在安全防火牆威脅防禦上配置遠端訪問VPN服務的威脅檢測

目錄

簡介

本檔案介紹在思科安全防火牆威脅防禦(FTD)上為遠端存取VPN服務設定威脅偵測的程式。

必要條件

思科建議您瞭解以下主題：

- 思科安全防火牆威脅防禦(FTD)。
- Cisco Secure Firewall Management Center (FMC)。
- FTD上的遠端存取VPN (RAVPN)。

需求

以下列出的思科安全防火牆威脅防禦版本支援這些威脅檢測功能：

- 7.0版本系列-> 7.0.6.3版和此特定系列的更高版本支援。

> 註：這些功能目前在7.1、7.2、7.3或7.4版系列中不受支援。本檔案會在可用時更新。

採用元件

本文檔中描述的資訊基於以下硬體和軟體版本：

- 思科安全防火牆威脅防禦虛擬版本7.0.6.3。

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

遠端訪問VPN服務的威脅檢測功能使您能夠防範以下任一情況：

1. 連線嘗試使遠端訪問VPN服務無效。也就是說，嘗試連線到僅供內部使用的服務。
2. 客戶端啟動攻擊，即攻擊者開始嘗試連線遠端訪問VPN頭端，但未能從單個主機重複嘗試連線。
3. 對遠端訪問VPN服務的身份驗證嘗試反覆失敗（暴力使用者名稱/密碼掃描攻擊）。

這些攻擊，即使嘗試訪問失敗，也會消耗計算資源，並阻止有效使用者連線到遠端訪問VPN服務。

當您啟用這些服務時，安全防火牆會自動避開超過已配置閾值的主機（IP地址），以防止進一步嘗試，直到您手動刪除IP地址的迴避。

注意：預設情況下，所有遠端訪問VPN的威脅檢測服務都處於停用狀態。

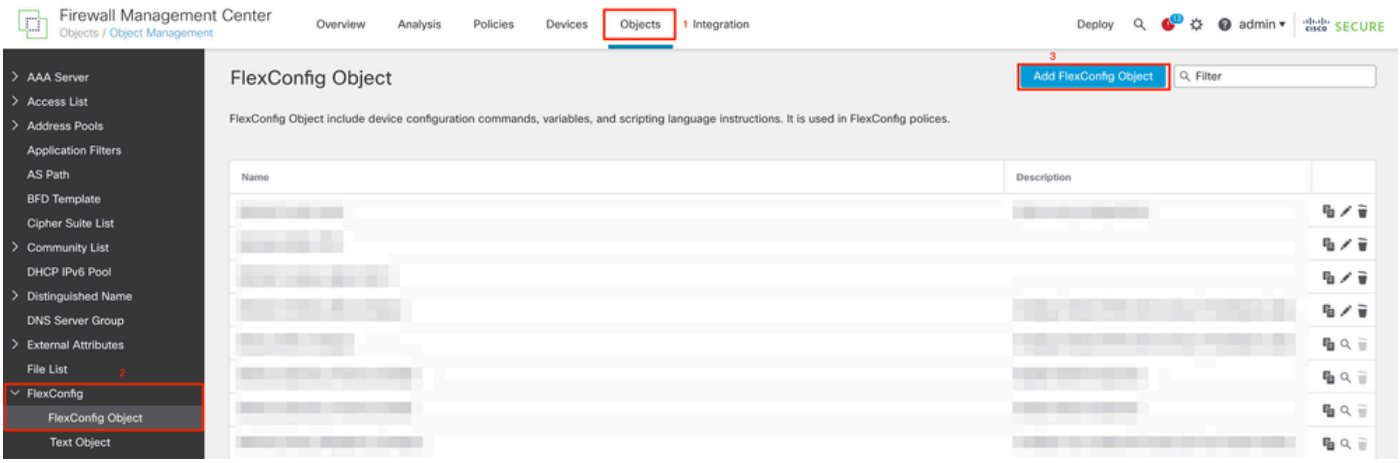
設定

注意：當前僅透過FlexConfig支援在安全防火牆威脅防禦上配置這些功能。

---

1. 登入安全防火牆管理中心。

2. 要配置FlexConfig對象，請導航到對象>對象管理> FlexConfig > FlexConfig對象，然後按一下增加FlexConfig對象。



3. 打開Add FlexConfig Object窗口後，增加所需的配置以啟用遠端接入VPN的威脅檢測功能：

- FlexConfig對象名稱：enable-threat-detection-ravpn
- FlexConfig對象說明：啟用遠端訪問VPN服務的威脅檢測。

- 部署：一次
- 文字：附加。
- 文本框：根據下文介紹的可用功能增加「威脅檢測服務」命令。

注意：您可以使用同一FlexConfig對象為遠端接入VPN啟用3個可用的威脅檢測功能，或者可以為要啟用的每個功能單獨建立一個FlexConfig對象。

功能1：嘗試連線到內部（無效）VPN服務的威脅檢測

要啟用此服務，請在FlexConfig object文本框中增加threat detection service invalid-vpn-access命令。

功能2：遠端訪問VPN客戶端發起攻擊的威脅檢測

要啟用此服務，請在FlexConfig object文本框中增加threat detection service remote-access-client-initiations hold-down <minutes> threshold <count>命令，其中：

- hold-down <minutes>定義最後一次啟動嘗試之後的一段時間，在此期間將計算連續連線嘗試。如果在此時間段內連續連線嘗試的次數達到配置的閾值，則會避開攻擊者的IPv4地址。您可以將此期間設定為1到1440分鐘。
- threshold <count>是在抑制時間段內觸發shun所需的連線嘗試次數。您可以將閾值設定為5到100。

例如，如果抑制週期是10分鐘，閾值是20，如果在任何10分鐘範圍內有20次連續連線嘗試，IPv4地址將自動迴避。

注意：在設定抑制和閾值時，請將NAT使用情況考慮在內。如果使用PAT（允許來自同一IP地址的許多請求），請考慮較高的值。這可確保有效使用者有足夠的時間進行連線。例如，在飯店中，許多使用者可以在短時間內嘗試連線。

功能3：遠端訪問VPN身份驗證失敗的威脅檢測

要啟用此服務，請在FlexConfig object文本框中增加threat detection service remote-access-authentication hold-down<minutes> threshold <count>命令，其中：

- hold-down <minutes>定義最後一次失敗嘗試之後的時間段，在此時間段內將計算連續失敗次數。如果連續身份驗證失敗的次數在此時間段內達到配置的閾值，則攻擊者的IPv4地址將被迴避。您可以將此期間設定為1到1440分鐘。
- threshold <count>是在抑制時間段內觸發shun所需的失敗身份驗證嘗試次數。您可以設定介於1到100之間的臨界值。

例如，如果抑制週期是10分鐘，閾值是20，如果在任何10分鐘範圍內有20次連續身份驗證失敗，則會自動迴避IPv4地址。

注意：在設定抑制和閾值時，請將NAT使用情況考慮在內。如果使用PAT（允許來自同一IP地

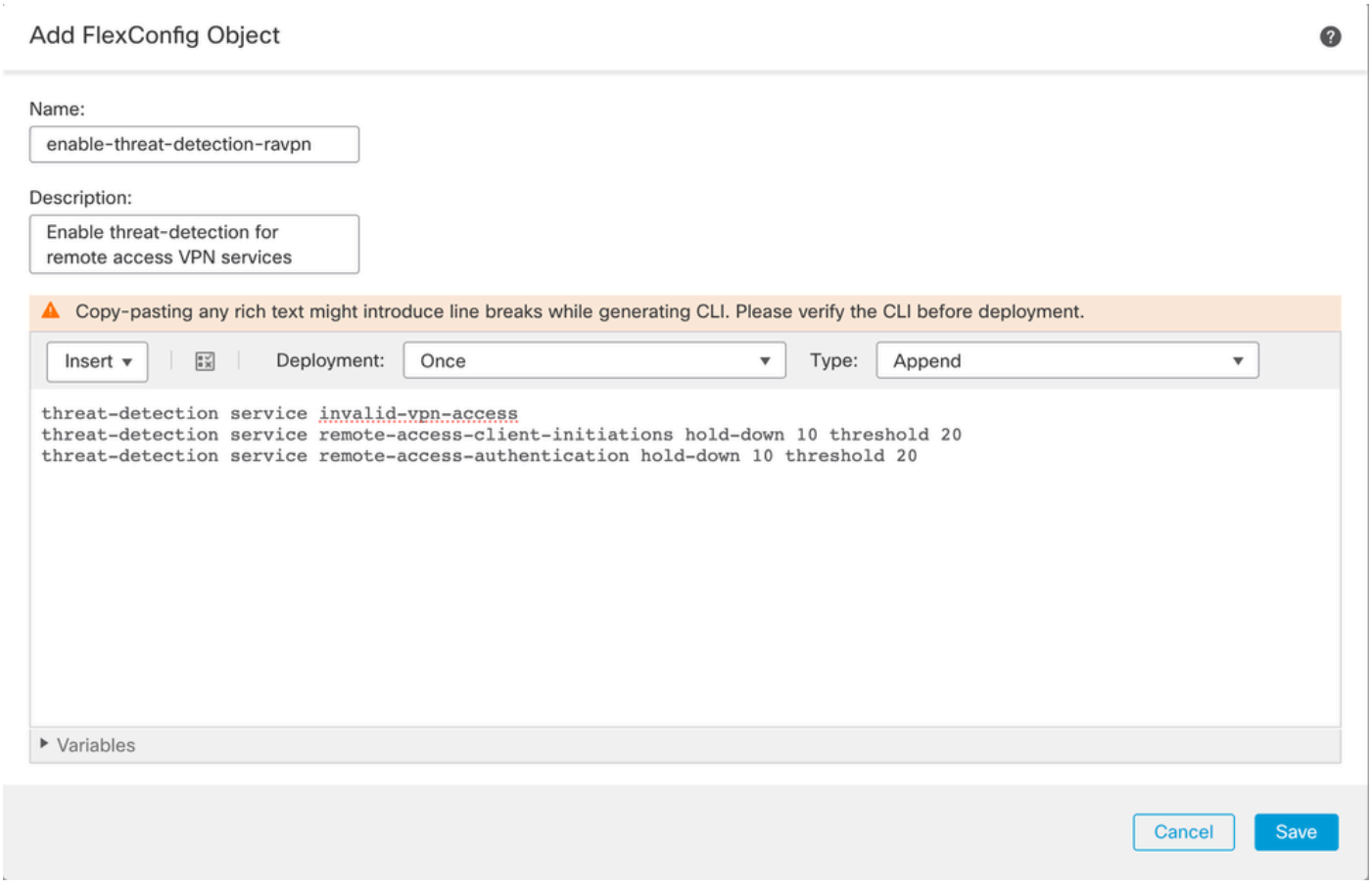
址的許多請求），請考慮較高的值。這可確保有效使用者有足夠的時間進行連線。例如，在飯店中，許多使用者可以在短時間內嘗試連線。

注意：尚不支援透過SAML進行身份驗證失敗。

此示例配置為遠端訪問VPN啟用三種可用的威脅檢測服務，抑制期為10分鐘，客戶端發起和身份驗證嘗試失敗時的閾值為20。根據您的環境要求配置hold-down 和threshold值。

此示例使用單個FlexConfig對象來啟用3個可用功能。

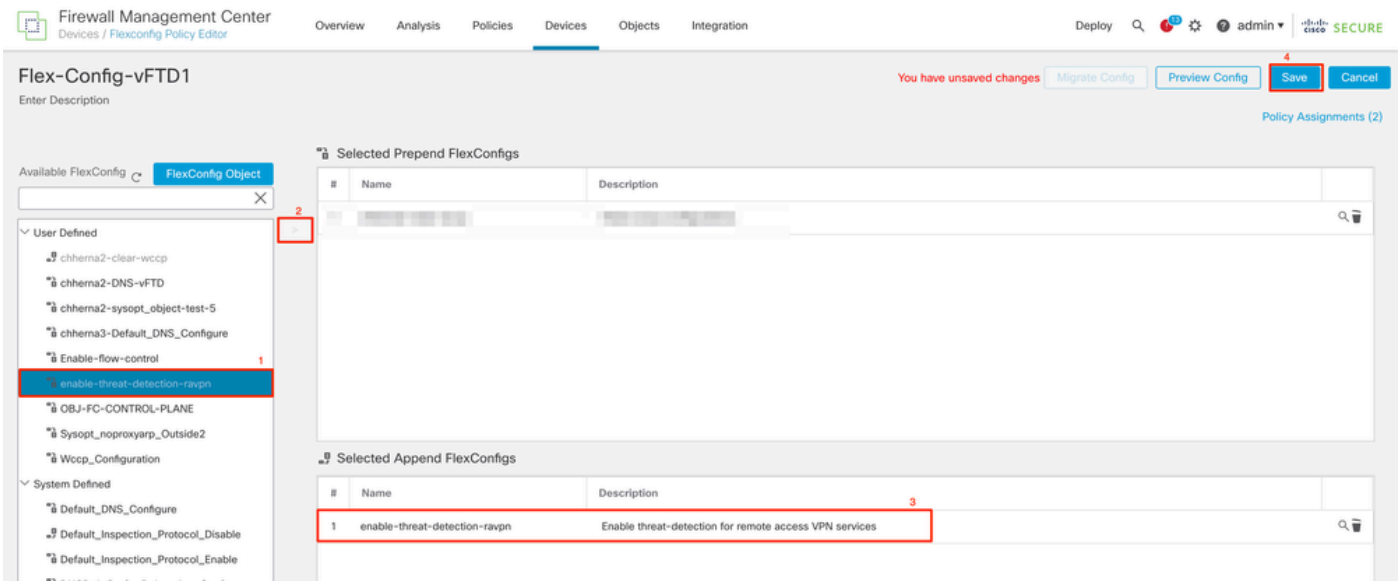
```
threat-detection service invalid-vpn-access
threat-detection service remote-access-client-initiations hold-down 10 threshold 20
threat-detection service remote-access-authentication hold-down 10 threshold 20
```



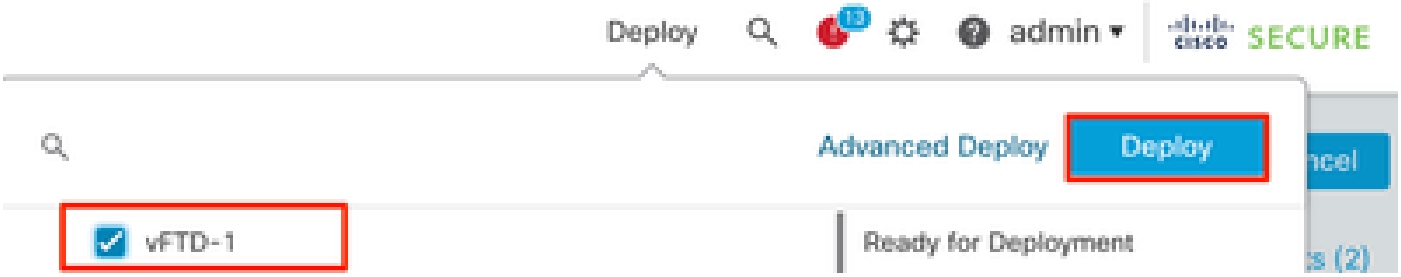
4. 儲存FlexConfig物件。

5. 導航到裝置> FlexConfig，然後選擇分配給安全防火牆的FlexConfig策略。

6. 從左窗格中顯示的可用FlexConfig對象，選擇您在步驟3中配置的FlexConfig對象，按一下「>」，然後儲存更改。



7. 部署變更並進行驗證。



驗證

要顯示威脅檢測RAVPN服務的統計資訊，請登入FTD的CLI並運行show threat-detection service [service] [entries|details]命令。其中服務可以是：remote-access-authentication、remote-access-client-initiations或invalid-vpn-access。

您可以新增下列引數來進一步限制檢視：

- entries -僅顯示威脅檢測服務正在跟蹤的條目。例如，驗證嘗試失敗的IP位址。
- details -顯示服務詳細資訊和服務條目。

運行show threat-detection service命令以顯示啟用的所有威脅檢測服務的統計資訊。

<#root>

```
ciscoftd# show threat-detection service
```

```
Service: invalid-vpn-access State : Enabled
```

```
    Hold-down : 1 minutes
    Threshold : 1
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0

Service: remote-access-authentication State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
    Total entries: 2

Name: remote-access-client-initiations State : Enabled

    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          0
        recording   :          0
        unsupported :          0
        disabled    :          0
    Total entries: 0
```

要檢視針對遠端訪問身份驗證服務跟蹤的潛在攻擊者的更多詳細資訊，請運行show threat-detection service <service> entries命令。

```
ciscoftd# show threat-detection service remote-access-authentication entries
Service: remote-access-authentication
    Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1        721         0
  2 192.168.100.102/ 32              outside              2        486       114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

要檢視特定威脅檢測遠端接入VPN服務的一般統計資訊和詳細資訊，請運行show threat-detection service <service> details命令。

```
ciscoftd# show threat-detection service remote-access-authentication details
Service: remote-access-authentication
```

```
    State     : Enabled
    Hold-down : 10 minutes
    Threshold : 20
    Stats:
        failed      :          0
        blocking    :          1
        recording   :          4
        unsupported :          0
        disabled    :          0
     Total entries: 2

Idx Source              Interface            Count          Age         Hold-down
--- ------------------- -------------------- -------------- ----------- ---------
  1 192.168.100.101/ 32              outside              1         721           0
  2 192.168.100.102/ 32              outside              2         486         114
Total number of IPv4 entries: 2

NOTE: Age is in seconds since last reported. Hold-down is in seconds remaining.
```

注意：條目僅顯示威脅檢測服務跟蹤的IP地址。如果IP地址已滿足規避條件，則blocking 計數增加，並且IP地址不再顯示為條目。

此外，您可以監控VPN服務應用的分流方法，並使用以下命令刪除單個IP地址或所有IP地址的分流方法：

- show shun [ip_address]

顯示迴避的主機，包括那些由VPN服務的威脅檢測自動迴避的主機，或使用shun命令手動迴避的主機。您可以選擇將檢視限制為指定的IP地址。

- no shun ip_address [interface if_name]

僅從指定的IP地址刪除shun。如果地址在多個介面上被迴避，而您希望在某些介面上保留shun不變，則您可以選擇性地指定shun的介面名稱。

- clear shun

從所有IP地址和所有介面刪除shun。

注意：VPN服務的威脅檢測規避的IP地址不會顯示在show threat-detection shun命令中，該命令僅適用於掃描威脅檢測。

要閱讀與遠端訪問VPN的威脅檢測服務相關的每個命令輸出和可用系統日誌消息的所有詳細資訊，請參閱命令參考文檔。

相關資訊

- 如需其他幫助，請聯絡技術支援中心(TAC)。需有有效的支援合約：思科全球支援聯絡人。
- 您還可以訪問Cisco VPN社群此處。
- 思科技術支援與下載

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）。