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

목차

<u>관련 정보</u>

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 이상 의 다양한 플러그인이 포함된 전면적인 업그레이드 기능인 Snort 3을 공식적으로 출시했습니다. 이 를 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 사 항이 구축되면 Snort 재시작 불가
- Cisco Success Network로 전송되는 Snort 3 관련 텔레메트리 데이터 및 더 나은 문제 해결 로 그를 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 이 하 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 구축 에서는 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 가이 드를 읽고 이해하는 것이 좋습니다. 기능 제한 및 마이그레이션 지침에 각별히 유의하십시오. Snort 3으로의 업그레이드는 영향을 최소화하도록 설계되었지만 기능이 정확하게 매핑되지 는 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 명령 을 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

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.



예 2: FTD는 snort 버전 3을 실행합니다.

ahaha cisco.	Firepower Device Manager	Monitoring Poli	Cies Objects Device: firepower	> 🚑 Ø	? : admin Administrator
	🕫 Security Policie	es			
	$\square \rightarrow \bigcirc$ SSL Dec	ryption $ ightarrow$ () Identity	$ ightarrow$ \bigcirc Security Intelligence $ ightarrow$ \bigcirc NAT $ ightarrow$	Access Control \rightarrow Recess Control \rightarrow	
	4 policies		Inspection Engine: 3.1	.0.100-11 Tilter by policy name	\$ +

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 활성화 된 Snort 버전을 확인합니다.

예 1: FTD는 snort 버전 2를 실행합니다.

VFID-1 Cisco Firepower Threat Defense for VMwares Device Routing Interfaces Interfaces Device Ceneral	Firepower Management Center Devices / NGFW Device Summary	Overview Analysis	Policies Devices Objects Integr	ration		Deploy 🔍 💕 🌣 🚳 adı
General ✓ ± ∓ Name: vF1D-1 Transfer Packets: Ves Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Disabled Inspection Engine None Inspection Engine Sont 3 Nexew: None	1 power Threat Defense for VMware Routing Interfaces Inline Sets	DHCP				
Name: vFTD-1 Transfer Packets: Yes Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Disabled URL Filtering: Yes AnyConnect Apex: No AnyConnect Apex: No AnyConnect Apex: No AnyConnect VPN Only: No Nett Upgrade to our new and improved Snort 3 Snort 3 is the latest version of the most powerful, industry-standard ispection engine at the heart Defense devices. With significant improvements to performance and security efficacy, there is a to to be excited about Learn more Note A switching snort versions requires a deployment to complete the process. Because Snort must be stopod so that the new version can be stored, there will be monentary traffic loss. None	eral	/±+	License	/	System	0 G
Transfer Packets: Yes Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Disabled URL Filtering: Yes AnyConnect Apex: Non AnyConnect Apex: Non AnyConnect VPN Only: Non Inspection Engine: Sonot 2 NEW Upgrade to our new and improved Snort 3 Status: Sonot 1s is the latest version of the most powerful, industry-standard inspection engine at the heart of Fingower Thread Defense devices. Whis significant improvements to performance and security efficacy, there is a tot to be excised about Learm more Nonital_Health_Policy 2018-02-28 14:46:00 Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be stated, there wersion can be stopped so that the new version can be stopped so that the new	e:	vFTD-1	Performance Tier :	FTDv - Variable	Model:	Cisco Firepower Threat Defense for VMware
Mode: Routed Compliance Mode: None TLS Crypto Acceleration: Disabled TLS Crypto Acceleration: Disabled Malware: Yes Threat: Yes URL Fittering: Yes AryConnect Apex: No AryConnect VPN Only: No 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 excluded about team more A Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be stored in the new version can be	sfer Packets:	Yes	Base:	Yes	Serial:	
Compliance Mode: None Malware: Yes Time Zone: UTC (TLS Crypto Acceleration: Disabled Threat: Yes Version: UTC (TLS Crypto Acceleration: Disabled Threat: Yes Time Zone: UTC (Malware: Yes Time Zone: Version: UTC (Version: UTC (Markage Rules: No AnyConnect Apex: No No No AnyConnect VPN Only: No	e:	Routed	Export-Controlled Features:	Yes	Time:	2023-04-20 00:57:11
TLS Crypto Acceleration: Disabled Intract: Yes Version: URL Filtering: Yes AnyConnect Apex: No AnyConnect VPN Only: No AnyConnect VPN Only: No Inspection Engine: Snort 2 NEW Upgrade to our new and improved Snort 3 Status: Intral_Health_Policy 2018-02-28 14:46:00 Sond 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 true to the westion can be stated, there is a stated, there wersion can be stated. None	pliance Mode:	None	Malware:	Yes	Time Zone:	UTC (UTC+0:00)
URL Filtering: Yes AnyConnect Apex: No AnyConnect VPN Only: No Inspection Engine: Snot 2) New Upgrade to our new and improved Snot 3 Sond 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Treat Defense devices. With aginficant improvements to performance and security efficacy, there is a lot to be excited about! Learn more A Switching snort versions requires a deployment to complete the process. Because Snot must be stopped so that the new version can be starde, three will be momentary traffic loss.	Crypto Acceleration:	Disabled	Threat:	Yes	Version:	7.0.4
AnyConnect Apex: No AnyConnect VPN Only: No Inspection Engine Inspection Engine Ins			URL Filtering:	Yes	Time Zone setting for Time	UTC (UTC+0:00)
AnyConnect Plus: No AnyConnect VPN Only: No Inspection Engine: Snot 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 A Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be statted, there will be momentary traffic loss.			AnyConnect Apex:	No	based Rules:	
Inspection Engine No Inspection Engine Snot 2 NEW Upgrade to our new and improved Snot 3 Status: Snot 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 Health A switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version can be stated, there will be momentary traffic loss. None			AnyConnect Plus:	No		
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 Inspection more Inspection engine at the new version requires a deployment to complete the process. Because Snort must be stopped so that the new version can be stated, there will be momentary traffic loss. Inspection engine at the work of the there will be momentary traffic loss. Inspection engine at the work of the there will be momentary traffic loss. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. Inspection engine at the heart of Firepower Threat Defense devices. In			AnyConnect VPN Only:	No		
Inspection Engine: Snot 2 NEW Upgrade to our new and improved Snort 3 Status: ● Host: Status: St	ection Engine		Health		Management	/ 🕥
New Upgrade to our new and improved Snort 3 Policy: Initial_Health_Policy 2018-02-28 14:46:00 Status: Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Firepower Threat Defense devices. With lot to be excited about! Learn more Excluded: None ▲ Switching snort versions requires a deployment to complete the process. Because Snort must be stopped so that the new version cane be stated, there will be momentary traffic loss. Status: Managementary	ection Engine:	Snort 2	Status:	0	Host:	
Snort 3 is the latest version of the most powerful, industry-standard inspection engine at the heart of Finepower Threat Defense devices. With lot to be excited about! Learn more Excluded: None FMC Access Interface: Management Management Management Management Subthing 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.	Upgrade to our new and improved Snort	3	Policy: Initial_Health	Policy 2018-02-28 14:46:00	Status:	0
A 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.	t 3 is the latest version of the most powerful, in oction engine at the heart of Firepower Threat D ficant improvements to performance and security be excited about! Learn more	dustry-standard Defense devices. With ity efficacy, there is a	Excluded:	None	FMC Access Interface:	Management Interface
	witching snort versions requires a deployment to ess. Because Snort must be stopped so that the ed, there will be momentary traffic loss.	o complete the e new version can be				
Note: If the device uses an Intrusion Policy that has custom Intrusion Rule, Snort 3 will not be able to migrate those rules.	: If the device uses an Intrusion Policy that has o t 3 will not be able to migrate those rules.	custom Intrusion Rule,				
Upgrade	ide					

예 2: FTD는 snort 버전 3을 실행합니다.

Firepower Management Center Devices / NGFW Device Summary	er Overview Analysis	Policies Devices Objects Integration	'n		Deploy Q 🗳 🌣 🔕 adm
TD1010-1 isco Firepower 1010 Threat Defense Device Routing Interfaces Inline S	ets DHCP SNMP				
General	/±+	License	1	System	O C
Name:	FTD1010-1	Base:	Yes	Model:	Cisco Firepower 1010 Threat Defense
Transfer Packets:	Yes	Export-Controlled Features:	Yes	Serial:	
Mode:	Routed	Malware:	Yes	Time:	2023-04-20 01:44:01
Compliance Mode:	None	Threat:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	URL Filtering:	Yes	Version:	7.0.4
		AnyConnect Apex:	Yes	Time Zone setting for Time based	(UTC-05:00) America/New_York
		AnyConnect Plus:	Yes	Rules:	(0.0 0.00)
		AnyConnect VPN Only:	No	Inventory:	View
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	0	Host:	
Revert to Short 2		Policy: Initial_Health_P	olicy 2018-02-28 14:46:00	Status:	0
		Excluded:	None	FMC Access Interface:	Management Interface
significant improvements to performance and	security efficacy, there is a				
lot to be excited about! Learn more					
Switching snort versions requires a deploy process. Because Snort must be stopped so t started, there will be momentary traffic loss.	ment to complete the that the new version can be				
Note: If the device uses an Intrusion Policy the Snort 3 will not be able to migrate those rules	at has custom Intrusion Rule,				
Upgrade					

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.

cisco (Defense Orchestrate	or	Inven	tory				Q Search	Ø 7 •	0· 🖷	? - mex_firewall_tac_test	٠
≡ +	lide Menu								,	FTDv @		
🖮 D	ashboard	Ŀ		evices Templates Q	Search by Device Name, IP Address	i, or Serial Number		Displaying 3 of 3 results	•	Device Details		~
e In	nventory	- 10	All F	TD						Location	n/a	
Configu	uration		•	Name 0		Conf	figuration Status 0	Connectivity \$		Model	Cisco Firepower Threat Defense for Azure	
(i) p	olicies	>		FTDv		0.5	Synced	Online		Serial Version	72.0	
ۍ	bjects	>	-	FTD			-,			Onboarding	Registration Key	
.å. V	IPN	>	0	FTDV-LC				Pending Setup		Snort Version	2.9.21-102	
Events	& Monitoring			testiled						O Synced		
√~ A	inalytics	>		FTD				Pending Setup		Your device's co	nfiguration is up-to-date.	
() c	hange Log									Device Actions	~	
د 🗎	obs									C Charles for (hanne	
Ж т	ools & Services	>								C Manage Lic	enses	
⊚ s	ettings	>								Workflows Remove		

예 2: FTD는 snort 버전 3을 실행합니다.

cisco	Defense Orchestrate	or	Invent	ory				Q Search	₽	•	۵. ج	•	mex_firewall_t	tac_test 🗸
≡	Hide Menu							.		,	FTDv @			
b	Dashboard	U		vices Templates	Search by Device Nam	e, IP Address, or Serial Numbe	ar	Displaying 3 of 3 results			Device Details			v
	Inventory	- 18	AL FT	D							Location	n/a		
Config	puration		•	Name 0			Configuration Status 0	Connectivity 0			Model	Cisco Fire Azure	power Threat Defer	nse for
۲	Policies	>		FTDv			6 Not Sunced	Online			Serial	720		
٠	Objects	>		FTD			W Not Synceric	Crimine			Onboarding	Registrati	on Key	
-å-	VPN	>		FTDv-LC FTD				Pending Setup			Snort Version	3.1.21.1-12	6	
Event	s & Monitoring Analytics	>	0	testftd FTD				Pending Setup			Not Synced The configuration your device's configuration	has been m	odified in FMC. Syn	chronize noes from
۲	Change Log										FMC Deploymen	page		
۵	Jobs										Device Actions			÷
*	Tools & Services	>									Check for C	hanges		
\$	Settings	>									C Manage Lic Workflows	enses		

관련 정보

- <u>Cisco Firepower 릴리스 정보, 버전 6.7.0</u>
- <u>Cisco Firepower 릴리스 노트, 버전 7.0</u>
- <u>Snort 3 웹 사이트</u>
- <u>기술 지원 및 문서 Cisco Systems</u>

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 번 역 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.