配置防火牆威脅防禦模組化策略框架

目錄

簡介

本檔案介紹防火牆威脅防禦(FTD)模組化原則架構(MPF)

必要條件

需求

本文件沒有特定需求。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 思科安全防火牆3130威脅防禦版本10.0.0（內部版本140）
- 防火牆管理中心(FMC)版本10.0.0（內部版本140）

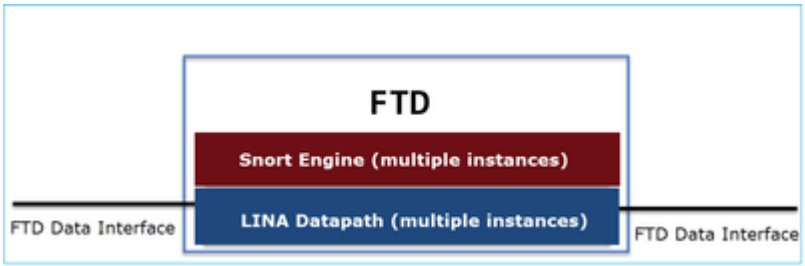
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

FTD資料平面概觀

FTD 是一個整合的軟體映像，其中包括 2 個主引擎：

- Datapath（也稱為LINA）
- Snort 引擎



LINA資料路徑和Snort引擎是FTD資料平面的主要部分。

MPF成分

MPF使用以下元件：

- class-map匹配所需的流量。
- policy-map將操作應用於與類對映匹配的相關流量。
- service-policy全域性應用策略對映（在所有介面上）或在特定介面上。

功能方向性

有關功能方向性，請參閱ASA配置指南：

https://www.cisco.com/c/en/us/td/docs/security/asa/asa924/configuration/firewall/asa-924-firewall-

config/inspect-service-policy.html

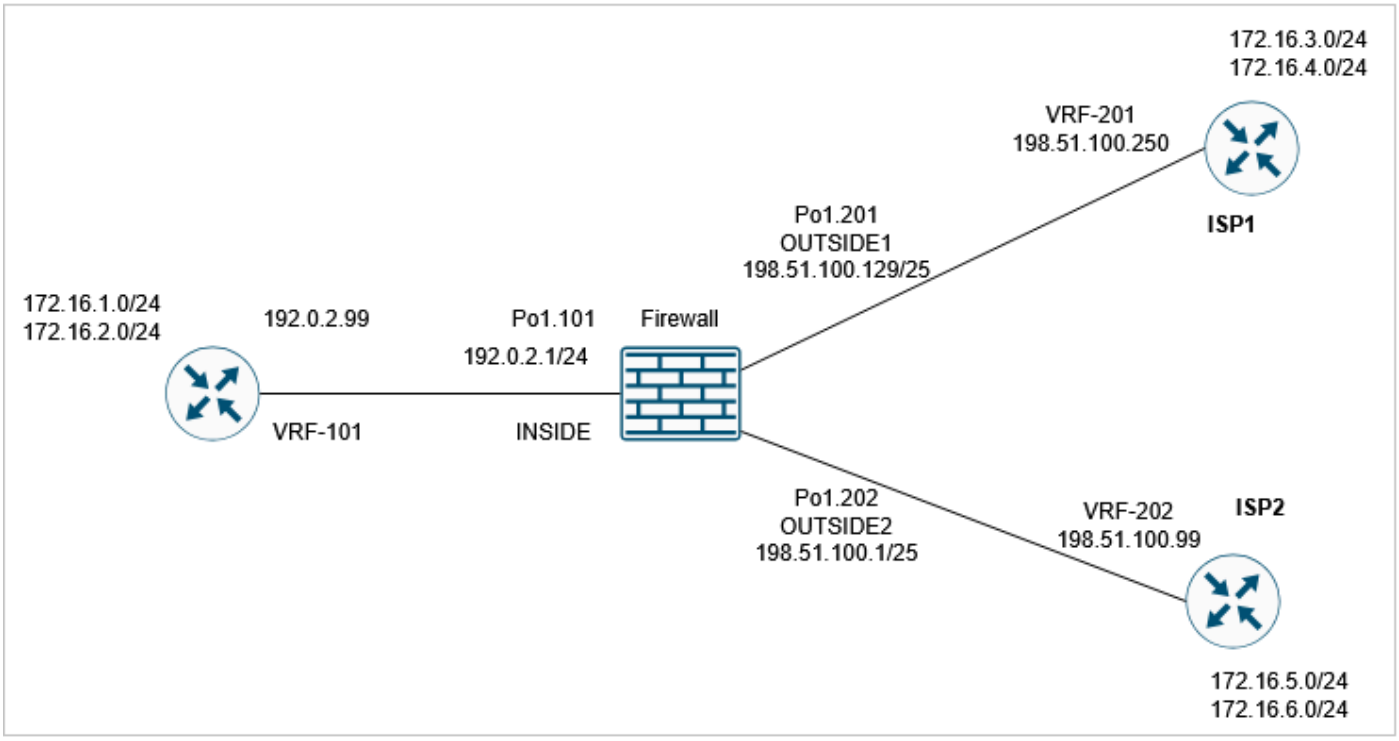
與FTD相關的功能會突出顯示：

Table 2. Feature Directionality

Feature	Single Interface Direction	Global Direction
Application inspection (multiple types)	Bidirectional	Ingress
NetFlow Secure Event Logging filtering	N/A	Ingress
QoS input policing	Ingress	Ingress
QoS output policing	Egress	Egress
QoS standard priority queue	Egress	Egress
TCP and UDP connection limits and timeouts, and TCP sequence number randomization	Bidirectional	Ingress
TCP normalization	Bidirectional	Ingress
TCP state bypass	Bidirectional	Ingress
User statistics for Identity Firewall	Bidirectional	Ingress

設定

拓撲



預設MPF配置(10.0.0):

<#root>

```
firewall#
```

show run 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

firewall#
```

show run class-map

```
!
class-map inspection_default
 match default-inspection-traffic
class-map class_snmp
 match port udp eq 4161
!
firewall#
```

show run service-policy

```
service-policy global_policy global
```

任務1.在FTD上全域性禁用SIP檢測

此任務中的要求在FTD LINA引擎中停用SIP檢查。一個原因可能是影響傳輸流量的策略要求或與SIP相關的軟體缺陷。

解決方案

在禁用SIP檢測之前，首先確認它已應用於傳輸流量：

<#root>

firewall#

packet-tracer input INSIDE udp 172.16.1.1 5060 172.16.3.1 5060

...
Phase: 8

Type: INSPECT

Subtype: inspect-sip

Result: ALLOW

Elapsed time: 34788 ns
Config:

class-map inspection_default

match default-inspection-traffic

policy-map global_policy

```
 class inspection_default


  inspect sip


service-policy global_policy global


Additional Information:
...
Result:
input-interface: INSIDE(vrfid:0)
input-status: up
input-line-status: up
output-interface: OUTSIDE1(vrfid:0)
output-status: up
output-line-status: up

Action: allow


Time Taken: 326018 ns
```

全域性禁用SIP檢測有兩種方法：

情境 1:從FTD CLI停用SIP

<#root>

>

configure inspection sip disable

```
Building configuration...
Cryptochecksum: ef7528dc 7338986d 6714a3a2 4770528e

7818 bytes copied in 0.250 secs
[OK]
```

驗證

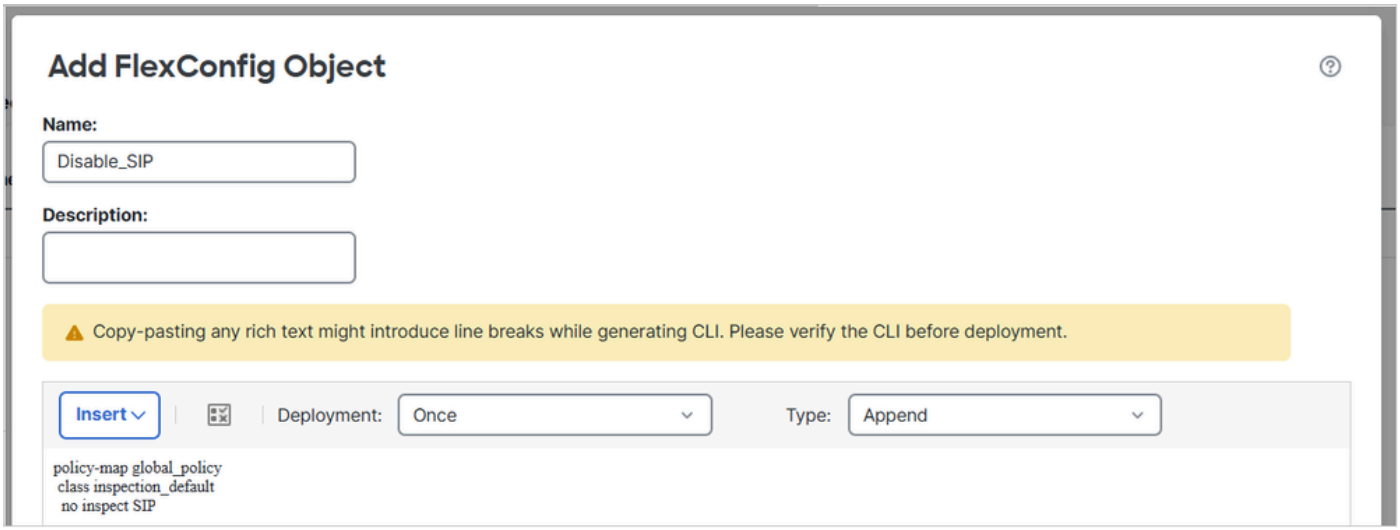
<#root>

>

```
show running-config policy-map | include sip

>
```

情境 2:使用FlexConfig禁用SIP

在FMC上，導覽至Devices > FlexConfig，然後建立FlexConfig對象：




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

應用 選擇FlexConfig策略並選擇Preview Config以進行預覽：

最後，部署策略。

驗證

```
<#root>

firewall#

show run policy-map | include sip

firewall#
```

注意 — 您需要從LINA連線表中清除現有的SIP連線，以便不進行SIP檢查而重新建立連線。您可以使用此命令驗證現有的SIP連線：

```
<#root>

firewall#

show conn port 5060
```

任務2.禁用特定主機的SIP檢測

在本任務中，要求對這些網路之間的流量禁用SIP檢測：

- 源：172.16.1.0/24
- DST:172.16.3.0/24

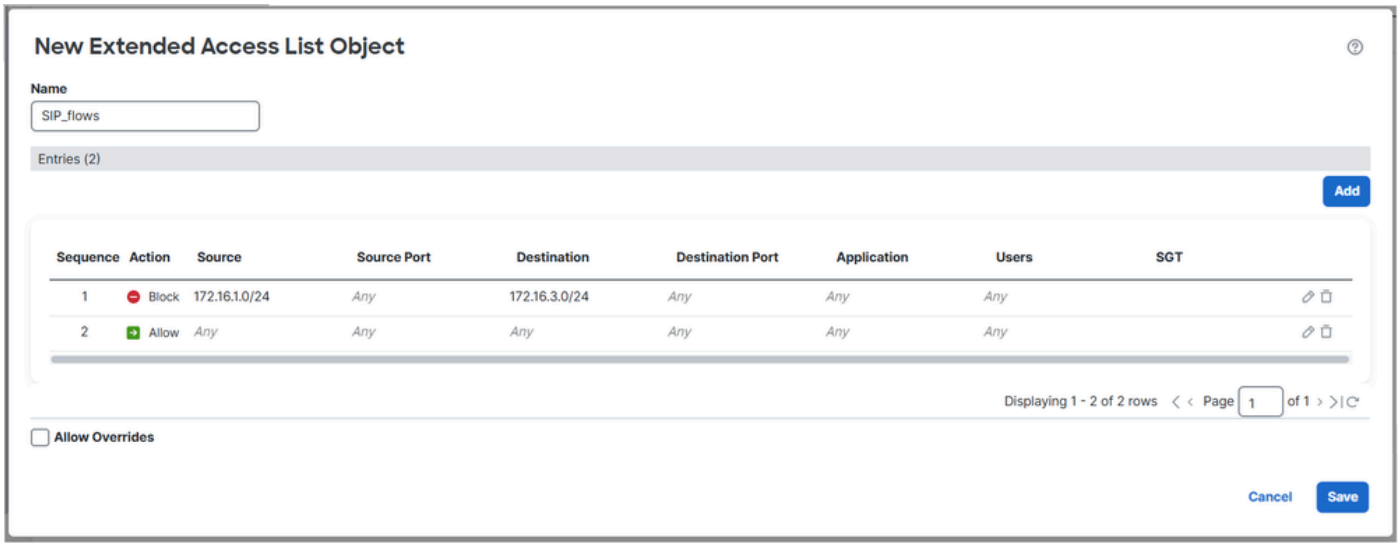
這樣做的一個原因可能是與SIP相關的軟體缺陷會影響傳輸流量

解決方案

使用FlexConfig。

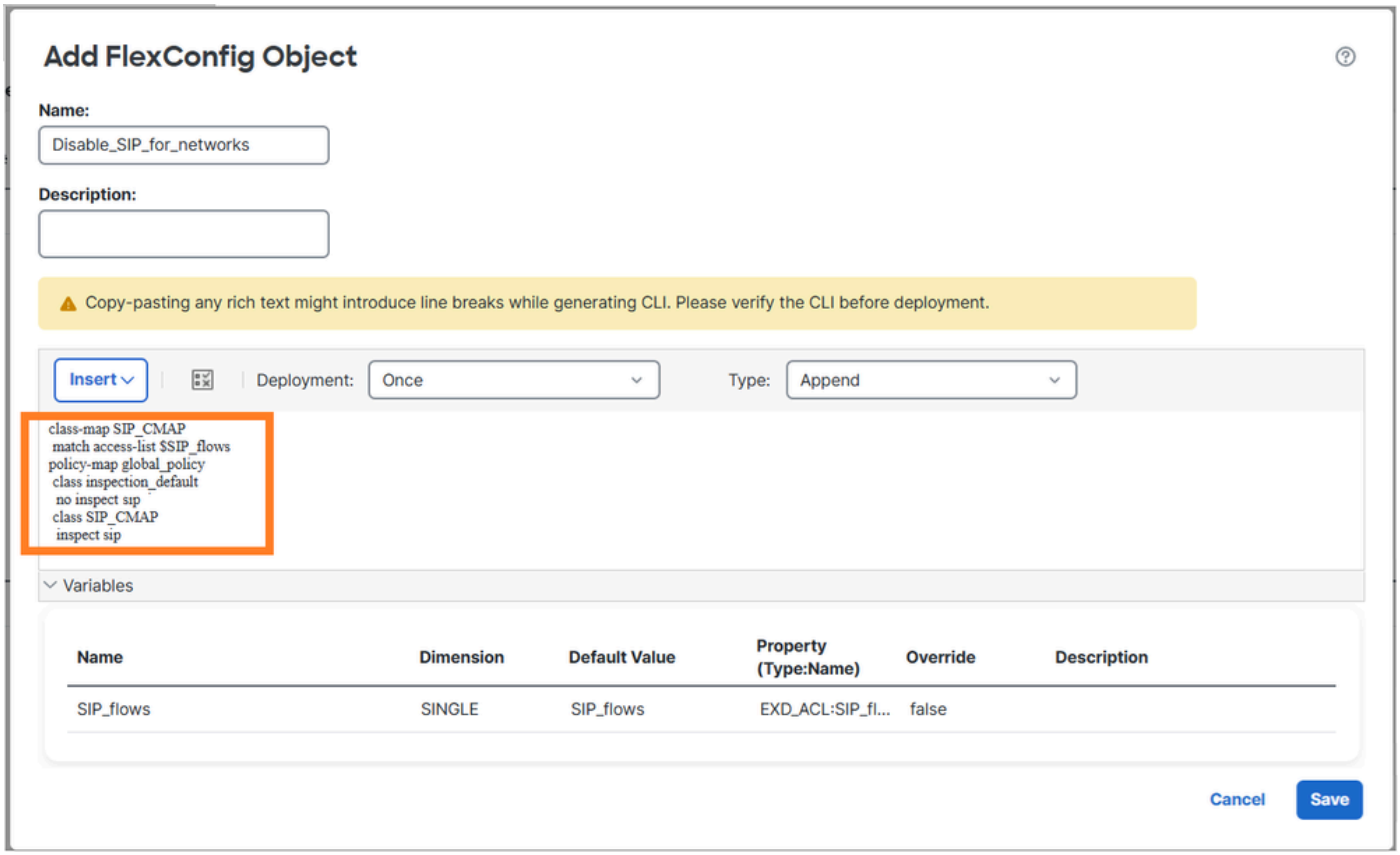
步驟 1

導覽至Objects > Access List > Extended，然後建立與感興趣的流量匹配的擴展訪問清單。您必須使用Block操作，因為目標是排除特定流量。此外，新增一個Allow規則以匹配其餘流量：



步驟 2

使用與SIP訪問控制清單(ACL)匹配的類對映建立FlexConfig對象，並將其應用於global_policy:



已配置的FlexConfig對象：

```
class-map SIP_CMAP
 match access-list $SIP_flows
policy-map global_policy
 class inspection_default
  no inspect sip
 class SIP_CMAP
  inspect sip
```

附註

配置permit ACL時，請嘗試儘可能具體地(例如put protocol ports)，以避免任何潛在的CPU影響。本任務中的示例未指定協定埠，因此可以在生產中避免。

驗證 1

<#root>

firewall#

show run policy-map | begin global

```
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 SIP_CMAP




  inspect sip



 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP

firewall#

show run class-map



!

class-map SIP_CMAP




 match access-list SIP_flows



class-map inspection_default
 match default-inspection-traffic
class-map class_snmp
 match port udp eq 4161

firewall#

show run access-list SIP_flows



access-list SIP_flows extended deny ip 172.16.1.0 255.255.255.0 172.16.3.0 255.255.255.0
access-list SIP_flows extended permit ip any any
```

驗證 2

未由SIP檢查檢查的流量具有deny=true:

<#root>

```
firewall#

packet-tracer input INSIDE udp 172.16.1.1 5060 172.16.3.1 5060 detail | begin INSPECT



Type: INSPECT



Subtype: inspect-sip


Result: ALLOW
Elapsed time: 37910 ns
Config:

class-map SIP_CMAP



 match access-list SIP_flows



policy-map global_policy



 class SIP_CMAP



  inspect sip



service-policy global_policy global


Additional Information:
```

```
 Forward Flow based lookup yields rule:
 in id=0x14af42cfa810, priority=70, domain=inspect-sip,

deny=true




hits=1

, user_data=0x000014af4570bea0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0


      src ip/id=172.16.1.0, mask=255.255.255.0, port=0, tag=any




      dst ip/id=172.16.3.0, mask=255.255.255.0, port=0, tag=any,


       dscp=0x0, input_ifc=INSIDE(vrfid:0), output_ifc=any
...
```

SIP檢查所檢查的流量具有deny=false:

<#root>

```
firewall#

packet-tracer input INSIDE udp 172.16.2.1 5060 172.16.3.1 5060 detail | begin INSPECT




Type: INSPECT




Subtype: inspect-sip


Result: ALLOW
Elapsed time: 34788 ns
Config:
class-map SIP_CMAP
 match access-list SIP_flows
policy-map global_policy
 class SIP_CMAP
  inspect sip
service-policy global_policy global
```

```
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x14af459099d0, priority=70, domain=inspect-sip,
```

deny=false

```
       hits=1, user_data=0x000014af4570bea0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
       src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
       dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any,
...
```

驗證 3

當防火牆檢查封包時，「sip」檢查計數器會增加：

<#root>

```
firewall#
```

show service-policy inspect sip

```
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: class_snmp
    Class-map: SIP_CMAP
      Inspect: sip ,
```

packet 2

```
, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0
...
firewall#
```

packet-tracer input INSIDE udp 172.16.2.1 5060 172.16.3.1 5060

```
firewall#
```

show service-policy inspect sip

```
Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
    Class-map: class_snmp
    Class-map: SIP_CMAP
```

```
      Inspect: sip ,

packet 3

, lock fail 0, drop 0, reset-drop 0, 5-min-pkt-rate 0 pkts/sec, v6-fail-close 0 sctp-drop-override 0
               tcp-proxy: bytes in buffer 0, bytes dropped 0


...
```

任務3.為特定主機配置TCP狀態旁路

在本任務中，要求為這些網路之間的流量啟用TCP狀態旁路：

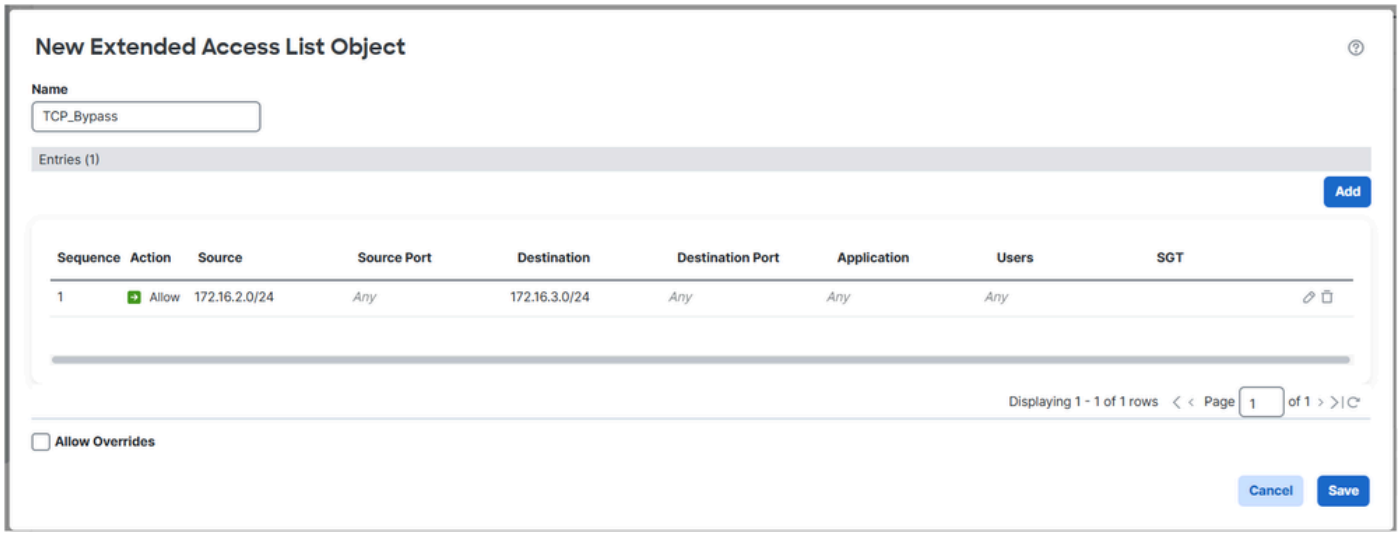
- 源：172.16.2.0/24
- DST:172.16.3.0/24

通常，不建議使用TCP狀態旁路，但可以將其用作處理非對稱流的臨時解決方法。

情境 1

步驟 1

建立與相關流量相符的延伸型ACL:

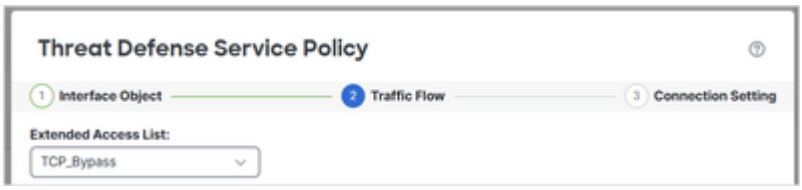


步驟 2

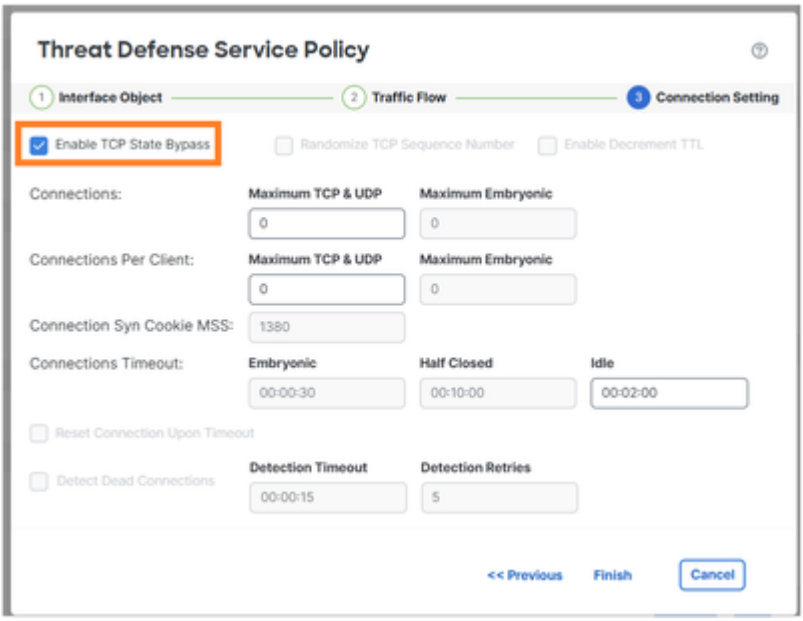
編輯分配給FTD的訪問控制策略(ACP)，選擇Advanced Settings頁籤並編輯Threat Defense Service策略。選擇Add Rule，然後選擇下一步。

步驟 3

選擇延伸型ACL:



步驟 4



步驟 5

選擇完成、確定、儲存和部署。

結果是：

<#root>

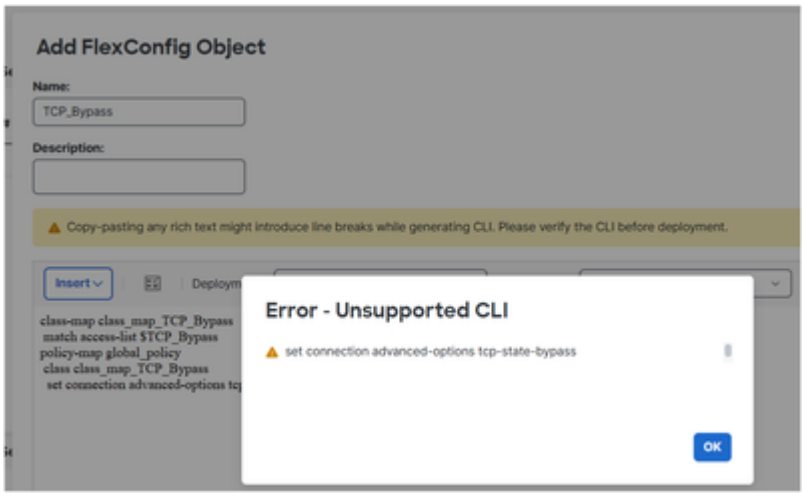
```
firewall#

show run policy-map global_policy


!
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_map_TCP_Bypass
```

```
  set connection random-sequence-number disable
```

```
  set connection advanced-options tcp-state-bypass
```

```
class class_snmp
 inspect snmp
class class-default
 set connection advanced-options UM_STATIC_TCP_MAP
```

附註： 在之前的FMC版本（如6.x）中，您可以使用FlexConfig來設定TCP狀態略過。在較新版本中不支援此功能：



驗證

<#root>

```
firewall#
```

```
packet-tracer input INSIDE tcp 172.16.2.1 1111 172.16.3.1 80 detail | begin CONN
```

```
Type: CONN-SETTINGS
Subtype:
Result: ALLOW
Elapsed time: 334 ns
Config:
```

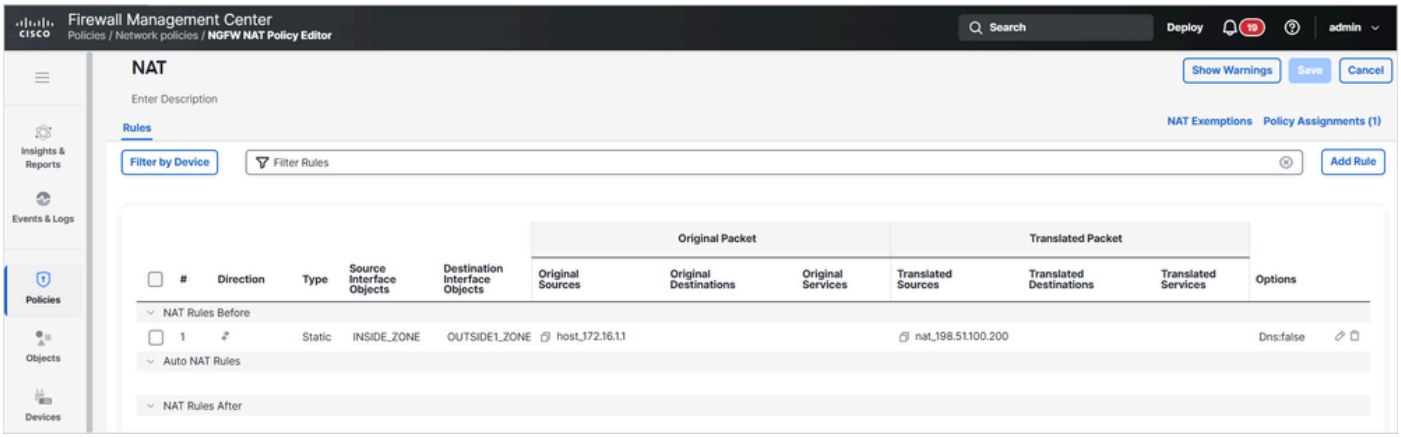
```
class-map class_map_TCP_Bypass
```

```
 match access-list TCP_Bypass


policy-map global_policy


 class class_map_TCP_Bypass


  set connection conn-max 0 embryonic-conn-max 0 random-sequence-number disable syn-cookie-mss 1380


  set connection advanced-options tcp-state-bypass


service-policy global_policy global
Additional Information:
 Forward Flow based lookup yields rule:
 in id=0x14af45906b70, priority=7, domain=conn-set, deny=false


hits=1

, user_data=0x000014af45906df0, cs_id=0x0, use_real_addr, flags=0x0, protocol=0

       src ip/id=172.16.2.0, mask=255.255.255.0, port=0, tag=any



       dst ip/id=172.16.3.0, mask=255.255.255.0, port=0, tag=any,


       dscp=0x0, input_ifc=INSIDE(vrfid:0), output_ifc=any
...
```

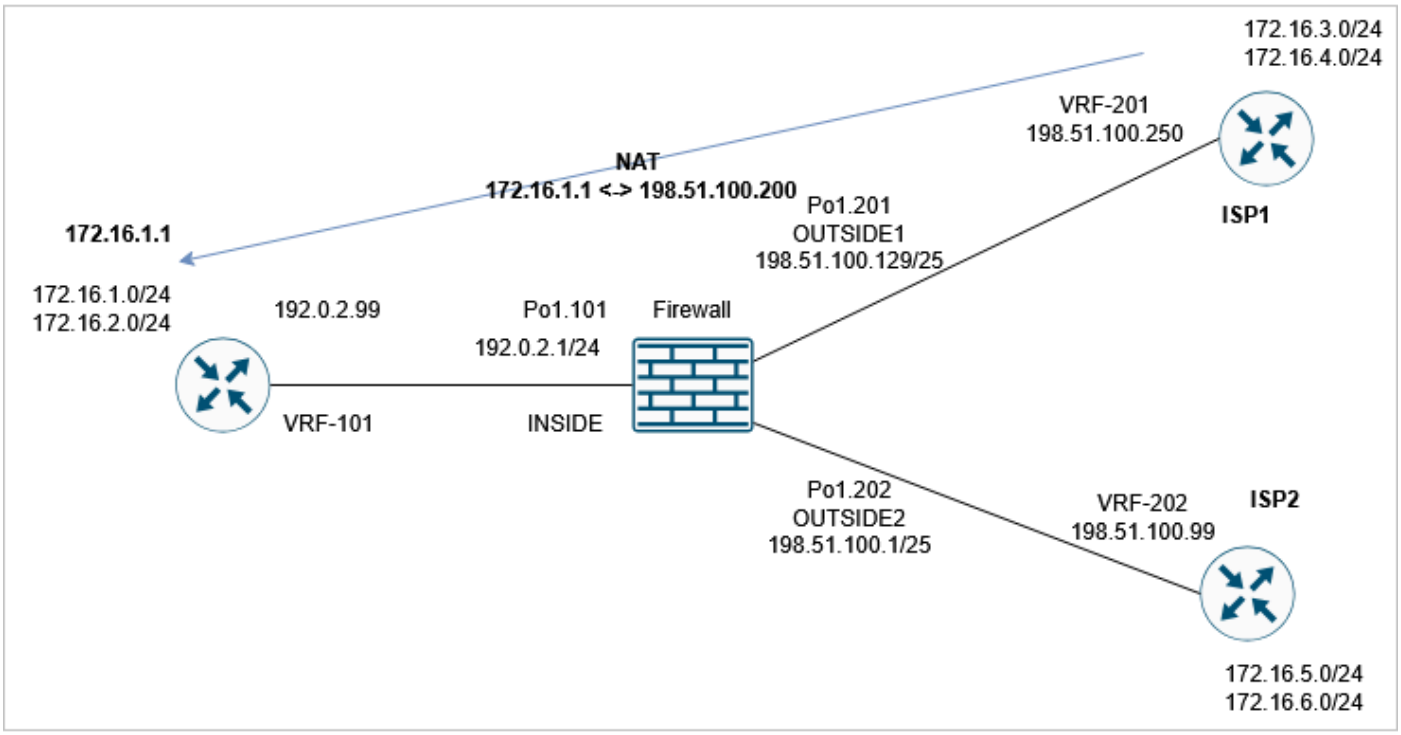
任務4. Traceroute輸出修改

必備條件

在FTD上設定靜態NAT，使位於INSIDE介面之後的IP 172.16.1.1在OUTSIDE1主機上顯示為198.51.100.200:



然後從ISP1運行traceroute到198.51.100.200（主機172.16.1.1）：



<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)
```

```
  1 192.0.2.99 1 msec 1 msec *
```

需求

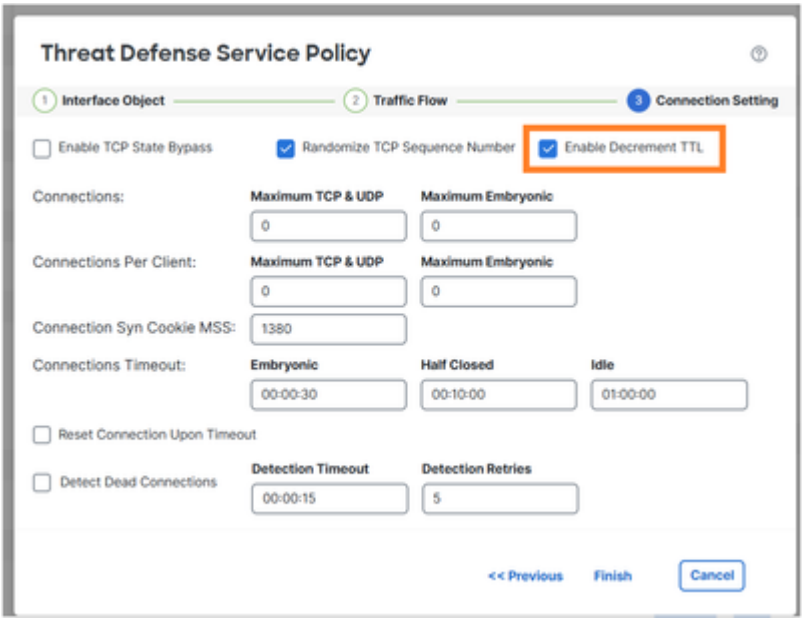
修改FTD組態，使traceroute符合以下輸出：

<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

  1 198.51.100.129 1 msec 1 msec *



  2 198.51.100.200 1 msec 2 msec *
```

解決方案

該解決方案包括兩個配置步驟：
1.降低TTL:



進行此變更後，traceroute會顯示防火牆躍點：

<#root>

router1#

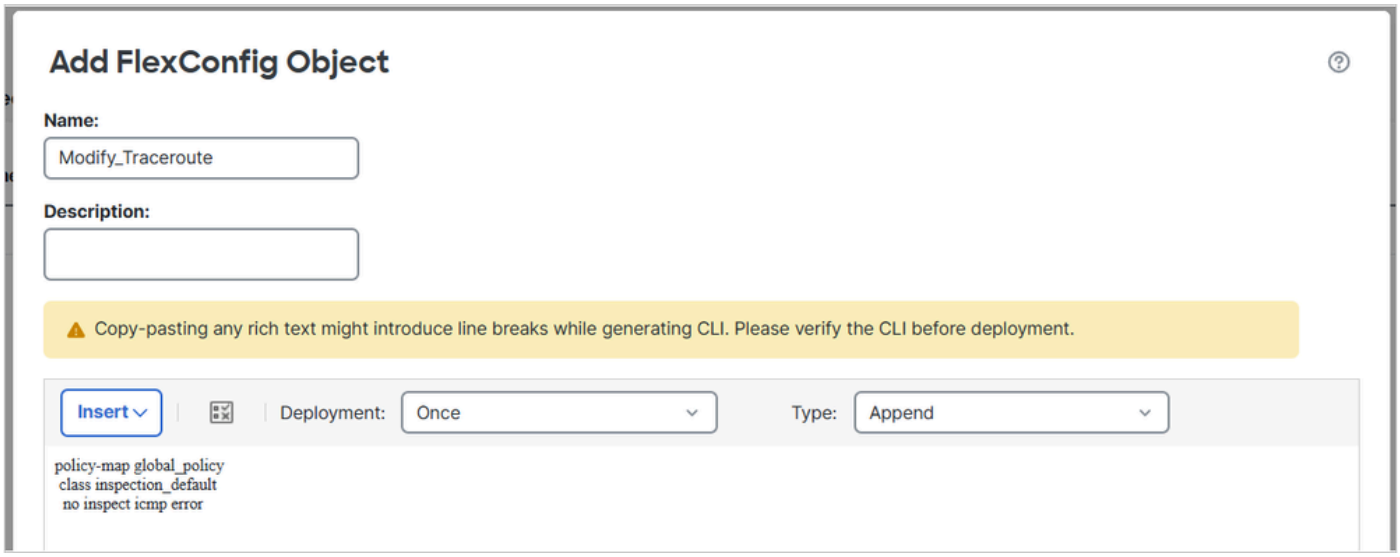
traceroute vrf VRF-201 198.51.100.200

Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

1 198.51.100.129 1 msec 1 msec *

2 192.0.2.99 1 msec 1 msec *

2.禁用ICMP錯誤檢查：




```
policy-map global_policy
 class inspection_default
   no inspect icmp error
```

驗證

traceroute顯示遠端主機的已轉換NAT IP位址和FTD介面IP位址：

<#root>

```
router1#

traceroute vrf VRF-201 198.51.100.200


Type escape sequence to abort.
Tracing the route to 198.51.100.200
VRF info: (vrf in name/id, vrf out name/id)

  1 198.51.100.129 1 msec 1 msec *



  2 198.51.100.200 1 msec 2 msec *
```

任務5.設定連線超時

需求

將此流的超時更改為1週：

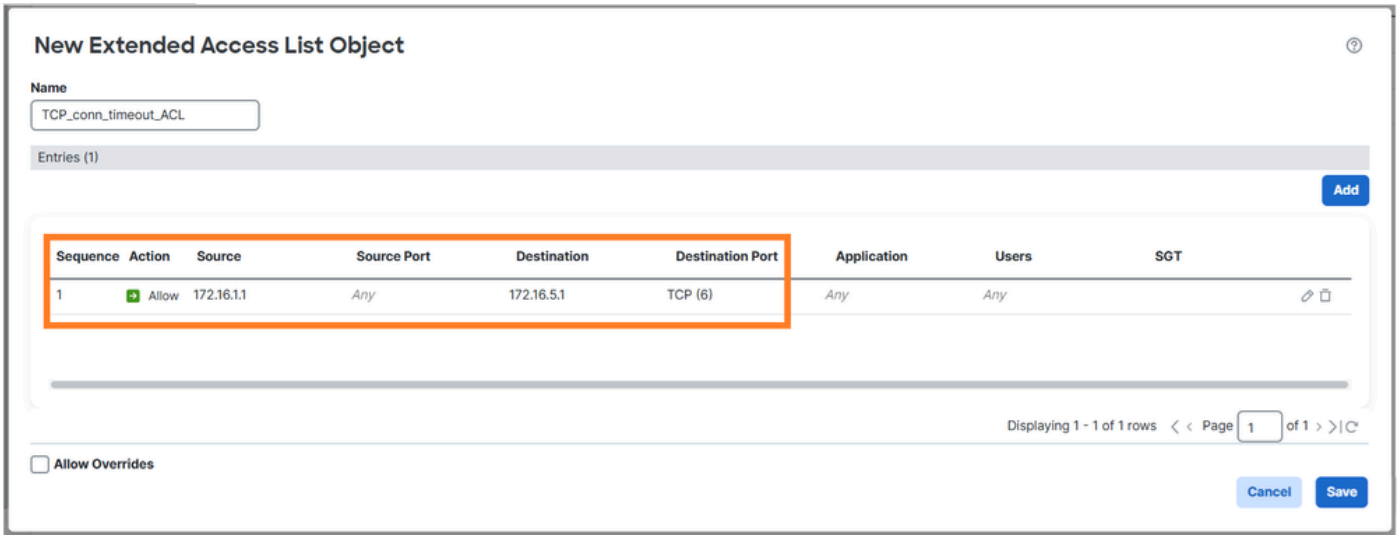
- 通訊協定：TCP
- 源：172.16.1.1
- DST:172.16.5.1

解決方案

要設定每個流的超時，您需要使用服務策略。

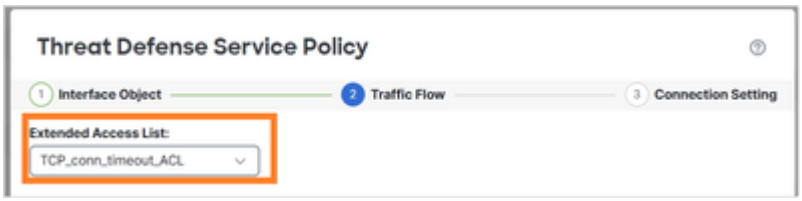
步驟 1

導覽至Objects > Access List，然後建立與相關流量相符的延伸型ACL:

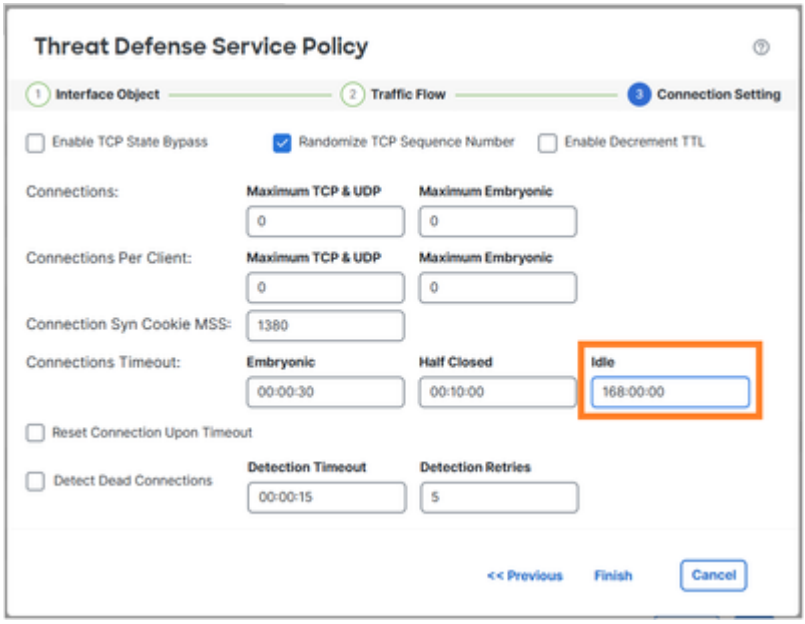


步驟 2

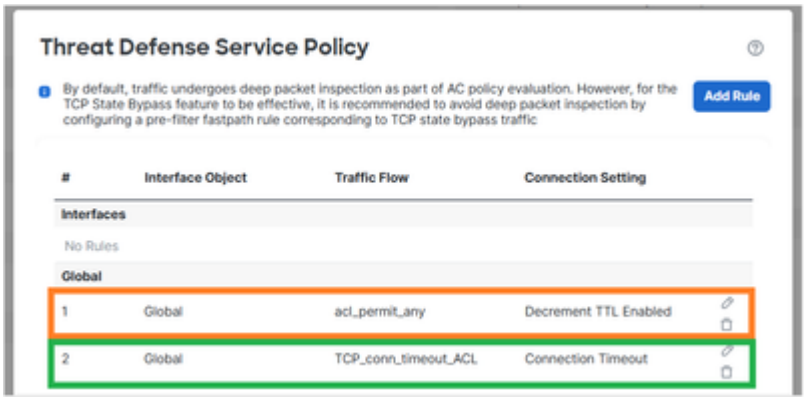
配置使用步驟1中建立的ACL的MPF策略：



設定連線空閒超時：



從上一個任務中刪除規則，因為它與新要求重疊：



驗證

已部署的策略對映配置：

<#root>

```
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 ip-options UM_STATIC_IP_OPTIONS_MAP
  inspect sip

 class class_map_TCP_conn_timeout_ACL




  set connection timeout idle 168:00:00



 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

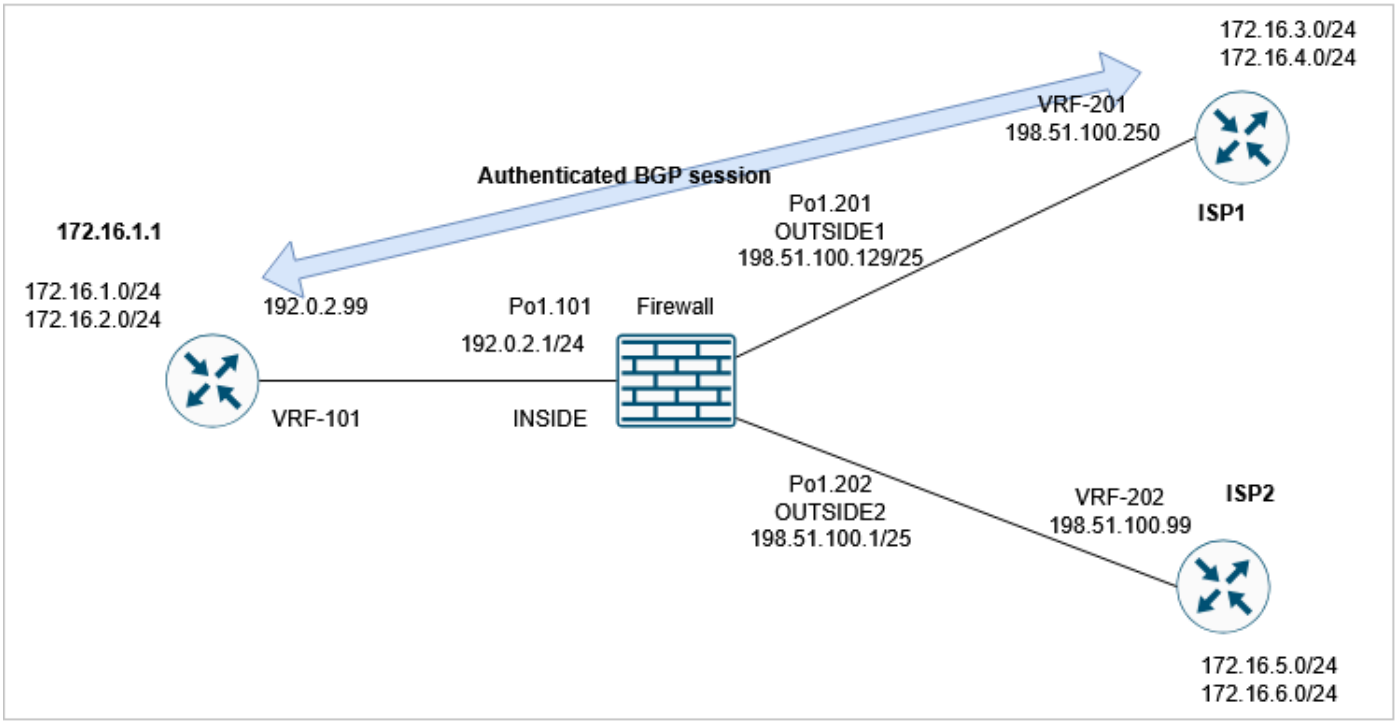
起始從172.16.1.1到172.16.5.1的新TCP連線，並檢查FTD的連線表：

```
<#root>

firewall#

show conn long address 172.16.5.1



...
TCP OUTSIDE2: 172.16.5.1/23 (172.16.5.1/23) INSIDE: 172.16.1.1/29389 (172.16.1.1/29389), flags UIoN1N7,

timeout 7D0h


, bytes 349, flow id 72, Snort id 6, rule id 268439559, Rx-RingNum 27, Internal-Data0/1
Initiator: 172.16.1.1, Responder: 172.16.5.1
Connection lookup keyid: 890
```

任務6.通過FTD的BGP驗證

必備條件

透過FTD設定BGP作業階段。BGP會話需要使用身份驗證。



驗證

使用預設FTD設定時，不會建立BGP作業階段。在路由器上，您可以看到：

<#root>

```
router1#
*May 21 07:51:23.595:
```

%TCP-6-BADAUTH: Invalid MD5 digest

```
 from 192.0.2.99(24591) to 198.51.100.250(179) tableid - 3
*May 21 07:51:25.595: %TCP-6-BADAUTH: Invalid MD5 digest from 192.0.2.99(24591) to 198.51.100.250(179)
*May 21 07:51:29.595: %TCP-6-BADAUTH: Invalid MD5 digest from 192.0.2.99(24591) to 198.51.100.250(179)
```

在FTD上，您看到兩端無法建立BGP TCP連線（連線旗標表示僅接收TCP SYN封包）：

<#root>

```
firewall#
```

```
show conn port 179


3 in use, 16 most used
Inspect Snort:
        preserve-connection: 2 enabled, 0 in effect, 15 most enabled, 0 most in effect

TCP OUTSIDE1 198.51.100.250:41090 INSIDE 192.0.2.99:179, idle 0:00:00, bytes 0,

flags aA N1


TCP OUTSIDE1 198.51.100.250:179 INSIDE 192.0.2.99:53629, idle 0:00:02, bytes 0,

flags aA N1
```

解決方案

若要允許透過FTD進行驗證的BGP作業階段，必須滿足以下兩個條件：

1. 必須允許TCP MD5（選項19）通過FTD。
2. 必須禁用TCP序列號隨機化。

預設情況下允許TCP MD5選項：

9.6(2)	Default handling of the named options was changed to allow a packet if it contains a single option of a given type, and drop the packet if there are more than one option of that type. Also, the **md5**, **mss**, **allow multiple**, and **mss maximum** keywords were added. The default for the MD5 option was changed from clear to allow.

<#root>

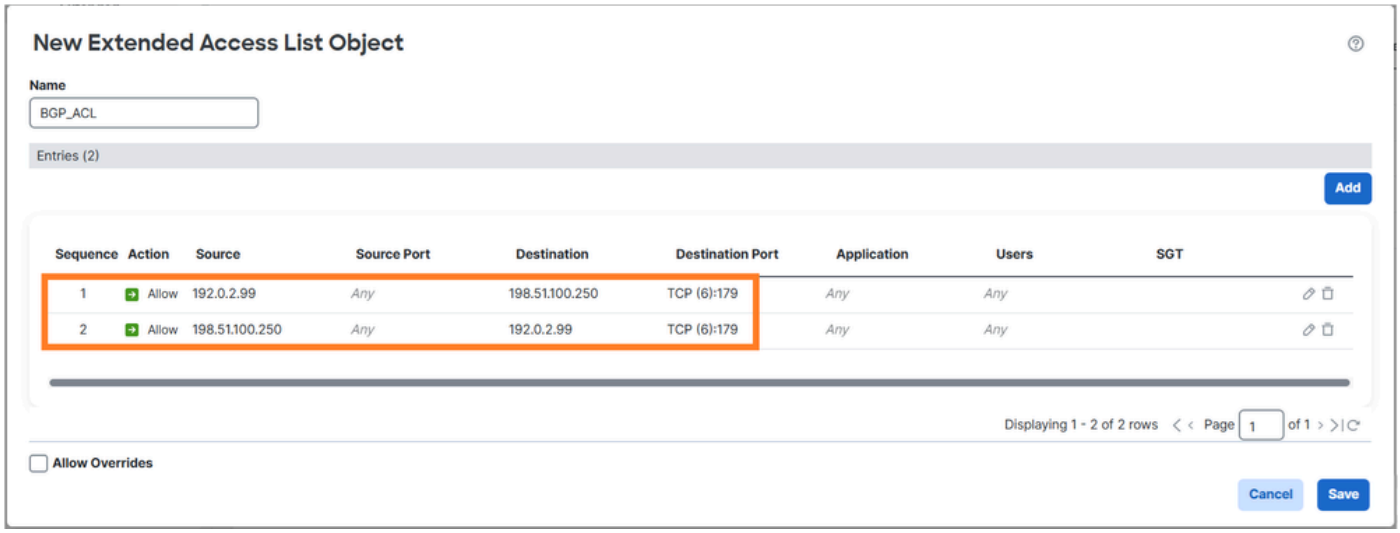
```
firewall#

show run all tcp-map


!
tcp-map UM_STATIC_TCP_MAP
  no check-retransmission
  no checksum-verification
  exceed-mss allow
  queue-limit 0 timeout 4
  reserved-bits allow
```

```
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options mss allow

  tcp-options md5 allow



  ttl-evasion-protection
  urgent-flag allow
  window-variation allow-connection
```

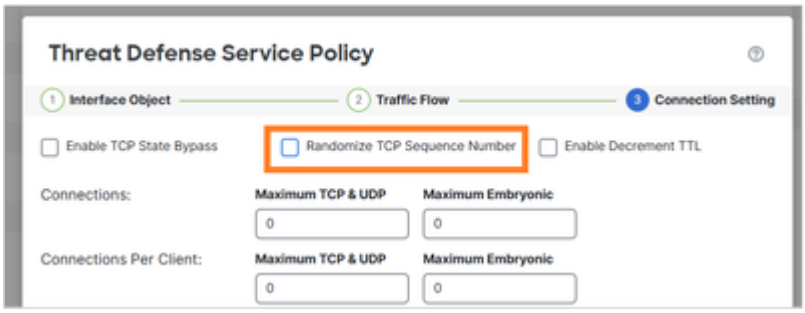
全域性禁用TCP初始序列號(ISN)隨機化：

```
<#root>

>

configure tcp-randomization disable


Building configuration...
Cryptochecksum: f8ac5587 7ccc635e bff886a1 bcab820c

8284 bytes copied in 0.260 secs
[OK]
>
```

或（首選方法）建立與BGP連線匹配的擴展訪問清單：



並使用威脅防禦服務策略禁用TCP序列號隨機化：



驗證

已部署的策略對映配置：

<#root>

```
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 ip-options UM_STATIC_IP_OPTIONS_MAP
```

```
  inspect sip

 class class_map_BGP_ACL



  set connection random-sequence-number disable


 class class_snmp
  inspect snmp
 class class-default
  set connection advanced-options UM_STATIC_TCP_MAP
```

BGP作業階段是透過FTD建立：

```
<#root>

firewall#

show conn long port 179


...

TCP OUTSIDE1: 198.51.100.250/49863 (198.51.100.250/49863) INSIDE: 192.0.2.99/179 (192.0.2.99/179), flags

, idle 44s, uptime 1m40s, timeout 1h0m, bytes 274, flow id 111, Snort id 3, rule id 268439559, Rx-RingN

Initiator: 198.51.100.250, Responder: 192.0.2.99


  Connection lookup keyid: 83487134
```

提示：您可以為BGP流量配置預過濾器快速路徑規則以避免Snort檢測。

任務7.失效連線檢測(DCD)

需求

在FTD上為目的地為主機172.16.3.1的TCP流量設定DCD。

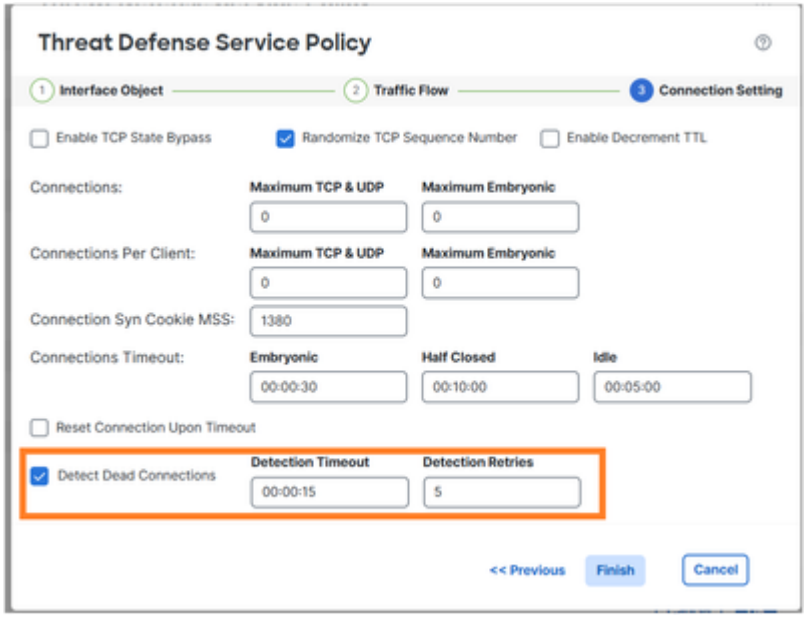
解決方案

DCD記錄在：

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/advanced-access-service-policies.html#id_71048

1.導航到對象>訪問清單，然後建立與所需流量匹配的訪問清單。

2.編輯分配給防火牆的ACP，導航到Advanced選項，然後選擇Threat Defense Service Policy以啟用DCD:



部署的配置：

```
access-list DCD_ACL extended permit object-group ProxySG_ExtendedACL_81604390279 any host 172.16.3.1
!
class-map class_map_DCD_ACL
 match access-list DCD_ACL
policy-map global_policy
 class class_map_DCD_ACL
  set connection timeout dcd
```

工作方式

設定FTD擷取以檢視後端作業：

```
<#root>
firewall#
capture CAPI interface INSIDE match tcp host 172.16.3.1 any

firewall#
capture CAPO interface OUTSIDE1 match tcp host 172.16.3.1 any
```

透過防火牆建立TCP連線：

```
<#root>
firewall#
show conn long address 172.16.3.1 | begin 172.16.3.1

TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7
idle 1m18s
, uptime 1m22s,
timeout 5m0s
, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Internal-Data0/1
  Initiator: 192.0.2.99, Responder: 172.16.3.1

  DCD probes sent: Initiator 0, Responder 0 Connection lookup keyid: 76292550
```

最初，防火牆擷取中並未顯示DCD封包：

```
<#root>
firewall#
```

show capture

capture CAPI type raw-data interface INSIDE [

Capturing - 0 bytes

]
  match tcp host 172.16.3.1 any
capture CAPO type raw-data interface OUTSIDE1 [

Capturing - 0 bytes

]
  match tcp host 172.16.3.1 any

當閒置連線達到閒置逾時時，FTD會將偽造的TCP ACK訊息傳送到來源和目的地：

<#root>

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1

TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 4m59s

, uptime 5m3s, timeout 5m0s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Inte
  Initiator: 192.0.2.99, Responder: 172.16.3.1
  DCD probes sent: Initiator 0, Responder 0 Connection lookup keyid: 76292550

firewall#

show conn long address 172.16.3.1 | begin 172.16.3.1

TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 0s

, uptime 5m3s, timeout 15s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Inter
  Initiator: 192.0.2.99, Responder: 172.16.3.1

DCD probes sent: Initiator 1

, Responder 0 Connection lookup keyid: 76292550

```
firewall#

 show conn long address 172.16.3.1 | begin 172.16.3.1


TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7
  Initiator: 192.0.2.99, Responder: 172.16.3.1


DCD probes sent: Initiator 1, Responder 1

 Connection lookup keyid: 76292550
```

如果兩個回覆均被重置，則重置空閒計時器：

<#root>

```
firewall#

show capture CAPI



3 packets captured

1: 09:01:30.433952 802.1Q vlan#101 P0 172.16.3.1.23 > 192.0.2.99.23241: . ack 3271882019 win 32757
2: 09:01:30.434334 802.1Q vlan#101 P0

192.0.2.99.23241 > 172.16.3.1.23: . ack 1746306341 win 32746


3: 09:01:30.955654 802.1Q vlan#101 P0 172.16.3.1.23 > 192.0.2.99.23241: . ack 3271882019 win 32757
3 packets shown
firewall#

 show capture CAPO



3 packets captured

1: 09:01:30.434364 802.1Q vlan#201 P0 192.0.2.99.23241 > 172.16.3.1.23: . ack 111661490 win 32746
2: 09:01:30.955288 802.1Q vlan#201 P0 192.0.2.99.23241 > 172.16.3.1.23: . ack 111661490 win 32746
3: 09:01:30.955639 802.1Q vlan#201 P0

172.16.3.1.23 > 192.0.2.99.23241: . ack 3875469573 win 32757


3 packets shown

firewall#
```

```
show conn long address 172.16.3.1 | begin 172.16.3.1


TCP OUTSIDE1: 172.16.3.1/23 (172.16.3.1/23) INSIDE: 192.0.2.99/23241 (192.0.2.99/23241), flags UIO N1N7

idle 1m29s


, uptime 6m33s, timeout 5m0s, bytes 129, flow id 127, Snort id 4, rule id 268439559, Rx-RingNum 13, Int
  Initiator: 192.0.2.99, Responder: 172.16.3.1
  DCD probes sent: Initiator 1, Responder 1 Connection lookup keyid: 76292550
```

附註：DCD在解除安裝的連線上不起作用（「o」標誌）。

相關資訊

https://www.cisco.com/c/en/us/td/docs/security/secure-firewall/management-center/device-config/100/management-center-device-config-10-0/advanced-access-service-policies.html#id_71048

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）。