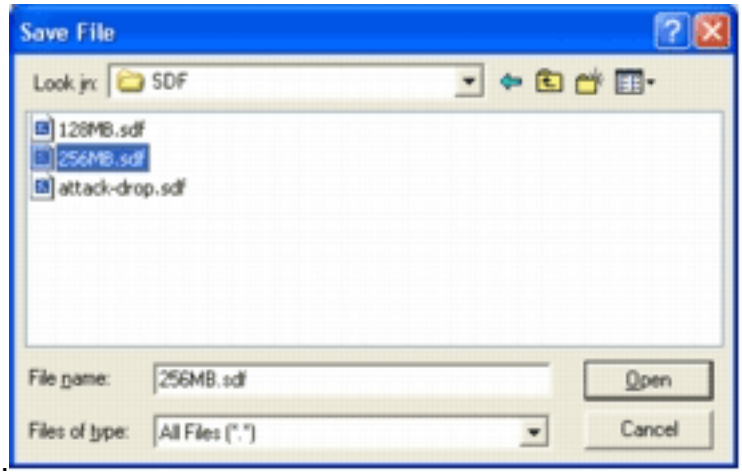
UI의 맨 위에 전역 설정이 표시됩니다. UI의 아래쪽 절반은 현재 구성된 SDF 위치를 보여줍니다. 이 경우 플래시 메모리의 256MB.sdf 파일이 구성됩니다.

3. 파일 메뉴에서 **파일 관리**를 선택합니다.파일 관리 대화 상자가 나타납니다

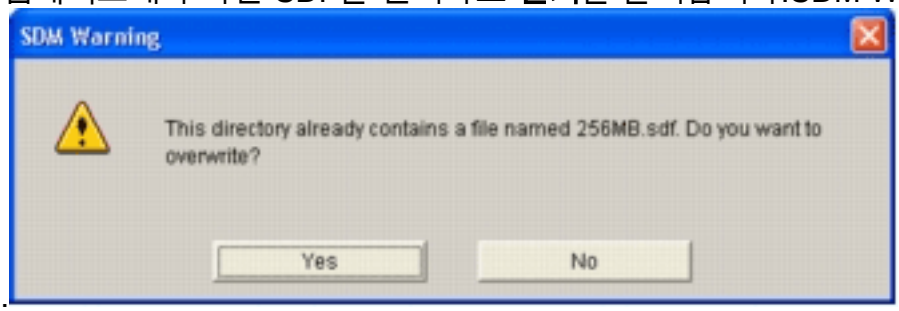


.

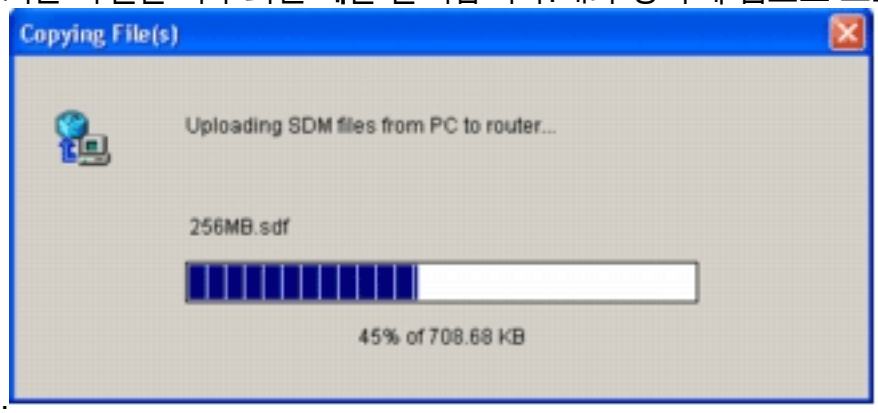
4. **PC에서 파일 로드를 클릭합니다**.Save File 대화 상자가 나타납니다



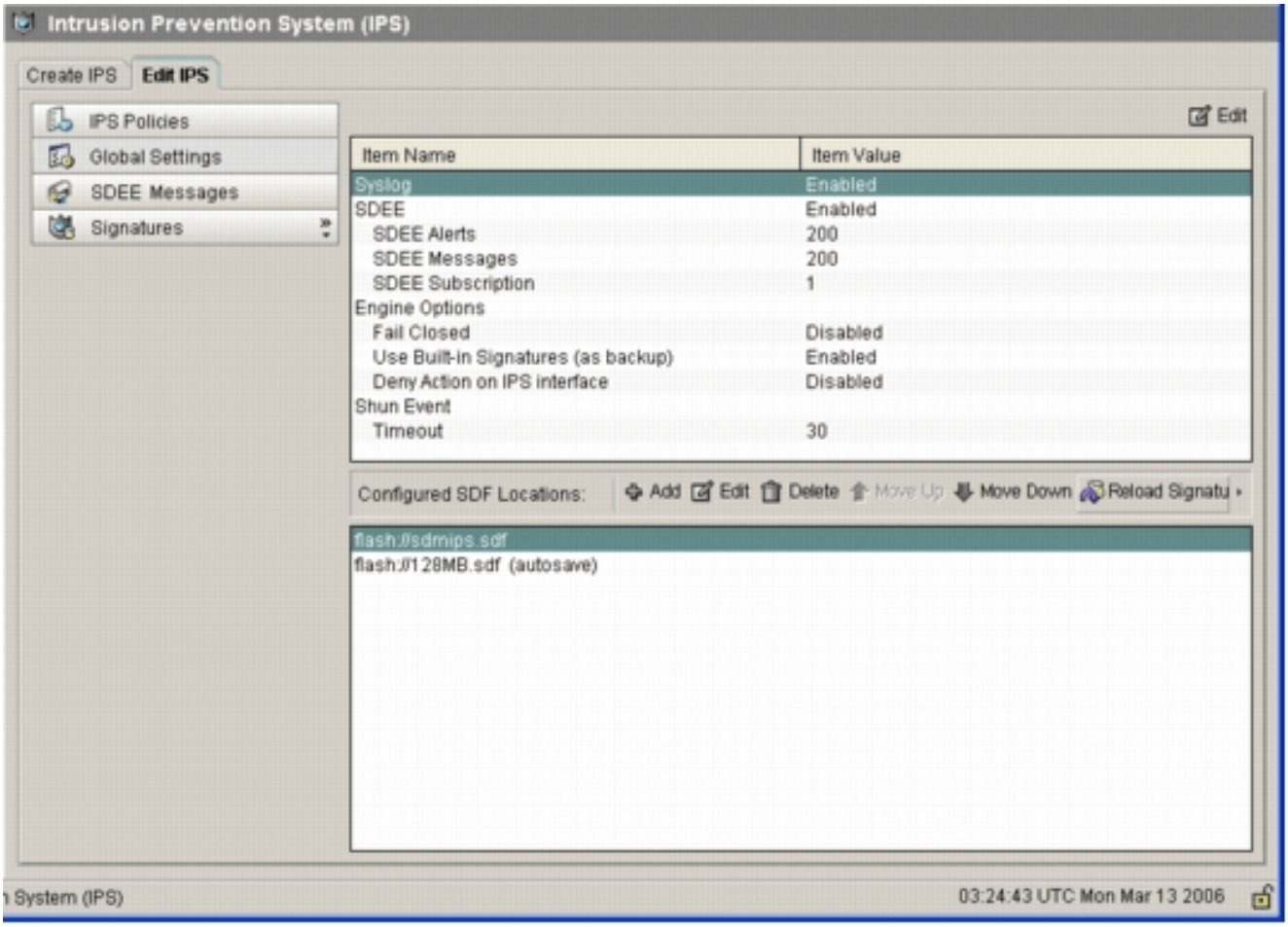
5. 업데이트해야 하는 SDF를 선택하고 **열기**를 클릭합니다.SDM Warning 메시지가 나타납니다



6. 기존 파일을 바꾸려면 **예**를 클릭합니다.대화 상자에 업로드 프로세스의 진행률이 표시됩니다



7. 업로드 프로세스가 완료되면 SDF 위치 툴바에 있는 **Reload Signatures**를 클릭합니다. 이 작업은 Cisco IOS IPS를 다시 로드합니다



참고: IOS-Sxxx.zip 패키지에는 Cisco IOS IPS에서 지원하는 모든 서명이 포함되어 있습니다. 이 서명 패키지에 대한 업그레이드는 Cisco.com에서 제공되는 즉시 게시됩니다. 이 패키지에 포함된 서명을 업데이트하려면 2단계를 참조하십시오.

관련 정보

- Cisco 침입 방지 시스템
- 보안 제품 필드 알림(CiscoSecure Intrusion Detection 포함)
- Technical Support - Cisco Systems