IPS 서명 형식 4.x를 5.x로 마이그레이션

목차

소개

Cisco IOS® Release 12.4(11)T 이상에서 Cisco IOS IPS(Intrusion Prevention System)는 Cisco IPS 소프트웨어 버전 5.x 서명 형식을 지원합니다. 5.x 서명 형식은 다른 Cisco 어플라이언스 기반 IPS 제품에서도 사용되는 버전 기반 서명 정의 XML 형식입니다. Cisco IPS 버전 4.x에서 시그니처 및 SDF(signature definition file)에 대한 지원은 이 릴리스와 Cisco IOS T-Train 소프트웨어 릴리스에서 중단됩니다.

버전 4.x 서명 형식 SDF를 사용하여 Cisco IOS IPS를 실행하는 고객은 Cisco IOS IPS를 재구성하여 Cisco의 사전 정의된 서명 범주, 기본 및 고급 서명 세트 또는 Cisco IOS IPS 마이그레이션 유틸리티를 사용하여 이전 버전 4.x SDF 파일을 Cisco IPS 버전 5.x 형식 서명 세트로 마이그레이션할 수 있습니다.

이 문서에서는 Cisco IPS 4.x 형식 SDF에서 마이그레이션하고 Cisco IOS Release 12.4(11)T 이상에서 마이그레이션된 서명 세트를 활성화하는 방법에 대해 설명합니다. Cisco IOS Release 12.4(11)T 이상에서 Cisco IOS IPS를 구성하는 방법에 대한 자세한 내용은 IPS 5.x Signature Format Support and Useability Enhancements를 참조하십시오.

참고: Cisco IOS Release 12.4(11)T 이상 이미지로 업그레이드하기 전에 Cisco IOS IPS 마이그레이션을 실행하는 것이 좋습니다.

사전 요구 사항

요구 사항

이 문서에 대한 특정 요건이 없습니다.

사용되는 구성 요소

이 문서의 정보는 Cisco IOS Release 12.4(11)T 이상을 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 표기 규칙을 참고하십시오.

버전 4.x SDF 파일 마이그레이션 단계

마이그레이션 스크립트에는 Cisco IOS Release 12.4(11)T 이전 릴리스를 실행하는 라우터에서 사용되는 Cisco IOS IPS 컨피그레이션 정보가 포함된 Cisco IPS 4.x 형식 SDF 파일 및 (선택 사항) CLI 컨피그레이션 파일이 필요합니다.

마이그레이션 스크립트는 라우터 컨피그레이션 파일 내에서 비활성화된 **ip ips 시그니처 <*sigid*> [<*sigsubid*>]를** 포함하는 명령을 검색합니다. 컨피그레이션 파일에 이 CLI 명령이 포함되어 있지 않으면 마이그레이션 스크립트에서 CLI 컨피그레이션 파일을 읽을 필요가 없습니다. 시그니처 변환은 SDF만을 기반으로 합니다.

Cisco IOS IPS를 Cisco IOS Release 12.4(11)T 이상으로 업그레이드하기 전에 마이그레이션 스크립트를 실행하는 경우 Execute the Cisco IOS IPS Migration Script(Cisco IOS IPS 마이그레이션 스크립트 실행)의 프로세스를 따릅니다.

Cisco IOS IPS를 Cisco IOS Release 12.4(11)T 이상으로 업그레이드한 후 마이그레이션 스크립트를 실행하는 경우 다음 단계를 완료합니다.

1. 위에서 설명한 대로 CLI 명령, **ip ips signature <*sigid*> [<*sigsubid*>]을(를) 비활성화해야** 하는지 확인합니다.
2. 라우터의 CLI 컨피그레이션을 파일에 저장하려면 **copy running-config flash:ipscfg.cfg** 명령을 사용합니다.이 명령은 ipscfg.cfg라는 파일에서 기존 라우터 컨피그레이션을 플래시에 *백업합니다*. 마이그레이션 프로세스에서는 전체 4.x에서 5.x 서명 형식 변환에 이 파일을 사용합니다.
3. Execute the Cisco IOS IPS Migration Script로 진행합니다.

Cisco IOS IPS 마이그레이션 스크립트 실행

마이그레이션 스크립트는 다음 URL에서 Cisco.com에서 사용할 수 있습니다. http://www.cisco.com/cgi-bin/tablebuild.pl/ios-v5sigup 마이그레이션 스크립트를 라우터의 플래시 또는 TFTP(Trivial File Transfer Protocol) 서버와 같은 라우터가 액세스할 수 있는 위치에 저장합니다.

마이그레이션 스크립트는 SDF를 Cisco IPS 버전 4.x 형식에서 버전 5.x 형식으로 변환합니다. 마이그레이션 스크립트는 다음 서명 매개변수만 지원합니다.

- 심각도
- 작업
- 활성화됨

또한 마이그레이션 스크립트는 IOS IPS 컨피그레이션 파일에서도 읽을 수 있으며 Cisco IOS Release 12.4(11)T 이전 릴리스에서 CLI **ip ips signature <sigid> <sigsubid> disabled** 명령으로 구성된 비활성화된 시그니처를 마이그레이션할 수 있습니다.

참고: Cisco가 아닌 사용자 지정 서명은 이 스크립트로 변환되지 않습니다.

이 예에서는 Cisco IOS IPS 5.x 서명 형식 지원을 사용하여 Cisco IOS Release 12.4(11)T에서 IPS 4.x 형식의 파일 sdmips.*sdf*를 Cisco IOS IPS로 마이그레이션하는 방법을 보여줍니다.

```
C2821#tclsh flash:ios-ips-migrate.tbc
This migration script will migrate Signature Definition Files
     from 4.x format to 5.x format.
The migration script will migrate only the following signature
     parameters - severity, action, enabled - for Cisco (non-custom) signatures.
Do you want to continue? [y/n] y
Please choose an IOS config file from which to migrate IOS IPS configuration.
Config File: [startup-config]
The following SDF locations were found configured in startup-config:
  flash://sdmips.sdf
Please provide SDF to migrate from the above list or of your own
     choice: flash:// sdmips.sdf
Migrating following SDF file (this will a take few minutes):
  flash://sdmips.sdf
Time Elapsed: 0:02:23
Migration completed successfully. The migrated file is
  C2821-sigdef-delta.xml
C2821#
```

먼저 마이그레이션 스크립트에는 기능에 대한 간략한 텍스트가 표시됩니다. 그런 다음 스크립트에서는 Cisco IOS IPS의 현재(마이그레이션 전) 컨피그레이션을 읽을 위치를 선택할 수 있는 옵션을 제공합니다. 기본값은 시작 컨피그레이션에서 읽습니다. 컨피그레이션을 TFTP 서버 또는 라우터의 플래시에 저장한 경우 프롬프트에서 위치를 지정합니다.

예를 들면 다음과 같습니다.

스크립트에서 TFTP **서버** 192.168.1.5에서 CLI 컨피그레이션을 로드하도록 알리려면 tftp://192.168.1.5/<*router CLI configuration*>을 사용합니다.

플래시에 저장된 파일에서 읽으려면 flash://<***saved-configuration***>을 사용합니다.

Cisco IOS Software 릴리스 12.4(11)T에서 마이그레이션된 서명을 Cisco IOS IPS로 로드

서명 마이그레이션이 완료되면 라우터의 이미지를 Cisco IOS Release12.4(11)T로 업그레이드합니다(아직 수행하지 않은 경우). 라우터가 다시 로드되면 다음 단계를 완료합니다.

1. Cisco IOS IPS를 활성화합니다.이 출력은 Cisco 2821 라우터에서 Cisco IOS IPS를 활성화하는 방법을 보여줍니다. Cisco IOS IPS를 구성하는 방법에 대한 자세한 내용은 IPS 5.x Signature Format Support and Useability Enhancements를 참조하십시오.

   ```
   C2821#mkdir ips
   Create directory filename [ips]?
   Created dir flash:ips
   C2821#conf t
   Enter configuration commands, one per line. End with CNTL/Z.
   C2821(config)#ip ips name MYIPS
   C2821(config)#ip ips config location ips
   C2821(config)#ip ips signature-category
   C2821(config-ips-category)#category all
   C2821(config-ips-category-action)#retired true
   C2821(config-ips-category-action)#exit
   C2821(config-ips-category)#exit
   ```

```
Do you want to accept these changes? [confirm]y
C2821(config)#
```

2. 암호화 서명 공개 키를 구성하려면 이 키를 복사하여 라우터에 붙여 넣습니다.

```
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
 exit
 exit
```

3. 다음 예와 같이 인터페이스에서 Cisco IOS IPS를 활성화합니다.

```
C2821(config)#
C2821(config)#interface gigabitEthernet 0/0
C2821(config-if)#ip ips MYIPS in
C2821(config-if)#ip ips MYIPS out
C2821(config-if)#exit
```

4. **copy** 명령을 사용하여 최신 서명 패키지를 로드합니다.

```
C2821#copy tftp://192.168.1.5/IOS-S253-CLI.pkg idconf
```

이 명령은 서명 패키지 IOS-*S253-CLI.pkg*에서 Cisco IOS IPS로 서명을 로드합니다.**참고: ios-ips 시그니처 카테고리가 모두** 1단계에서 구성되었으며 모든 시그니처를 폐기합니다. 서명 패키지가 성공적으로 로드되면 선택된 서명이 없고 컴파일됩니다.

5. 마이그레이션된 XML 파일을 Cisco IOS IPS에 로드하려면 다음 명령을 사용합니다.***<router-hostname>*-sigdef-delta.xml**예를 들면 다음과 같습니다.

```
copy flash:C2821-sigdef-delta.xml idconf
```

라우터가 버전 5.x 형식의 서명 파일을 구문 분석하면 마이그레이션이 완료됩니다.

6. 서명 요약 상태를 확인하려면 **show ip ips signature count** 명령을 사용한 다음 모든 시그니처에 대한 특정 세부 정보를 보려면 **show ip ips signature details** 명령을 사용합니다.

관련 정보

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