瞭解第一個響應程式程式（安全防火牆版）

目錄

[簡介](#)
[必要條件](#)
[需求](#)
[採用元件](#)
[背景資訊](#)
[自動化電子郵件](#)
[指令碼/命令](#)
[此電子郵件的原因](#)
[自動化電子郵件](#)
[簡介欄](#)
[資料請求塊](#)
[生成的命令](#)
[Firepower.py指令碼](#)
[自動化](#)
[互動](#)
[指令碼的預期輸出](#)
[常見問題](#)
[電子郵件安全/URL重寫](#)
[解決步驟](#)
[DNS故障](#)
[解決步驟](#)
[無法開啟/建立日誌檔案](#)
[解決步驟](#)
[無法開啟/寫入通知檔案](#)
[解決步驟](#)
[鎖定sf_troubleshoot.pid檔案失敗](#)
[解決步驟](#)
[上傳問題](#)
[解決步驟](#)

簡介

本檔案介紹思科安全防火牆的首次回應程式的使用和執行。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案以思科安全防火牆產品為基礎。

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

First Responder計畫由TAC建立，旨在使為未決案例提供診斷資料更容易、更快速。該計畫有兩個主要組成部分：

自動化電子郵件

此電子郵件在案例開始時發出，並附上有關如何收集和上傳診斷資料以進行TAC分析的說明。有多種技術可以利用此系統，而且每封電子郵件都會對映到建立案例時選擇的「技術」和「子技術」。

指令碼/命令

First Responder計畫的每個實施都有自己的獨特方式處理資料的收集和交付。安全防火牆實施利用TAC創作的firepower.py Python指令碼來完成此操作。自動電子郵件過程會生成一個單行命令，該命令特定於此特定情況，可以複製該命令並將其貼上到Secure Firewall裝置的CLI中運行。

此電子郵件的原因

已為第一個響應程式啟用某些技術。這意味著，每次針對其中一項啟用的技術開啟案例時，都會傳送第一響應方電子郵件。如果您收到第一響應者電子郵件且認為資料請求不相關，請忽略通訊。

對於安全防火牆使用案例，第一個響應程式僅限於Firepower威脅防禦(FTD)軟體。如果運行自適應安全裝置(ASA)代碼庫，請忽略此電子郵件。由於這兩個產品運行在同一硬體上，通常可以觀察到ASA案例是在Secure Firewall技術空間中建立的，因此會生成第一個響應方電子郵件。

自動化電子郵件

以下是作為此程式的一部分發出的自動電子郵件的示例：

```
From: first-responder@cisco.com <first-responder@cisco.com>
Sent: Thursday, September 1, 2022 12:11 PM
To: John Doe <john.doe@cisco.com>
Cc: attach@cisco.com
Subject: SR 666666666 - First Responder Automated E-mail

Dear John,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution and the steps to collect them:

*** Troubleshoot File ***
```

```
* Connect to the device using SSH
* Issue the command expert, skip this step for FMC version 6.4.x and earlier
* Issue the command sudo su
* When prompted for the password, enter your password.
* For FMC 6.4 or FTD 6.7 and later issue the command
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

* For FMC 6.3 or FTD 6.6 and earlier issue the command
curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &

For more information on what this command does, or to understand why you are receiving this e-
mail - please refer to
<LINK_TO_THIS_ARTICLE>

For 6.3 and earlier versions we recommend confirming cxd.cisco.com resolves to <CURRENT_CXD_IP1>
or
<CURRENT_CXD_IP2>. Furthermore, we recommend validating the SHA checksum of the file by running
url -s -k https://cxd.cisco.com/public/ctfr/firepower.py | shasum which should output
<CURRENT_SHA>.

If you are unable to upload troubleshooting files (or would prefer not to), please let us know
what
hardware and software version ou are running if you have not already.

Sincerely, First Responder Team
```

用於第一響應者程式的自動電子郵件被分為兩個部分，稱為介紹塊和資料請求塊。

簡介欄

introduction block是包含在每個第一個響應者電子郵件中的靜態字串。該介紹句僅用於提供資料請求塊的上下文。 以下是介紹塊的示例：

```
Dear <NAME>,

In an effort to resolve your case faster it may be necessary to collect some diagnostic data
from your environment.
Based on the problem statement you provided, below are a few pieces of data that would help
speed the resolution
and the steps to collect them:
```

資料請求塊

資料請求塊是第一響應程式的核心。每個資料塊是一組預定義的步驟，用於為給定技術收集資料。如**背景資訊**部分所述，每個資料請求塊都對映到一個特定的技術。這是選擇用於開啟支援案例的技術。通常，自動電子郵件包含單個資料請求塊。但是，如果所選技術有多個資料請求塊對映到它，則在電子郵件中包含多個資料請求。以下是包含多個資料請求的資料請求塊的示例格式：

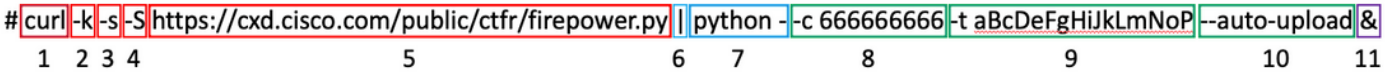
```
*** <REQUEST NAME 1> ***

<REQUEST 1 STEPS>

*** <REQUEST NAME 2> ***

<REQUEST 2 STEPS>
```

例如，在Secure Firewall中，當有人請求幫助解決遠端訪問VPN(RA-VPN)與Firepower威脅防禦

(FTD)有關的問題時，通常會包含多個資料請求塊，因為VPN技術還配置了一個對映的資料請求塊，用於幫助收集DART捆綁包。

生成的命令

具體來說，對於Secure Firewall使用案例，系統將為每個案例生成唯一的一行命令，作為自動電子郵件的一部分。以下是一行命令結構的明細：



1. curl命令用於下載最新版本的firepower.py指令碼
2. **-k**標誌是用於在連線期間忽略證書錯誤的捲曲選項。
3. **-s** 標誌是捲曲在靜默模式下運行的選項。這用於抑制正常捲曲輸出，因為它有雜訊。
4. **-S** 標誌是捲曲顯示錯誤的選項。這用於強制捲曲在啟用silent選項的情況下仍顯示輸出錯誤。
5. 承載最新版本的firepower.py指令碼的URL。此路徑指示curl命令拉出要運行的指令碼的最新正文。
6. 這是Linux管道，它將curl命令的輸出（python指令碼的內容）傳遞到下一步中的執行語句。
7. 在此步驟中，裝置上的python二進位制通過附加的「 — 」呼叫。 這指示python從stdin獲取源（因為指令碼的內容從curl通過管道傳輸）。
8. **-c**標誌是firepower.py指令碼的一個輸入引數，它指示資料必須上載到的案例編號。此666666666項後的範例值是案件編號。
9. **-t** 標誌是firepower.py指令碼的輸入引數，它表示為此特定案例生成的唯一令牌（密碼）。此選項後面的aBcDeFgHiJkLmNoP值是此案例的示例令牌。
10. **—auto-upload標誌**是firepower.py指令碼的一個特殊引數，它指示指令碼在自動化模式下運行。有關此主題的詳細資訊，可在特定於指令碼的部分中找到。
11. **&** 指示整個命令在後台運行，這允許使用者在指令碼執行時繼續與其shell互動。

附註：6.4之前的任何FMC版本和6.7之前的任何FTD版本都需要使用 — k標誌，因為CXD使用的根證書在FMC 6.4版和FTD 6.7版之前不受Firepower裝置的信任，這會導致證書驗證失敗。

Firepower.py指令碼

該指令碼的主要目標是從安全防火牆裝置生成並上傳診斷捆綁包，稱為「故障排除」。 要生成此故障排除檔案，firepower.py指令碼只需呼叫負責生成此捆綁的內建sf_troubleshoot.pl指令碼。此指令碼與從GUI生成故障排除時呼叫的指令碼相同。除了故障排除檔案，指令碼還能夠收集未包含在故障排除套件中的其他診斷資料。目前，可以收集到的唯一附加資料是Core Files — 但在將來需要時可以對其進行擴展。指令碼可在「自動化」或「互動」模式下運行：

自動化

運行指令碼時使用「 — auto-upload」選項時，此模式已啟用。此選項禁用互動式提示、啟用核心檔案收集並自動將資料上傳到案件。自動電子郵件生成的單行命令包括「 — auto-upload」選項。

互動

這是指令碼的預設運行模式。在此模式下，使用者會收到提示以確認是否收集其他診斷資料（如核心檔案）。無論執行模式如何，有意義的輸出都會列印到螢幕上，並記錄到日誌檔案中，以指示指

令碼執行的進度。指令碼本身通過內嵌代碼註釋進行了大量記錄，可在 https://cxd.cisco.com/public/ctfr/firepower.py下載/檢視。

指令碼的預期輸出

以下是成功執行指令碼的示例：

```
root@ftd:/home/admin# curl -k -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c
666666666 -t aBcDeFgHiJkLmNoP --auto-upload &
[1] 26422
root@ftd:/home/admin#
`/var/common/first_responder_notify` successfully uploaded to 666666666
Running sf_troubleshoot.pl command to create a troubleshoot file...
Troubleshoot file successfully generated at /ngfw/var/common/results-08-30-2022--135014.tar.gz
Attempting to upload troubleshoot to case...
##################################################################################################
############################## 100.0%
`/ngfw/var/common/results-08-30-2022--135014.tar.gz` successfully uploaded to 666666666
Found the following core files:
(0 B) - /ngfw/var/common/core_FAKE1.gz
(0 B) - /ngfw/var/common/core_FAKE2.gz
(0 B) - /ngfw/var/common/core_FAKE3.gz
Successfully created /ngfw/var/common/cores_666666666-1661867858.tar.gz
Attempting core file upload...
##################################################################################################
############################## 100.0%
`/ngfw/var/common/cores_6666666660-1661867858.tar.gz` successfully uploaded to 666666666
FINISHED!
```

請注意，此輸出示例包括核心檔案上傳。如果您的裝置上不存在核心檔案，則會顯示一條消息 "No core files found. Skipping core file processing" 顯示出來。

常見問題

以下是您可以遇到的一些常見問題（按照流程/執行的順序）：

電子郵件安全/URL重寫

通常，會觀察到終端使用者具有某種級別的電子郵件安全功能來重寫該URL。這將更改作為自動電子郵件的一部分生成的單行命令。這會導致執行失敗，因為用於提取指令碼的URL已被重新寫入並且無效。以下是預期的一行命令的範例：

```
curl -s -S https://cxd.cisco.com/public/ctfr/firepower.py | python - -c 666666666 -t
aBcDeFgHiJkLmNoP --auto-upload &
```

解決步驟

如果電子郵件中命令中的URL不是「https://cxd.cisco.com/public/ctfr/firepower.py」，則該URL可能會在傳送過程中被重新寫入。要解決此問題，只需在運行命令之前替換URL即可。

DNS故障

當裝置無法解析用於下載指令碼的URL時，經常出現此curl錯誤：

```
curl: (6) Could not resolve host: cxd.cisco.com
```

解決步驟

要解決此問題，請檢查裝置上的DNS設定，以確保裝置能夠正確解析URL以繼續。

無法開啟/建立日誌檔案

指令碼首先嘗試做的事情之一是在當前工作目錄中建立名為first-responder.log的日誌檔案（如果該檔案已存在，請將其開啟）。如果此操作失敗，則會顯示一個錯誤，指示出現簡單的許可權問題：

```
Permission denied while trying to create log file. Are you running this as root?
```

作為此操作的一部分，所有其它錯誤都以以下格式標識並列印到螢幕上：

```
Something unexpected happened while trying to create the log file. Here is the error:
----------



----------
```

解決步驟

要解決此錯誤，只需以管理使用者（如「admin」或「root」）身份運行指令碼即可。

無法開啟/寫入通知檔案

作為指令碼執行的一部分，將在系統上建立名為「first_responder_notify」的0位元組檔案。然後，此檔案會作為此程式自動化的一部分上傳到案例。此檔案被寫入「/var/common」目錄。如果執行指令碼的使用者沒有足夠的許可權將檔案寫入此目錄，則指令碼將顯示以下錯誤：

```
Failed to create file -> `/var/common/first_responder_notify`. Permission denied. Are you
running as root?
```

解決步驟

要解決此錯誤，只需以管理使用者（如「admin」或「root」）身份運行指令碼即可。

> **附註**：如果遇到與許可權無關的錯誤，螢幕上將顯示捕獲全部錯誤 "Unexpected error while trying to open file -> `/var/common/first_responder_notify`. Please check first-responder.log file for full error".可在first-responder.log中找到完整的異常正文。

鎖定sf_troubleshoot.pid檔案失敗

為了確保一次僅運行一個故障排除生成過程，故障排除生成指令碼會嘗試在繼續之前鎖定/var/sf/run/sf_troubleshoot.pid檔案。如果指令碼無法鎖定檔案，則會顯示錯誤：

```
Failed to run the `sf_troubleshoot.pl` command - existing sf_troubleshoot process detected.
Please wait for existing process to complete.
```

解決步驟

在大多數情況下，此錯誤表示單獨的故障排除生成任務已在處理中。有時，這是使用者意外連續兩次執行單行命令的結果。若要解決此問題，請等待當前的疑難解答生成作業完成，然後重試。

> **附註**：如果sf_troubleshoot.pl指令碼本身發生錯誤，則螢幕上將顯示此錯誤 "Unexpected PROCESS error while trying to run `sf_troubleshoot.pl` command. Please check first-responder.log file for full error". 可在first-responder.log中找到完整的異常正文。

上傳問題

指令碼中有一個公用上載函式，負責在整個指令碼執行過程中所有檔案上載。此函式只是一個python包裝器，用於執行curl上傳命令以將檔案傳送到案件。因此，執行期間遇到的任何錯誤都會返回為curl錯誤代碼。如果上傳失敗，則此錯誤會在螢幕上顯示：

```
[FAILURE] Failed to upload `/var/common/first_responder_notify` to 666666666. Please check the
first-responder.log file for the full error
```

檢查first-responder.log檔案以檢視完整錯誤。通常，first-responder.log檔案如下所示：

```
08/29/2022 06:51:57 PM - WARNING - Upload Failed with the following error:
----------
Command '['curl', '-k', '--progress-bar',
'https://666666666:aBcDeFgHiJkLmNoP@cxd.cisco.com/home/',
'--upload-file', '/var/common/first_responder_notify']' returned non-zero exit status 6
----------
```

解決步驟

在這種情況下，curl返回退出狀態6，這意味著「*Couldn* not resolve host」。 嘗試解析主機名cxd.cisco.com 時，這是簡單的DNS故障。請參閱curl文檔以解碼任何未知退出狀態。

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）。