在安全終端雲控制檯中配置IP允許和阻止清單

目錄

簡介

本文檔介紹Cisco Secure Endpoint中的IP允許/阻止功能。

必要條件

需求

思科建議您擁有思科安全終端門戶的訪問許可權。

採用元件

本文檔中的資訊基於安全終端控制檯。

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。

使用安全端點配置IP允許/阻止清單

什麼是IP允許/阻止清單？

IP塊和允許清單與裝置流關聯一起使用，以定義自定義IP地址檢測。建立清單後，可以在策略中定義除思科情報源之外使用清單或單獨使用清單。 這些清單可以定義為使用單個IP地址、CIDR塊或IP地址和埠組合。當您提交清單時，會在後端合併冗餘地址。

IP地址示例

如果您將這些專案新增至清單：

- 192.0.2.0/24
- 192.0.2.15
- 192.0.2.135
- 192.0.2.200

清單的處理結果為：

- 192.0.2.0/24

但是，如果還包含埠，則結果會有所不同：

- 192.0.2.0/24
- 192.0.2.15:80
- 192.0.2.135
- 192.0.2.200

清單的處理結果為：

- 192.0.2.0/24
- 192.0.2.15:80

什麼是IP允許清單？

透過IP允許清單，您可以指定從不希望檢測的IP地址。您的IP allowed清單中的條目在IP blocked清單以及Cisco Intelligence Feed中建立覆蓋。您可以選擇增加單個IP地址、整個CIDR塊，或者使用埠號指定IP地址。

什麼是IP阻止清單？

IP阻止清單允許您指定要在任何一台電腦連線到它們時檢測到的IP地址。您可以選擇增加單個IP地址、整個CIDR塊，或者使用埠號指定IP地址。當電腦連線到您清單中的IP地址時，所採取的操作取決於您在策略的「網路」部分中指定的內容。

什麼是隔離IP允許清單？

隔離IP允許清單指定在隔離期間未被阻止的IP地址。 隔離IP允許清單與IP允許清單不同，因為隔離IP允許清單不支援規則中的埠號。

建立IP允許/阻止清單

步驟 1.要建立IP清單，請導航到安全終端門戶中的爆發控制並按一下IP Block & Allow Lists選項，如圖所示。

Outbreak Control

CUSTOM DETECTIONS

Simple

Advanced

Android

APPLICATION CONTROL

Blocked Applications

按一下Upload，然後按一下Browse以選擇CSV檔案，然後按一下Upload。對於清單型別，請選擇是希望此清單為允許清單、阻止清單還是隔離允許。

步驟 5.完成後，儲存IP地址清單配置。

其他配置示例

要將埠增加到塊或允許清單（不考慮IP地址），可以在相應的清單中增加兩個條目，其中XX是要阻止的埠號：

- 0.0.0.1/1:XX
- 128.0.0.1/1:XX

注意：上傳的IP清單最多可以包含10,000行，或者最大為2 MB。目前僅支援IPv4位址。要提高效能並包含更多地址，請使用CIDR塊。

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）。