FTD(Firepower 위협 방어)에서 실행되는 활성 Snort 버전 확인

목차

소개

이 문서에서는 Cisco FTD(Firepower Threat Defense)가 Cisco FDM(Firepower Device Manager), Cisco FMC(Firepower Management Center) 또는 Cisco CDO(Defense Orchestrator)에서 관리되는 경우 실행하는 활성 snort 버전을 확인하는 단계에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco FMC(Firepower 관리 센터)
- Cisco FTD(Firepower 위협 방어)
- Cisco FDM(Firepower 장치 관리자)
- CDO(Cisco Defense Orchestrator)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD(Firepower Threat Defense) v6.7.0 및 7.0.0
- Cisco FMC(Firepower Management Center) v6.7.0 및 7.0.0
- CDO(Cisco Defense Orchestrator)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바

이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

SNORT® Intrusion Prevention System은 성능 향상, 빠른 처리, 네트워크 확장성 개선, 200개 이상의 다양한 플러그인이 포함된 전면적인 업그레이드 기능인 Snort 3을 공식적으로 출시했습니다. 이를 통해 사용자는 네트워크에 대한 맞춤형 설정을 생성할 수 있습니다.

Snort 3의 이점은 다음과 같습니다(이에 제한되지 않음).

- 성능 향상
- SMBv2 검사 개선
- 새로운 스크립트 탐지 기능
- HTTP/2 검사
- 사용자 지정 규칙 그룹
- 사용자 지정 침입 규칙을 더욱 쉽게 작성할 수 있도록 하는 구문
- 침입 이벤트의 인라인 결과가 '삭제되었을 것'인 이유
- VDB, SSL 정책, 맞춤형 애플리케이션 탐지기, 종속 포털 ID 소스, TLS 서버 ID 검색에 변경 사항이 구축되면 Snort 재시작 불가
- Cisco Success Network로 전송되는 Snort 3 관련 텔레메트리 데이터 및 더 나은 문제 해결 로그를 통해 서비스 가용성 향상

6.7.0 Cisco FTD(Firepower Threat Defense)를 위해 Snort 3.0 지원이 도입되었는데, 이는 FTD가 Cisco FDM(Firepower Device Manager)을 통해 관리되는 경우에 한합니다.

참고: FDM에서 관리하는 새 6.7.0 FTD 구축의 경우 Snort 3.0이 기본 검사 엔진입니다. 이전 릴리스에서 FTD를 6.7로 업그레이드할 경우 Snort 2.0은 활성 검사 엔진으로 유지되지만 Snort 3.0으로 전환할 수 있습니다.

참고: 이 릴리스의 경우 Snort 3.0은 가상 라우터, 시간 기반 액세스 제어 규칙 또는 TLS 1.1 이하 연결의 암호 해독을 지원하지 않습니다. 이러한 기능이 필요하지 않은 경우에만 Snort 3.0을 활성화합니다.

그런 다음 Firepower 버전 7.0에는 Cisco FDM과 Cisco FMC(Firepower Management Center)에서 모두 관리하는 Firepower Threat Defense 장치에 대한 Snort 3.0 지원이 도입되었습니다.

참고: 새로운 7.0 FTD 구축의 경우 이제 Snort 3이 기본 검사 엔진입니다. 업그레이드된 구축에서는 Snort 2를 계속 사용하지만 언제든지 전환할 수 있습니다.

⚠ 주의: Snort 2.0과 3.0 사이를 자유롭게 오갈 수 있으므로 필요한 경우 변경 사항을 되돌릴 수 있습니다. 버전을 전환할 때마다 트래픽이 중단됩니다.

⚠ 주의: Snort 3으로 전환하기 전에 Firepower Management Center Snort 3 컨피그레이션 가이드를 읽고 이해하는 것이 좋습니다. 기능 제한 및 마이그레이션 지침에 각별히 유의하십시오. Snort 3으로의 업그레이드는 영향을 최소화하도록 설계되었지만 기능이 정확하게 매핑되지는 않습니다. 업그레이드 전 계획과 준비는 트래픽이 예상대로 처리되도록 하는 데 도움이 됩니다.

FTD에서 실행되는 활성 Snort 버전 확인

FTD CLI(Command Line Interface)

FTD에서 실행되는 활성 snort 버전을 확인하려면 FTD CLI에 로그인하고 show snort3 status 명령을 실행합니다.

예 1: 출력이 표시되지 않으면 FTD에서 Snort 2를 실행합니다.

```
<#root>

>

show snort3 status


>
```

예 2: 출력에 "Currently running Snort 2"가 표시되면 FTD에서 Snort 2를 실행합니다.

```
<#root>

>

show snort3 status

Currently running Snort 2
```

예 3: 출력에 "Currently running Snort 3"이 표시되면 FTD에서 Snort 3을 실행합니다.

```
<#root>

>

show snort3 status
```

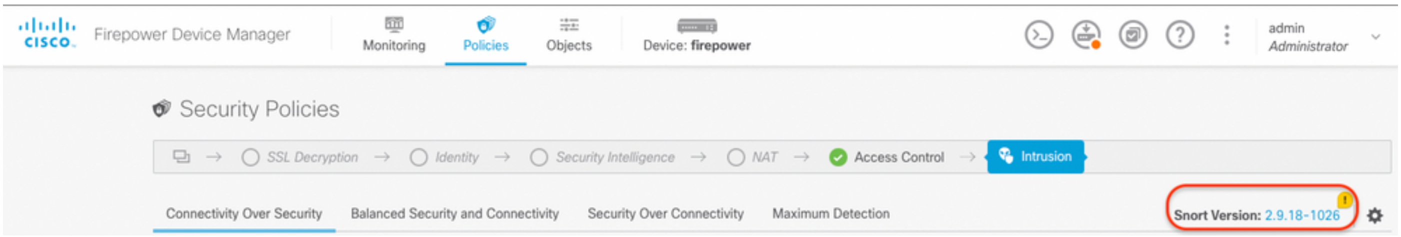
```
Currently running Snort 3
```

Cisco FDM에서 관리하는 FTD

Cisco FDM에서 관리하는 FTD에서 실행되는 활성 snort 버전을 확인하려면 다음 단계를 진행합니다.

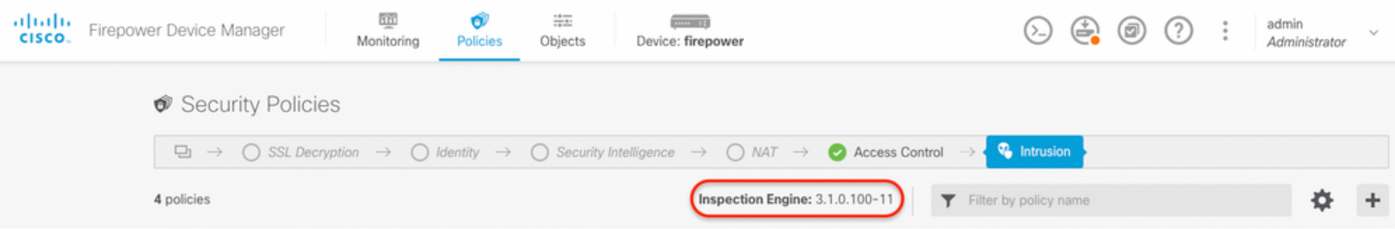
1. FDM 웹 인터페이스를 통해 Cisco FTD에 로그인합니다.
2. 주 메뉴에서 Policies를 선택합니다.
3. 그런 다음 Intrusion(침입) 탭을 선택합니다.
4. Snort Version 또는 Inspection Engine 섹션을 찾아 FTD에서 활성화된 Snort 버전을 확인합니다.

예 1: FTD는 snort 버전 2를 실행합니다.



Snort Version: 2.9.18-1026

예 2: FTD는 snort 버전 3을 실행합니다.



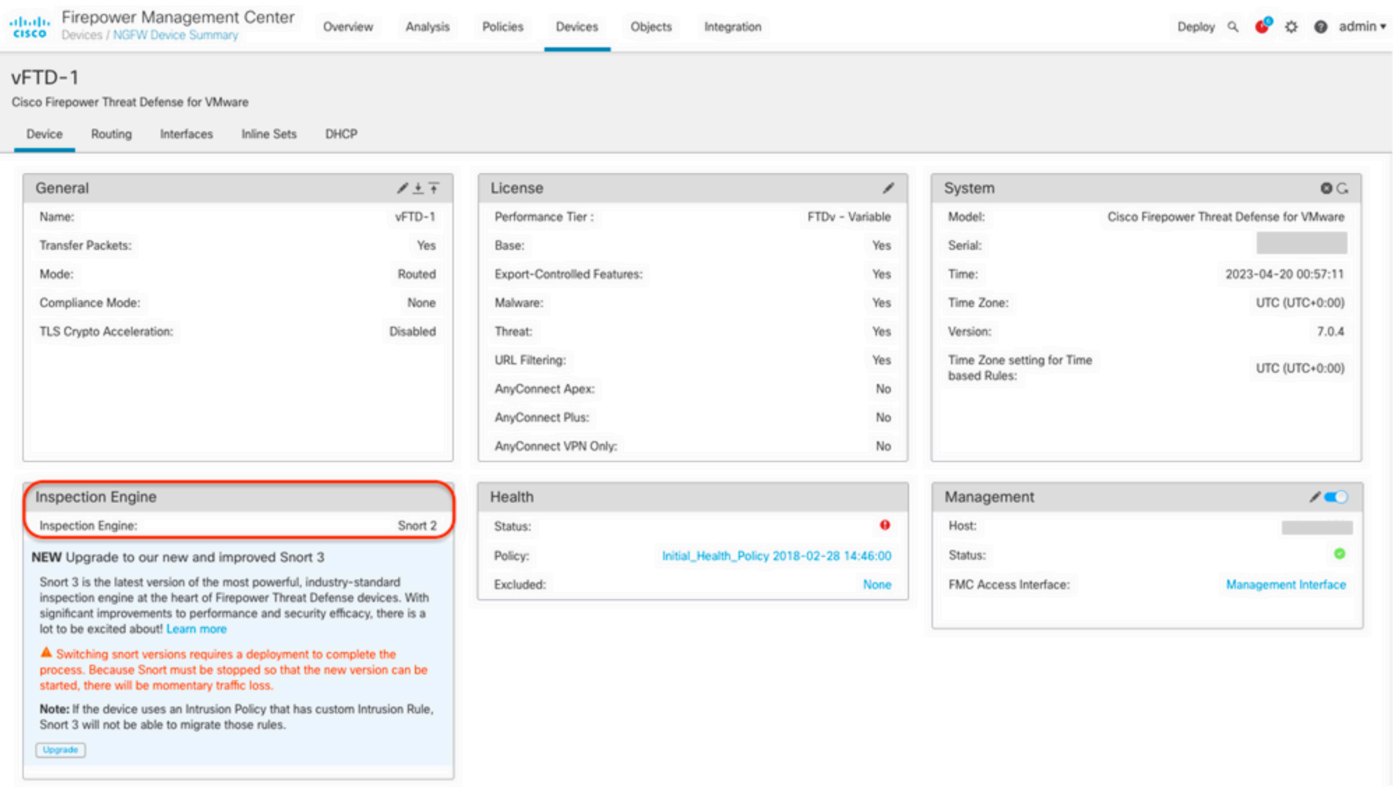
Inspection Engine: 3.1.0.100-11

FTD에서 관리 Cisco FMC

Cisco FMC에서 관리하는 FTD에서 실행되는 활성 Snort 버전을 확인하려면 다음 단계를 진행합니다.

1. Cisco FMC 웹 인터페이스에 로그인합니다.
2. Devices 메뉴에서 Device Management를 선택합니다.
3. 그런 다음 적절한 FTD 디바이스를 선택합니다.
4. 편집 연필 아이콘을 클릭합니다.
5. Device(디바이스) 탭을 선택하고 Inspection Engine(검사 엔진) 섹션을 찾아 FTD에서 활성화된 Snort 버전을 확인합니다.

예 1: FTD는 snort 버전 2를 실행합니다.



vFTD-1

Cisco Firepower Threat Defense for VMware

General

Name: vFTD-1

Transfer Packets: Yes

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

License

Performance Tier : FTDv - Variable

Base: Yes

Export-Controlled Features: Yes

Malware: Yes

Threat: Yes

URL Filtering: Yes

AnyConnect Apex: No

AnyConnect Plus: No

AnyConnect VPN Only: No

System

Model: Cisco Firepower Threat Defense for VMware

Serial: [redacted]

Time: 2023-04-20 00:57:11

Time Zone: UTC (UTC+0:00)

Version: 7.0.4

Time Zone setting for Time based Rules: UTC (UTC+0:00)

Inspection Engine

Inspection Engine: Snort 2

NEW Upgrade to our new and improved Snort 3

Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With significant improvements to performance and security efficacy, there is a lot to be excited about! Learn more

⚠ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

Health

Status: ●

Policy: Initial_Health_Policy 2018-02-28 14:46:00

Excluded: None

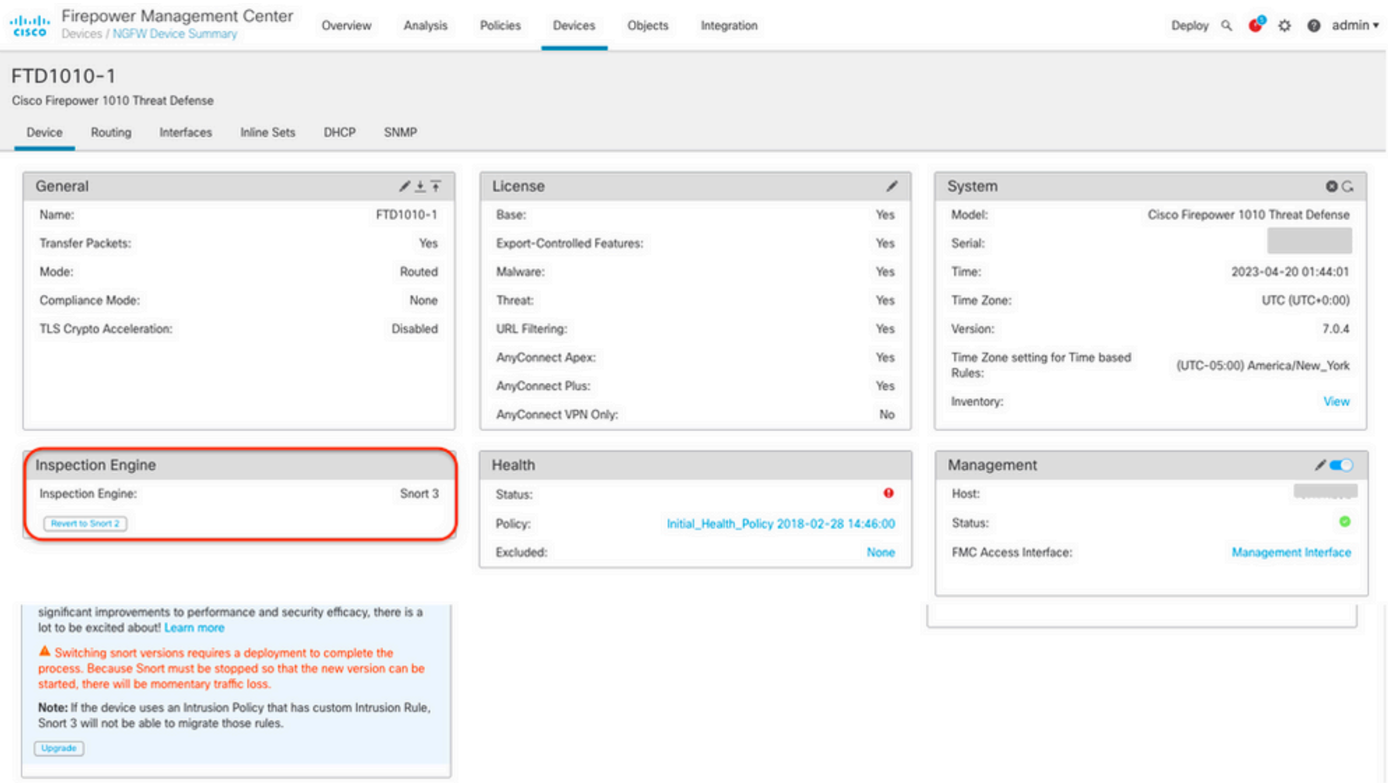
Management

Host: [redacted]

Status: ●

FMC Access Interface: Management Interface

예 2: FTD는 snort 버전 3을 실행합니다.



FTD1010-1

Cisco Firepower 1010 Threat Defense

General

Name: FTD1010-1

Transfer Packets: Yes

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

License

Base: Yes

Export-Controlled Features: Yes

Malware: Yes

Threat: Yes

URL Filtering: Yes

AnyConnect Apex: Yes

AnyConnect Plus: Yes

AnyConnect VPN Only: No

System

Model: Cisco Firepower 1010 Threat Defense

Serial: [redacted]

Time: 2023-04-20 01:44:01

Time Zone: UTC (UTC+0:00)

Version: 7.0.4

Time Zone setting for Time based Rules: (UTC-05:00) America/New_York

Inventory: View

Inspection Engine

Inspection Engine: Snort 3

significant improvements to performance and security efficacy, there is a lot to be excited about! Learn more

⚠ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be momentary traffic loss.

Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.

Health

Status: ●

Policy: Initial_Health_Policy 2018-02-28 14:46:00

Excluded: None

Management

Host: [redacted]

Status: ●

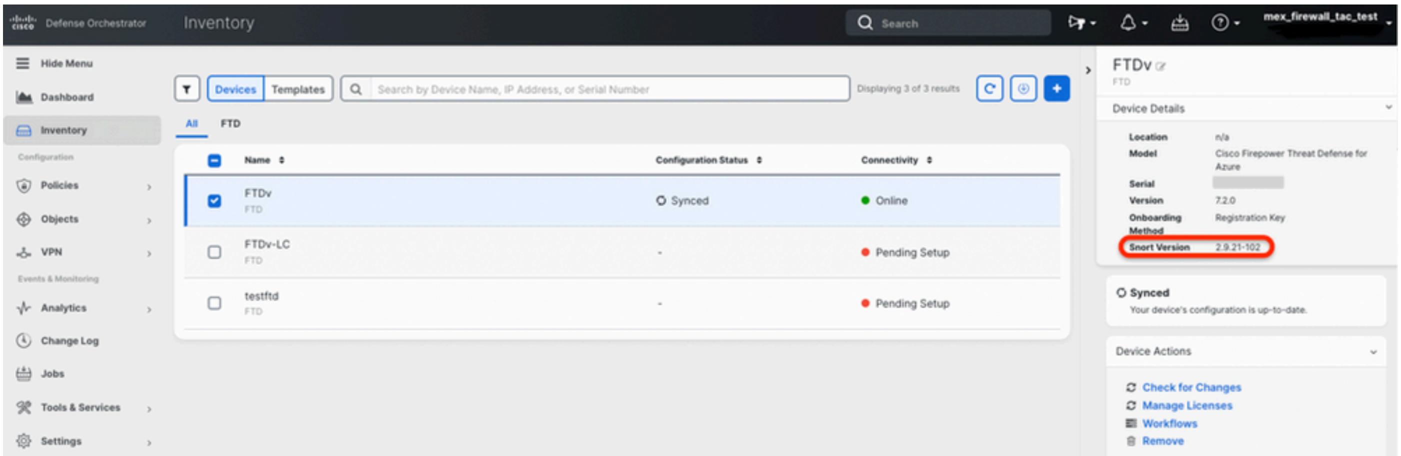
FMC Access Interface: Management Interface

FTD에서 관리 Cisco CDO

Cisco Defense Orchestrator에서 관리하는 FTD에서 실행되는 활성 Snort 버전을 확인하려면 다음 단계를 진행합니다.

1. Cisco Defense Orchestrator 웹 인터페이스에 로그인합니다.
2. Inventory(인벤토리) 메뉴에서 적절한 FTD 디바이스를 선택합니다.
3. Device Details(디바이스 세부사항) 섹션에서 Snort Version(Snort 버전)을 찾습니다.

예 1: FTD는 snort 버전 2를 실행합니다.



[redacted]

	Name	Configuration Status	Connectivity
☑	FTDv FTD	Synced	● Online
□	FTDv-LC FTD	-	● Pending Setup
□	testftd FTD	-	● Pending Setup

FTDv
FTD

Device Details

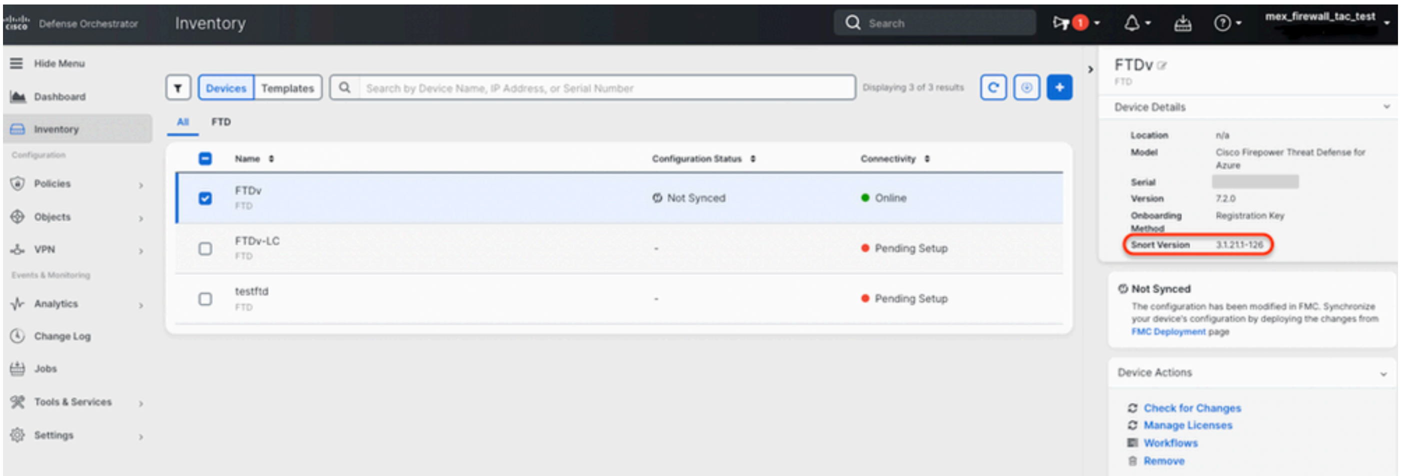
Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	2.9.21-102

Synced
Your device's configuration is up-to-date.

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove

예 2: FTD는 snort 버전 3을 실행합니다.



[redacted]

	Name	Configuration Status	Connectivity
☑	FTDv FTD	Not Synced	● Online
□	FTDv-LC FTD	-	● Pending Setup
□	testftd FTD	-	● Pending Setup

FTDv
FTD

Device Details

Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	3.1.21.1-126

Not Synced
The configuration has been modified in FMC. Synchronize your device's configuration by deploying the changes from FMC Deployment page

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove

관련 정보

- Cisco Firepower 릴리스 정보, 버전 6.7.0
- Cisco Firepower 릴리스 노트, 버전 7.0
- Snort 3 웹 사이트
- 기술 지원 및 문서 – Cisco Systems

이 번역에 관하여