IPS 6.X — 通過IDM啟用/禁用特定事件摘要

目錄

<u>簡介</u> <u>必要條件</u> <u>需求</u> <u>採用元件</u> <u>慣例</u> <u>使用IDM啟用/禁用特定事件的摘要</u> <u>IDM配置</u> 相關資訊

<u>簡介</u>

本文檔介紹如何使用IPS裝置管理器(IDM)在Intrusion Prevention System(IPS)軟體版本6.x中啟用/禁 用特定事件的摘要。

註意:必須在IPS裝置中配置訪問清單,以允許從安裝了IDM和<u>IEV(IDS事件檢視</u>器)等管理軟體的主 機或網路進行訪問,並正常工作。有關詳細資訊,請參閱<u>使用命令列介面5.0配置Cisco Intrusion</u> <u>Prevention System感測器</u>的<u>更改訪問清單</u>部分。

<u>必要條件</u>

<u>需求</u>

本文是根據已安裝IPS 6.x且工作正常的假設編寫的。

<u>採用元件</u>

本檔案中的資訊是根據執行軟體版本6.0(2)E1的Cisco 4200系列IPS感應器。

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。如果您的網路正在作用,請確保您已瞭解任何指令可能造成的影響。

<u>慣例</u>

如需文件慣例的詳細資訊,請參閱思科技術提示慣例。

使用IDM啟用/禁用特定事件的摘要

為了清楚瞭解,本節提供啟用/禁用簽名ID摘要的**示例:5748.**

<u>IDM配置</u>

請完成以下步驟。

- 1. 啟動IDM。
- 2. 按一下Home以檢視IDM的首頁。此頁顯示裝置資訊。



3. 選擇Configuration > Policies > Signature Definitions > sig0 > Signature Configuration > Select By:簽名ID,顯示感測器中的所有可用簽名。

Home Configuration	Monitoring	C Back	Forward Refresh Help				CISC
Sensor Setup	sig0 Signature Co Select By:	ntiguration	Custom Signature Wizard Signature \	/ariables Mi	scellaneous		
Known Host Key:	Sig ID	Subsig D	Name	Enabled	Severity		Select All
Certificates	1000	0	IP options-Bad Option List	Yes	Informational		
Trusted Hosts	1004	0	IP options-Loose Source Route	No	High		Actions
server centricate	1006	0	IP options-Strict Source Route	Yes	High		
	1007	0	IPv6 over IPv4	No	Informational		Edit
sau users	1101	0	Unknown IP Protocol	Yes	Informational		Destant Defe
	1102	0	Impossible IP Packet	Yes	High		Restore Defau
	1104	0	IP Localhost Source Spoof	Yes	High		
Interface Pairs	1107	0	RFC 1918 Addresses Seen	No	Informational		Enable
VLAN Pairs	1108	0	IP Packet with Proto 11	Yes	High	- 88 -	E1108010
VLAN Groups	1109	3	Cisco IOS Interface DoS	No	Medium		Disable
Bypass	1109	2	Cisco IOS Interface DoS	No	Medium	1331	
🖓 Traffic Flow Notificati	1109	1	Cisco IOS Interface DoS	No	Medium		
Analysis Engine	1109	0	Cisco IOS Interface DoS	No	Medium		Add
Situal Sensors	1200	0	IP Fragmentation Buffer Full	Yes	Informational		Clone
Policies	1201	0	IP Fragment Overlap	No	Informational		Delete
Event Action Rules	1202	0	IP Fragment Overrun - Datagram T	Yes	High		
N rules0	1203	0	IP Fragment Overwrite - Data is O	Yes	High	+	
 Select Bv下拉選單	。 中選擇Sie	a ID . 🖇	 然後輸入Sig ID 5748 以		 定簽名。		
Cisco IDM 5.0 - 10.77.241 14	2	j , ,		· <u> </u>			

i 🚽			0	\odot	•	?				ahaha
Home	Configuration	Monitoring	Back	Forward	Refresh	Help				CISCO
Sensor Setup Network 	Hosts orlized Keys	sig0 Signature Con Select By	figuration (Custom Signatu	re Wizard Sk] Enter Sig D	gnature Ve (eg. 1000	ariables Mi)-2000): 57	scellaneous		Find
Knov Sens	vn Host Key: or Key	Sig ID _	Subsig ID		Name		Enabled ,	Severity	F	Select All
Trust	es ted Hosts er Certificate	5748 5748	5	Non-SMTP Ses Non-SMTP Ses	sion Start sion Start		Yes Yes	Informational Informational		Actions
S Time		5748 5748	3	Non-SMTP Ses Non-SMTP Ses	sion Start sion Start		Yes Yes	Informational	-1	Edit
Interface Con	rfiguration	5748	1	Non-SMTP Ses Non-SMTP Ses	sion Start sion Start		Yes Yes	Informational Low	<u> </u>	Restore Defaults
interface	s Pains ins									Enable
VLAN Gr Bypass	oups									Disable
Analysis Eng	ow Notificati Ine									Add
Global Va	ariables									Clone
Signature	tion Rules								-	Delete
Anomaly	Detections									

5. 按一下Edit以編輯簽名。

6. 在「編輯特徵碼」視窗中,選擇**「特徵碼定義」>「警報頻率」>「摘要模式」**,然後在「摘要

模式」下拉選單中將Summary操作更改為Fire all。



7. 確保「指定全域性摘要閾值」設定為否。



相關資訊

- <u>思科入侵防禦系統支援頁面</u>
- Cisco IPS裝置管理員支援頁面
- IOS IPS入門
- 技術支援與文件 Cisco Systems