N-Partner

N-REPORTER

如何使用 N-Reporter 接收 McAfee IntruShield IDS Audit Log

V1.1.2 (简体)

(01-01-02-001) 2013/08/06

前言

这份文件主要描述如何使用 N-Reporter 接收 McAfee IntruShield Syslog。着重于如何设定 McAfee IntruShield Syslog Fowrwarding，使得 N-Reporter 能正确的处理 McAfee IntruShield Syslog。

N-Reporter 为 N-Partner 所有。为目前业界主要的 Syslog 分析仪。能够统计分析接收的 Syslog，产生各式各样的专业报表。

McAfee IntruShield IDS 为 Network Intrusion Detection 的设备。能够将网络现况的分析结果透过 Syslog 送给 N-Reporter。

注：McAfee IntruShield IDS 为 McAfee 公司之注册商标。

文件章节如下：

连络信息.....1

McAfee IntruShield Syslog Forwarding 设定.....2

McAfee Network Security Manager Syslog forwording 设定.....3

连络信息

N-Partner 公司连络方式：
TEL: +886-4-23752865
FAX: +886-4-23757458
有关技术问题请洽：
Email: support@npartnertech.com
Skype：support@npartnertech.com
有关业务相关问题请洽：
Email: sales@npartnertech.com

McAfee IntruShield Syslog Forwarding 设定

McAfee IntruShield IDS 可以透过 Fault Notification Syslog Forwarder 送出 Syslog 给第三方的 syslog application。例如 :N-Reporter。

设定的步骤如下：

►**step1：**请使用管理者权限登入 IntruShield IDS。

►**step2：**打开 syslog forwarder 的页面。

►**step3：**启动下列的选项并输入必要的数值：

- ✓ Enable Syslog Forwarder: Yes
- ✓ Forward Alerts: With Severity low and above
- ✓ Syslog Server: 请输入 N-Reporter 设备的 IP
- ✓ Port: 514

►**step4：**选择 Message Preference: Customized，然后点选 Edit 按钮，进入编辑客制化 syslog messages 的页面。

►**step5：**请将下面的文字复制后或贴上：

```
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，没有任何的换行符号。

►**step6：**点选 Save 按钮。

►**step7：**点选 Apply 按钮。

►**step8：**设定完成。接下来，IntruShield IDS 即会把新产生的 Syslog 送至 N-Reporter。

McAfee Network Security Manager Syslog forwording 设定

►**step1：**请使用管理者权限登入
Network Security Manager➔IPS Setting➔Alert Notification➔Syslog。

►**step2：**打开 Syslog forwarder 的页面。

►**step3：**启动下列的选项并输入必要的数值：

- ✓ Enable Syslog Forwarder：Yes
- ✓ Server Name or IP Address：请输入 N-Reporter 设备的 IP
- ✓ UDP Port：514
- ✓ Send Notification IF：勾选 The following notification filter is matched: Severity Informational and above

►**step4：**选择 Message Preference: Customized，然后点选 Edit 按钮，进入编辑客制化 syslog messages 的页面。

►**step5：**请将下面的文字复制后或贴上：

```
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=$IV_ATTACK_COUNT$
```

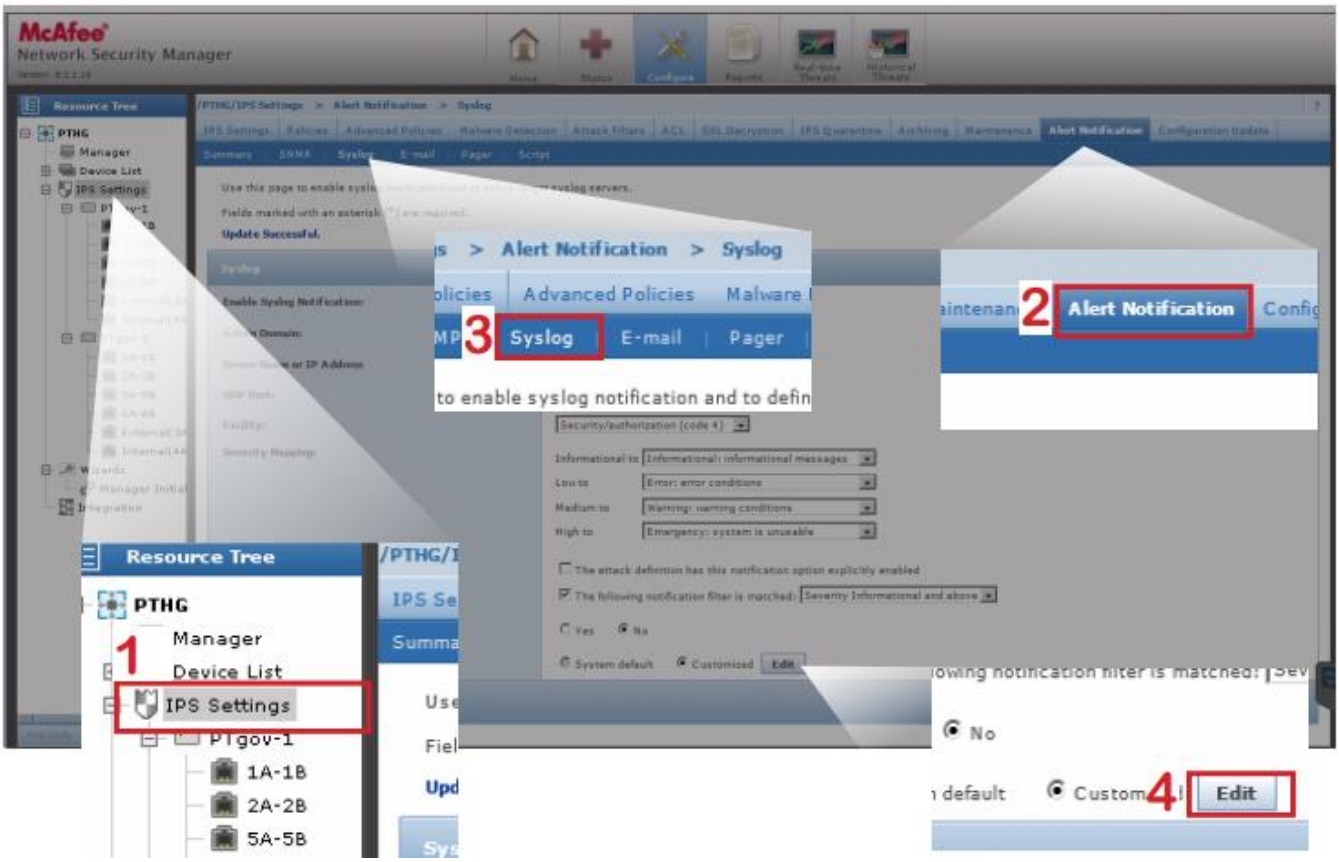
※注意：上述的格式，没有任何的换行符号。

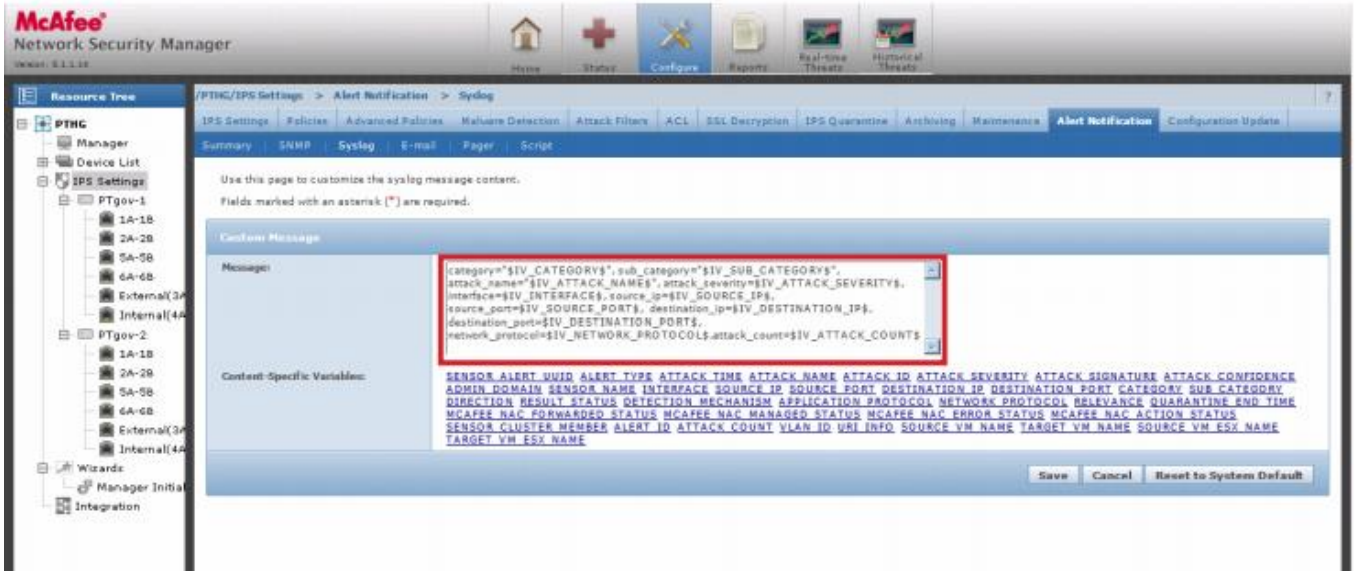
►**step6：**点选 Save 按钮。

►**step7：**点选 Apply 按钮。

►**step8：**设定完成。接下来，IntruShield IDS 即会把新产生的 Syslog 送至 N-Reporter。

实际范例如下:





採購與銷售合作：sales@npartnertech.com

技術諮詢：support@npartnertech.com