ESA常見問題：爆發過濾器/病毒爆發過濾器(VOF)常見問題

目錄

簡介

本檔案介紹並回答一些有關思科電子郵件安全裝置(ESA)上的爆發過濾器或病毒爆發過濾器(VOF)的常見問題。

什麼是爆發過濾器？

> **注意**：請確保檢視《User Guide》，瞭解當前運行的AsyncOS for Email Security版本。 例如，Cisco Email Security Appliances的AsyncOS 13.0使用手冊，章節：爆發過濾器

爆發過濾器可保護您的網路免受大規模病毒爆發和較小的非病毒攻擊（如網路釣魚詐騙和惡意軟體分發）的侵擾。與大多數防惡意軟體安全軟體不同，思科在收集資料和發佈軟體更新之前無法檢測新的爆發，而是在爆發時收集資料並即時將更新資訊傳送到ESA，以防止這些消息到達您的使用者。

思科使用全球流量模式制定規則，以確定傳入郵件是否安全或是否為病毒發作的一部分。可能是病毒發作一部分的郵件將被隔離，直到根據來自思科的更新病毒發作資訊或由Sophos和McAfee發佈的新防病毒定義確定它們是安全的。

用於小規模非病毒攻擊的郵件使用看似合法的設計、收件人資訊和自定義URL，這些URL指向僅在短時間內線上且網路安全服務未知的網路釣魚和惡意軟體網站。爆發過濾器分析消息的內容並搜尋URL連結以檢測此類非病毒攻擊。爆發過濾器可以重寫URL以通過Web安全代理將流量重定向到可能有害的網站，這樣會警告使用者他們嘗試訪問的網站可能是惡意網站，或者完全阻止該網站。

即使沒有在ESA上運行Sophos或McAfee Anti-Virus，我是否可以使用爆發過濾器？

除了病毒爆發過濾器之外，思科建議您啟用Sophos或McAfee Anti-Virus，以增強對病毒附件的防禦。但是，爆發過濾器可以獨立運行，而無需啟用Sophos或McAfee Anti-Virus。

爆發過濾器何時隔離郵件？

郵件包含的檔案附件達到或超過當前爆發規則以及郵件管理員設定的閾值時，郵件將被隔離。思科將當前爆發規則發佈到具有有效功能金鑰的每個ESA。系統會隔離可能屬於爆發一部分的郵件，直到根據思科更新的爆發資訊確定這些郵件是安全的，或者由Sophos和McAfee發佈新的防病毒定義。

如何編寫爆發過濾器規則？

爆發規則由思科安全智慧操作(SIO)發佈，這是一個安全生態系統，將全球威脅資訊、基於聲譽的服務和思科安全裝置的複雜分析連線起來，提供更強大的保護，以及更快的響應時間。 預設情況下，裝置會每5分鐘檢查並下載新的爆發規則，作為服務更新的一部分。

SIO由三個部分組成：

- SenderBase — 世界上最大的威脅監控網路和漏洞資料庫。
- Talos，思科全球安全分析師和自動化系統團隊。
- 動態更新、即時更新在爆發時自動傳送到裝置。

是否存在配置爆發過濾器的最佳實踐？

會。 對服務水準的建議如下：

- 啟用*自適應規則*
- 將*Maximum Message Size to Scan*設定為2M
- 已啟用*Web互動跟蹤*

傳入郵件策略級別的配置需要逐個客戶、逐個策略確定。

如何報告不正確的爆發過濾器規則？

您可以通過以下兩種方式之一報告誤報或漏報：

1. 開啟思科支援案例：https://mycase.cloudapps.cisco.com/case
2. 使用Talos開啟信譽票證：https://talosintelligence.com/reputation_center/support

以下是我們可以完善爆發過濾規則的條件：

- 副檔名
- 檔案簽名(Magic)（表示其「true」型別的檔案的二進位制簽名）
- URL
- 檔名
- 檔案大小

當爆發隔離區填滿時會發生什麼？

當隔離區超出為其分配的最大空間時，或者如果郵件超出最大時間設定，將自動從隔離區修剪郵件以將其保持在限制範圍內。報文以先進先出(FIFO)方式刪除。換句話說，最舊的郵件首先被刪除。可以將隔離區配置為釋放（即，傳送）或刪除必須從隔離區修剪的消息。如果選擇釋放郵件，可以選擇使用您指定的文本標籤主題行，該文本將提醒收件人郵件已被強制離開隔離區。

從爆發隔離區釋放後，防病毒模組會重新掃描郵件，並根據防病毒策略執行操作。根據此策略，郵件可能會被傳送、刪除或傳遞病毒附件。從爆發隔離區放行後，在重新掃描過程中通常會發現病毒。可以查閱ESA mail_logs或郵件跟蹤，以確定隔離區中記錄的單個郵件是否被發現是病毒郵件，以及郵件是否以及如何傳送。

系統隔離區填滿之前，當隔離區已滿75%時，會傳送警報；當隔離區已滿95%時，會傳送另一個警報。Outbreak Quarantine（爆發隔離區）具有額外的管理功能，允許您刪除或釋放所有符合特定病毒威脅級別(VTL)的郵件。 這樣，在收到針對特定病毒威脅的防病毒更新後，即可輕鬆清除隔離區。

爆發規則的威脅級別的含義是什麼？

病毒爆發過濾器在威脅級別介於0和5之間運行。威脅級別評估病毒爆發的可能性。根據病毒爆發的風險，威脅級別會影響對可疑檔案的隔離。威脅級別基於多種因素，包括但不限於網路流量、可疑檔案活動、來自防病毒供應商的輸入以及Cisco SIO的分析。此外，爆發過濾器允許郵件管理員增加或減少威脅級別對其網路的影響。

級別	風險	含義
0	無	該報文沒有風險是 威脅.
1	低	該報文的風險是 威脅 很低。
2	低/中	該報文的風險是 威脅 低到中。這是「疑犯」 威脅.
3	中	該郵件是已確認的病毒爆發的一部分，或者其內容有中到大風險，即 威脅.
4	高	該郵件可能已被確認是大規模爆發的一部分，或者其內容非常危險。
5	極致	該消息的內容被確證為爆發的一部分，該爆發可能是非常大規模的，也可能是非常大規模的，也

發生病毒爆發時如何發出警報？

當爆發過濾器收到新的/更新規則來提升特定型別郵件配置檔案的隔離威脅級別時，可以通過傳送到已配置的警報電子郵件地址的電子郵件提醒您。當威脅級別低於配置的閾值時，將傳送另一個警報。因此，您可以監控病毒連線的進度。 這些電子郵件作為「資訊」電子郵件傳送。

> **附註**：為確保您能收到這些電子郵件通知，請使用**alertconfig**命令或GUI驗證在CLI中傳送警報的電子郵件地址：**系統管理>警報**。

配置或檢視配置

- GUI:安全服務(Security Services)>爆發過濾器(Outbreak Filters)，並檢視**編輯全域性設定(Edit Global Settings)。..(Edit Global Settings...)**
- CLI: **outbreakconfig > setup**

範例：

```
> outbreakconfig

NOTICE: This configuration command has not yet been configured for the current cluster mode
(Machine esa2.hc3033-47.iphmx.com).
```

```
What would you like to do?
1. Switch modes to edit at mode "Cluster Hosted_Cluster".
2. Start a new, empty configuration at the current mode (Machine esa2.hc3033-47.iphmx.com).
3. Copy settings from another cluster mode to the current mode (Machine esa2.hc3033-
47.iphmx.com).
[1]>

Outbreak Filters: Enabled

Choose the operation you want to perform:
- SETUP - Change Outbreak Filters settings.
- CLUSTERSET - Set how the Outbreak Filters are configured in a cluster.
- CLUSTERSHOW - Display how the Outbreak Filters are configured in a cluster.
[]> setup

Outbreak Filters: Enabled
Would you like to use Outbreak Filters? [Y]>

Outbreak Filters enabled.

Outbreak Filter alerts are sent when outbreak rules cross the threshold (go above or back down
below), meaning that new messages of certain types could be quarantined or will no longer be
quarantined, respectively.


Would you like to receive Outbreak Filter alerts? [Y]> y

What is the largest size message Outbreak Filters should scan?
[2097152]>

Do you want to use adaptive rules to compute the threat level of messages? [Y]>

Logging of URLs is currently enabled.

Do you wish to disable logging of URL's? [N]>

Web Interaction Tracking is currently enabled.

Do you wish to disable Web Interaction Tracking? [N]>

The Outbreak Filters feature is now globally enabled on the system. You must use the
'policyconfig' command in the CLI or the Email Security Manager in the GUI to enable Outbreak
Filters for the desired Incoming and Outgoing Mail Policies.
```

相關資訊

- Cisco Email Security Appliance — 最終使用手冊
- 技術支援與文件 - Cisco Systems