排解由於FTD上的LINA通訊協定檢查而導致的流量捨棄的疑難問題

目錄

簡介

本文說明如何識別模組化原則框架(MPF)的LINA通訊協定檢查是否會捨棄Cisco安全FTD中的流量。

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)。
- 思科安全防火牆管理員中心(FMC)。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 虛擬思科安全防火牆威脅防禦(FTD)版本7.4.2
- 虛擬思科安全防火牆管理器中心(FMC)版本7.4.2

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

對於在使用者資料包中嵌入IP定址資訊或在動態分配的埠上開啟輔助通道的服務，防火牆中需要檢查引擎。

協定檢查可通過檢查網路資料包的內容並根據所使用的應用或協定阻止或修改流量來幫助防止惡意流量進入網路。
因此，檢查引擎會影響整體吞吐量。防火牆預設啟用幾個常用檢測引擎，可能需要根據網路啟用其他檢測引擎。

預設配置

預設情況下，FTD LINA設定包含與所有預設應用程式檢查流量相符的原則。

該檢查應用於所有介面上的流量（全域性策略）。

預設應用檢測流量包括到每個協定的預設埠的流量。您只能應用一個全域性策略，因此，如果要更改全域性策略（例如，將檢測應用於非標準埠，或新增預設情況下未啟用的檢測），則需要編輯預設策略或禁用該策略並應用新的策略。

透過system support diagnostic-cli在LINA、FTD Command Line Interface(CLI)上執行show running-config policy-map指令以取得資訊。

```
firepower# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
```

```
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
```

標識由於MPF協定檢查而丟棄的資料包

即使流量與分配給防火牆的訪問控制策略(ACP)一致，在某些場景中，檢查過程也會因防火牆接收的特定流量行為、不受支援的設計、應用標準或檢查限制而終止連線。

在流量故障排除期間，可使用以下過程：

- 在流量流經的介面（入口和出口介面）上設定即時捕獲日誌，命令：

```
firepower# capture

        [interface

        ][match


           [port

           ]

             [port

             ]]
```

使用捕獲時，可以包括packet number X trace detail選項，它必須提供連線所經歷的結果分階段（與packet tracer命令相同），但使用此選項可以確保它是即時流量。

```
firepower# show capture

        packet number X trace detail
```

- 設定即時加速安全路徑(ASP)丟棄，捕獲型別asp-drop顯示ASP丟棄的資料包或連線，在文檔的相關連結中有一個原因清單，命令：

```
firepower# capture

        [type

        ] [interface

         ][match


            [port

            ]

              [port

              ]]
```

可以忽略協定檢查丟棄，因為在packet Tracer階段可以觀察到允許的結果。因此，始終使用即時捕獲日誌驗證丟棄原因至關重要。

常見丟棄錯誤消息

加速安全路徑(ASP)丟棄通常用於調試以幫助排除網路問題。show asp drop命令用於顯示這些丟棄的資料包或連線，從而提供丟棄原因的見解，這可能包括NAT故障、檢查失敗或訪問規則拒絕等問題。

有關ASP刪除的要點：

- 幀丟棄:這些都是與單個資料包相關的丟包，例如封裝無效或沒有通往主機的路由。
- Flow Drops:它們與連線相關，例如訪問規則拒絕的流或NAT故障。
- 用法:該命令主要用於調試，並且輸出可以更改。

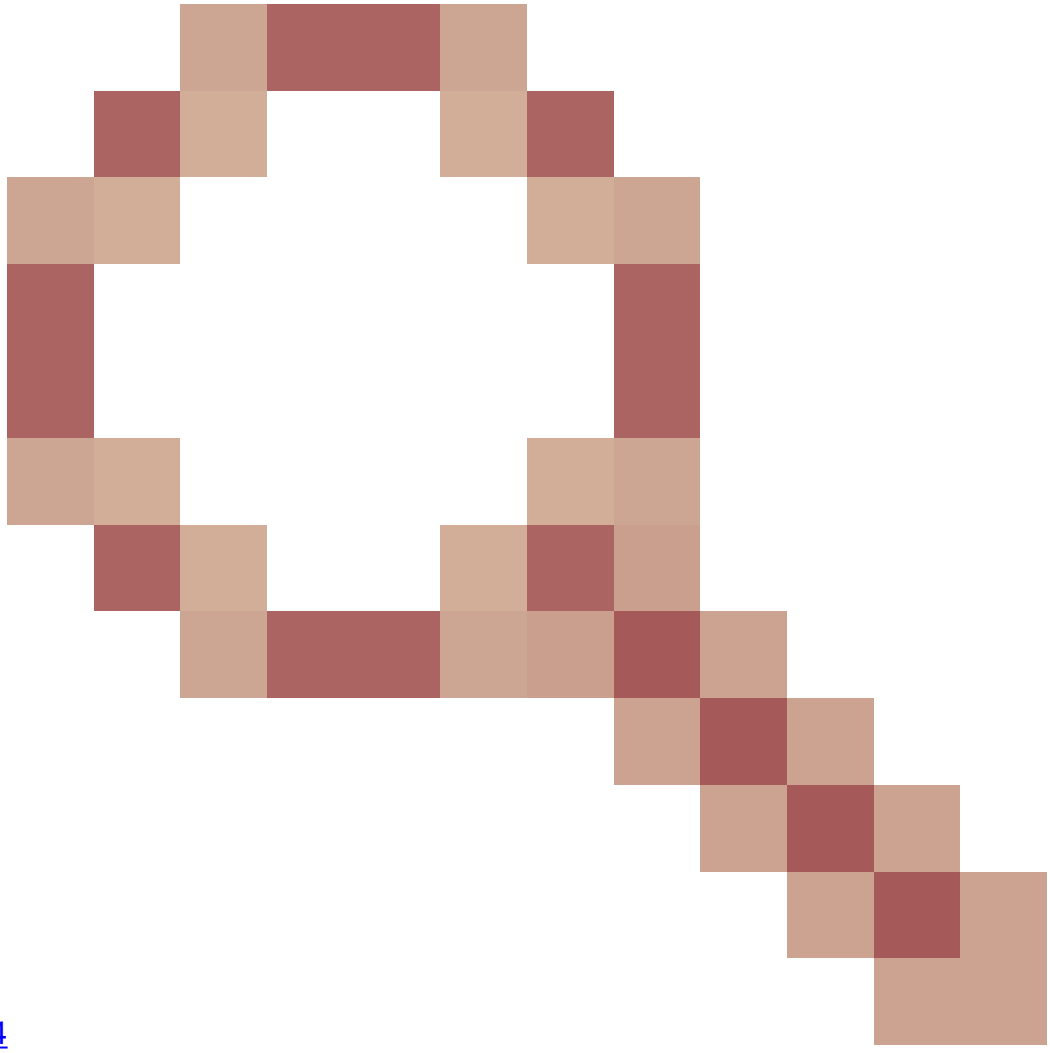
這些錯誤消息或丟棄原因是在故障排除過程中可能遇到的示例。它們可以根據正在使用的檢查協定進行延遲。

SUN RPC檢測丟棄示例

此方案適用於AWS部署中的單臂代理FTDv，即Geneve封裝的RPC流量（如果已啟用Sun Rpc檢測），則連線將斷開。

輸出顯示用於Sun Rpc檢測的ASP丟包，Sun Rcp使用埠111作為目標最後一個資料包是使用6081作為目標的通用封裝埠。您可以觀察到，輸出中的丟棄原因為「無有效鄰接關係」

```
firepower# show capture asp-drop
...
8: 16:23:02.462958 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
9: 16:23:09.769338 10.0.0.5.780 > 172.16.0.3.111: P 1795131583:1795131679(96) ack 526534108 win 29200 D
10: 16:23:10.148658 172.16.0.3.111 > 10.0.0.5.780: . ack 4026726685 win 26880 Drop-reason: (no-adjacenc
11: 16:23:10.463004 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
12: 16:23:26.462729 10.0.0.5.780 > 172.16.0.3.111: . ack 526534108 win 29200 Drop-reason: (no-adjacency)
13: 16:23:27.548692 10.79.67.11.60855 > 10.79.67.4.6081: udp 176 [GENEVE segment-id 0 payload-length 13
```



思科錯誤ID CSCwj00074

FTDv單臂代理在啟用inspect sunrpc的情況下捨棄無鄰接流量

在LINA引擎的ASP中，流量會作為「無效鄰接關係」捨棄，因為源和目的地MAC位址在三次握手的第二個封包(SYN/ACK)之後突然填充到全部為零。

ASP刪除原因：

名稱:無鄰接關係
無有效鄰接關係：
　當安全裝置收到的現有流上的資料包不再具有有效的輸出鄰接關係時，此計數器會增加。如果下一跳不再可訪問，或者通常在動態路由環境中發生了路由更改，則會發生這種情況。

解決方案：禁用sunrpc檢查。

SQL*NET檢測丟棄示例

此方案適用於AWS部署中的單臂代理FTDv，如果啟用Sql*Nel檢查，Geneve封裝的流量將被丟棄。

輸出適用於合併的封包擷取（您可以看到相同的封包編號）：
第一行：asp-drop packet capture not encapsulation， Sql*Net使用1521埠作為目標。

第二行：LINA上的VNI介面asp-drop，Geneve使用封裝連線埠6081作為目的地。

輸出中有兩個不同的捨棄原因，因為您可以觀察它們是「tcp-buffer-timeout」和「tcp-not-syn」

```
95    2024-12-14 07:55:58.771764    172.16.0.14    10.0.8.2    TCP    251    53905 → 1521 [PSH, ACK] Se
95: 07:55:58.771764       10.7.0.3.64056 > 10.7.2.5.6081:  udp 209 [GENEVE segment-id 0 payload-length 1

96    2024-12-14 07:55:58.771780    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53905 -
96: 07:55:58.771780       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length

99    2024-12-14 07:55:58.997049    172.16.0.14    10.0.8.2    TCP    308    53903 → 1521 [PSH, ACK] Se
99: 07:55:58.997049       10.7.0.3.64056 > 10.7.2.5.6081:  udp 266 [GENEVE segment-id 0 payload-length 2

100    2024-12-14 07:55:58.997079    172.16.0.14    10.0.8.2    TCP    1514    [TCP Out-Of-Order] 53903
100: 07:55:58.997079       10.7.0.3.64056 > 10.7.2.5.6081:  udp 1472 [GENEVE segment-id 0 payload-length
```

ASP刪除原因：

名稱:tcp-buffer-timeout
TCP無序資料包緩衝區超時：
　當隊列中的無序的TCP資料包在緩衝區中保留時間過長時，此計數器會遞增，資料包會被丟棄。通常，TCP資料包在經過安全裝置檢查的連線上按順序排列，或者當資料包傳送到SSM進行檢查時。當下一個預期的TCP封包在一段時間內未到達時，排隊的無序封包會被捨棄。

建議：
　下一個期望的TCP資料包不會到達，因為網路擁塞在繁忙的網路中是正常的。終端主機中的TCP重新傳輸機制必須重新傳輸資料包，會話可以繼續。

名稱:tcp-not-syn
第一個TCP資料包不是SYN:
　收到非SYN資料包，作為未攔截且未固定的連線的第一個資料包。

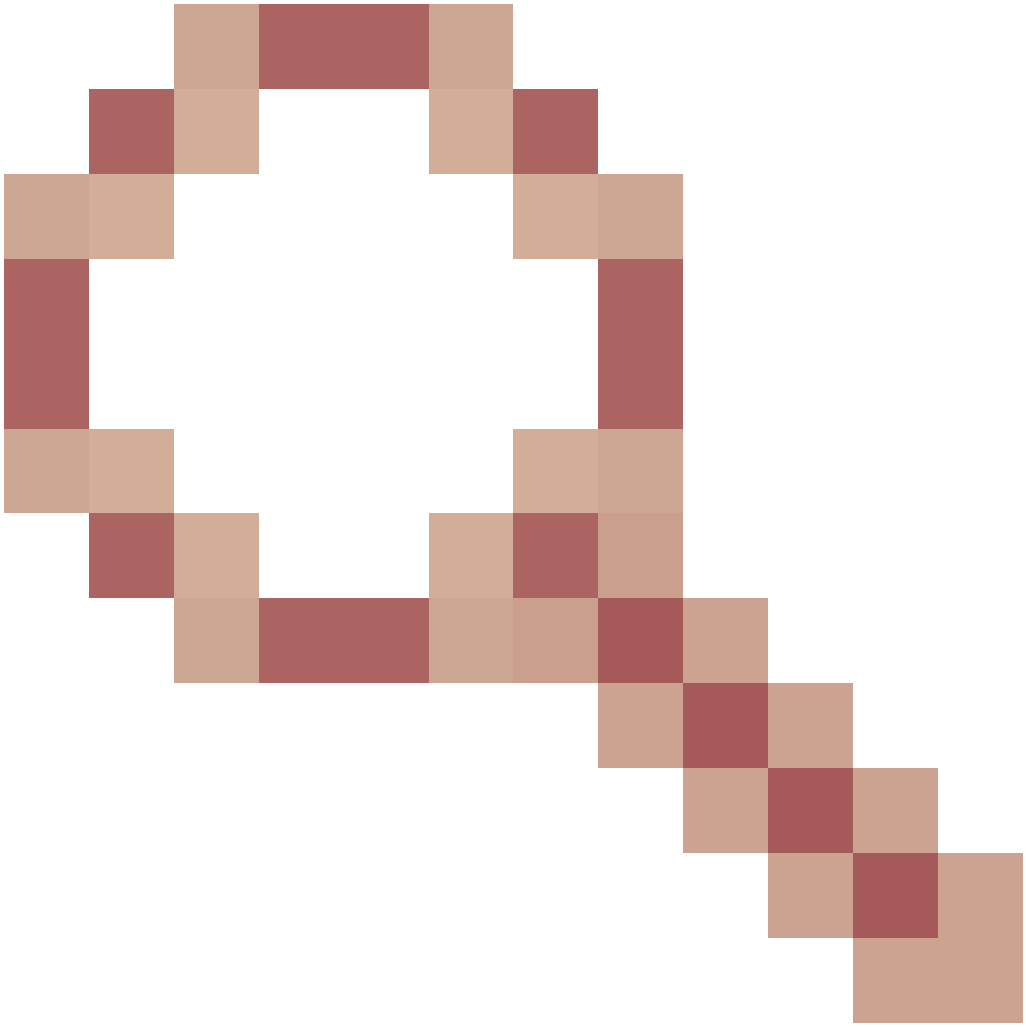
建議：
　在正常情況下，當裝置已關閉連線，並且客戶端或伺服器仍認為連線已開啟並繼續傳輸資料時，可以看到這種情況。 發生此情況的一些範例發生在發出「clear local-host」或「clear xlate」之後。此外，如果最近未刪除連線，並且計數器快速增加，則裝置可能受到攻擊。擷取監聽器追蹤軌跡，協助找出原因。

解決方案：當SQL資料傳輸與SQL控制TCP埠1521發生在同一埠時，禁用SQL*Net檢測。啟用SQL*Net檢查時，安全裝置將充當代理，並將客戶端視窗大小從65000減小到約16000，從而引起資料傳輸問題。

ICMP檢測丟棄示例

此案例適用於FTD叢集環境。
ICMP標頭的ICMP識別符號可用作流中5元組的源埠，因此ping資料包的所有5元組都是相同的，ASP丟棄原因為「inspect-icmp-seq-num-not-matched」，正如您在此輸出中看到的那樣。

```
firepower#show cap asp-drop
 1: 19:47:09.293136 10.0.5.8 > 10.50.0.53 icmp: echo reply Drop-reason: (inspect-icmp-seq-num-not-match
```



思科錯誤 ID CSCvb92417

集群ASA丟棄到機箱的ICMP應答並返回原因「inspect-icmp-seq-num-not-matched」

ASP刪除原因：

名稱:inspect-icmp-seq-num-not-matched
ICMP Inspect seq num not matched:
　當ICMP回應回覆消息中的序列號與之前在同一連線上通過裝置的任何ICMP回應消息都不匹配時，此計數器必須遞增。

解決方案：禁用ICMP檢測。在群集環境中：群集中有兩個或多個FTD，而ICMP流量可以是非對稱的。觀察到ICMP流量刪除存在延遲，後續ping會在清除前一個ping流量之前快速傳送。在這種情況下，可能會發生連續ping封包遺失。

SIP檢測丟棄示例

在這種情況下，呼叫僅持續五分鐘，然後連線斷開。使用RTP時，SIP檢測可以丟棄連線。
正如您在介面VoIP流量的資料包捕獲輸出中觀察到的那樣，SIP流量中的BYE標誌表示此時電話呼

叫已關閉。

```
1    2023-10-13 18:39:03.421456    10.6.6.66    172.16.3.77    SIP/SDP    1055    Request: INVITE sip:1
2    2023-10-13 18:39:03.448325    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
3    2023-10-13 18:39:03.525424    172.16.3.77    10.6.6.66    SIP    687    Status: 401 Unauthorized |
4    2023-10-13 18:39:03.525943    10.6.6.66    172.16.3.77    SIP    425    Request: ACK sip:123456789
5    2023-10-13 18:39:03.527331    10.6.6.66    172.16.3.77    SIP/SDP    1343    Request: INVITE sip:1
6    2023-10-13 18:39:03.553544    172.16.3.77    10.6.6.66    SIP    497    Status: 100 Trying |
7    2023-10-13 18:39:05.902815    172.16.3.77    10.6.6.66    SIP/SDP    992    Status: 183 Session Pr
8    2023-10-13 18:39:06.091822    172.16.3.77    10.6.6.66    SIP/SDP    967    Status: 180 Ringing |
9    2023-10-13 18:39:13.114435    172.16.3.77    10.6.6.66    SIP/SDP    1063    Status: 200 OK (INVIT
10    2023-10-13 18:39:13.115899    10.6.6.66    172.16.3.77    SIP    560    Request: ACK sip:55663399
11    2023-10-13 18:40:29.206593    172.16.3.77    10.6.6.66    SIP    642    Request: UPDATE sip:FD3a5
12    2023-10-13 18:40:29.207630    10.6.6.66    172.16.3.77    SIP    659    Status: 200 OK (UPDATE) |
13    2023-10-13 18:41:09.940854    10.6.6.66    172.16.3.77    SIP    684    Request: BYE sip:33445566
14    2023-10-13 18:41:10.003066    172.16.3.77    10.6.6.66    SIP    659    Status: 200 OK (BYE) |
```

在此其他示例中，系統日誌顯示使用PAT的對映IP，該IP僅有一個可用埠，並且SIP會話位於同一埠，由於埠分配，SIP失敗。如果正在使用PAT，則SIP檢測可以斷開連線。

ASP刪除原因為："由於達到每主機PAT埠塊限制X而無法建立從IP/埠到IP/埠的UDP連線"和"被檢查引擎終止，原因 — 根據'service resetinboud'配置重置"

```
Nov 18 2019 10:19:34: %FTD-6-607001: Pre-allocate SIP Via UDP secondary channel for 3111:10.11.0.13/506
Nov 18 2019 10:19:35: %FTD-6-302022: Built backup stub TCP connection for identity:172.16.2.20/2325 (17
Nov 18 2019 10:19:38: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:38: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
Nov 18 2019 10:19:39: %FTD-3-305016: Unable to create UDP connection from 3111:10.11.0.12/50195 to 3121
Nov 18 2019 10:19:39: %FTD-4-507003: udp flow from 3111:10.11.0.12/5060 to 3121:10.21.0.12/5060 termina
```

ASP刪除原因：

名稱:async-lock-queue-limit
超出非同步鎖定隊列限制：
　每個非同步鎖定工作隊列的限製為1000。當嘗試向工作隊列傳送更多SIP資料包時，必須丟棄資料包。
建議：
　只能丟棄SIP流量。當SIP資料包具有相同的父鎖定且可以排入相同的非同步鎖定隊列時，可能導致塊耗盡，因為只有單個核心處理所有介質。如果非同步鎖定隊列的大小超出限制時SIP資料包嘗試排隊，則必須丟棄該資料包。

名稱:sp-looping-address
looping-address:
　當流中的源地址和目的地址相同時，此計數器會遞增。 啟用地址隱私的SIP流被排除，因為這些流通常具有相同的源地址和目的地址。

建議：

此計數器可以遞增有兩個可能條件。一種是裝置收到源地址等於目標的資料包時。這表示一種DoS攻擊。 第二種情況是，裝置的NAT配置將源地址與目標地址相同。

名稱:父項關閉
父流已關閉：
當從屬流的父流關閉時，從屬流也關閉。 例如，FTP資料流（從屬流）在其控制流（父流）終止時，可以使用此特定原因將其關閉。 當二次流（銷孔）被其控制應用關閉時，也給出了這個原因。 例如，當收到BYE消息時，SIP檢測引擎（控制應用）必須關閉相應的SIP RTP流（輔助流）。

解決方案：禁用SIP檢測。由於通訊協定限制：

- SIP檢測僅支援「聊天」功能。不支援白板、檔案傳輸和應用程式共用。不支援RTC客戶端5.0。
- 使用PAT時，包含沒有埠的內部IP地址的任何SIP報頭欄位都無法轉換，因此內部IP地址可能會洩露到外部。如果要避免此洩漏，請配置NAT而不是PAT。
- 預設情況下，使用預設檢測對映啟用SIP檢測，包括：
  * SIP即時消息(IM)擴展：已啟用.
  * SIP埠上的非SIP流量：Dropped.
  *隱藏伺服器和終端IP地址：已停用.
  *遮蔽軟體版本和非SIP URI:已停用.
  *確保到達目標的跳數大於0:已啟用.
  * RTP一致性：未強制執行。
  * SIP一致性：不執行狀態檢查和報頭驗證。

疑難排解

以下是一些用於解決與LINA MPF通訊協定檢查相關的流量問題的建議命令。

- Show service-policy顯示已啟用的LINA MPF檢查的服務策略統計資訊。

```
firepower# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
      Inspect: dns preset_dns_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/s
      Inspect: ftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: h323 h225 _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: h323 ras _default_h323_map, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate
      Inspect: rsh, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-clo
      Inspect: rtsp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sqlnet, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
      Inspect: skinny, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sunrpc, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-
               tcp-proxy: bytes in buffer 0, bytes dropped 0
      Inspect: sip , packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
               tcp-proxy: bytes in buffer 0, bytes dropped 0
```

```
      Inspect: netbios, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail
      Inspect: tftp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
      Inspect: icmp error, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-f
      Inspect: ip-options UM_STATIC_IP_OPTIONS_MAP, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-
    Class-map: class_snmp
      Inspect: snmp, packet 0, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-cl
    Class-map: class-default

      Default Queueing      Set connection policy:         drop 0
      Set connection advanced-options: UM_STATIC_TCP_MAP
        Retransmission drops: 0                   TCP checksum drops : 0
        Exceeded MSS drops  : 0                   SYN with data drops: 0
        Invalid ACK drops   : 0                   SYN-ACK with data drops: 0
        Out-of-order (OoO) packets : 0            OoO no buffer drops: 0
        OoO buffer timeout drops : 0              SEQ past window drops: 0
        Reserved bit cleared: 0                   Reserved bit drops : 0
        IP TTL modified     : 0                   Urgent flag cleared: 0
        Window varied resets: 0
        TCP-options:
          Selective ACK cleared: 0                Timestamp cleared  : 0
          Window scale cleared : 0
          Other options cleared: 0
          Other options drops: 0
```

show service-policy inspect http命令的輸出示例顯示http統計資訊：

```
firepower# show service-policy inspect http
    Global policy:
      Service-policy: global_policy
        Class-map: inspection_default
          Inspect: http http, packet 1916, drop 0, reset-drop 0
            protocol violations
              packet 0
            class http_any (match-any)
              Match: request method get, 638 packets
              Match: request method put, 10 packets
              Match: request method post, 0 packets
              Match: request method connect, 0 packets
              log, packet 648
```

- 在要檢查的介面上設定asp-drop捕獲。

```
Syntax
#Capture


        type asp-drop


         match
```

```
for example
#Capture asp type asp-drop all match ip any any
#Capture asp type asp-drop all match ip any host x.x.x.x
#Capture asp type asp-drop all match ip host x.x.x.x host x.x.x.x
```

如何啟用或停用特定的LINA MPF應用程式檢查

以下是在Cisco安全防火牆威脅防禦中啟用或禁用MPF LINA應用檢查的可用選項。

- 透過FlexConfig進行組態：您需要具有對FMC UI的管理員訪問許可權，此更改對配置是永久性的。
- 透過FTD CLI進行組態：您需要具有對FTD CLI的管理員訪問許可權，此更改不是永久更改，如果發生重新啟動或新部署，則會刪除配置。

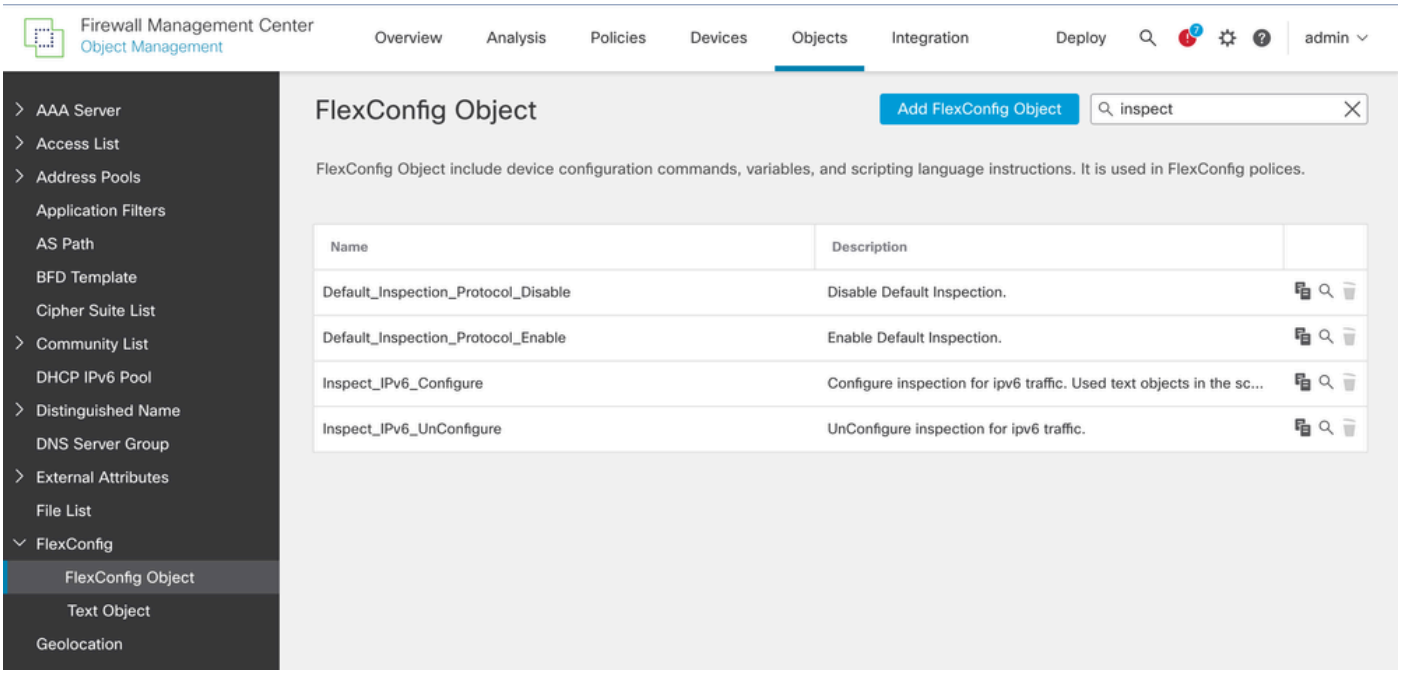
透過FlexConfig進行組態

FlexConfig是一種最後選用方法，用於配置基於ASA的功能，這些功能與威脅防禦相容，但在管理中心中無法進行配置。

永久禁用或啟用檢測的配置位於通過FMC UI的FlexConfig上，可以全域性應用該配置，也可以僅應用於特定流量。

步驟 1.

在FMC UI上，導航到Objects > Object Management > FlexConfig > FlexConfig Object，您可以在那裡找到預設協定檢測對象的清單。



預設FlexConfig協定檢查對象

步驟 2.

要禁用特定協定檢查，可以建立FlexConfig對象。

導航到對象>對象管理> FlexConfig > FlexConfig對象>新增FlexConfig對象

在本示例中，要從global_policy禁用SIP檢測，其語法必須是：

```
policy-map global_policy
 class inspection_default
  no inspect sip
```

配置FlexConfig對象時，可以選擇部署頻率和型別。

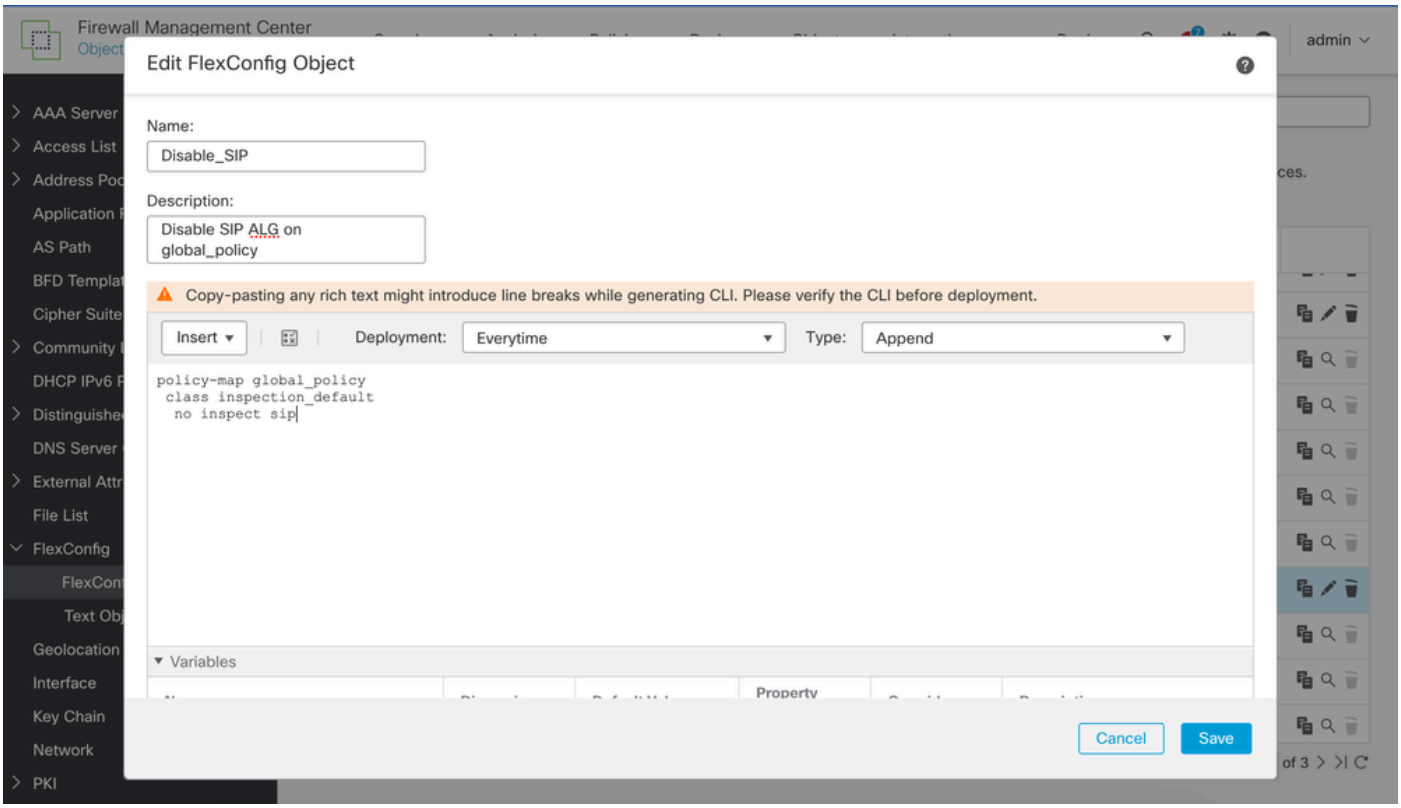
部署

- 如果FlexConfig對象指向系統管理的對象，例如網路或ACL對象，請選擇Everytime。否則，無法部署對象的更新。
- 如果對象中唯一要做的就是清除配置，則使用一次。然後，在下次部署後從FlexConfig策略中刪除該對象。

類型

- 附加（預設值。）對象中的命令放置在管理中心策略生成的配置的結尾。如果使用策略對象變數（指向從託管對象生成的對象），則必須使用「附加」。如果為其他策略生成的命令與對象中指定的命令重疊，則必須選擇此選項，以便不會覆蓋您的命令。這是最安全的選項。

- 預置。對象中的命令置於管理中心策略生成的配置的開頭。通常，對於清除或否定配置的命令，應使用prepend。



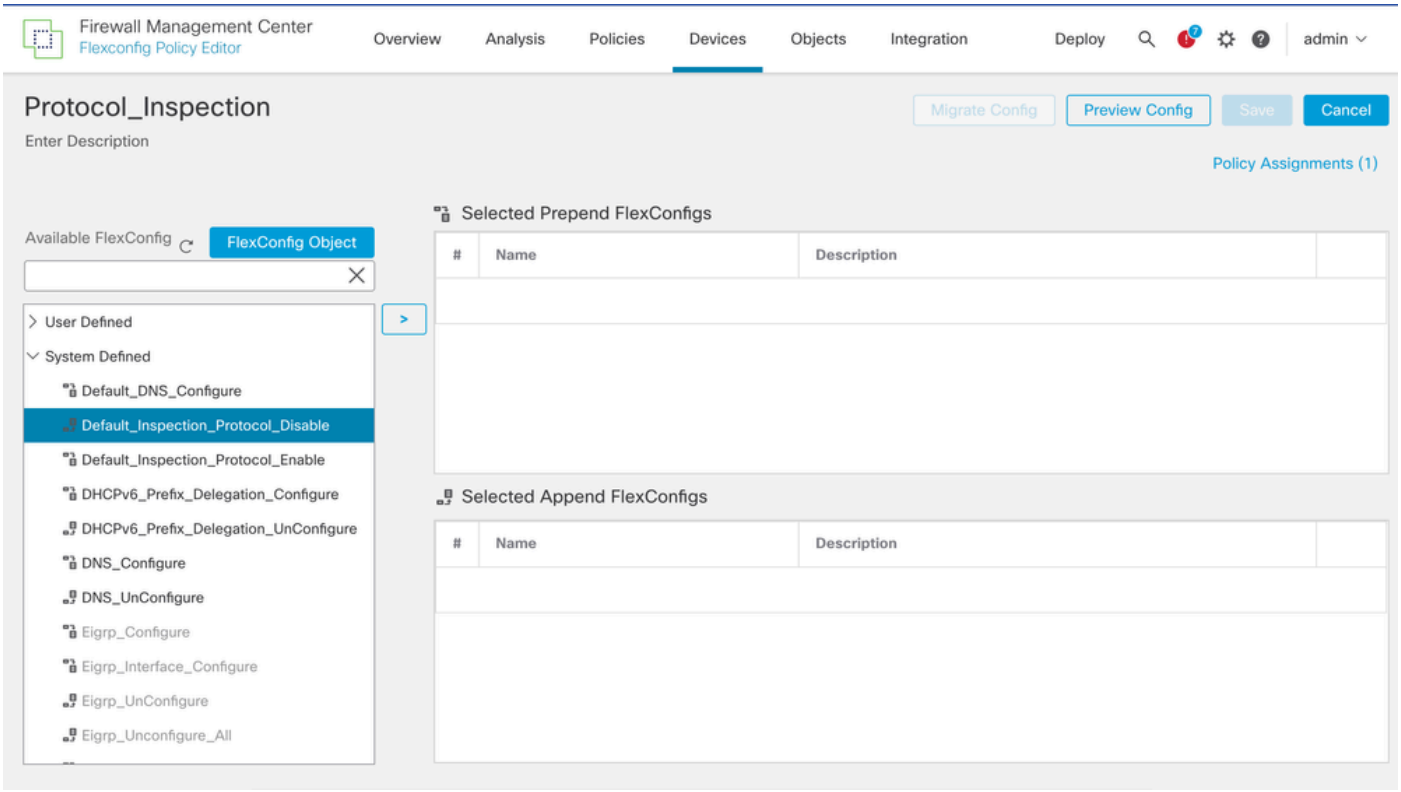
建立一個對象，以禁用預設的global_policy中的單個協定

步驟 3.

在分配給LINA的FlexConfig策略中新增對象。

導覽至Devices > FlexConfig，選擇應用於防火牆且存在丟棄問題的FlexConfig策略。

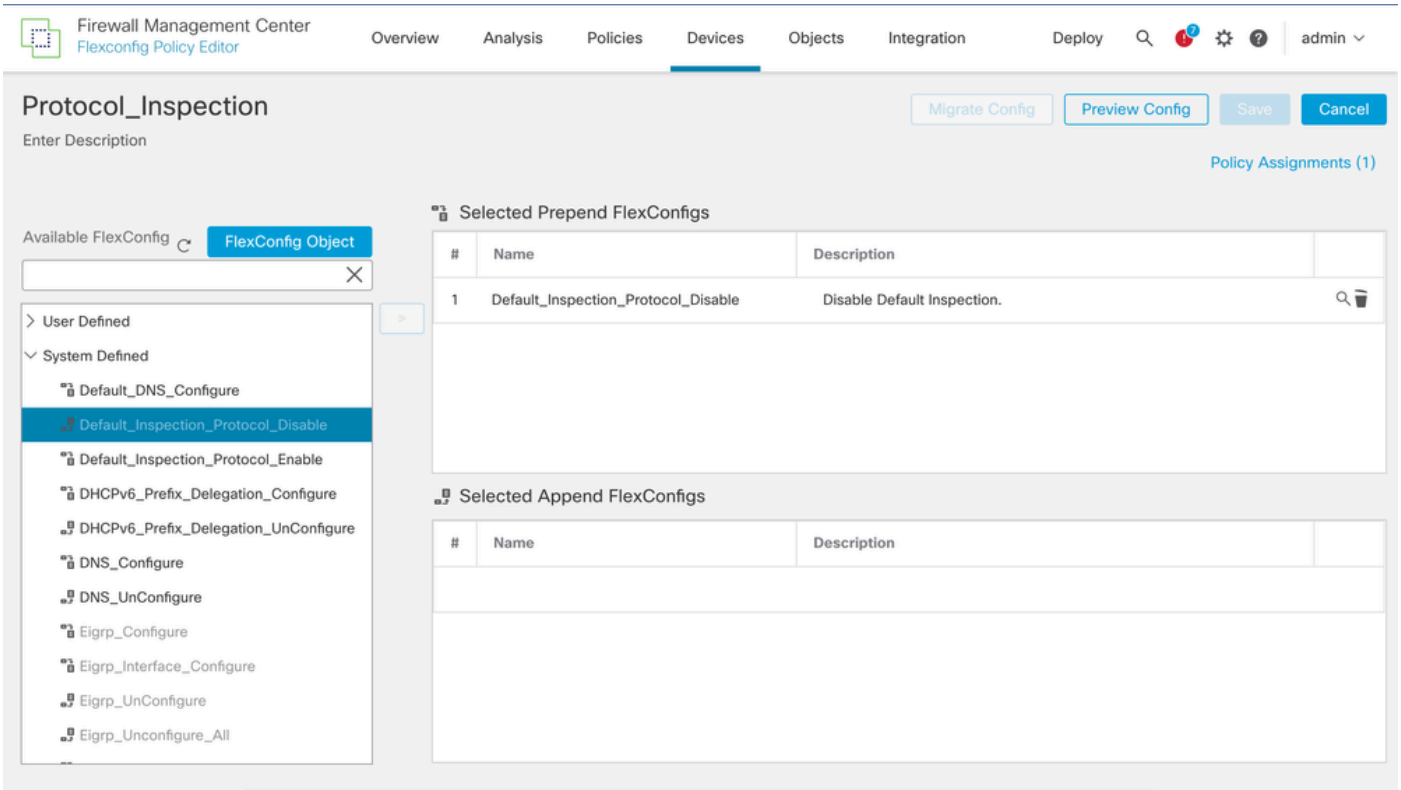
要全域性禁用所有檢查，請選擇「系統定義的FlexConfig對象」下的「對象Default_Inspection_Protocol_Disable」，然後按一下中間的藍色箭頭將其新增到FlexConfig策略中。



選擇系統定義的對象以禁用所有協定檢查

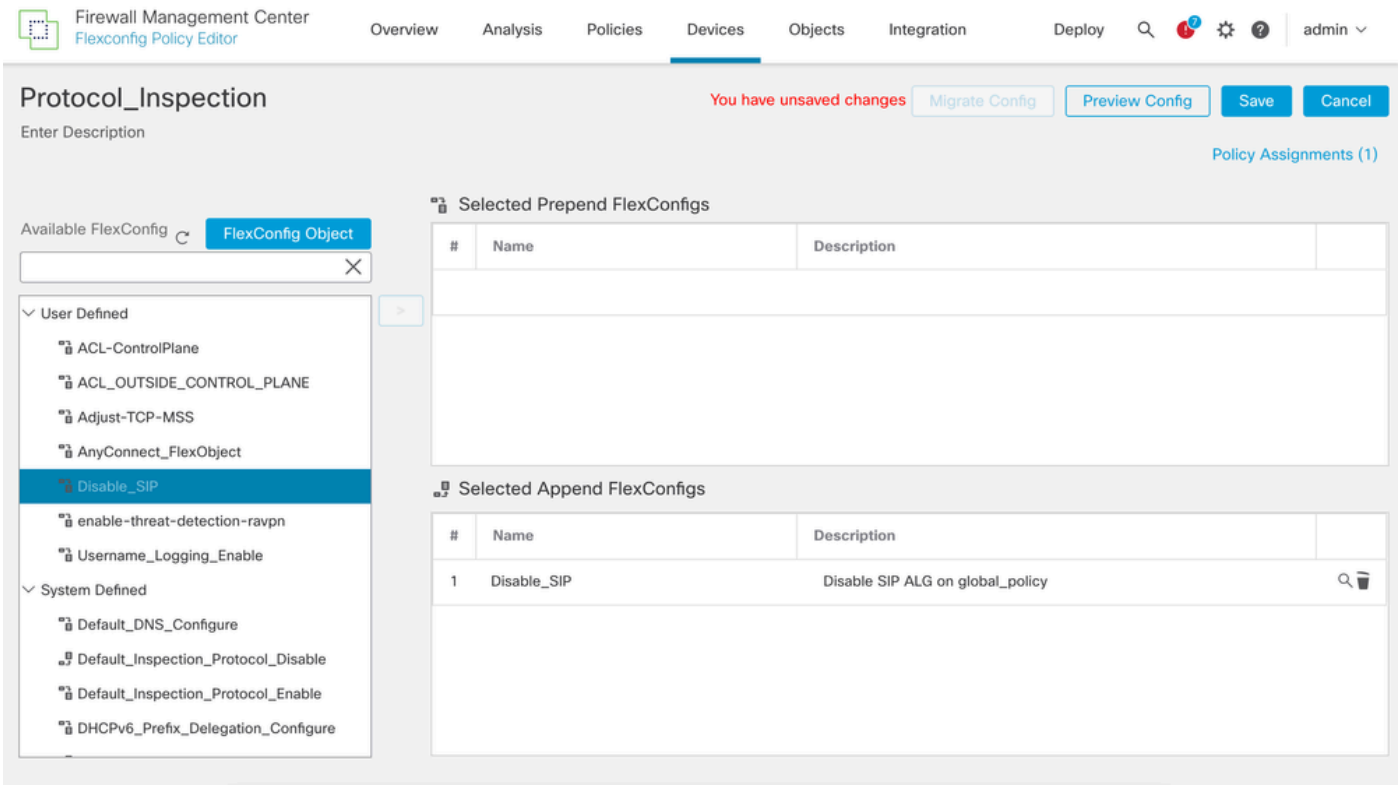
步驟 4.

選中後，確認它顯示在右框中，不要忘記儲存並部署配置以生效。



用於禁用所有協定檢測的選定對象

步驟 5.
要禁用單個協定檢測，請從「使用者定義」(User defined)清單中選擇先前建立的對象，然後使用框之間的箭頭將其新增到策略中。



選擇以從global_policy禁用單個協定檢查

步驟 6.

選中後，確認它顯示在右框中，不要忘記儲存並部署配置以生效。

使用FTD CLI進行組態

此解決方案可以從FTD CLI立即應用，以測試檢查是否影響流量。但是，如果發生重新啟動或新部署，則不會儲存配置更改。

必須在清潔模式下從FTD CLI執行命令。

```
> configure inspection


        disable

for example
> configure inspection SIP disable
```

驗證

要驗證協定禁用是否有效，請執行show running-config policy-map命令。在本例中，SIP檢測被禁用，因為它不再出現在預設協定清單中。

```
firepower# show running-config policy-map
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum client auto
  message-length maximum 512
  no tcp-inspection
policy-map type inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 parameters
  eool action allow
  nop action allow
  router-alert action allow
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect netbios
  inspect tftp
  inspect icmp
  inspect icmp error
  inspect ip-options UM_STATIC_IP_OPTIONS_MAP
 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
!
firepower#
```

相關資訊

技術支援與文件 - Cisco Systems

- 應用層協定檢測入門
- 基本Internet協定檢查
- Show ASP Drop命令用法

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）。