確定在Firepower威脅防禦(FTD)上運行的活動 Snort版本

目錄
<u>必要條件</u>
<u>需求</u>
採用元件
<u>背景資訊</u>
<u>判斷在FTD上執行的作用中Snort版本</u>
<u>FTD命令列介面(CLI)</u>
由Cisco FDM管理的FTD
由思科FMC管理的FTD
由思科CDO管理的FTD
<u>相關資訊</u>

簡介

本文檔介紹在思科Firepower裝置管理器(FDM)、思科Firepower管理中心(FMC)或思科Defense Orchestrator(CDO)管理思科Firepower威脅防禦(FTD)時,確認其運行的活動Snort版本的步驟。

必要條件

需求

思科建議您瞭解以下主題:

- Cisco Firepower Management Center(FMC)
- Cisco Firepower威脅防禦(FTD)
- Cisco Firepower裝置管理員(FDM)
- Cisco Defense Orchestrator(CDO)

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- Cisco Firepower威脅防禦(FTD)v6.7.0和7.0.0
- 思科Firepower管理中心(FMC)v6.7.0和7.0.0
- Cisco Defense Orchestrator(CDO)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

背景資訊

SNORT®入侵防禦系統正式推出了Snort 3, 這是一種全面的升級, 具有提高效能、加快處理速度、 提高網路可擴充性等改進和新功能,並且擁有200多個外掛,因此使用者可以為其網路建立自定義 設定。

Snort 3的優勢包括,但不限於:

- 改進的效能
- 改進的SMBv2檢測
- 新的指令碼檢測功能
- HTTP/2檢測
- 自定義規則組
- 使自定義入侵規則更易於編寫的語法
- 入侵事件中「would have dropped」內聯結果的原因
- 將更改部署到VDB、SSL策略、自定義應用檢測器、強制網路門戶身份源和TLS伺服器身份發 現時,不重新啟動Snort
- 由於Snort 3特定的遙測資料傳送到思科成功網路,並且故障排除日誌更出色,因此可維護性 得到提高

對Snort 3.0的支援是為6.7.0思科Firepower威脅防禦(FTD)引入的,此時正通過Cisco Firepower裝置 管理器(FDM)管理FTD。

 註:對於由FDM管理的新6.7.0 FTD部署,Snort 3.0是預設檢測引擎。如果您將FTD從舊版本 升級到6.7,則Snort 2.0仍舊是作用中檢查引擎,但您可以切換到Snort 3.0。

 註:對於此版本,Snort 3.0不支援虛擬路由器、基於時間的訪問控制規則或TLS 1.1或更低連 線的解密。僅在不需要這些功能時才啟用Snort 3.0。

然後,Firepower 7.0版引入了對Cisco FDM和Cisco Firepower管理中心(FMC)管理的Firepower威脅 防禦裝置的Snort 3.0支援。

 註:對於新的7.0 FTD部署,Snort 3現在是預設檢測引擎。已升級的部署繼續使用Snort 2,但 您可以隨時進行切換。

🗥 注意:您可以在Snort 2.0和3.0之間自由切換,以便根據需要恢復更改。每次切換版本時流量 都會中斷。

⚠ 注意:在切換到Snort 3之前,強烈建議您閱讀並理解《<u>Firepower Management Center Snort</u> <u>3配置指南》</u>。請特別注意功能限制和遷移說明。雖然升級到Snort 3是為了將影響降至最低而 設計的,但功能並不完全對應。升級之前的計畫和準備工作可以幫助您確保按照預期處理流量 。

判斷在FTD上執行的作用中Snort版本

FTD命令列介面(CLI)

若要判斷在FTD上執行的作用中Snort版本,請登入FTD CLI並執行show snort3 status命令:

範例1:當沒有顯示輸出時,FTD會執行Snort 2。

<#root>

>

show snort3 status

>

範例2:當輸出顯示「Currently running Snort 2」時,FTD會執行Snort 2。

<#root>

>

show snort3 status

Currently running Snort 2

範例3:當輸出顯示「Currently running Snort 3」時,FTD會執行Snort 3。

<#root>

>

show snort3 status

Currently running Snort 3

由Cisco FDM管理的FTD

若要判斷在Cisco FDM管理的FTD上執行的作用中Snort版本,請繼續執行以下步驟:

- 1. 通過FDM Web介面登入到Cisco FTD。
- 2. 從主選單中選擇Policies。
- 3. 然後,選擇Intrusion頁籤。
- 4. 尋找「Snort版本」或「檢查引擎」一節,以確認FTD中處於使用中的Snort版本。

範例1:FTD執行snort版本2。

alialia cisco.	Firepower Device Manager	Monitoring	Ø Policies	Objects D	Device: firepower		(>)		0	?	:	admin Administrator
	🛷 Security Policie	es										
	$\square \rightarrow \bigcirc$ SSL Decr	yption \rightarrow \bigcirc k	dentity \rightarrow (O Security Intellige	ence \rightarrow \bigcirc NAT	ightarrow Access Control $ ightarrow$	🔏 Intrusi	on				
	Connectivity Over Security	Balanced Secur	ity and Connect	tivity Security O	Iver Connectivity Max	rimum Detection				Snort	Versio	n: 2.9.18-1026

範例2: FTD執行snort版本3。

ahaha cisco.	Firepower Device Manager	Monitoring P	olicies Objects	Device: firepower	\odot		?	:	admin Administrator	~
	Security Policies	S								
	$\square \rightarrow \bigcirc$ SSL Decryp	ption $ ightarrow$ (dent	tity \rightarrow \bigcirc Security	Intelligence \rightarrow \bigcirc NAT \rightarrow	⊘ Access Control → <	ion				
	4 policies			Inspection Engine: 3	.1.0.100-11 Filter by policy	name			۵	+

由管理的FTD Cisco FMC

若要判斷在Cisco FMC管理的FTD上執行的作用中Snort版本,請繼續執行以下步驟:

- 1. 登入到Cisco FMC Web介面。
- 2. 從Devices選單中選擇Device Management。
- 3. 然後,選擇適當的FTD裝置。
- 4. 按一下Edit鉛筆圖示。
- 5. 選擇Device索引標籤,並檢視Inspection Engine部分,以確認FTD中處於活動狀態的Snort版本:

範例1:FTD執行snort版本2。

Firepower Management Cente Devices / NGFW Device Summary	CVerview Analysis	Policies Devices Objects Integ	ration		Deploy Q 🗳 🌣 🚳 admin
VFTD-1 Cisco Firepower Threat Defense for VMware Device Routing Interfaces Inline Se	ts DHCP				
General	/±∓	License	1	System	0 G
Name:	vFTD-1	Performance Tier :	FTDv - Variable	Model:	Cisco Firepower Threat Defense for VMware
Transfer Packets:	Yes	Base:	Yes	Serial:	
Mode:	Routed	Export-Controlled Features:	Yes	Time:	2023-04-20 00:57:11
Compliance Mode:	None	Malware:	Yes	Time Zone:	UTC (UTC+0:00)
TLS Crypto Acceleration:	Disabled	Threat:	Yes	Version:	7.0.4
		URL Filtering:	Yes	Time Zone setting for Time	UTC (UTC+0:00)
		AnyConnect Apex:	No	based Rules:	
		AnyConnect Plus:	No		
		AnyConnect VPN Only:	No		
Inspection Engine		Health		Management	/
Inspection Engine:	Snort 2	Status:		Host:	
NEW Upgrade to our new and improved S	inort 3	Policy: Initial_Health	_Policy 2018-02-28 14:46:00	Status:	•
Snort 3 is the latest version of the most power inspection engine at the heart of Firepower Thr significant improvements to performance and so lot to be excited about! Learn more	ful, industry-standard reat Defense devices. With security efficacy, there is a	Excluded:	None	FMC Access Interface:	Management Interface
Switching snort versions requires a deploym process. Because Snort must be stopped so th started, there will be momentary traffic loss.	nent to complete the hat the new version can be				
Note: If the device uses an Intrusion Policy that Snort 3 will not be able to migrate those rules.	t has custom Intrusion Rule,				
Upgrade					

範例2: FTD執行snort版本3。

Firepower Management Cent Devices / NGFW Device Summary	er Overview Analysis	Policies Devices Objects	Integration		Deploy Q 🗳 🌣 🔞 adr
TD1010-1 sco Firepower 1010 Threat Defense Device Routing Interfaces Inline S	iets DHCP SNMP				
General	/±+	License	1	System	Ø G
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	Inventory:	View
		AnyConnect VPN Only:	No	intentory.	
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	0	Host:	
Revent to Short 2		Policy: Initial_	Health_Policy 2018-02-28 14:46:00	Status:	c
		Excluded:	None	FMC Access Interface:	Management Interface
significant improvements to performance and lot to be excited about! Learn more A Switching snort versions requires a deploy process. Because Snort must be stopped so started, there will be momentary traffic loss. Note: If the device uses an Intrusion Policy th Snort 3 will not be able to migrate those rules	security efficacy, there is a ment to complete the that the new version can be at has custom Intrusion Rule, 5.				

由管理的FTD Cisco CDO

若要判斷在Cisco Defense Orchestrator管理的FTD上執行的作用中Snort版本,請繼續執行以下步驟:

- 1. 登入到Cisco Defense Orchestrator網路介面。
- 2. 從Inventory功能表中選擇適當的FTD裝置。
- 3. 在Device Details部分中,查詢Snort Version:

範例1:FTD執行snort版本2。

-ibiilii cisco Defense Orchestra	itor	Inventory		Q Search	7 • △• 曲 ⑦•	mex_firewall_tac_test
Hide Menu					, FTDv @	
📥 Dashboard		Devices Templates Q Search by Device Name, IP Address, or Serial N	lumber	Displaying 3 of 3 results C 🛞 +	Device Details	v
inventory		All FTD			Location n/a	
Configuration		Name ©	Configuration Status 0	Connectivity \$	Model Cisco Azure	Firepower Threat Defense for
Policies	>	FTDv	O Synced	Online	Serial Version 7.2.0	
Objects	>	FTD			Onboarding Regis Method	tration Key
"Č. VPN	\rightarrow	FTDV-LC FTD		Pending Setup	Snort Version 2.9.2	1-102
Events & Monitoring		tartfrd			O Synced	
√ Analytics	>	FTD FTD	-	Pending Setup	Your device's configuration	on is up-to-date.
(Change Log					Device Actions	
dobs 💮					C Charle for Charge	
😤 Tools & Services	>				Ø Manage Licenses	
Settings	>				Workflows Remove	

範例2: FTD執行snort版本3。

cisco Defense Orchestra	ator	Invent	tory				Q	Search	6 7 ()	۰ ۵۰ d	⑦ ▪ mex_firewall_tac_test .
Hide Menu										FTDv @	
Dashboard			vices Templates	Q Search by Device Nam	e, IP Address, or Serial Num	ber	°	Displaying 3 of 3 results	COT	Device Details	~
Inventory		AI FT	TD							Location	n/a
Configuration		•	Name 0			Configuration Status	c	Connectivity 0		Model	Cisco Firepower Threat Defense for Azure
Policies	>		FTDv			Ch Not Support		Online		Serial	
Objects	>		FTD			W Not Synced		Unang		Onboarding	Registration Key
₀å₀ VPN	>	0	FTDv-LC					Pending Setup		Snort Version	3.1.211-126
Events & Monitoring	>	0	testftd FTD				•	Pending Setup		Not Synced The configuration way device's con-	has been modified in FMC. Synchronize
Change Log										FMC Deployment	t page
(+) Jobs										Device Actions	¥
😤 Tools & Services	>									C Check for C	hanges
Settings	>									C Manage Lic Workflows Remove	enses

相關資訊

- <u>Cisco Firepower發行說明,版本6.7.0</u>
- <u>Cisco Firepower發行說明,版本7.0</u>
- <u>Snort 3網站</u>
- <u>技術支援與文件 Cisco Systems</u>

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。