

# Cisco Integrated Services Router 4000 Series에 Snort IPS 구축

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[네트워크 다이어그램](#)

[구성](#)

[플랫폼 UTD 컨피그레이션](#)

[서비스 플레인 및 데이터 플레인 컨피그레이션](#)

[다음을 확인합니다.](#)

[문제 해결](#)

[디버깅](#)

[관련 정보](#)

---

## 소개

이 문서에서는 IOx 방법을 사용하여 Cisco ISR(Integrated Services Router) 4000 Series에 Snort IPS 및 Snort IDS 기능을 구축하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco Integrated Services Routers 4000 Series(최소 8GB DRAM)
- 기본 IOS-XE 명령 환경
- 기본적인 Snort 지식
- 1년 또는 3년의 서명 서브스크립션이 필요합니다.
- IOS-XE 16.10.1a 이상

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- 17.9.3a 릴리스를 실행하는 ISR4331/K9.
- 17.9.3a 릴리스용 UTD 엔진 TAR.

- ISR4331/K9용 SecurityK9 라이선스.

VMAN 메서드는 이제 사용되지 않습니다.

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

## 배경 정보

Snort IPS 기능은 Cisco 4000 Series Integrated Services Router 및 Cisco Cloud Services Router 1000v Series의 지사에 IPS(Intrusion Prevention System) 또는 IDS(Intrusion Detection System)를 제공합니다. 이 기능은 오픈 소스 Snort를 사용하여 IPS 및 IDS 기능을 활성화합니다.

Snort는 실시간 트래픽 분석을 수행하고 IP 네트워크에서 위협이 탐지되면 경고를 생성하는 오픈 소스 IPS입니다. 또한 프로토콜 분석, 콘텐츠 조사 또는 행적을 수행하고 버퍼 오버플로, 스텔스 포트 스캔 등 다양한 공격 및 프로브를 탐지할 수 있습니다. Snort 엔진은 Cisco Integrated Services Router 4000 Series 및 Cloud Services Router 1000v Series에서 가상 컨테이너 서비스로 실행됩니다.

Snort IPS 기능은 네트워크 침입 탐지 또는 방지 모드로 작동하며 Cisco Integrated Services Router 4000 Series 및 Cloud Services Router 1000v Series에서 IPS 또는 IDS 기능을 제공합니다.

- 네트워크 트래픽을 모니터링하고 정의된 규칙 집합에 대해 분석합니다.
- 연결 분류를 수행합니다.
- 일치하는 규칙에 대한 작업을 호출합니다.

네트워크 요구 사항을 기반으로 합니다. Snort IPS는 IPS 또는 IDS로 활성화할 수 있습니다. IDS 모드에서는 Snort가 트래픽을 검사하고 알림을 보고하지만 공격을 방지하기 위한 어떤 조치도 취하지 않습니다. IPS 모드에서는 IDS처럼 트래픽을 검사하고 알림을 보고하지만 공격을 방지하기 위한 조치가 취해집니다.

Snort IPS는 ISR 라우터에서 서비스로 실행됩니다. 서비스 컨테이너는 가상화 기술을 사용하여 애플리케이션을 위한 Cisco 장치에 호스팅 환경을 제공합니다. Snort 트래픽 검사는 인터페이스별로 활성화되거나 지원되는 모든 인터페이스에서 전역적으로 활성화됩니다. Snort 센서에는 2개의 VirtualPortGroup 인터페이스가 필요합니다. 첫 번째 VirtualPortGroup은 관리 트래픽에 사용되고, 두 번째 VirtualPortGroup은 포워딩 플레인과 Snort 가상 컨테이너 서비스 간의 데이터 트래픽에 사용됩니다. 추측 IP 주소는 이러한 VirtualPortGroup 인터페이스에 대해 구성해야 합니다. 관리 VirtualPortGroup 인터페이스에 할당된 IP 서브넷은 서명 서버 및 경고/보고 서버와 통신할 수 있어야 합니다.

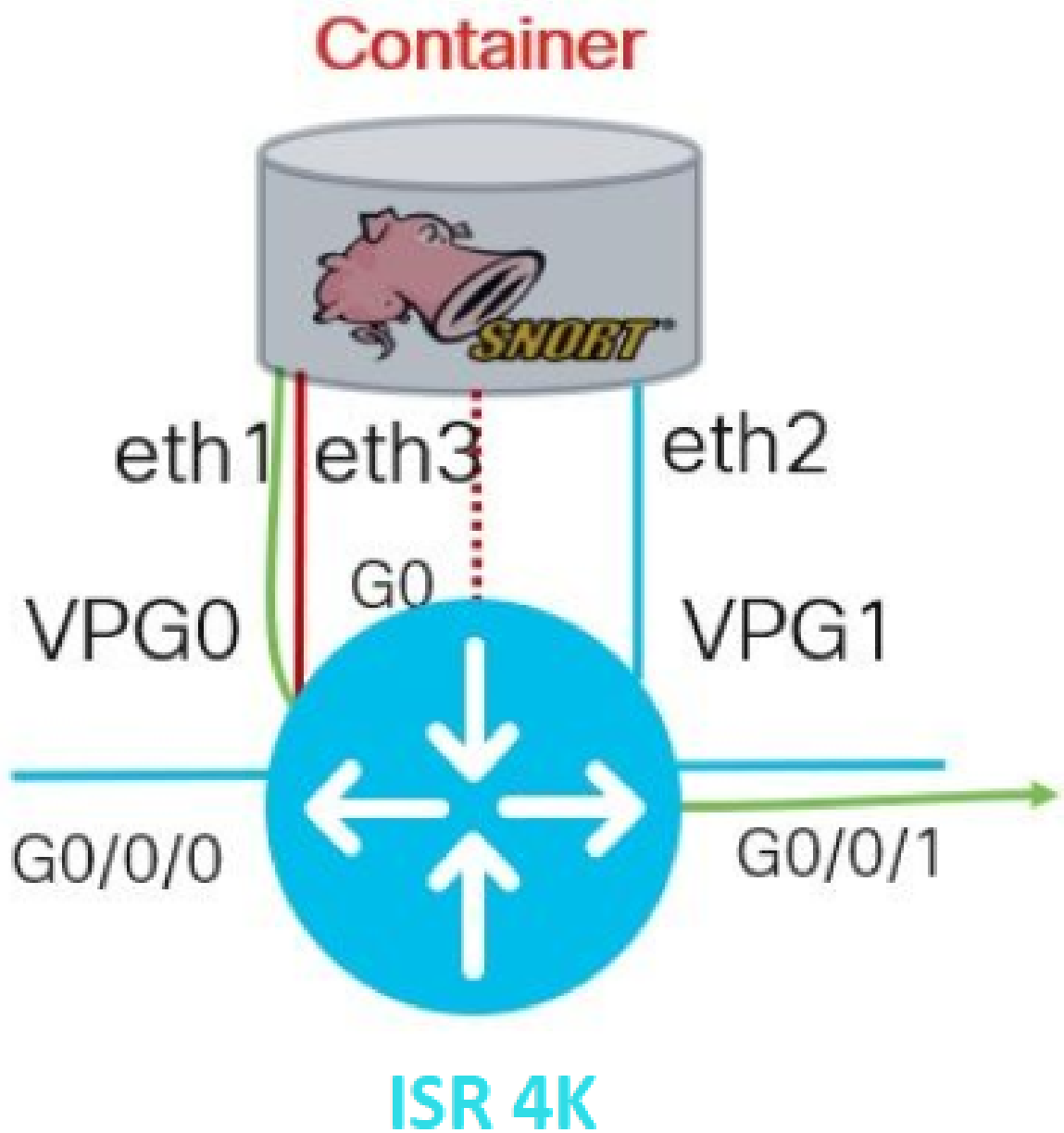
Snort IPS는 트래픽을 모니터링하고 외부 로그 서버 또는 IOS syslog에 이벤트를 보고합니다. IOS syslog에 로그인을 활성화하면 로그 메시지의 잠재적 볼륨 때문에 성능에 영향을 미칠 수 있습니다. Snort 로그를 지원하는 외부 서드파티 모니터링 툴을 로그 수집 및 분석에 사용할 수 있습니다.

Cisco 4000 Series Integrated Services Router 및 Cisco Cloud Services Router 1000v Series의 Snort IPS는 시그니처 패키지 다운로드를 기반으로 합니다. 서브스크립션에는 두 가지 유형이 있습니다.

- 커뮤니티 서명 패키지.
- 구독자 기반 서명 패키지입니다.

커뮤니티 서명 패키지 규칙 집합은 위협에 대해 제한된 적용 범위를 제공합니다. 가입자 기반 서명 패키지 규칙 집합은 위협으로부터 최상의 보호를 제공합니다. 여기에는 익스플로잇 사전 커버리지가 포함되며, 보안 사고 또는 새로운 위협의 사전 발견에 대응하여 업데이트된 시그니처에 가장 빠르게 액세스할 수 있는 기능도 제공합니다. 이 서브스크립션은 Cisco에서 완벽하게 지원되며 패키지는 Cisco.com에서 업데이트됩니다. 서명 패키지는 software.cisco.com에서 다운로드할 수 있습니다. Snort 서명 정보는 snort.org에서 확인할 수 있습니다.

## 네트워크 다이어그램



# 구성

## 플랫폼 UTD 컨피그레이션

1단계. Virtual VirtualPortGroups 인터페이스를 구성합니다.

```
Router#configure terminal
Router(config)#interface VirtualPortGroup0
Router(config-if)#description Management Interface
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

```
Router(config)#interface VirtualPortGroup1
Router(config-if)#description Data Interface
Router(config-if)#ip address 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

2단계. 글로벌 컨피그레이션 모드에서 IOx 환경을 활성화합니다.

```
Router(config)#iox
```

3단계. vnic 컨피그레이션으로 앱 호스팅을 구성합니다.


```
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#app-vnic gateway0 virtualportgroup 0 guest-interface 0
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.1.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

```
Router(config-app-hosting)#app-vnic gateway1 virtualportgroup 1 guest-interface 1
Router(config-app-hosting-gateway0)#guest-ipaddress 192.168.2.2 netmask 255.255.255.252
Router(config-app-hosting-gateway0)#exit
```

4단계(선택 사항) 리소스 프로필을 구성합니다.

```
Router(config-app-hosting)#app-resource package-profile low [low,medium,high]
Router(config-app-hosting)#end
```

---

 참고: 이 설정이 정의되지 않으면 시스템은 기본 app-resource config(낮음)를 사용합니다. 기

---

---

 본 프로필 컨피그레이션이 변경될 경우 ISR에서 사용 가능한 리소스가 충분해야 합니다.

---

5단계. UTD.tar 파일을 사용하여 앱 호스팅을 설치합니다.

```
Router#app-hosting install appid UTD package bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
```

---


 참고: bootflash에서 올바른 UTD.tar 파일을 유지하면 설치를 계속할 수 있습니다. Snort 버전이 UTD 파일 이름에 지정됩니다.

---

다음 syslog는 UTD 서비스가 제대로 설치되었음을 나타냅니다.

```
Installing package 'bootflash:iox-iosxe-utd.16.12.08.1.0.24_SV2.9.16.1_XE16.12
*Jun 26 19:25:35.975: %VMAN-5-PACKAGE_SIGNING_LEVEL_ON_INSTALL: R0/0: vman: Pa
*Jun 26 19:25:50.746: %VIRT_SERVICE-5-INSTALL_STATE: Successfully installed v
*Jun 26 19:25:53.176: %IM-6-INSTALL_MSG: R0/0: ioxman: app-hosting: Install su
```

---


 참고: 'show app-hosting list'를 사용하는 경우 상태는 'Deployed'여야 합니다.

---

6단계. 앱 호스팅 서비스를 시작합니다.

```
Router#configure terminal
Router(config)#app-hosting appid UTD
Router(config-app-hosting)#start
Router(config-app-hosting)#end
```

---

 참고: 앱 호스팅 서비스를 시작한 후에는 앱 호스팅 상태가 '실행 중'이어야 합니다. 자세한 내용을 보려면 '앱 호스팅 목록 표시' 또는 '앱 호스팅 세부 정보 표시'를 사용하십시오.

---


다음 syslog 메시지는 UTD 서비스가 제대로 설치되었음을 나타냅니다.

```
*Jun 26 19:55:05.362: %VIRT_SERVICE-5-ACTIVATION_STATE: Successfully activated
*Jun 26 19:55:07.412: %IM-6-START_MSG: R0/0: ioxman: app-hosting: Start succee
```

서비스 플레인 및 데이터 플레인 컨피그레이션.

성공적으로 설치한 후에는 서비스 플레인을 구성해야 합니다. Snort IPS는 IPS(Intrusion Prevention System) 또는 IDS(Intrusion Detection System)로 구성하여 검사할 수 있습니다.

---

 경고: 'securityk9' 라이선스 기능이 UTD 서비스 플레인 컨피그레이션을 계속 진행하도록 활성화되었는지 확인합니다.

---

1단계. UTD(Unified Threat Defense) 표준 엔진(서비스 플레인) 구성

```
Router#configure terminal
Router(config)#utd engine standard
```

2단계. 원격 서버에 대한 긴급 메시지 로깅을 활성화합니다.

```
Router(config-utd-eng-std)#logging host 192.168.10.5
```


3단계. Snort 엔진에 대한 위협 검사를 활성화합니다.

```
Router(config-utd-eng-std)#threat-inspection
```

4단계. 위협 탐지를 IPS(Intrusion Prevention System) 또는 IDS(Intrusion Detection System)로 구성

```
Router(config-utd-engstd-insp)#threat [protection,detection]
```

---


 참고: 'Protection'은 IPS에 사용되고 'Detection'은 IDS에 사용됩니다. 'Detection'이 기본값입니다.

---

5단계. 보안 정책을 구성합니다.

```
Router(config-utd-engstd-insp)#policy [balanced, connectivity, security]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

---

 참고: 기본 정책은 'balanced'입니다.

---


## 6단계(선택 사항) UTD-allowed list(UTD 허용 목록) 생성(화이트리스트)

```
Router#configure terminal
Router(config)#utd threat-inspection whitelist
```

## 7단계(선택 사항) 화이트리스트에 표시할 Snort 시그니처 ID를 구성합니다.

```
Router(config-utd-whitelist)#generator id 40 signature id 54621 comment FILE-OFFICE traffic from network
Router(config-utd-whitelist)#end
```

---

 참고: ID '40'이(가) 예로 사용됩니다. Snort 서명 정보를 확인하려면 공식 Snort 문서를 확인하십시오.

---

## 8단계(선택 사항) Threat Inspection 컨피그레이션에서 Allowed List를 활성화합니다.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#whitelist
```

## 9단계. Snort 서명을 자동으로 다운로드하도록 서명 업데이트 간격을 구성합니다.

```
Router#config terminal
Router(config)#utd engine standard
Router(config-utd-eng-std)#threat-inspection
Router(config-utd-engstd-insp)#signature update occur-at [daily, monthly, weekly] 0 0
```

---

 주: 첫 번째 숫자는 시간을 24시간 형식으로 정의하고, 두 번째 숫자는 분을 나타냅니다.

---


 경고: UTD 서명 업데이트는 업데이트 시 간략한 서비스 중단을 생성합니다.

---

## 10단계. 시그니처 업데이트 서버 매개변수를 구성합니다.

```
Router(config-utd-engstd-insp)#signature update server [cisco, url] username cisco password cisco12
```

---

 참고: 'cisco'를 사용하여 Cisco 서버를 사용하거나 'url'을 사용하여 업데이트 서버의 사용자 지정 경로를 정의합니다. Cisco 서버의 경우 사용자 이름과 비밀번호를 입력해야 합니다.

---

11단계. 로깅 레벨을 활성화합니다.

```
Router(config-utd-engstd-insp)#logging level [alert,crit,debug,emerg,info,notice,warning]
Router(config-utd-engstd-insp)#exit
Router(config-utd-eng-std)#exit
```

12단계. utd 서비스를 활성화합니다.

```
Router#configure terminal
Router(config)#utd
```

13단계(선택 사항) VirtualPortGroup 인터페이스에서 UTD 서비스로 데이터 트래픽을 리디렉션합니다.

```
Router#configure terminal
Router(config)#utd
Router(config-utd)#redirect interface virtualPortGroup
```

---

 참고: 리디렉션이 구성되지 않은 경우 자동으로 검색됩니다.

---

14단계. ISR의 모든 레이어 3 인터페이스에 대해 UTD를 활성화합니다.

```
Router(config-utd)#all-interfaces
```

15단계. 엔진 표준을 활성화합니다.

```
Router(config-utd)#engine standard
```

다음 syslog 메시지는 UTD가 제대로 활성화되었음을 나타냅니다.




```
*Jun 27 23:41:03.062: %LINEPROTO-5-UPDOWN: Line protocol on Interface Tunnel0
*Jun 27 23:41:13.039: %IOSXE-2-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
*Jun 27 23:41:22.457: %IOSXE-5-PLATFORM: R0/0: cpp_cp: QFP:0.0 Thread:000 TS:0
```

## 16단계(선택 사항) UTD 엔진 장애에 대한 작업 정의(UTD 데이터 플레인)

```
Router(config-engine-std)#fail close
Router(config-engine-std)#end
Router#copy running-config startup-config
Destination filename [startup-config]?
```

---

 참고: 'Fail close' 옵션은 UTD 엔진이 실패할 때 모든 IPS/IDS 트래픽을 삭제합니다. 'Fail open' 옵션은 UTD 장애에 대한 모든 IPS/IDS 트래픽을 허용합니다. 기본 옵션은 'fail open'입니다.

---

## 다음을 확인합니다.

VirtualPortGroups IP 주소 및 인터페이스 상태를 확인합니다.

```
Router#show ip interface brief | i VirtualPortGroup
VirtualPortGroup0 192.168.1.1 YES NVRAM up up
VirtualPortGroup1 192.168.2.1 YES NVRAM up up
```

VirtualPortGroup 컨피그레이션을 확인합니다.

```
Router#show running-config | b interface
interface VirtualPortGroup0
description Management Interface
ip address 192.168.1.1 255.255.255.252
!
interface VirtualPortGroup1
description Data Interface
ip address 192.168.2.1 255.255.255.252
!
```

앱 호스팅 구성을 확인합니다.

```
Router#show running-config | b app-hosting
app-hosting appid UTD
app-vnic gateway0 virtualportgroup 0 guest-interface 0
```

```
guest-ipaddress 192.168.1.2 netmask 255.255.255.252
app-vnic gateway1 virtualportgroup 1 guest-interface 1
guest-ipaddress 192.168.2.2 netmask 255.255.255.252
start
end
```

iox 활성화를 확인합니다.

```
Router#show running-config | i iox
iox
```

UTD 서비스 플레인 컨피그레이션을 확인합니다.

```
Router#show running-config | b engine
utd engine standard
logging host 192.168.10.5
threat-inspection
threat protection
policy security
signature update server cisco username cisco password KcEDIO[gYafNZheBHBD`CC\g`_cSeFAAB
signature update occur-at daily 0 0
logging level info
whitelist
utd threat-inspection whitelist
generator id 40 signature id 54621 comment FILE-OFFICE traffic
utd
all-interfaces
redirect interface VirtualPortGroup1
engine standard
fail close
```

```
Router#show utd engine standard config
UTD Engine Standard Configuration:
```

IPS/IDS : Enabled

Operation Mode : Intrusion Prevention  
Policy : Security

Signature Update:  
Server : cisco  
User Name : cisco  
Password : KcEDIO[gYafNZheBHBD`CC\g`\_cSeFAAB  
Occurs-at : daily ; Hour: 0; Minute: 0

Logging:  
Server : 192.168.10.5  
Level : info  
Statistics : Disabled  
Hostname : router

System IP : Not set

Whitelist : Enabled  
Whitelist Signature IDs:  
54621, 40

Port Scan : Disabled

Web-Filter : Disabled

앱 호스팅 상태를 확인합니다.

```
Router#show app-hosting list
App id                               State
-----
UTD                                   RUNNING
```

앱 호스팅 세부 정보를 확인합니다.

```
Router#show app-hosting detail
App id : UTD
Owner : ioxm
State : RUNNING
Application
Type : LXC
Name : UTD-Snort-Feature
Version : 1.0.7_SV2.9.18.1_XE17.9
Description : Unified Threat Defense
Author :
Path : /bootflash/secapp-utd.17.09.03a.1.0.7_SV2.9.18.1_XE17.9.x86_64.tar
URL Path :
Multicast : yes
Activated profile name :
```

```
Resource reservation
Memory : 1024 MB
Disk : 752 MB
CPU :
CPU-percent : 25 %
VCPUs : 0
```

```
Platform resource profiles
Profile Name CPU(unit) Memory(MB) Disk(MB)
-----
```

```
Attached devices
Type Name Alias
-----
```

```
Disk /tmp/xml/UtdLogMappings-IOX
Disk /tmp/xml/UtdIpsAlert-IOX
Disk /tmp/xml/UtdDaqWcapi-IOX
Disk /tmp/xml/UtdUrf-IOX
Disk /tmp/xml/UtdTls-IOX
```

Disk /tmp/xml/UtdDaq-IOX  
Disk /tmp/xml/UtdAmp-IOX  
Watchdog watchdog-503.0  
Disk /tmp/binos-IOX  
Disk /opt/var/core  
Disk /tmp/HTX-IOX  
Disk /opt/var  
NIC ieobc\_1 ieobc  
Disk \_rootfs  
NIC mgmt\_1 mgmt  
NIC dp\_1\_1 net3  
NIC dp\_1\_0 net2  
Serial/Trace serial3

#### Network interfaces

-----  
eth0:  
MAC address : 54:0e:00:0b:0c:02  
IPv6 address : ::  
Network name :  
eth:  
MAC address : 6c:41:0e:41:6b:08  
IPv6 address : ::  
Network name :  
eth2:  
MAC address : 6c:41:0e:41:6b:09  
IPv6 address : ::  
Network name :  
eth1:  
MAC address : 6c:41:0e:41:6b:0a  
IPv4 address : 192.168.2.2  
IPv6 address : ::  
Network name :

#### Process Status Uptime # of restarts

-----  
c\_lingr UP 0Y 0W 0D 21:45:29 2  
logger UP 0Y 0W 0D 19:25:56 0  
snort\_1 UP 0Y 0W 0D 19:25:56 0

#### Network stats:

eth0: RX packets:162886, TX packets:163855  
eth1: RX packets:46, TX packets:65

#### DNS server:

domain cisco.com  
nameserver 192.168.90.92

Coredump file(s): core, lost+found

Interface: eth2  
ip address: 192.168.2.2/30  
Interface: eth1  
ip address: 192.168.1.2/30

Address/Mask Next Hop Intf.

-----  
0.0.0.0/0 192.168.2.1 eth2  
0.0.0.0/0 192.168.1.1 eth1


## 문제 해결

1. Cisco ISR(Integrated Services Router)에서 XE 16.10.1a 이상 실행(IOx 방식) 보장
2. Securityk9 기능이 활성화된 상태에서 Cisco ISR(Integrated Services Router)이 라이선스되는지 확인합니다.
3. ISR 하드웨어 모델이 최소 리소스 프로필을 준수하는지 확인합니다.
4. Zone-Based Firewall SYN-cookie and Network Address Translation 64(NAT64)와 호환되지 않는 기능
5. 설치 후 UTD 서비스가 시작되었는지 확인합니다.
6. 수동 서명 패키지를 다운로드하는 동안 패키지의 버전이 Snort 엔진 버전과 동일한지 확인합니다. 버전이 일치하지 않으면 서명 패키지 업데이트가 실패할 수 있습니다.
7. 성능 문제가 있는 경우 CPU/메모리/스토리지 완성에 대해 알아보려면 'show app-hosting resource'와 'show app-hosting utilization appid"UTD-NAME'을 사용하십시오.

```
Router#show app-hosting resource
CPU:
Quota: 75(Percentage)
Available: 50(Percentage)
VCPU:
Count: 6
Memory:
Quota: 10240(MB)
Available: 9216(MB)
Storage device: bootflash
Quota: 4000(MB)
Available: 4000(MB)
Storage device: harddisk
Quota: 20000(MB)
Available: 19029(MB)
Storage device: volume-group
Quota: 190768(MB)
Available: 169536(MB)
Storage device: CAF persist-disk
Quota: 20159(MB)
Available: 18078(MB)
```

```
Router#show app-hosting utilization appid utd
Application: utd
CPU Utilization:
CPU Allocation: 33 %
CPU Used: 3 %
Memory Utilization:
Memory Allocation: 1024 MB
Memory Used: 117632 KB
Disk Utilization:
Disk Allocation: 711 MB
```

---

 경고: 높은 CPU, 메모리 또는 디스크 사용량을 확인할 수 있는 경우 Cisco TAC에 문의하십시오.

---

## 디버깅

장애가 발생할 경우 Snort IPS 정보를 수집하려면 아래 나열된 debug 명령을 사용합니다.

```
<#root>
```

```
debug virtual-service all
```

```
debug virtual-service virtualPortGroup
```

```
debug virtual-service messaging
```

```
debug virtual-service timeout
```

```
debug utd config level error [error, info, warning]  
debug utd engine standard all
```

## 관련 정보

Snort IPS 구축과 관련된 추가 문서는 여기에서 확인할 수 있습니다.

Snort IPS 보안 컨피그레이션 가이드

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_utd/configuration/xs-17/sec-data-utd-xe-17-book/snort-ips.html](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xs-17/sec-data-utd-xe-17-book/snort-ips.html)

가상 서비스 리소스 프로필

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_utd/configuration/xs-17/sec-data-utd-xe-17-book/snort-ips.html#id\\_31952](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xs-17/sec-data-utd-xe-17-book/snort-ips.html#id_31952)

라우터의 Snort IPS - 단계별 컨피그레이션

<https://community.cisco.com/t5/security-knowledge-base/router-security-snort-ips-on-routers-step-by-step-configuration/ta-p/3369186>

Snort IPS 트러블슈팅

[https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec\\_data\\_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept\\_C3C869E633A6475890475931DF83EBCC](https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/sec_data_utd/configuration/xe-17/sec-data-utd-xe-17-book/snort-ips.html#concept_C3C869E633A6475890475931DF83EBCC)

HW에 충분한 플랫폼 리소스가 없으므로 ISR4K Snort IPS가 구축되지 않음

<https://bst.cloudapps.cisco.com/bugsearch/bug/CSCwf57595>

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.