

# 如何設定 McAfee IntruShield IDS Audit Syslog

V005





N-Partner Technologies Co. 版權所有。未經 N-Partner Technologies Co. 書面許可,不得以任何形式仿製、拷貝、 謄抄或轉譯本手冊的任何內容。由於產品一直在更新中,N-Partner Technologies Co. 保留不告知變動的權利。

# 商標

本手冊內所提到的任何的公司產品、名稱及註冊商標、均屬其合法註冊公司所有。





前	言	1
1	McAfee InstruShield Syslog Forwarding	2
2	McAfee Network Security Manager Syslog forward-	
	ing	3
3	N-Reporter	5



本文件描述 N-Reporter 使用者如何設定 McAfee IntruShield Syslog。

註:本文件僅做為如何將日誌吐出的設定參考,建議您仍應聯繫設備或是軟體原廠尋求日誌輸出方式之協助。



# **1** McAfee InstruShield Syslog Forwarding

McAfee IntruShield IDS 可以透過 Fault Notification Syslog Forwarder 送出 Syslog 給 N-Reporter 。 設定步驟如下:

#### (1) 請使用管理者權限登入 IntruShield IDS

#### (2) 打開 syslog forwarder 的頁面。

(3) 啟動下列的選項並輸入必要的數值。

Enable Syslog Forwarder:Yes Forward Alerts:With Severity low and above Syslog Server:請輸入 N-Reporter/N-Cloud 設備 IP address Port:514

#### (4) 選擇 Message Preference: [Customized], 然後點選 [Edit] 按鈕, 進入編輯客製化 syslog message 的頁面。

#### (5) 請將下面的文字複製後貼上:

category="\$IV\_CATEGORY\$", sub\_category="\$IV\_SUB\_CATEGORY\$", attack\_name="\$IV\_ATTACK\_NAME\$", attack\_severity=\$IV\_ATTACK\_SEVERITY\$, interface=\$IV\_INTERFACE\$, source\_ip=\$IV\_SOURCE\_IP\$, source\_port=\$IV\_SOURCE\_PORT\$,destination\_ip=\$IV\_DESTINATION\_IP\$,destination\_port=\$IV\_DESTINATION\_ PORT\$, network\_protocol=\$IV\_NETWORK\_PROTOCOL\$,attack\_count=\$IV\_ATTACK\_COUNT\$

\*注意:上述的格式,沒有任何的換行符號。

- (6) 點選 [Save] 按鈕。
- (7) 點選 [Apply] 按鈕。
- (8) 設定完成。接下來,IntruShield IDS 即會把新產生的 Syslog 送至 N-Reporter/N-Cloud。



# 2 McAfee Network Security Manager Syslog forwarding

#### (1) 請使用管理者權限登入

[Network Security Manager] -> [IPS Setting] -> [Alert Notification] -> [Syslog]

#### (2) 打開 [Syslog forwarder] 的頁面。

#### (3) 啟動下列的選項並輸入必要的數值。

Enable Syslog Forwarder:Yes Server Name or IP Address:請輸入 N-Reporter/N-Cloud 設備 IP address UDP Port:514 Send Notification IF: 勾選 [The following notification filter is matched:] 選擇 [Severity Informational and above]

#### (4) 選擇 Message Preference: [Customized], 然後點選 [Edit] 按鈕, 進入編輯客製化 syslog message 的頁面。

#### (5) 請將下面的文字複製後貼上:

category="\$IV\_CATEGORY\$", sub\_category="\$IV\_SUB\_CATEGORY\$", attack\_name="\$IV\_ATTACK\_NAME\$", attack\_severity=\$IV\_ATTACK\_SEVERITY\$, interface=\$IV\_INTERFACE\$, source\_ip=\$IV\_SOURCE\_IP\$, source\_port=\$IV\_SOURCE\_PORT\$,destination\_ip=\$IV\_DESTINATION\_IP\$,destination\_port=\$IV\_DESTINATION\_ PORT\$, network\_protocol=\$IV\_NETWORK\_PROTOCOL\$,attack\_count=\$IV\_ATTACK\_COUNT\$

\*注意:上述的格式,沒有任何的換行符號。

(6) 點選 [Save] 按鈕。

- (7) 點選 [Apply] 按鈕。
- (8) 設定完成。接下來,IntruShield IDS 即會把新產生的 Syslog 送至 N-Reporter/N-Cloud。



#### 範例如下:



McAfee' Network Security Mar	nager	An A
E Resource Tree	/PTHG/EPS Settings > Alert Notific	ztien > Sydag
🗄 🔛 ртнс	195 Settings Folician Advanced	Palleins Maluare Detection Attack Filteev ACL SSL Decryption: 195 Quarantine Arthology Mannetonice Alert Notification Configuration Update
Manager	Summary SNMP Systeg	-mull Pager Script
B C IPS Settings B D PTgov-1	Use this page to customize the sys Fields marked with an asterisk (*)	Jag messinge content. nm required.
₩ 14-10 ₩ 2A-20	Castom Hessage	
SA-58 ■ CA-68 ■ External(3A ■ Internal(4A □ 07gov-2 ■ 1A-18	Messaget	Category="\$IV_CATEGORY\$", sub_category="\$IV_SUB_CATEGORY\$". attack_same="\$IV_ATTACK_NAME\$", attack_seventry=\$IV_ATTACK_SEVERITY\$. intmfsc=%IV_INTERFACE\$, source_go=%IV_DOURCE_18. source_sour=\$IV_SOURCE_PORTS, destination_go=%IV_DESTINATION_IP\$. destination_sect=\$IV_DESTINATION_PORTS. retherk_Brotoce!*\$IV_NETWORK_PROTOCOL\$.attack_count=\$IV_ATTACK_COUNT\$
<ul> <li>■ 2A-28</li> <li>■ 5A-58</li> <li>■ 6A-68</li> <li>■ External(3#</li> <li>■ Internal(4#</li> </ul>	Content Opecific Variables:	SENSOR ALERT UUID ALERT TYPE ATTACK TIME ATTACK NAME ATTACK ID ATTACK SEVERITY ATTACK SIGNATURE ATTACK CONFIDENCE ADMIN DOMAIN SENSOR NAME INTERFACE SQUIRCE IP SOURCE FORT DESTINATION PD BESTINATION PORT CATEGORY SUB CATEGORY DIRECTION RESULT STATUS DETECTION METHANISM APPLICATION PROTOCOL NETWORK PROTOCOL RELVANCE QUARANTURE END TIME MCAFFE NAC FORWARDED STATUS MCAFEE NAC MANAGED STATUS MCAFEE NAC ERROR STATUS MCAFEE NAC ACTION STATUS SENSOR CLUSTER HENBER ALERT ID ATTACK COUNT VLAN ID URL INFO SOURCE VM NAME TARGET VM NAME SOURCE VM ESX NAME TARGET VM ESX NAME
😑 🔎 Wizardz d <sup>ar</sup> Manager Initial		Save Cancel Reset to System Default
Integration		



# 3 N-Reporter

### (1) 新增 McAfee NSP 設備

[設備管理] -> [設備樹狀圖] -> 點選 [新增]





### (2) 選擇設備種類

選擇 [Firewall/ IPS/ Load Balancer/ NAC/ UTM/ WAF/ Wireless]-> 點選 [引導模式]





### (3) 設備基本設定

輸入設備名稱和IP->Syslog 資料格式選擇 [McAfee NSP]-> 點選 [下一步]

設備基本設定			^
設備名稱 *			
McAfee_NSP-192.168.3.88			
P *			
192.168.3.88			
所屬領域 *			
Global			~
Syslog 資料格式 🚯			
McAfee NSP		 	~
自定義資料格式 🕄 🕇 🕇			
未敵用			$\sim$
SNMP Model 1			
未啟用	 	 	~
Web 監控 🗊			
愈用網頁監控功能			



## (4) Syslog 相關設定

Facility 保持預設-> 點選 [下一步]

(若勾選 [Raw Data 保留] · 則 [事件查詢] 顯示 Raw Data 資訊)

晶 新増設備 - Syslog 相關設定		×
Sysiog 相關設定		^
Facility 1		
		~
編碼方式 		
UTF-8		~
Syslog 正規化資料保留天數上限 🗊		
Raw Data 保留與轉發 ✔ Raw Data 保留		
本設備於分時監控報表啟動 Syslog 轉發時,採用 Raw Data 格式		
■ 轉發方式將使用來源設備的 IP		
上一步	下一步	取消



### (5) 其他

設備 Icon 選擇 [Security]-> 接收狀態選擇 [啟用]-> 點選 [下一步]->[確認]

新增設備 - 其它	
其它	^
設備 Icon 🛛 🔘	
Security	~
備註 🛛	
特殊格式: [key]="value",可匯出成自訂名稱欄位。	
經緯度	
緯度 經度	
接收狀態	
上一步下	一步 取消

是否啟用預設報表,將套用置相同廠牌型號設備-> 點擊 [否]





