Firewall Threat Defense Modular Policy Framework configureren

Inhoud

Inleiding

Dit document beschrijft het Modular Policy Framework (MPF) van Firewall Threat Defense (FTD)

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten voor dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco Secure Firewall 3130 Threat Defense versie 10.0.0 (build 140)
- Firewall Management Center (FMC) versie 10.0.0 (build 140)

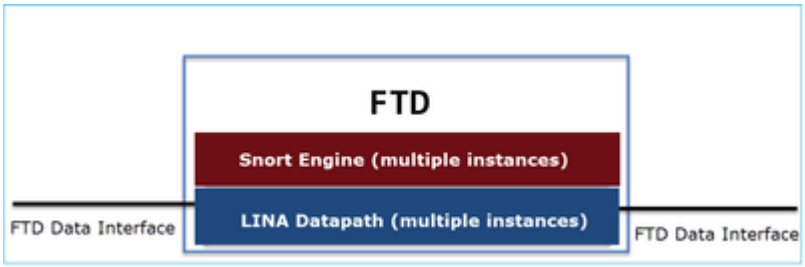
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Overzicht van het FTD-gegevensvlak

FTD is een unified software-image die bestaat uit twee hoofd-engines:

- Datapath (ook bekend als LINA)
- Snort-engine



De LINA Datapath en de Snort Engine zijn de belangrijkste onderdelen van het FTD Data Plane.

MPF Ingrediënten

MPF gebruikt deze componenten:

- Class-map komt overeen met het interessante verkeer.
- Policy-map past acties toe op het interessante verkeer dat overeenkomt met de klassenkaart.
- Service-policy past de policy-map globaal (op alle interfaces) of op een specifieke interface toe.

Kenmerkgerichtheid

Raadpleeg de configuratiegids van de ASA voor informatie over de richting van de functies:

https://www.cisco.com/c/en/us/td/docs/security/asa/asa924/configuration/firewall/asa-924-firewall-config/inspect-service-policy.html

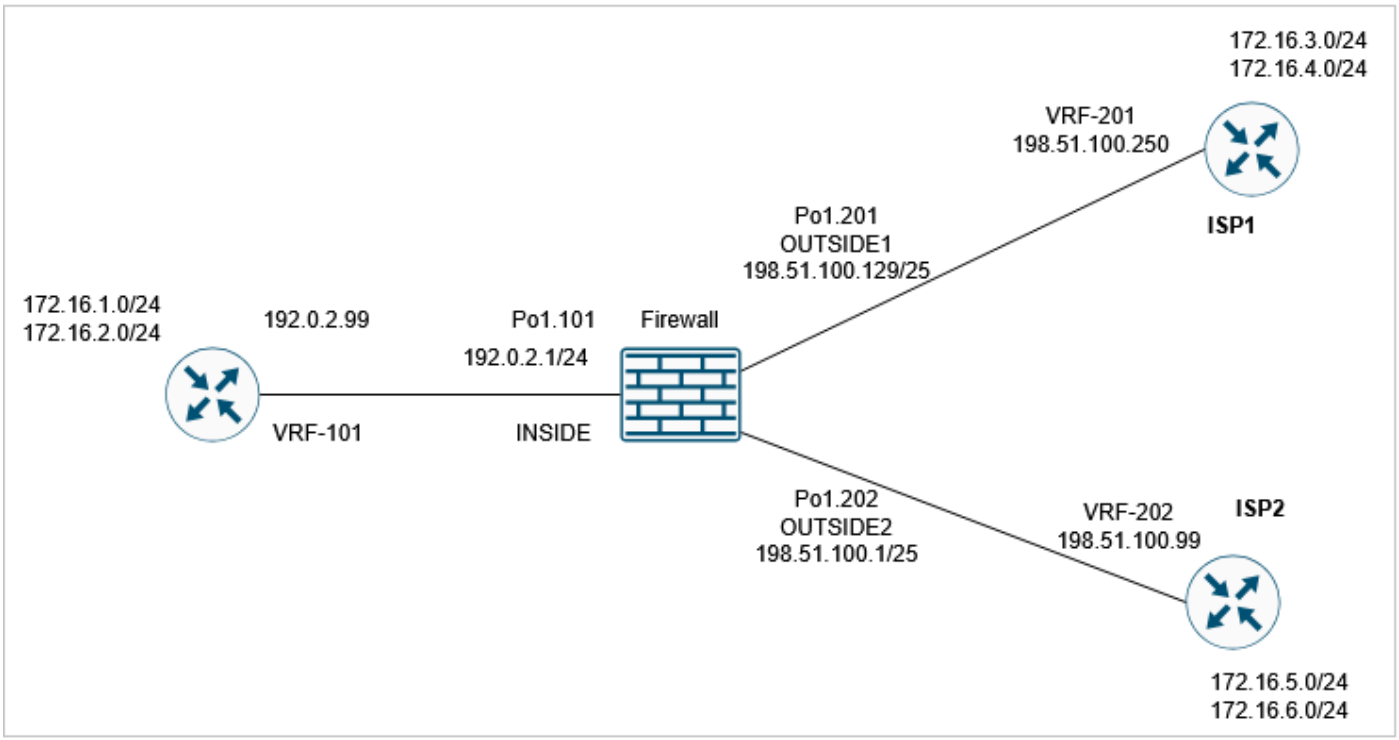
De kenmerken in verband met de FTD worden belicht:

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

Configureren

Topologie



De standaard MPF-configuratie (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
```

Taak 1. SIP-inspectie wereldwijd uitschakelen op FTD

De vereiste in deze taak is om SIP-inspectie in de FTD LINA-motor uit te schakelen. Een reden kan een beleidsvereiste zijn of een softwarefout met betrekking tot SIP die van invloed is op het transitverkeer.

Oplossing

Voordat u SIP-inspectie uitschakelt, moet u eerst bevestigen dat het wordt toegepast op transitoverkeer:

<#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

Er zijn 2 manieren om SIP-inspectie wereldwijd uit te schakelen:

Oplossing 1: SIP uitschakelen vanuit FTD CLISH CLI

<#root>

>

configure inspection sip disable

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

7818 bytes copied in 0.250 secs
[OK]

Verificatie

<#root>

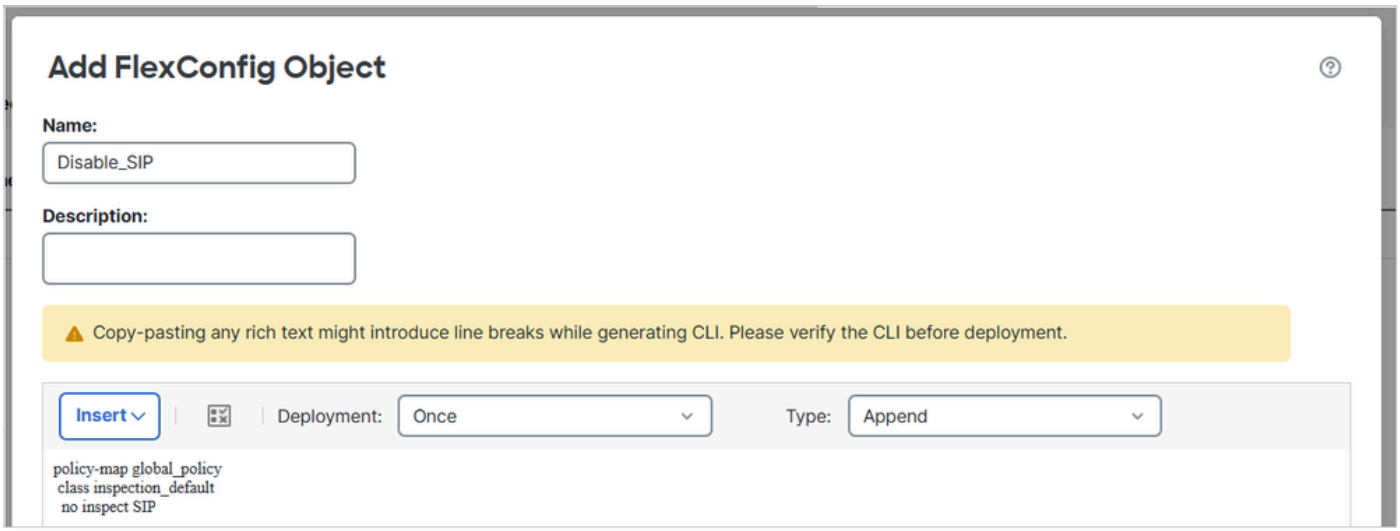
>

show running-config policy-map | include sip

>

Oplossing 2: SIP uitschakelen met FlexConfig

Navigeer in FMC naar Apparaten > FlexConfig en maak een FlexConfig-object:




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

toepassen Selecteer het FlexConfig-beleid en selecteer Voorbeeldconfiguratie om een voorbeeld te bekijken:

Tot slot: implementeer het beleid.

Verificatie

<#root>

```
firewall#

show run policy-map | include sip

firewall#
```

Opmerking – U moet de bestaande SIP-verbinding wissen uit de LINA-verbindingstabel, zodat de verbindingen opnieuw tot stand worden gebracht zonder SIP-inspectie. U kunt deze opdracht gebruiken om de bestaande SIP-verbindingen te controleren:

<#root>

```
firewall#

show conn port 5060
```

Taak 2. SIP-inspectie voor specifieke hosts uitschakelen

In deze taak is de vereiste om SIP-inspectie uit te schakelen voor verkeer tussen deze netwerken:

- SRC: 172.16.1.0/24
- DST: 172.16.3.0/24

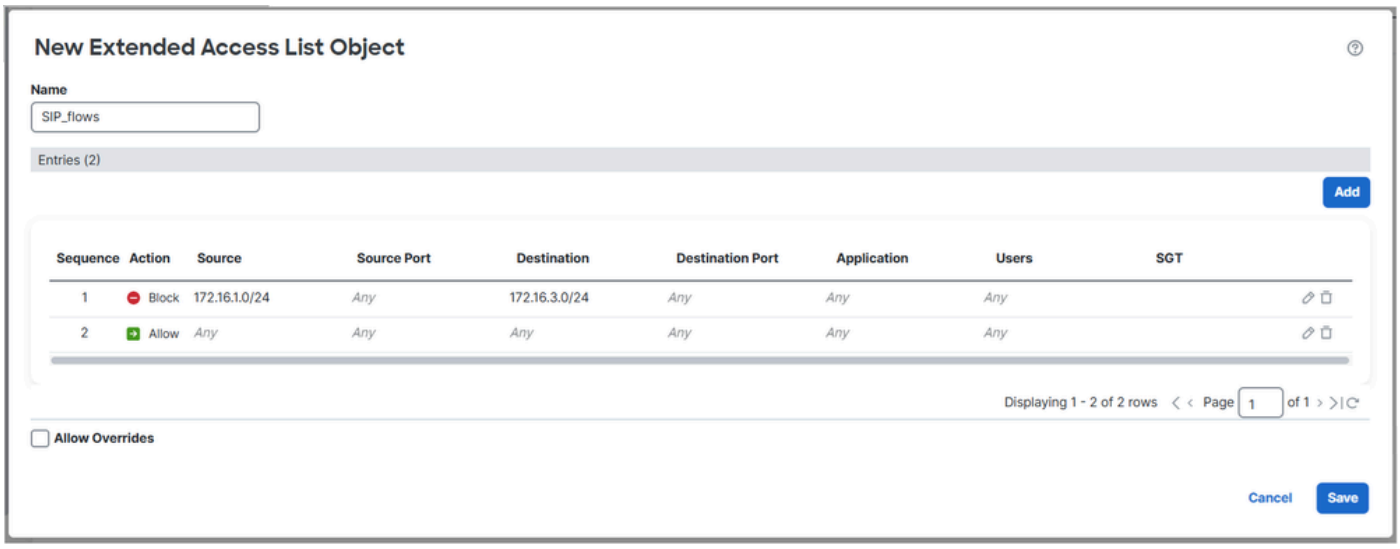
Een reden om dit te doen kan een softwaredefect zijn dat verband houdt met SIP en dat van invloed is op het transitverkeer

Oplossing

Gebruik FlexConfig.

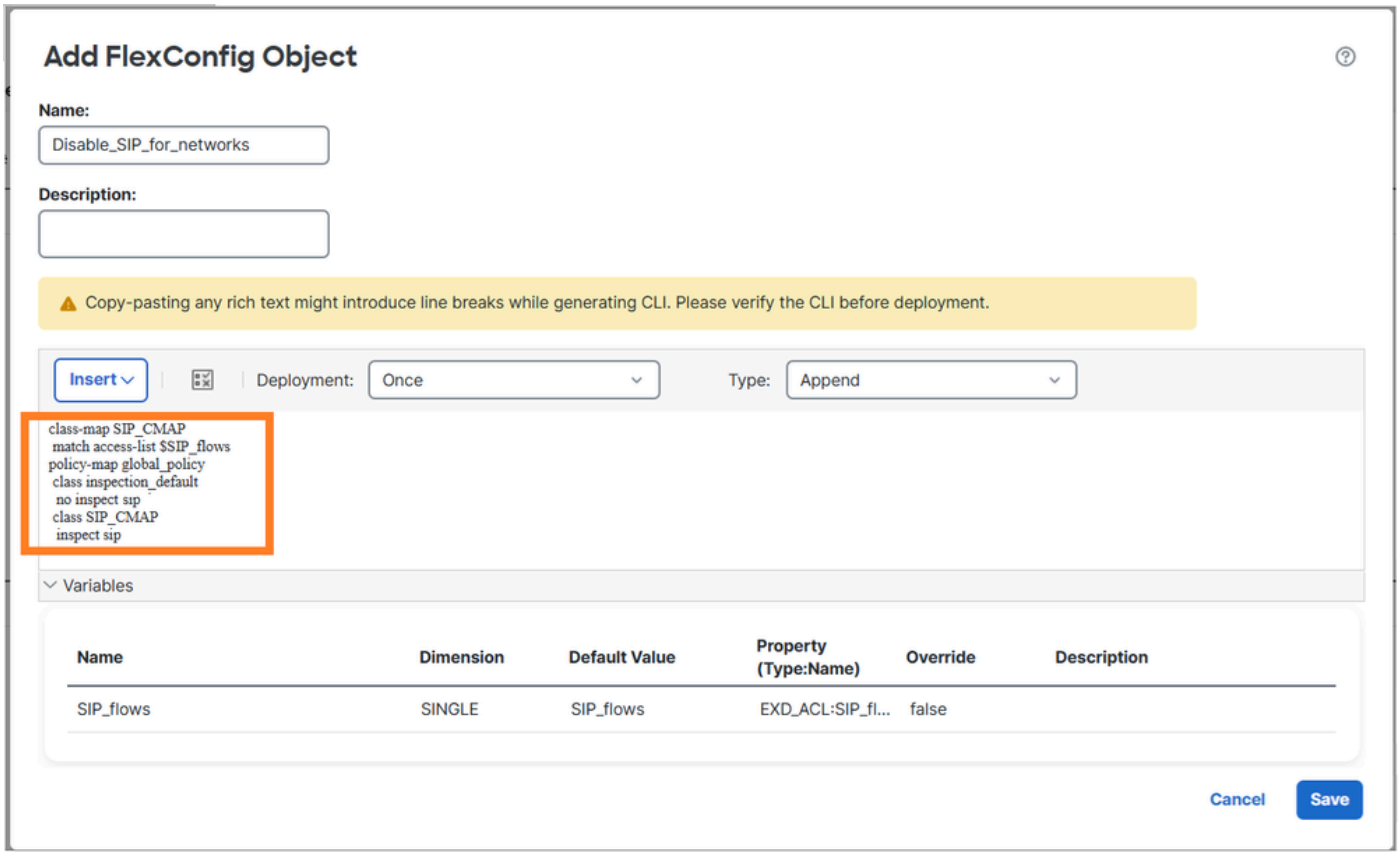
Stap 1

Navigeer naar Objecten > Toegangslijst > Uitgebreid en maak een uitgebreide toegangslijst die overeenkomt met het interessante verkeer. U moet de Block-actie gebruiken omdat het doel is om het specifieke verkeer uit te sluiten. Voeg daarnaast een regel Toestaan toe om overeen te komen met de rest van het verkeer:



Stap 2

Maak een FlexConfig-object met een klassentoewijzing die overeenkomt met de SIP Access Control List (ACL) en pas dit toe in het global_policy:



Het geconfigureerde object FlexConfig:

```
class-map SIP_CMAP
 match access-list $SIP_flows
```

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

Opmerking

Bij het configureren van de vergunning ACL proberen zo specifiek mogelijk (bijvoorbeeld put protocol poorten) om eventuele CPU impact te voorkomen. Het voorbeeld in deze taak specificeert geen protocolpoorten en kan in de productie worden vermeden.

Verificatie 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
```

Verificatie 2

Verkeer dat niet wordt geïnspecteerd door SIP-inspectie heeft 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
...
```

Verkeer dat wordt geïnspecteerd door SIP-inspectie heeft 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,
...
```

Verificatie 3

De "sip"-inspectieteller wordt verhoogd wanneer een pakket wordt geïnspecteerd door de firewall:

<#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

...
```

Taak 3. TCP State Bypass configureren voor specifieke hosts

In deze taak is het vereiste om TCP-statusbypass in te schakelen voor verkeer tussen deze netwerken:

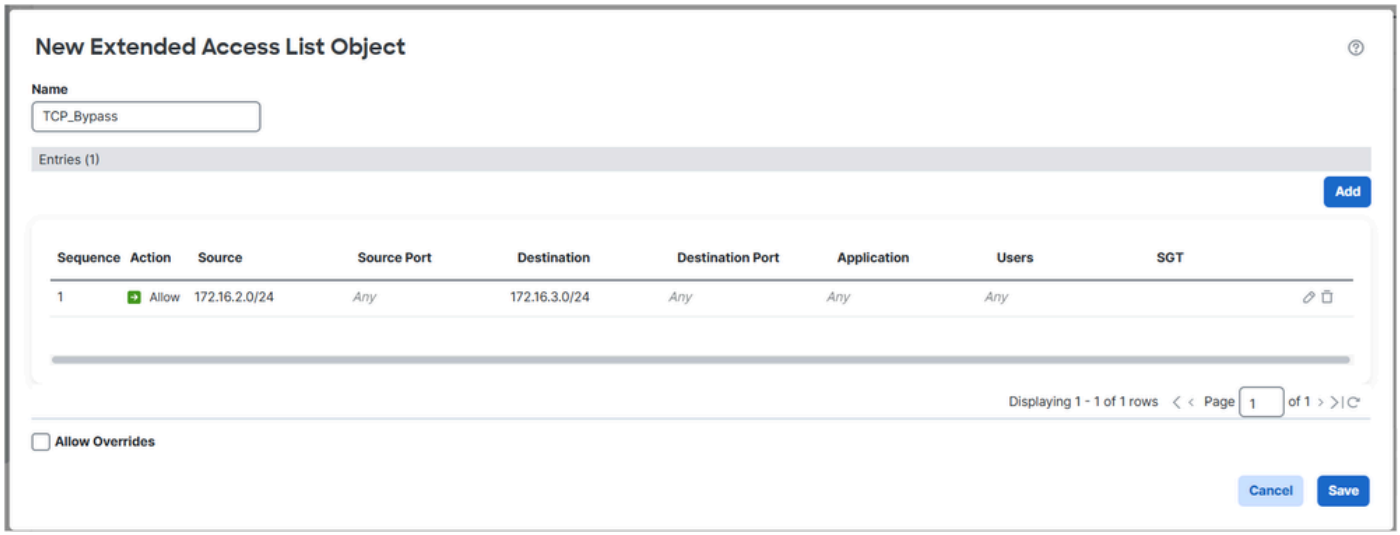
- SRC: 172.16.2.0/24
- DST: 172.16.3.0/24

In het algemeen wordt het niet aanbevolen om TCP state bypass te gebruiken, maar het kan worden gebruikt als een tijdelijke oplossing voor het omgaan met asymmetrische stromen.

Oplossing 1

Stap 1

Maak een uitgebreide ACL die overeenkomt met het interessante verkeer:

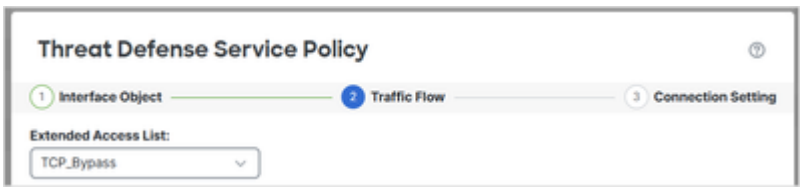


Stap 2

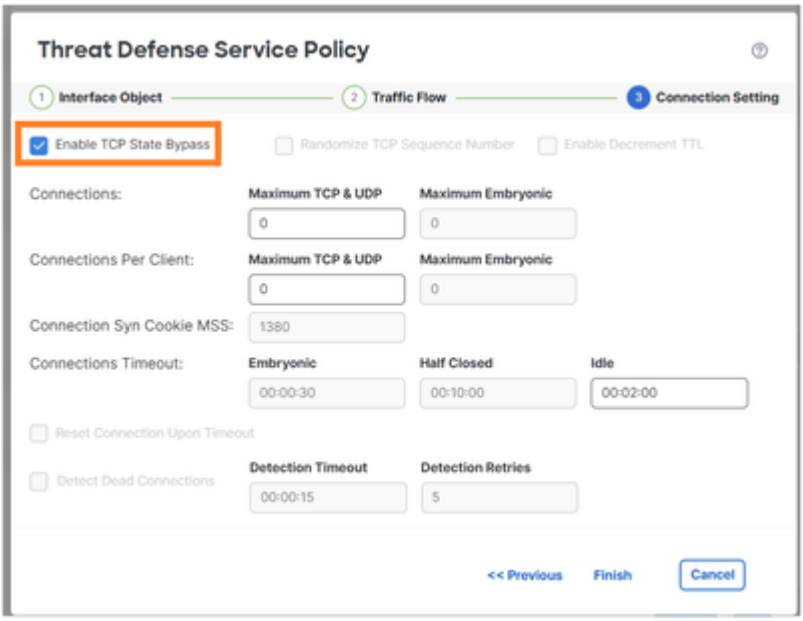
Bewerk het toegangscontrolebeleid (Access Control Policy, ACP) dat is toegewezen aan de FTD, selecteer het tabblad Geavanceerde instellingen en bewerk het beleid voor de bedreigingsverdedigingsdienst. Selecteer Regel toevoegen en Volgende.

Stap 3

Selecteer de uitgebreide ACL:



Stap 4



Stap 5

Selecteer Voltooien, OK, Opslaan en Implementeren.

Het resultaat:

<#root>

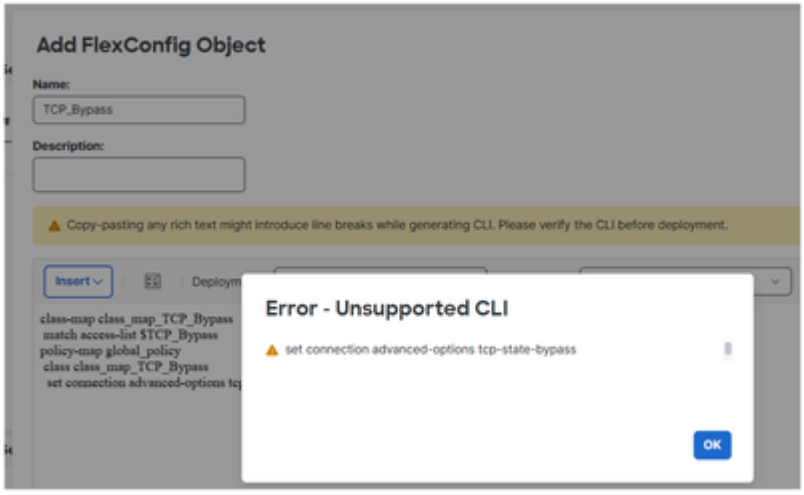
```
firewall#

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
```

Opmerking: In eerdere FMC-releases zoals 6.x kunt u FlexConfig gebruiken om de TCP-statusbypass te configureren. In nieuwere versies wordt dit niet ondersteund:



Verificatie

<#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:
```

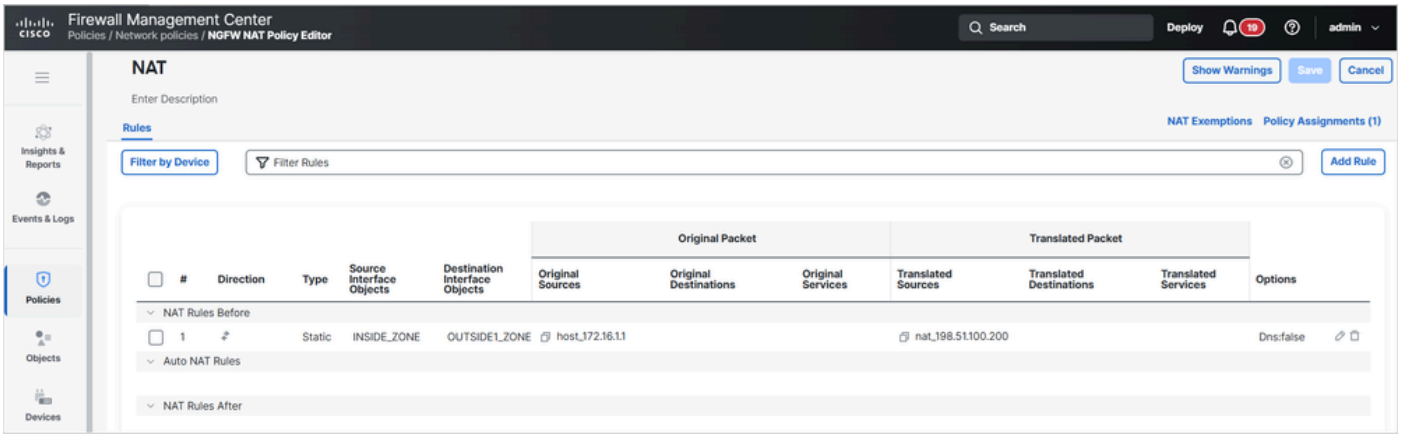
```
class-map class_map_TCP_Bypass
```

```
 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
...
```

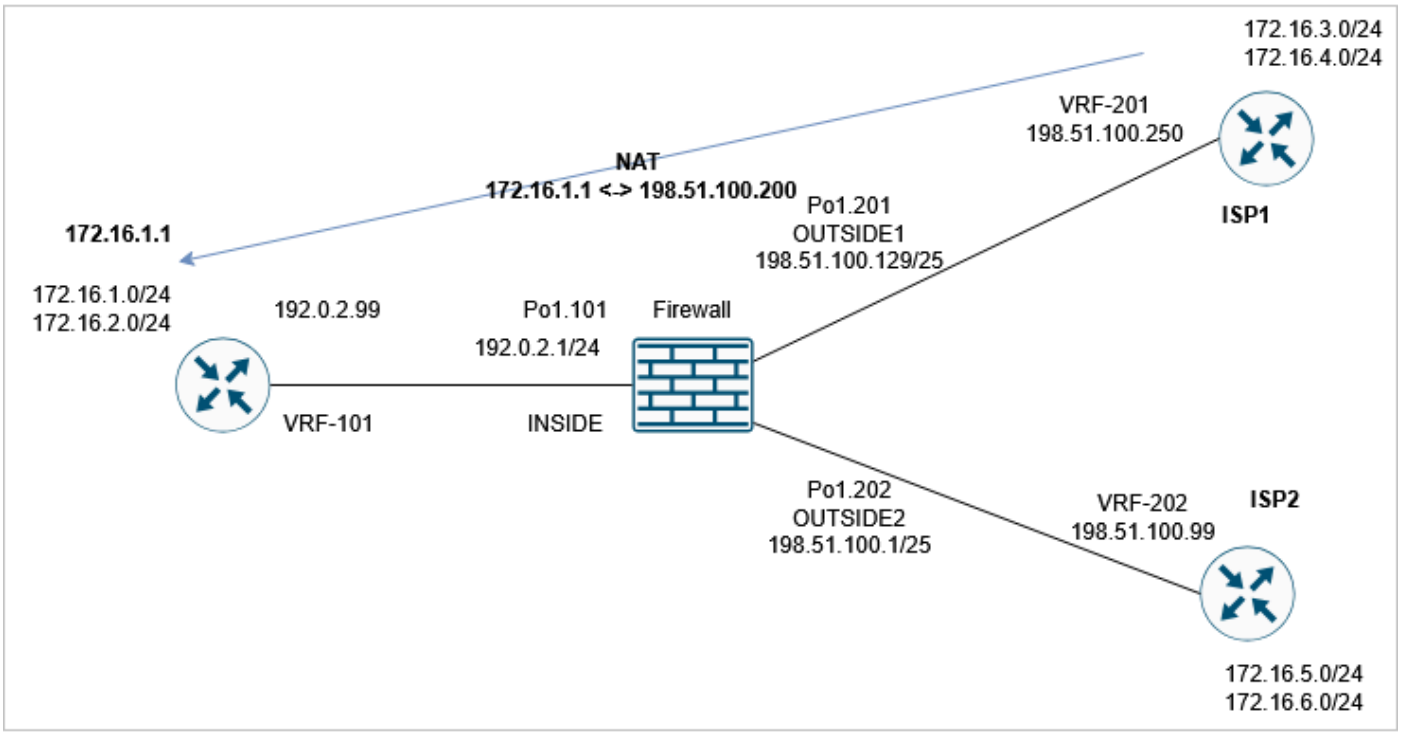
Taak 4. Uitvoerwijziging traceroute

Voorwaarde

Configureer statische NAT op FTD zodat IP 172.16.1.1 achter de INSIDE-interface wordt weergegeven als 198.51.100.200 op OUTSIDE1-hosts:



Voer vervolgens een traceroute uit van ISP1 naar 198.51.100.200 (host 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 *
```

eis

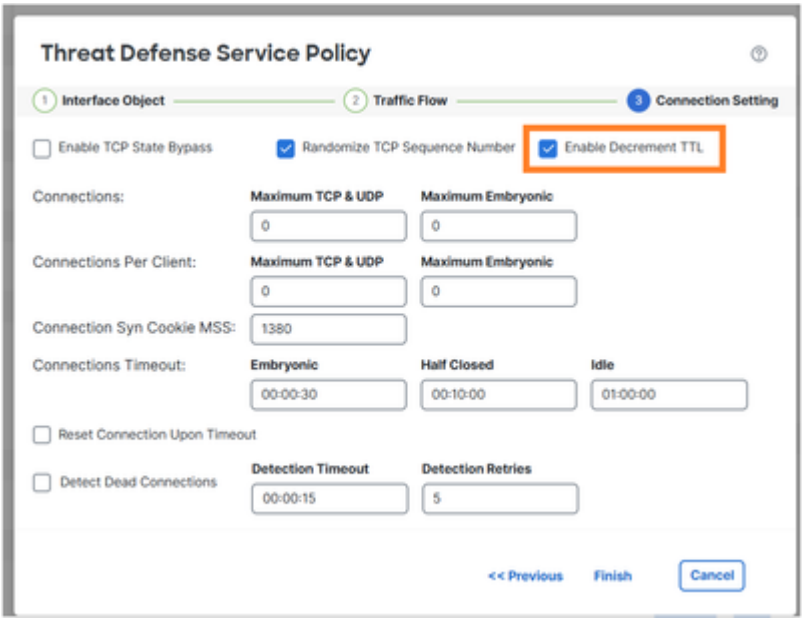
Wijzig de FTD-configuratie zodat de traceroute overeenkomt met deze uitvoer:

<#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 *
```

Oplossing

De oplossing bestaat uit twee configuratiestappen:
1. De TTL verlagen:



Na deze wijziging onthult de traceroute de firewall hop:

<#root>

router1#

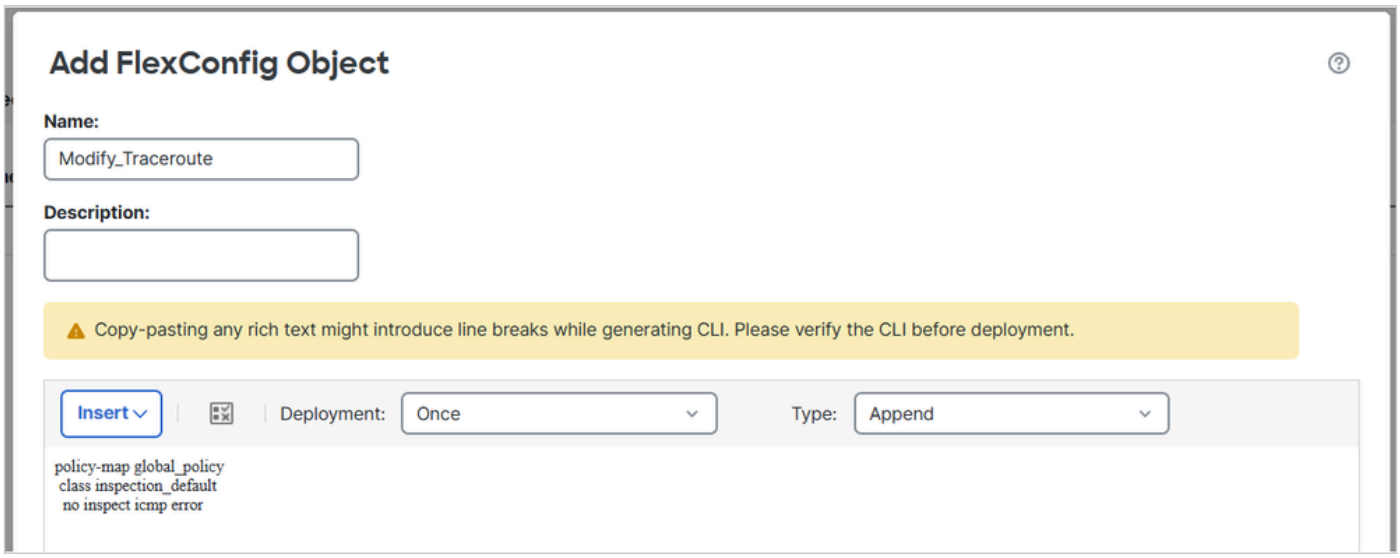
traceroute vrf VRF-201 198.51.100.200

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. Schakel ICMP-foutinspectie uit:




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

Verificatie

De traceroute toont het vertaalde NAT IP-adres van de externe host en het IP-adres van de FTD-interface:

<#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 *
```

Taak 5. Verbindingstime-outs instellen

eis

Wijzig de time-out in 1 week voor deze stroom:

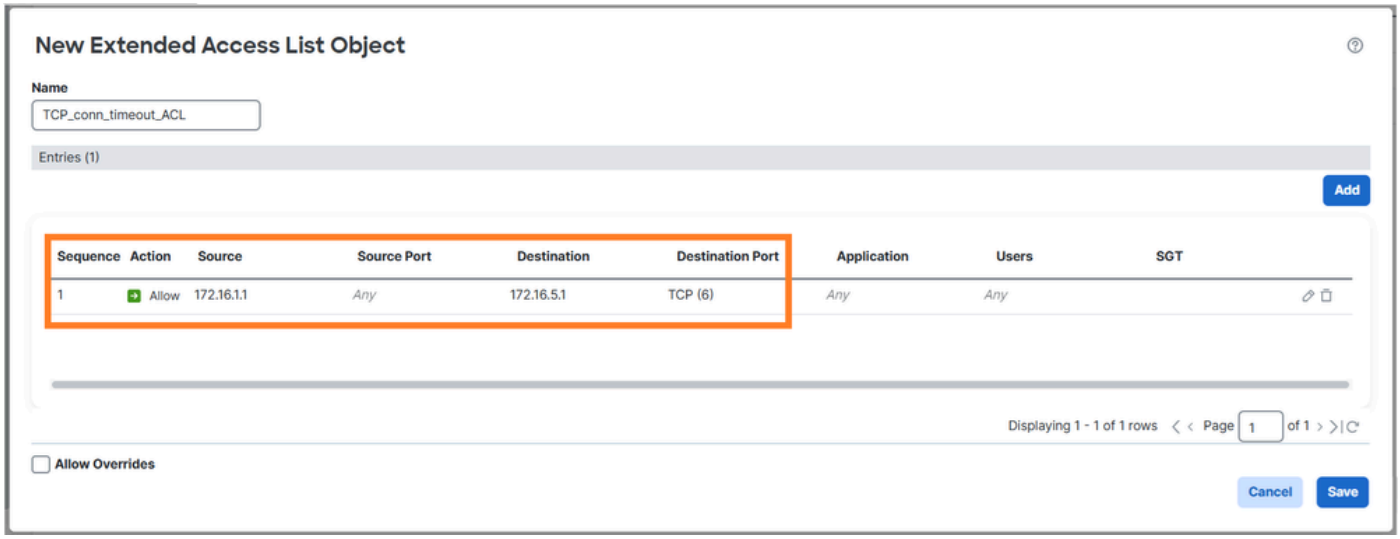
- Protocol: TCP
- SRC: 172.16.1.1
- DST: 172 16 5 1

Oplossing

Om de time-out per flow in te stellen, moet u Servicebeleid gebruiken.

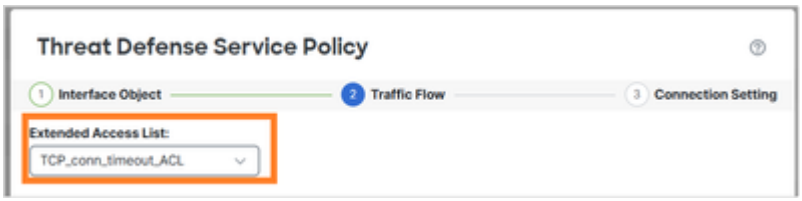
Stap 1

Navigeer naar Objecten > Toegangslijst en maak een uitgebreide ACL die overeenkomt met het interessante verkeer:

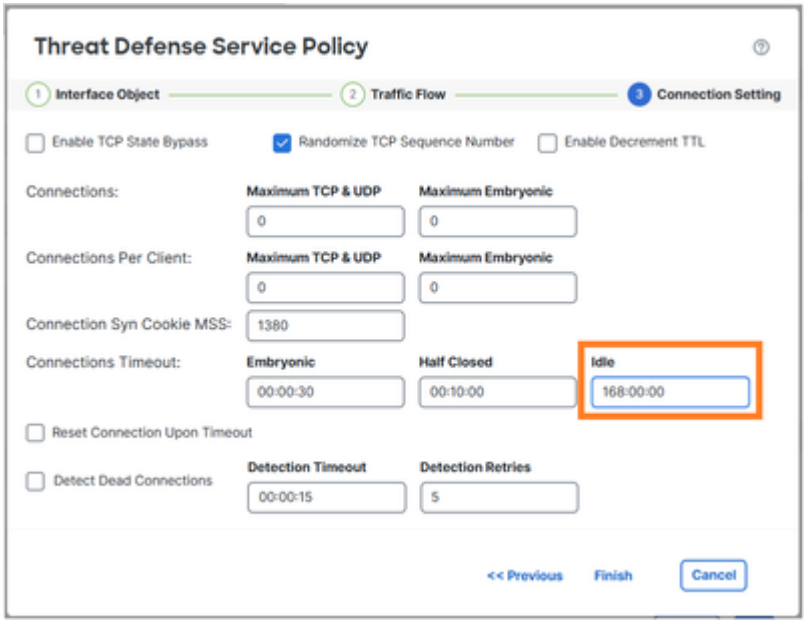


Stap 2

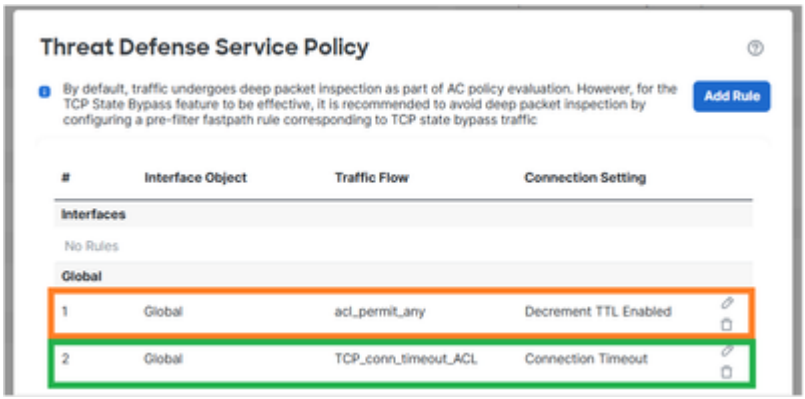
Configureer een MPF-beleid dat gebruikmaakt van de ACL die is gemaakt in stap 1:



De time-out voor inactieve verbinding instellen:



Verwijder de regel uit de vorige taak omdat deze overlapt met de nieuwe vereiste:



Verificatie

De configuratie van de geïmplementeerde beleidskaart:

<#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
```

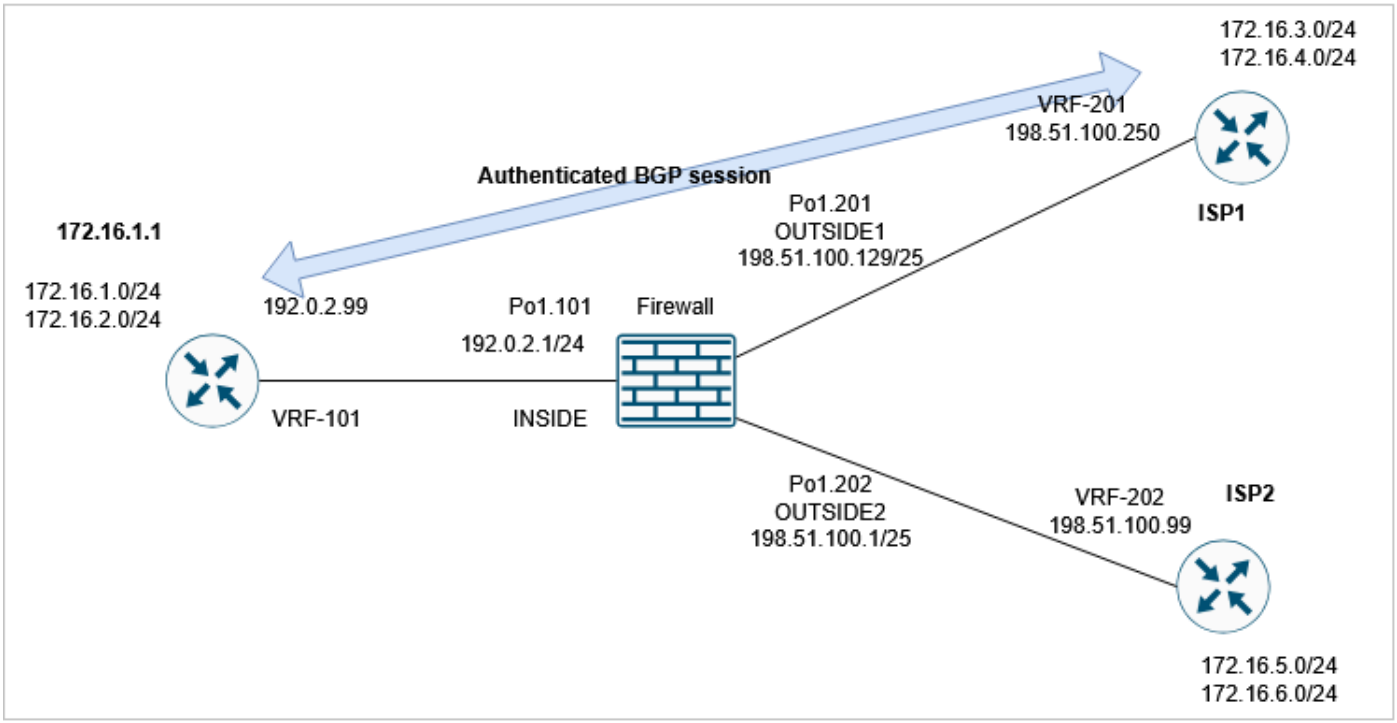
Start een nieuwe TCP-verbinding van 172.16.1.1 tot 172.16.5.1 en controleer de verbindingstabel van de FTD:

```
<#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
```

Taak 6. BGP-verificatie via FTD

Voorwaarde

Configureer een BGP-sessie via de FTD. De BGP-sessie moet authenticatie gebruiken.



Verificatie

Met de standaard FTD-configuratie wordt de BGP-sessie niet ingesteld. Op de router ziet u:

<#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)
```

Op de FTD ziet u dat beide partijen er niet in slagen de BGP TCP-verbinding tot stand te brengen (de verbindingsvlaggen geven aan dat alleen TCP SYN-pakketten worden ontvangen):

<#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
```

Oplossing

Om een geauthenticeerde BGP-sessie via het FTD mogelijk te maken, moet aan deze 2 voorwaarden worden voldaan:

1. TCP MD5 (optie 19) moet via het FTD worden toegestaan.
2. Randomisatie van TCP-volgnummers moet worden uitgeschakeld.

De optie TCP MD5 is standaard toegestaan:

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
```

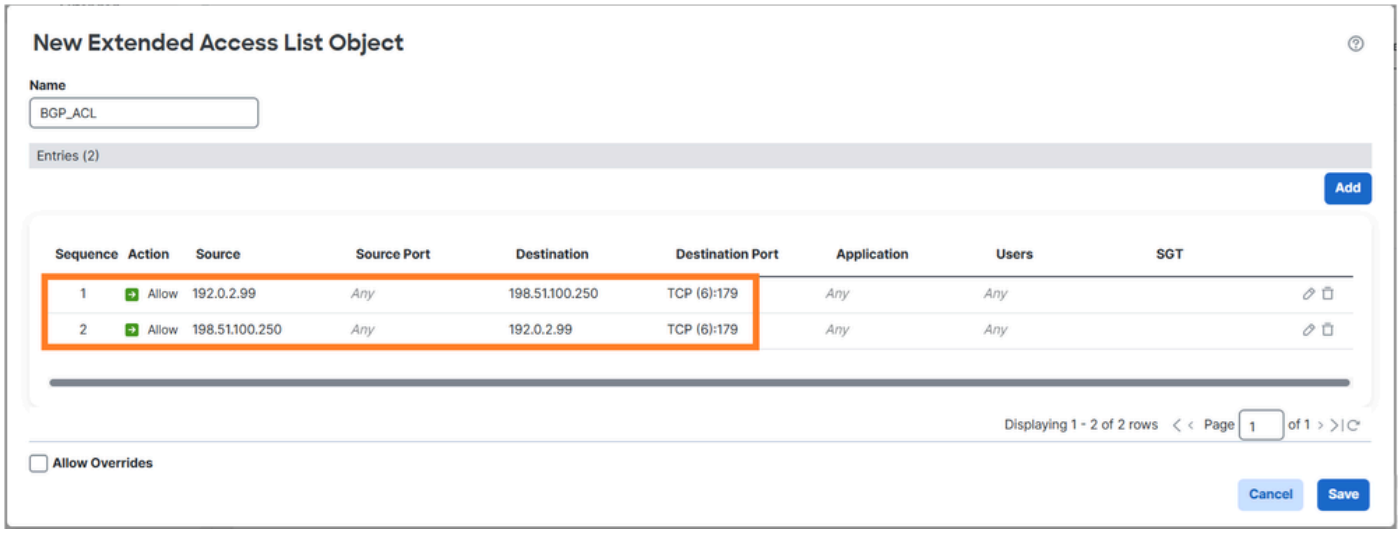
```
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options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

  tcp-options md5 allow



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

Randomisatie van het initieel volgnummer (ISN) van TCP wereldwijd uitschakelen:

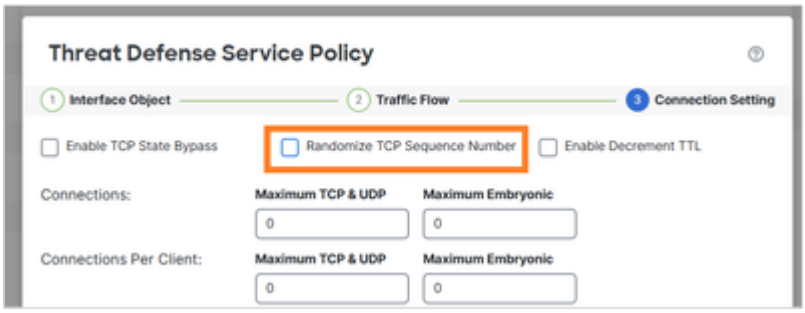
<#root>

```
>

configure tcp-randomization disable


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

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

of (de voorkeursmethode) u maakt een uitgebreide toegangslijst die overeenkomt met de BGP-verbinding:



en schakel de TCP-volgnummerrandomisatie uit met behulp van het Threat Defense Service Policy:



Verificatie

De configuratie van de geïmplementeerde beleidskaart:

<#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
```

De BGP-sessie wordt vastgesteld door middel van FTD:

<#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
```

Tip: U kunt een voorfilterregel voor het snelpad configureren voor het BGP-verkeer om Snort-inspectie te voorkomen.

Taak 7. Dead Connection Detection (DCD)

eis

Configureer DCD op FTD voor TCP-verkeer bestemd voor host 172.16.3.1.

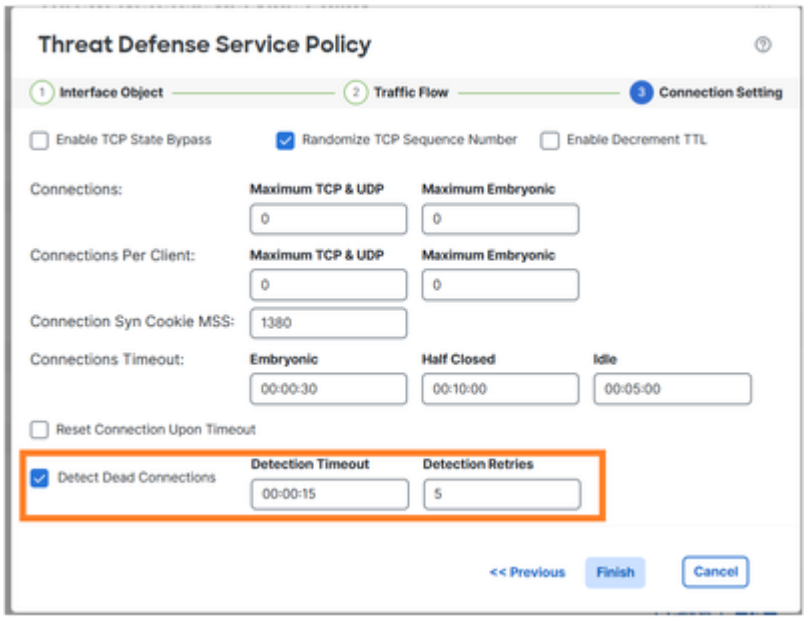
Oplossing

DCD is gedocumenteerd op:

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. Navigeer naar Objecten > Toegangslijst en maak een toegangslijst die overeenkomt met het interessante verkeer.

2. Bewerk de ACP die aan uw firewall is toegewezen, ga naar Geavanceerde opties en selecteer Beleid voor bedreigingsverdedigingsservice om DCD in te schakelen:



De geïmplementeerde configuratie:

```
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
```

Hoe het werkt

Configureer FTD-opnamen om de back-endbewerking te bekijken:

```
<#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
```

Maak een TCP-verbinding via de firewall:

```
<#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
```

In eerste instantie worden er geen DCD-pakketten weergegeven in de firewall-opnamen:

```
<#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
```

Wanneer een inactieve verbinding de inactieve time-out bereikt, verzendt de FTD vervalste TCP ACK-berichten naar de bron en bestemming:

```
<#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, Interr
  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

Als beide antwoorden, wordt de inactieve timer opnieuw ingesteld:

<#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
```

Opmerking: DCD werkt niet op geoffloade verbindingen ('o'-vlag).

Gerelateerde informatie

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.