5.x 형식 시그니처로 IPS 구성

목차

소개

이 문서에서는 Cisco IOS® IPS에서 5.x 형식 서명을 구성하는 방법에 대해 설명하며 다음 두 섹션으로 구성됩니다.

- 섹션 I. Getting Started Configuration Steps(컨피그레이션 시작 단계) - 이 섹션에서는 IOS IPS 5.x 형식 서명을 시작하기 위해 Cisco IOS CLI(Command-Line Interface)를 사용하는 데 필요한 단계를 제공합니다. 이 섹션에서는 다음 단계에 대해 설명합니다.1단계. IOS IPS 파일을 다운로드합니다.2단계. 플래시에 IOS IPS 컨피그레이션 디렉토리를 생성합니다.3단계. IOS IPS 암호화 키를 구성합니다.4단계. IOS IPS를 활성화합니다.5단계. IOS IPS 서명 패키지를 라우터에 로드합니다.각 단계와 특정 명령에 대해 자세히 설명하고 추가 명령과 참조를 제공합니다. 각 명령 아래에 컨피그레이션의 예가 표시됩니다.
- 섹션 2. 고급 구성 옵션 - 이 섹션에서는 서명 튜닝을 위한 고급 옵션에 대한 지침과 예를 제공합니다. 여기에는 다음 옵션이 포함됩니다.서명 사용 중지 또는 사용 중지 취소서명 활성화 또는 비활성화서명 작업 변경

사전 요구 사항

요구 사항

이 문서의 단계를 완료하기 전에 적절한 구성 요소(사용된 구성 요소에 설명)가 있는지 확인합니다.

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco Integrated Services Router(87x, 18xx, 28xx 또는 38xx)
- 128MB 이상의 DRAM 및 2MB 이상의 여유 플래시 메모리
- 라우터에 대한 콘솔 또는 텔넷 연결
- Cisco IOS 릴리스 12.4(15)T3 이상
- 유효한 CCO(Cisco.com) 로그인 사용자 이름 및 비밀번호
- 라이센스 서명 업데이트 서비스에 대한 현재 Cisco IPS 서비스 계약

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 표기 규칙을 참고하십시오.

섹션 I. 구성 시작 단계

1단계. IOS IPS 파일 다운로드

첫 번째 단계는 Cisco.com에서 IOS IPS 서명 패키지 파일 및 공용 암호화 키를 다운로드하는 것입니다.

Cisco.com에서 PC에 필요한 서명 파일을 다운로드합니다.

- 위치: http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-v5sigup(등록된 고객만 해당)
- 다운로드할 파일:IOS-Sxxx-CLI.pkg(등록된 고객만 해당) —최신 서명 패키지입니다.realm-cisco.pub.key.txt(등록된 고객만 해당) —IOS IPS에서 사용하는 공용 암호화 키입니다.

2단계. 플래시에 IOS IPS 컨피그레이션 디렉토리 생성

두 번째 단계는 필요한 서명 파일 및 컨피그레이션을 저장하는 라우터의 플래시에 디렉토리를 생성하는 것입니다. 또는 라우터의 USB 포트에 연결된 Cisco USB 플래시 드라이브를 사용하여 서명 파일 및 컨피그레이션을 저장할 수 있습니다. USB 플래시 드라이브가 IOS IPS 컨피그레이션 디렉토리 위치로 사용되는 경우 라우터의 USB 포트에 계속 연결되어 있어야 합니다. IOS IPS는 또한 적절한 쓰기 액세스 권한을 통해 모든 IOS 파일 시스템을 구성 위치로 지원합니다.

디렉토리를 생성하려면 라우터 프롬프트에서 다음 명령을 입력합니다. **mkdir <*디렉터리 이름*>**

예를 들면 다음과 같습니다.

```
router#mkdir ips
Create directory filename [ips]?
Created dir flash:ips
```

추가 명령 및 참조

플래시의 내용을 확인하려면 라우터 프롬프트에서 다음 명령을 입력합니다. **플래시 표시:**

예를 들면 다음과 같습니다.

```
router#dir flash:
Directory of flash:/
   5 -rw-   51054864 Feb 8 2008 15:46:14 -08:00
                    c2800nm-advipservicesk9-mz.124-15.T3.bin
   6 drw-      0 Feb 14 2008 11:36:36 -08:00 ips
64016384 bytes total (12693504 bytes free)
```

디렉토리 이름을 변경하려면 다음 명령을 사용합니다. **<*current name*> <*new name*> 이름*의* 이름 바꾸기**

예를 들면 다음과 같습니다.

```
router#rename ips ips_new
Destination filename [ips_new]?
```

3단계. IOS IPS 암호화 키 구성

세 번째 단계는 IOS IPS에서 사용하는 암호화 키를 구성하는 것입니다. 이 키는 1단계에서 다운로드된 realm-cisco.pub.key.txt 파일에 있습니다.

암호화 키는 Cisco 개인 키로 내용이 서명된 마스터 서명 파일(sigdef-default.xml)의 디지털 서명을 확인하는 데 사용되며, 모든 릴리스에서 그 신뢰성과 무결성을 보장합니다.

1. 텍스트 파일을 열고 파일의 내용을 복사합니다.
2. 라우터 구성 모드를 시작하려면 configure **terminal** 명령을 사용합니다.
3. 텍스트 파일 내용을 `<hostname>(config)#` 프롬프트 붙여넣습니다.
4. 라우터 컨피그레이션 모드를 종료합니다.
5. 암호화 키가 구성되었는지 확인하기 위해 라우터 프롬프트에 show run 명령을 입력합니다. 컨피그레이션에서 다음 출력이 표시되어야 합니다.

```
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
key-string
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
Quit
```

6. 컨피그레이션을 저장하려면 다음 명령을 사용합니다.**copy running-configure startup-configure 복사**

추가 명령 및 참조

키가 잘못 구성된 경우 먼저 암호화 키를 제거한 다음 다시 구성해야 합니다.

1. 키를 제거하려면 아래 나열된 순서대로 다음 명령을 입력합니다.

```
router#configure terminal
```

```
router(config)#no crypto key pubkey-chain rsa
router(config-pubkey-chain)#no named-key realm-cisco.pub signature
router(config-pubkey-chain)#exit
router(config)#exit
```

2. 컨피그레이션에서 키가 제거되었는지 확인하려면 **show run** 명령을 사용합니다.
3. 키를 재구성하려면 3단계의 절차를 완료합니다.

4단계. IOS IPS 활성화

네 번째 단계는 IOS IPS를 구성하는 것입니다. IOS IPS를 구성하려면 다음 절차를 완료합니다.

1. 규칙 이름을 생성하려면 **ip ips name <*rule name*> < *optional ACL*>** 명령을 사용합니다. (이는 인터페이스에서 IPS를 활성화하는 데 사용됩니다.)예를 들면 다음과 같습니다.
   ```
   router#configure terminal
   router(config)#ip ips name iosips
   ```

   이 규칙 이름으로 검사될 트래픽을 필터링하기 위해 선택적인 확장 또는 표준 ACL(Access Control List)을 지정할 수 있습니다. ACL에서 허용하는 모든 트래픽은 IPS에서 검사를 받습니다. ACL에서 거부된 트래픽은 IPS에서 검사하지 않습니다.
   ```
   router(config)#ip ips name ips list ?
   <1-199> Numbered access list
   WORD Named access list
   ```
2. IPS **서명 스토리지 위치를 구성하려면 ip ips config location flash:<*directory name*>** 명령을 사용합니다. (2단계에서 생성된 *ips* 디렉토리입니다.)예를 들면 다음과 같습니다.
   ```
   router(config)#ip ips config location flash:ips
   ```

3. IPS **SDEE** 이벤트 알림을 활성화하려면 ip ips notify sdee 명령을 사용합니다.예를 들면 다음과 같습니다.
   ```
   router(config)#ip ips notify sdee
   ```

   SDEE를 사용하려면 HTTP 서버를 활성화해야 합니다(**ip http server** 명령 사용). HTTP 서버가 활성화되지 않은 경우 라우터는 요청을 볼 수 없으므로 SDEE 클라이언트에 응답할 수 없습니다. SDEE 알림은 기본적으로 비활성화되어 있으며 명시적으로 활성화해야 합니다.IOS IPS는 이벤트 알림을 보내기 위해 syslog를 사용할 수도 있습니다. SDEE와 syslog는 IOS IPS 이벤트 알림을 보내기 위해 독립적으로 사용하거나 동시에 활성화할 수 있습니다. Syslog 알림은 기본적으로 활성화되어 있습니다. 로깅 콘솔이 활성화된 경우 IPS syslog 메시지가 표시됩니다. syslog를 활성화하려면 다음 명령을 사용합니다.
   ```
   router(config)#ip ips notify log
   ```

4. 미리 정의된 서명 범주 중 하나를 사용하도록 IOS IPS를 구성합니다.Cisco 5.x 형식 시그니처가 포함된 IOS IPS는 시그니처 카테고리(Cisco IPS 어플라이언스와 동일)와 함께 작동합니다. 모든 시그니처는 카테고리로 그룹화되고 카테고리는 계층적입니다. 이렇게 하면 쉽게 그룹화하고 조정할 수 있도록 서명을 분류할 수 있습니다.**경고:** *모든* 서명 범주는 서명 릴리스의 모든 서명을 포함합니다. IOS IPS는 한 번에 시그니처 릴리스에 포함된 모든 시그니처를 컴파일하고 사용할 수 없으므로 *모든 카테고리를 해제하지 마십시오*. 그렇지 않으면 라우터에 메모리가 부족합니다.**참고:** IOS IPS를 구성할 때 먼저 *모든* 카테고리의 모든 시그니처를 사용 중지한 다음 선택한 시그니처 카테고리를 사용 취소해야 합니다.**참고:** 라우터에서 시그니처 카테고리가 구성되는 순서도 중요합니다. IOS IPS는 컨피그레이션에 나열된 순서대로 category 명령을 처리합니다. 일부 시그니처는 여러 범주에 속합니다. 여러 카테고리가 구성되고 서명이 둘 이상의 카테고리에 속할 경우, 마지막으로 구성된 카테고리의 시그니처 속성(예: 사용 중지, 사용

중지 안 함, 작업 등)이 IOS IPS에서 사용됩니다.이 예에서는 "all" 카테고리의 모든 시그니처가 폐기된 다음 *IOS IPS Basic* 카테고리가 종료되지 않습니다.

```
router(config)#ip ips signature-category
router(config-ips-category)#category all
router(config-ips-category-action)#retired true
router(config-ips-category-action)#exit
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

5. 원하는 인터페이스에서 IPS 규칙을 활성화하고 규칙을 적용할 방향을 지정하려면 다음 명령을 사용합니다.**인터페이스 <*인터페이스 이름*>**ip ips **<*규칙 이름*> [*in | 출력*]**예를 들면 다음과 같습니다.

```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#exit
router(config)#exit
router#
```

in *인수는* 인터페이스로 들어가는 트래픽만 IPS에서 검사함을 의미합니다. out 인수는 인터페이스 밖으로 나가는 트래픽만 IPS에서 검사함을 의미합니다.IPS가 인터페이스의 내부 및 외부 트래픽을 모두 검사하도록 하려면 **동일한 인터페이스*에서*** in 및 out**에** 대한 IPS 규칙 이름**을** 별도로 입력합니다.

```
router(config)#interface GigabitEthernet 0/1
router(config-if)#ip ips iosips in
router(config-if)#ip ips iosips out
router(config-if)#exit
router(config)#exit
router#
```

5단계. 라우터에 IOS IPS 서명 패키지를 로드합니다.

마지막 단계는 1단계에서 다운로드한 서명 패키지를 라우터에 로드하는 것입니다.

참고: 시그니처 패키지를 라우터에 로드하는 가장 일반적인 방법은 FTP 또는 TFTP를 사용하는 것입니다. 이 절차에서는 FTP를 사용합니다. IOS IPS 서명 패키지를 로드하는 대체 방법은 이 절차의 *Additional Commands and* References 섹션을 참조하십시오. 텔넷 세션을 사용하는 경우 **terminal monitor** 명령을 사용하여 콘솔 출력을 봅니다.

서명 패키지를 라우터에 로드하려면 다음 단계를 완료하십시오.

1. 다운로드한 서명 패키지를 FTP 서버에서 라우터로 복사하려면 다음 명령을 사용합니다 .**ftp://<*ftp_user:password@Server_IP_address*>/<*signature_package*> idconf 복사참고:** copy **명령**의 끝**에** *idconf* **매개변수**를 사용해야 합니다.**참고:** 예:

```
router#copy ftp://cisco:cisco@10.1.1.1/IOS-S310-CLI.pkg idconf
Loading IOS-S310-CLI.pkg !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
[OK - 7608873/4096 bytes]
```

서명 패키지가 라우터에 로드된 후 바로 서명 컴파일이 시작됩니다. 로깅 레벨 6 이상이 활성화된 라우터의 로그를 볼 수 있습니다.

```
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDS_STARTED: 16:44:47 PST Feb 14 2008
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_READY: multi-string - build time 4 ms -
                      packets for this engine will be scanned
*Feb 14 16:44:47 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
```

```
                        2 of 13 engines
    *Feb 14 16:44:53 PST: %IPS-6-ENGINE_READY: service-http - build time 6024 ms -
                        packets for this engine will be scanned
    |
    output snipped
    |
    *Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-smb-advanced - 35 signatures -
                        12 of 13 engines
    *Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-smb-advanced - build time 16 ms -
                        packets for this engine will be scanned
    *Feb 14 16:45:18 PST: %IPS-6-ENGINE_BUILDING: service-msrpc - 25 signatures -
                        13 of 13 engines
    *Feb 14 16:45:18 PST: %IPS-6-ENGINE_READY: service-msrpc - build time 32 ms -
                        packets for this engine will be scanned
    *Feb 14 16:45:18 PST: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 31628 ms
```

2. 서명 패키지가 제대로 컴파일되었는지 확인하려면 **show ip ips signature count** 명령을 사용합니다.예를 들면 다음과 같습니다.

```
router#show ip ips signature count
Cisco SDF release version S310.0  signature package release version
Trend SDF release version V0.0
Signature Micro-Engine: multi-string: Total Signatures 8
multi-string enabled signatures: 8
multi-string retired signatures: 8
|
outpt snipped
|
Signature Micro-Engine: service-msrpc: Total Signatures 25
service-msrpc enabled signatures: 25
service-msrpc retired signatures: 18
service-msrpc compiled signatures: 1
service-msrpc inactive signatures - invalid params: 6
Total Signatures: 2136
Total Enabled Signatures: 807
Total Retired Signatures: 1779
Total Compiled Signatures:
      351  total compiled signatures for the IOS IPS Basic category
Total Signatures with invalid parameters: 6
Total Obsoleted Signatures: 11
router#
```

추가 명령 및 참조

다음 오류 메시지와 유사한 서명 컴파일 시 오류 메시지를 받으면 공개 암호화 키가 유효하지 않습니다.

```
%IPS-3-INVALID_DIGITAL_SIGNATURE: Invalid Digital Signature found (key not found)
```

자세한 내용은 3단계를 참조하십시오.

FTP 또는 TFTP 서버에 액세스할 수 없는 경우 USB 플래시 드라이브를 사용하여 서명 패키지를 라우터에 로드할 수 있습니다. 먼저 서명 패키지를 USB 드라이브에 복사하고 USB 드라이브를 라우터의 USB 포트 중 하나에 연결한 다음 *idconf* ***매개변수***와 함께 **copy** 명령**을** 사용하여 서명 패키지를 라우터에 복사합니다.

예를 들면 다음과 같습니다.

```
router#copy usbflash1:IOS-S310-CLI.pkg idconf
```

구성된 IOS IPS 스토리지 디렉토리에 6개의 파일이 있습니다. 이러한 파일은 다음 이름 형식을 사용합니다. <*router-name*>-sigdef-xxx.xml 또는 <*router-name*>-seap-xxx.xml

```
router#dir ips
Directory of flash:/ips/
7 -rw- 203419 Feb 14 2008 16:45:24 -08:00 router-sigdef-default.xml
8 -rw- 271 Feb 14 2008 16:43:36 -08:00 router-sigdef-delta.xml
9 -rw- 6159 Feb 14 2008 16:44:24 -08:00 router-sigdef-typedef.xml
10 -rw- 22873 Feb 14 2008 16:44:26 -08:00 router-sigdef-category.xml
11 -rw- 257 Feb 14 2008 16:43:36 -08:00 router-seap-delta.xml
12 -rw- 491 Feb 14 2008 16:43:36 -08:00 router-seap-typedef.xml
64016384 bytes total (12693504 bytes free)
router#
```

이러한 파일은 압축된 형식으로 저장되며 직접 편집 가능하거나 볼 수 없습니다. 각 파일의 내용은 다음과 같습니다.

- *router-sigdef-default.xml*은 모든 공장 기본 서명 정의를 포함합니다.
- *router-sigdef-delta.xml*에는 기본값에서 변경된 서명 정의가 포함되어 있습니다.
- *router-sigdef-typedef.xml*에 모든 서명 매개 변수 정의가 포함되어 있습니다.
- *router-sigdef-category.xml*에는 category ios_ips basic 및 advanced와 같은 시그니처 범주 정보가 포함됩니다.
- *router-seap-delta.xml*에는 기본 SEAP 매개변수에 대한 변경 사항이 포함되어 있습니다.
- *router-seap-typedef.xml에는* 모든 SEAP 매개 변수 정의가 포함되어 있습니다.

섹션 2. 고급 구성 옵션

이 섹션에서는 시그니처 튜닝을 위한 고급 IOS IPS 옵션에 대한 지침 및 예를 제공합니다.

서명 사용 중지 또는 사용 중지 취소

시그니처를 사용 중지하거나 사용 취소하는 것은 트래픽을 스캔하기 위해 IOS IPS에서 사용하는 서명을 선택하거나 선택 취소하는 것을 의미합니다.

- **시그니처**를 종료하면 IOS IPS는 스캔을 위해 해당 시그니처를 메모리로 컴파일하지 *않습니다*.
- **시그니처의** 종료를 해제하면 IOS IPS가 시그니처를 메모리로 컴파일하고 서명을 사용하여 트래픽을 스캔하도록 지시합니다.

IOS CLI(Command-Line Interface)를 사용하여 개별 시그니처 또는 시그니처 범주에 속하는 서명 그룹을 사용 중지하거나 사용 취소할 수 있습니다. 서명 그룹을 사용 중지하거나 사용 중지하면 해당 범주의 모든 서명이 사용 중지되거나 사용 중지되지 않습니다.

참고: 일부 폐기되지 않은 시그니처(개별 시그니처로 사용되지 않거나 폐기되지 않은 범주 내)는 메모리가 부족하거나 유효하지 않은 매개변수 또는 서명이 폐기된 경우 컴파일되지 않을 수 있습니다 .

이 예에서는 개별 서명을 폐기하는 방법을 보여 줍니다. 예를 들어, 서명 ID가 10인 서명 6130:

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
```

```
router(config-sigdef-sig-status)#retired true
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

다음 예에서는 IOS IPS Basic 카테고리에 속하는 모든 시그니처의 사용 중지를 해제하는 방법을 보여 줍니다.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
```

참고: IOS IPS Basic 및 IOS IPS Advanced 이외의 카테고리의 시그니처가 범주로 사용되지 않을 경우, 해당 카테고리의 특정 시그니처가 IOS IPS에서 지원되지 않으므로 일부 서명 또는 엔진 컴파일이 실패할 수 있습니다(아래 예 참조). 성공적으로 컴파일된(폐기되지 않은) 다른 모든 시그니처는 IOS IPS에서 트래픽을 스캔하는 데 사용됩니다.

```
Router(config)#ip ips signature-category
router(config-ips-category)#category os
router(config-ips-category-action)#retired false
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
*Feb 14 18:10:46 PST: Applying Category configuration to signatures ...
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDS_STARTED: 08:10:49 PST Feb 18 2008
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: multi-string - 8 signatures -
                      1 of 13 engines
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_READY: multi-string - build time 136 ms -
                      packets for this engine will be scanned
*Feb 14 18:10:49 PST: %IPS-6-ENGINE_BUILDING: service-http - 622 signatures -
                      2 of 13 engines
*Feb 14 18:10:50 PST: %IPS-4-META_ENGINE_UNSUPPORTED: service-http 5903:1 -
                      this signature is a component of the unsupported META engine
*Feb 14 18:24:42 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5754:0 -
                      compilation of regular expression failed
*Feb 14 18:24:49 PST: %IPS-4-SIGNATURE_COMPILE_FAILURE: service-http 5729:1 -
                      compilation of regular expression failed
```

서명 활성화 또는 비활성화

시그니처를 활성화 또는 비활성화하려면 패킷 또는 패킷 흐름이 시그니처와 일치할 때 IOS IPS에서 서명과 관련된 작업을 시행하거나 무시하는 것입니다.

참고: Enable 및 disable은 IOS IPS에서 사용할 서명을 선택 및 선택 취소하지 않습니다.

- 시그니처를 활성화하려면 일치하는 패킷(또는 패킷 흐름)에 의해 트리거될 때 서명이 연결된 적절한 작업을 수행합니다. 그러나 폐기되지 않은 AND에서 성공적으로 컴파일된 시그니처만 활성화되면 작업을 수행합니다. 즉, 서명이 사용되지 않는 경우 활성화된 경우에도 해당 서명은 컴파일되지 않으며(사용이 중단되었기 때문에) 연결된 작업을 수행하지 않습니다.
- 시그니처를 **비활성화하려면** 일치하는 패킷(또는 패킷 흐름)에 의해 트리거될 때 시그니처가 해

당 패킷과 관련된 적절한 작업을 수행하지 않음을 의미합니다. 다시 말해, 서명이 비활성화된 경우, 사용이 취소되지 않고 성공적으로 컴파일된 경우에도 시그니처와 관련된 작업을 수행하지 않습니다.

시그니처 카테고리를 기반으로 개별 서명 또는 시그니처 그룹을 활성화 또는 비활성화하려면 IOS CLI(Command-Line Interface)를 사용할 수 있습니다. 이 예에서는 서명 ID가 10인 서명 6130을 비활성화하는 방법을 보여줍니다.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#status
router(config-sigdef-sig-status)#enabled false
router(config-sigdef-sig-status)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

이 예에서는 IOS IPS Basic 카테고리에 속하는 모든 서명을 활성화하는 방법을 보여줍니다.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#enabled true
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

서명 작업 변경

IOS CLI(Command-Line Interface)를 사용하여 서명 카테고리를 기반으로 한 서명 또는 서명 그룹에 대한 서명 작업을 변경할 수 있습니다. 이 예에서는 서명 ID가 10인 서명 6130에 대해 알림, 삭제 및 재설정하도록 서명 작업을 변경하는 방법을 보여 줍니다.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
router(config)#ip ips signature-definition
router(config-sigdef)#signature 6130 10
router(config-sigdef-sig)#engine
router(config-sigdef-sig-engine)#event-action produce-alert
router(config-sigdef-sig-engine)#event-action deny-packet-inline
router(config-sigdef-sig-engine)#event-action reset-tcp-connection
router(config-sigdef-sig-engine)#exit
router(config-sigdef-sig)#exit
router(config-sigdef)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

이 예에서는 시그니처 IOS IPS Basic 카테고리에 속하는 모든 서명에 대한 이벤트 작업을 변경하는 방법을 보여줍니다.

```
router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z
router(config)#ip ips signature-category
```

```
router(config-ips-category)#category ios_ips basic
router(config-ips-category-action)#event-action produce-alert
router(config-ips-category-action)#event-action deny-packet-inline
router(config-ips-category-action)#event-action reset-tcp-connection
router(config-ips-category-action)#exit
router(config-ips-category)#exit
Do you want to accept these changes? [confirm]y
router(config)#
```

관련 정보

- Cisco IOS IPS(Intrusion Prevention System) 제품 및 서비스 페이지
- Cisco IOS IPS - 버전 5 서명 소프트웨어 다운로드
- IPS 5.x 서명 형식 지원 및 사용 편의성 향상
- Cisco Security Device Manager 소프트웨어 다운로드
- CCP를 사용하여 IOS IPS 구성 방법
- Cisco Intrusion Detection System Event Viewer 3DES Cryptographic Software 다운로드
- 기술 지원 및 문서 – Cisco Systems