Configuración del marco de políticas modulares de Firewall Threat Defence

Contenido

Introducción

Este documento describe el Marco de políticas modular (MPF) de Firewall Threat Defence (FTD)

Prerequisites

Requirements

No existen requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cisco Secure Firewall 3130 Threat Defence Versión 10.0.0 (Compilación 140)
- Firewall Management Center (FMC) versión 10.0.0 (Compilación 140)

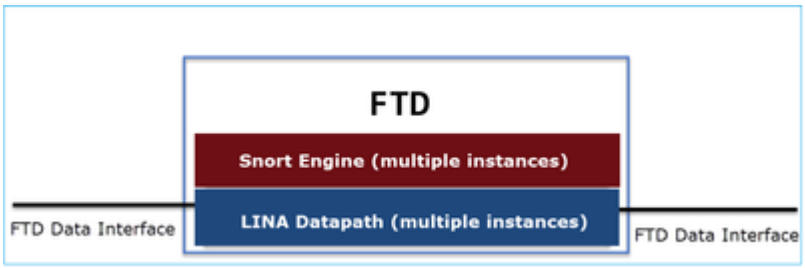
La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Visión General del Plano de Datos FTD

FTD es una imagen de software unificada que consta de 2 motores principales:

- Ruta de datos (también conocida como LINA)
- Motor Snort



La ruta de datos LINA y el motor Snort son las partes principales del plano de datos del FTD.

MPF Ingredientes

MPF utiliza estos componentes:

- class-map coincide con el tráfico interesante.
- policy-map aplica acciones al tráfico interesante coincidente con el class-map.
- service-policy aplica el policy-map globalmente (en todas las interfaces) o en una interfaz específica.

Direccionalidad de funciones

En cuanto a la direccionalidad de las funciones, consulte la guía de configuración de ASA:

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

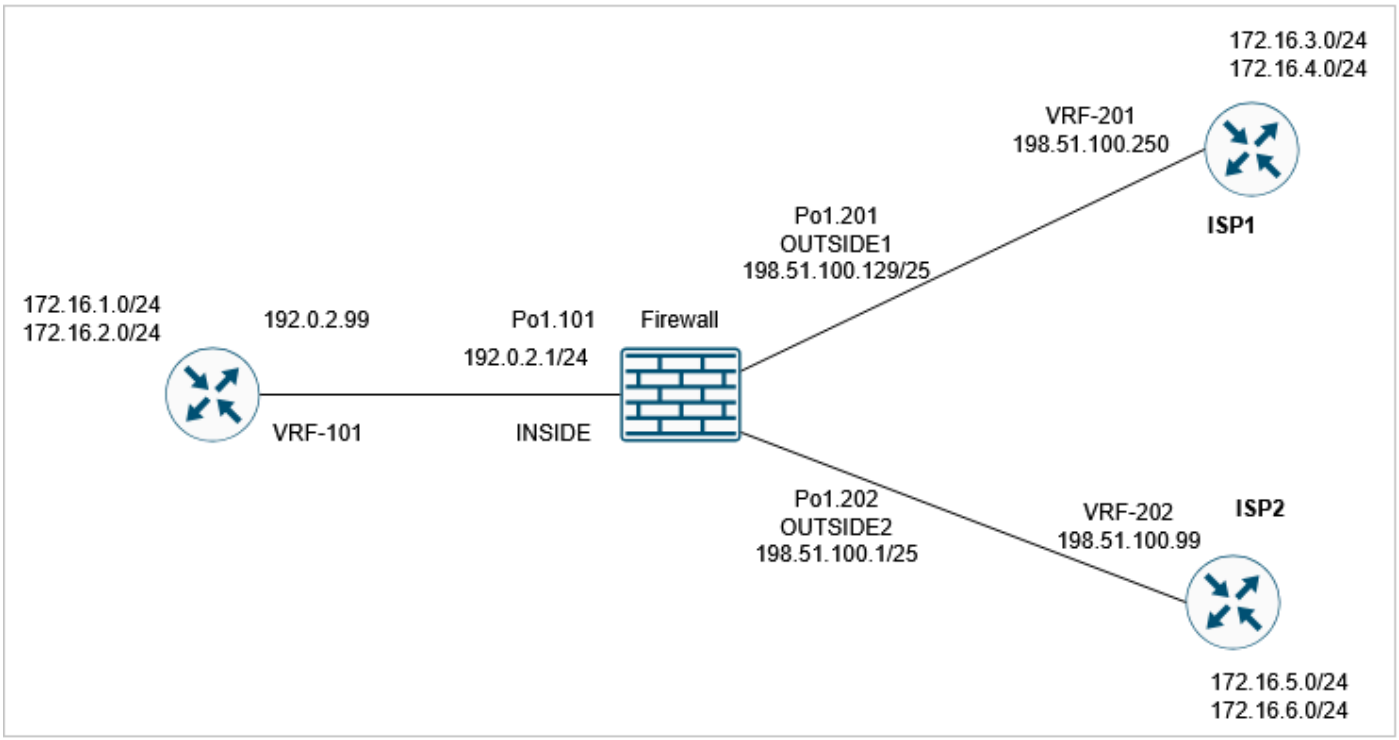
Se resaltan las funciones relacionadas con el FTD:

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

Configurar

Topología



La configuración predeterminada de MPF (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
```

Tarea 1. Desactivar globalmente la inspección de SIP en FTD

El requisito en esta tarea es inhabilitar la inspección SIP en el motor FTD LINA. Una razón puede ser un requisito de política o un defecto de software relacionado con SIP que afecta al tráfico de tránsito.

Solución

Antes de desactivar la inspección SIP, confirme primero que se aplica al tráfico de tránsito:

<#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

Existen 2 formas de deshabilitar globalmente la inspección de SIP:

Solución 1: Desactivar SIP de CLI de FTD CLISH

<#root>

>

configure inspection sip disable

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

7818 bytes copied in 0.250 secs
[OK]

Verificación

<#root>

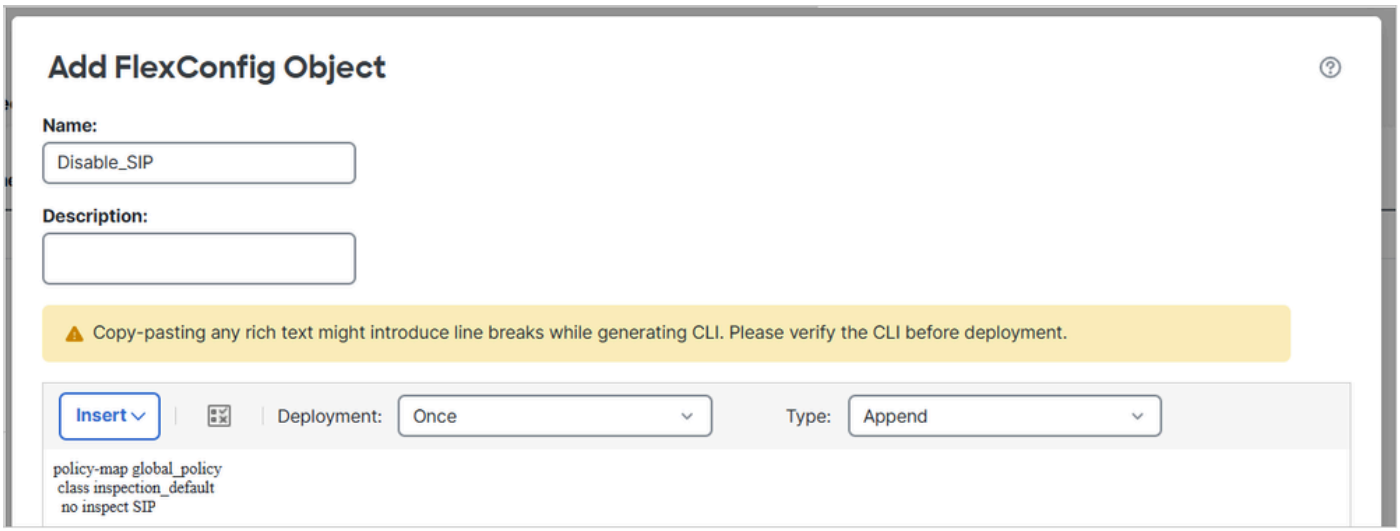
>

show running-config policy-map | include sip

>

Solución 2: Desactivar SIP mediante FlexConfig

En FMC, navegue hasta Devices > FlexConfig y cree un objeto FlexConfig:




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

Aplicar Utilice la política FlexConfig y seleccione Preview Config para obtener una vista previa de la misma:

Por último, implemente la política.

Verificación

<#root>

```
firewall#

show run policy-map | include sip

firewall#
```

Nota - Debe borrar la conexión SIP existente de la tabla de conexión LINA para que las conexiones se restablezcan sin inspección SIP. Puede utilizar este comando para verificar las conexiones SIP existentes:

<#root>

```
firewall#

show conn port 5060
```

Tarea 2. Desactivar la inspección de SIP para hosts específicos

En esta tarea, el requisito es inhabilitar la inspección SIP para el tráfico entre estas redes:

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

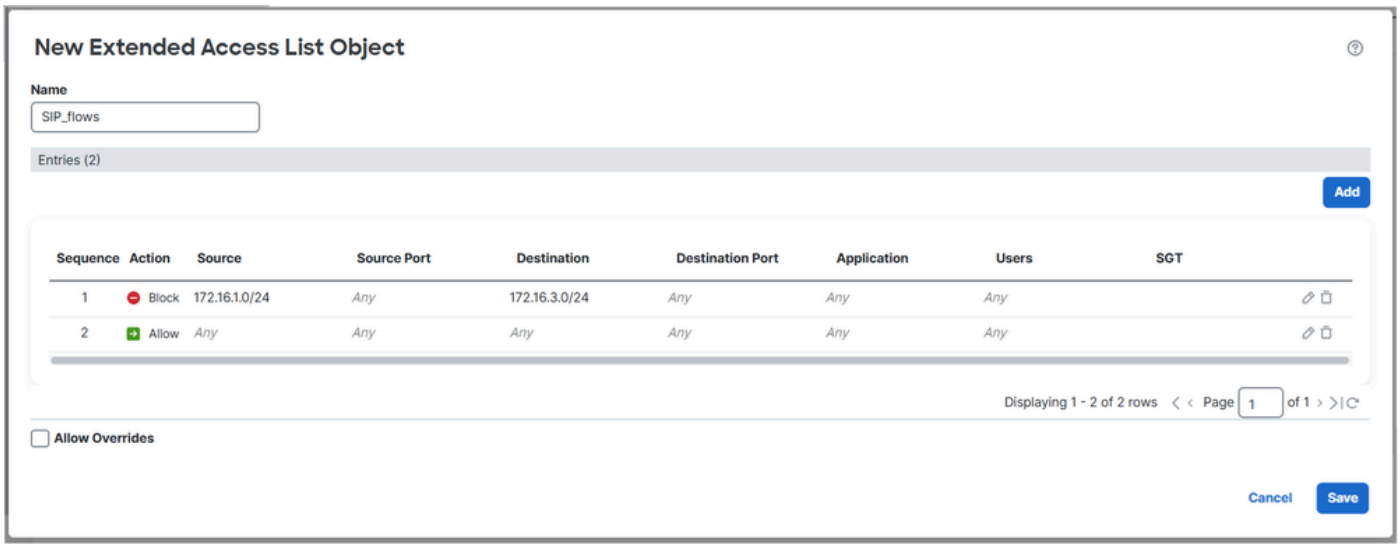
Una razón para hacer esto puede ser un defecto de software relacionado con SIP que afecta el tráfico de tránsito

Solución

Utilice FlexConfig.

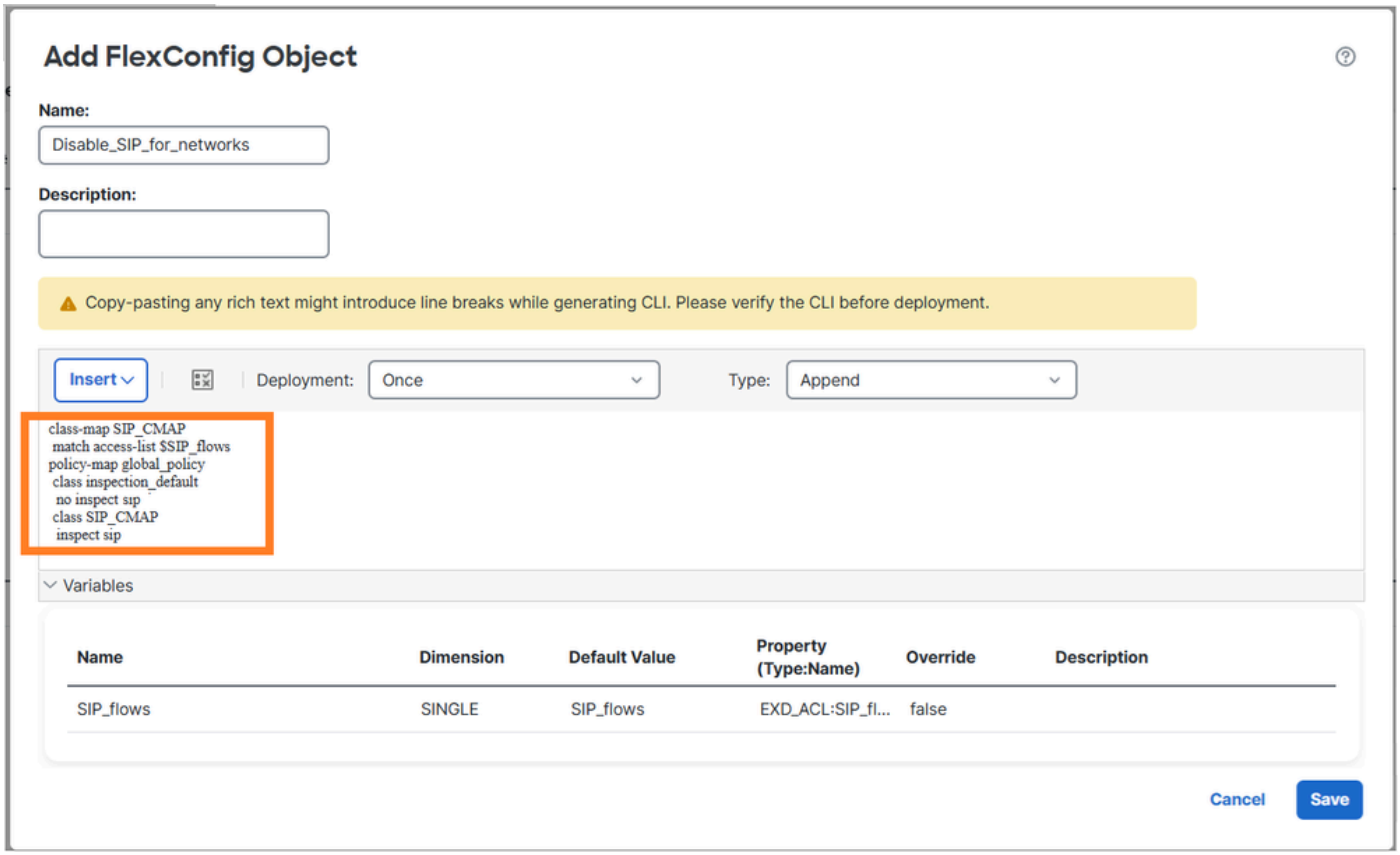
Paso 1

Navegue hasta Objetos > Lista de acceso > Extendida y cree una lista de acceso extendida que coincida con el tráfico interesante. Debe utilizar la acción Bloquear desde el objetivo de excluir el tráfico específico. Además, agregue una regla de permiso para que coincida con el resto del tráfico:



Paso 2

Cree un objeto FlexConfig con un mapa de clase que coincida con la lista de control de acceso (ACL) SIP y aplíquelo a global_policy:



El objeto FlexConfig configurado:

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

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

Nota

Al configurar la ACL permit, intente ser lo más específico posible (por ejemplo, coloque los puertos de protocolo) para evitar cualquier impacto potencial en la CPU. El ejemplo de esta tarea no especifica puertos de protocolo y se puede evitar en producción.

Verificación 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
```

Verificación 2

El tráfico que no es inspeccionado por la inspección SIP tiene 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
...
```

El tráfico que es inspeccionado por la inspección SIP tiene 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,
...
```

Verificación 3

El contador de inspección "sip" aumenta cuando el firewall inspecciona un paquete:

<#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


...
```

Tarea 3. Configuración de la omisión del estado TCP para hosts específicos

En esta tarea, el requisito es habilitar el desvío del estado TCP para el tráfico entre estas redes:

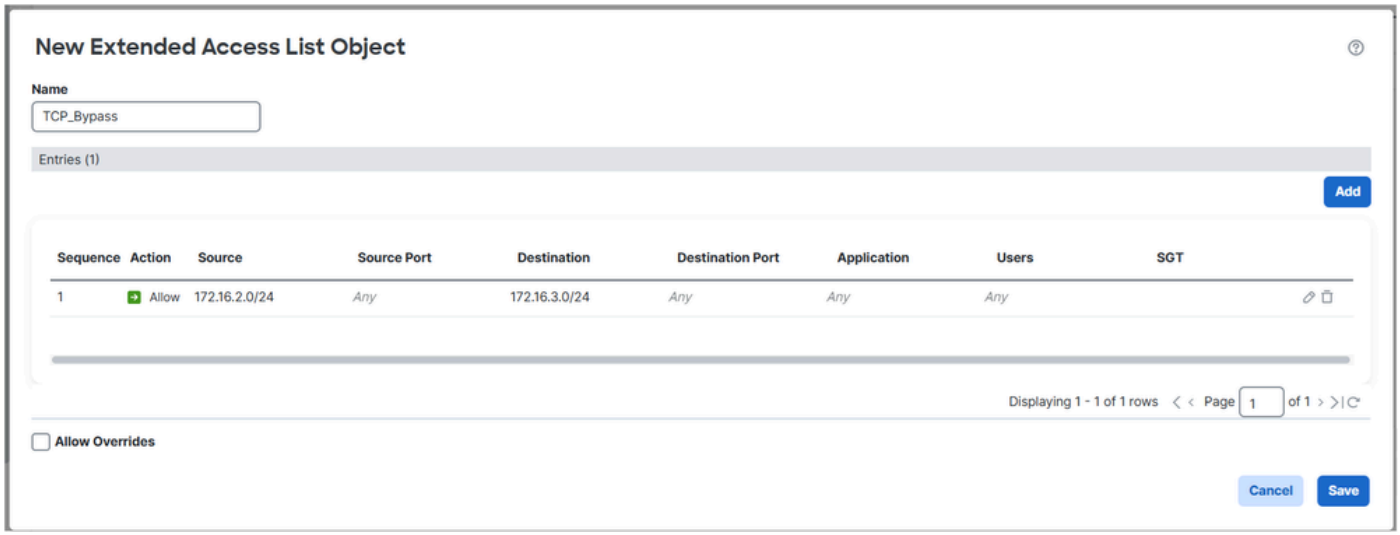
- SRC: 172.16.2.0/24
- DST: 172.16.3.0/24

En general, no se recomienda utilizar el desvío de estado TCP, pero se puede utilizar como una solución temporal para gestionar flujos asimétricos.

Solución 1

Paso 1

Cree una ACL extendida que coincida con el tráfico interesante:

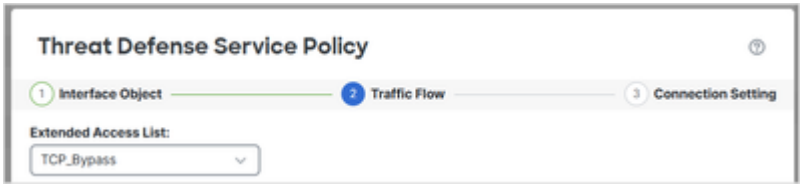


Paso 2

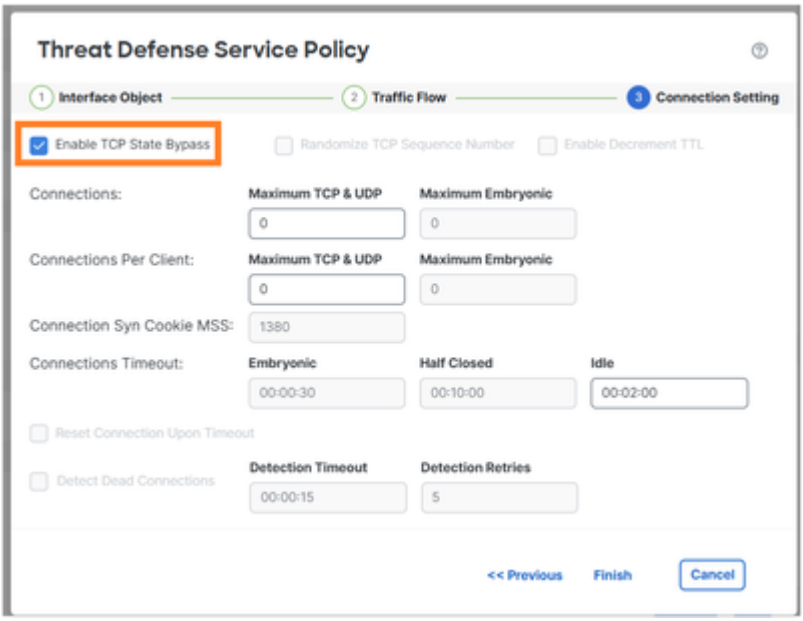
Edite la política de control de acceso (ACP) asignada al FTD, seleccione la pestaña Configuración avanzada y edite la política de servicio de Threat Defence. Seleccione Agregar regla y Siguiente.

Paso 3

Seleccione la ACL extendida:



Paso 4



Paso 5

Seleccione Finish, OK, Save and Deploy.

El resultado:

<#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
```

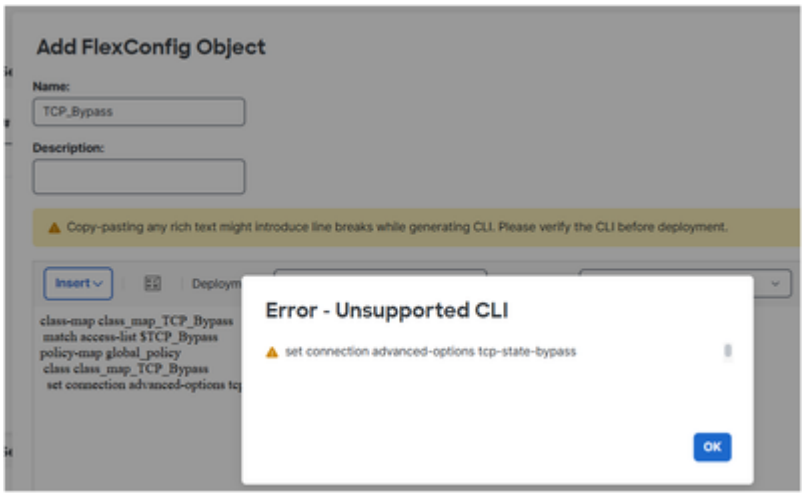
class class_map_TCP_Bypass

```
  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
```

Nota: En versiones anteriores de FMC como 6.x, puede utilizar FlexConfig para configurar el desvío del estado TCP. En las versiones más recientes esto no es compatible:



Verificación

<#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:
```

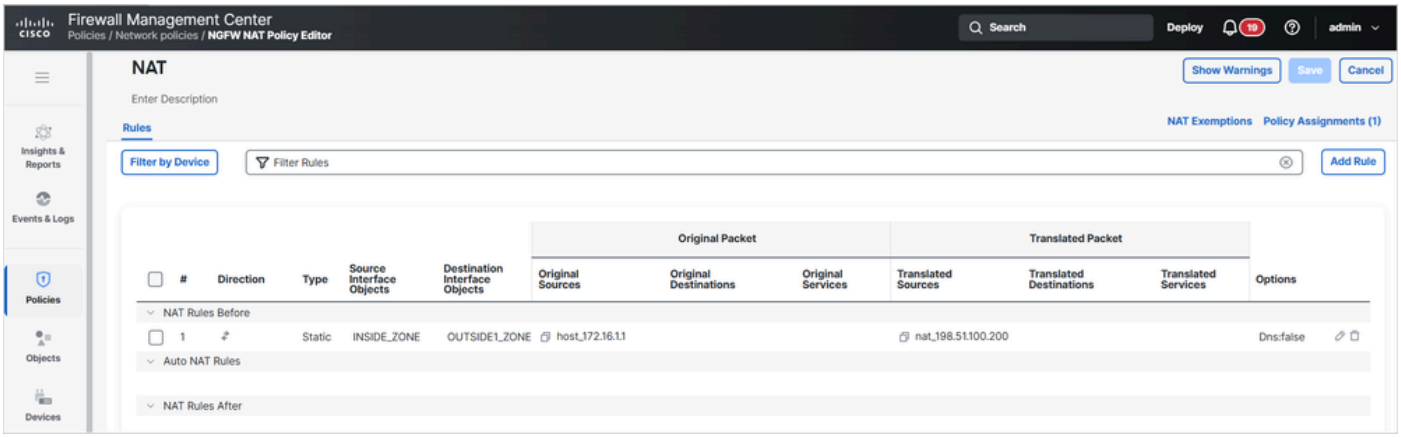
```
class-map class_map_TCP_Bypass
```

```
 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
...
```

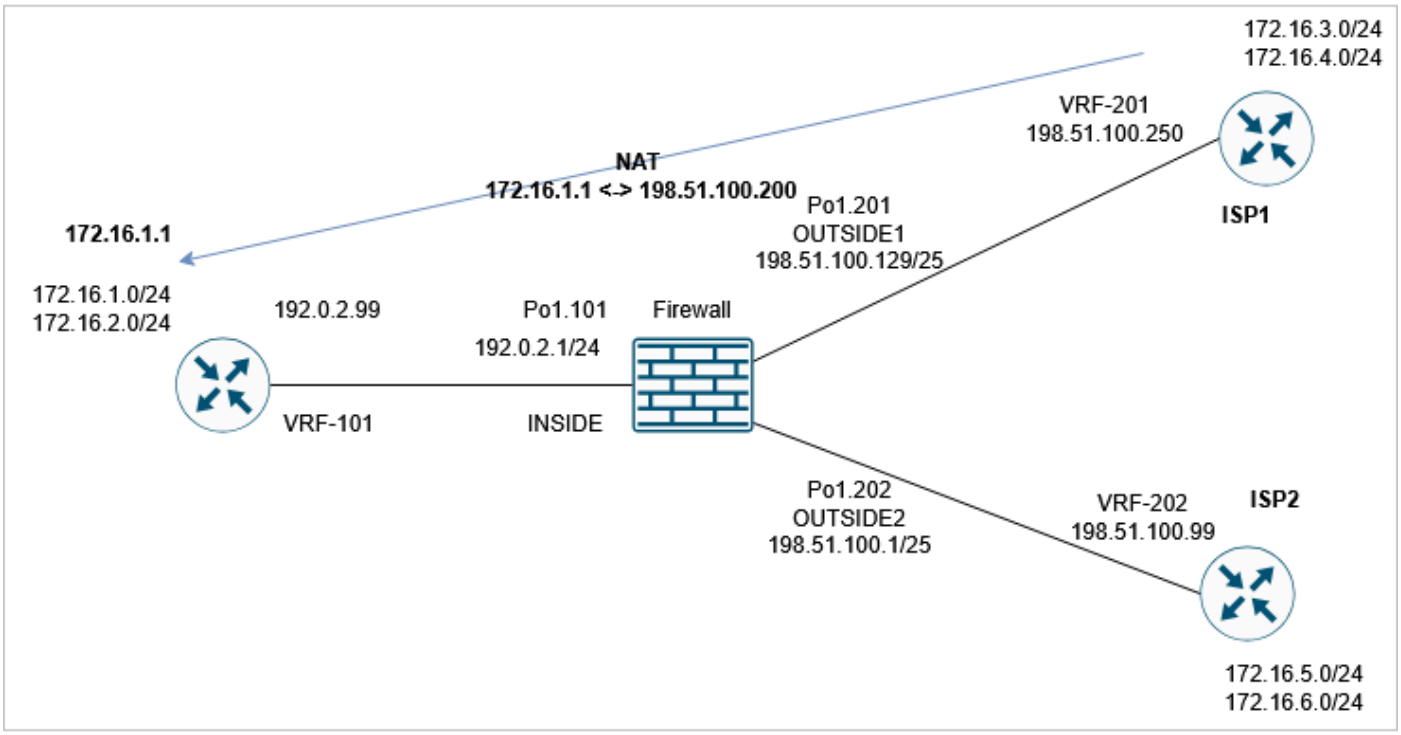
Tarea 4. Modificación del resultado de Traceroute

Requisito previo

Configure la NAT estática en FTD de modo que la IP 172.16.1.1 ubicada detrás de la interfaz INSIDE aparezca como 198.51.100.200 en los hosts OUTSIDE1:



Luego, ejecute un traceroute desde ISP1 a 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 *
```

Requisito

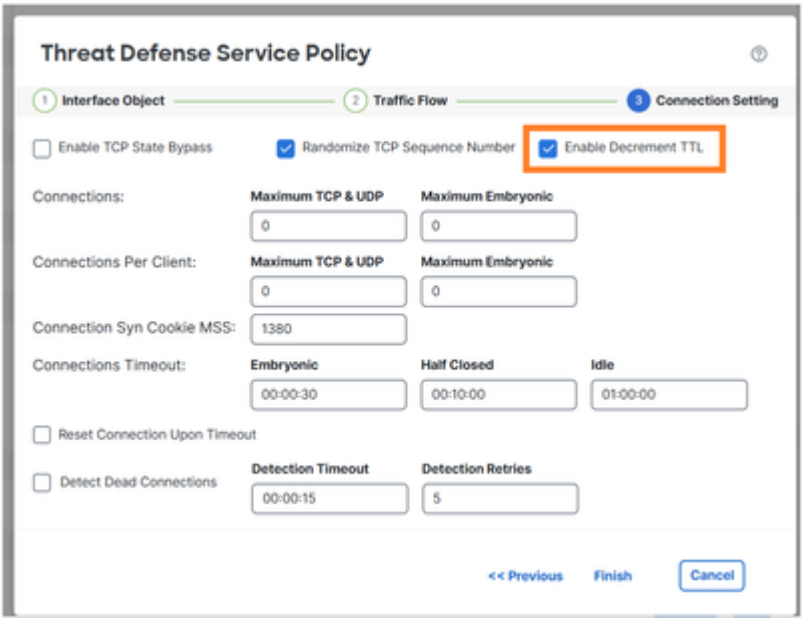
Modifique la configuración de FTD para que el traceroute coincida con esta salida:

<#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 *
```

Solución

La solución incluye dos pasos de configuración:
1. Reducir el TTL:

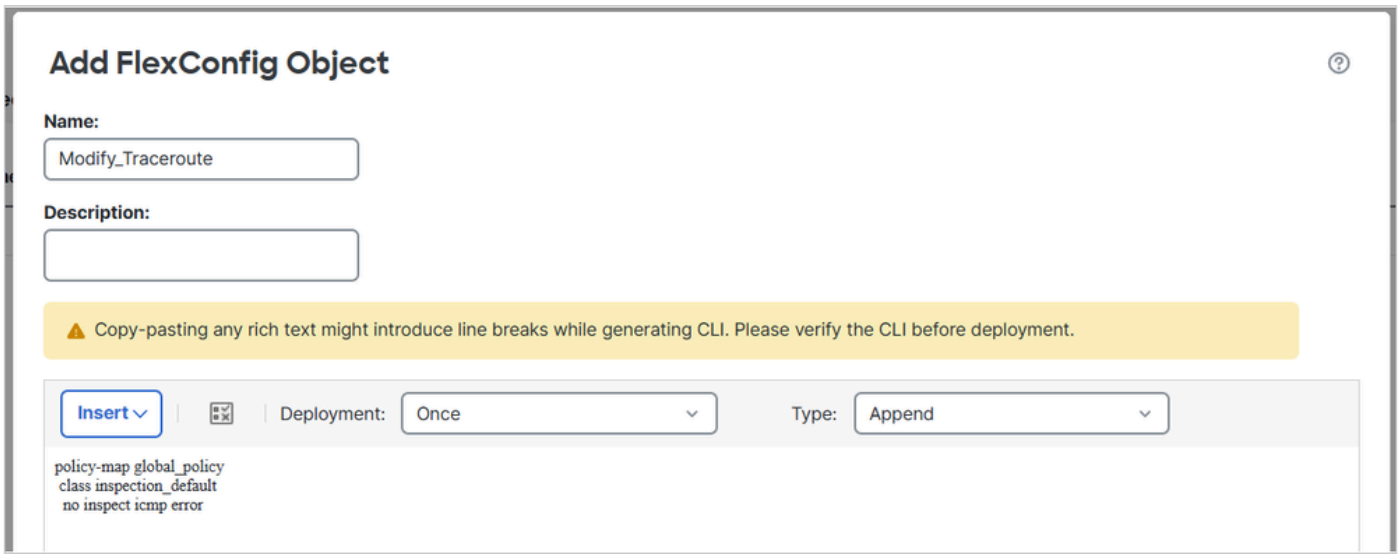


Después de este cambio, el traceroute muestra el salto del firewall:

<#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. Inhabilite la inspección de errores ICMP:




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

Verificación

El traceroute muestra la dirección IP de NAT traducida del host remoto y la dirección IP de la interfaz FTD:

<#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 *
```

Tarea 5. Establecer los tiempos de espera de conexión

Requisito

Cambie el tiempo de espera a 1 semana para este flujo:

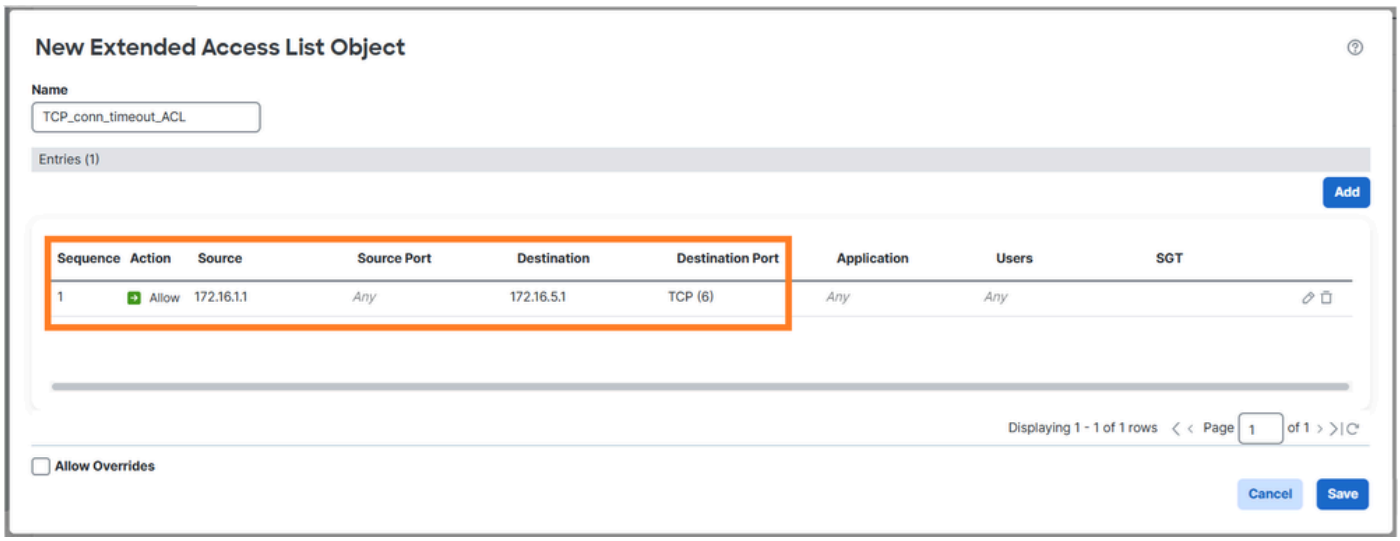
- Protocolo: TCP
- SRC: 172.16.1.1
- DST: 172.16.5.1

Solución

Para establecer el tiempo de espera por flujo, debe utilizar la política de servicio.

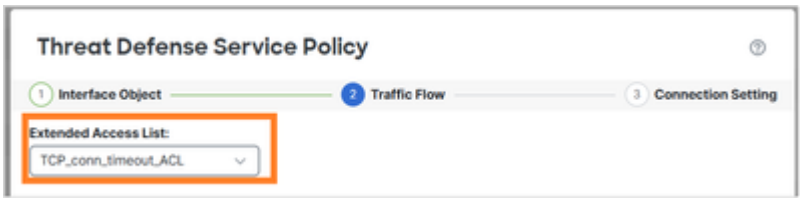
Paso 1

Navegue hasta Objetos > Lista de acceso y cree una ACL extendida que coincida con el tráfico interesante:

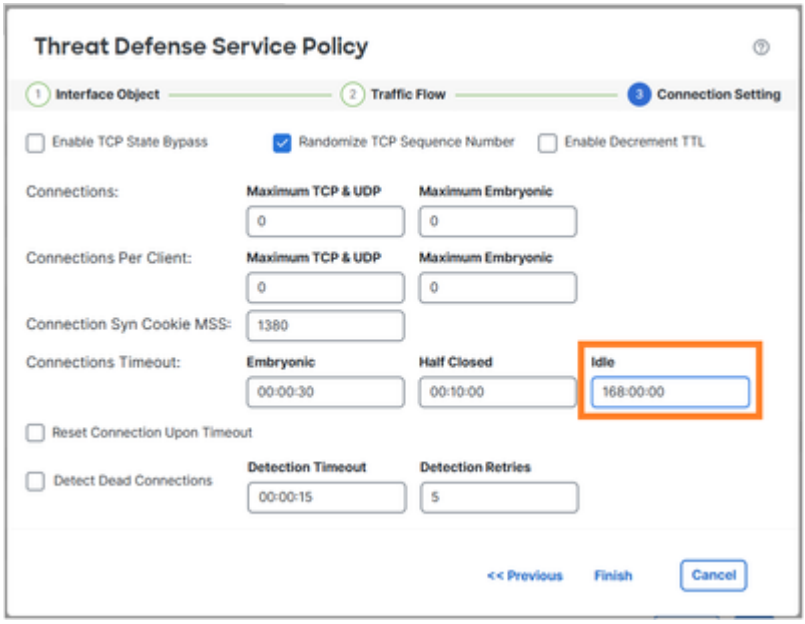


Paso 2

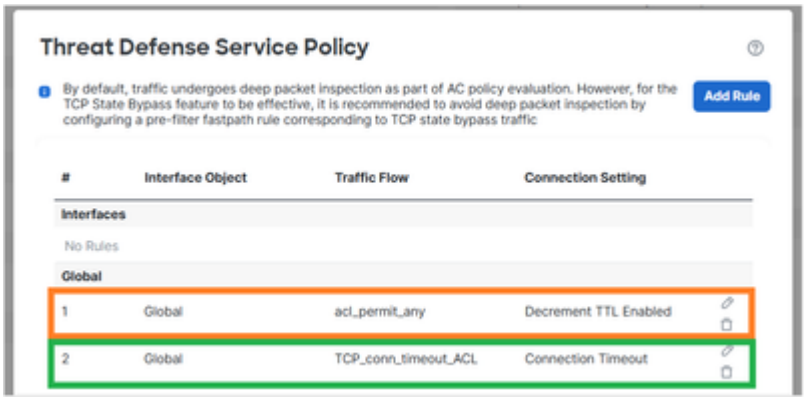
Configure una política MPF que utilice la ACL que se creó en el paso 1:



Establezca el tiempo de espera de inactividad de la conexión:



Elimine la regla de la tarea anterior, ya que se superpone con el nuevo requisito:



Verificación

La configuración de policy-map implementada:

<#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
```

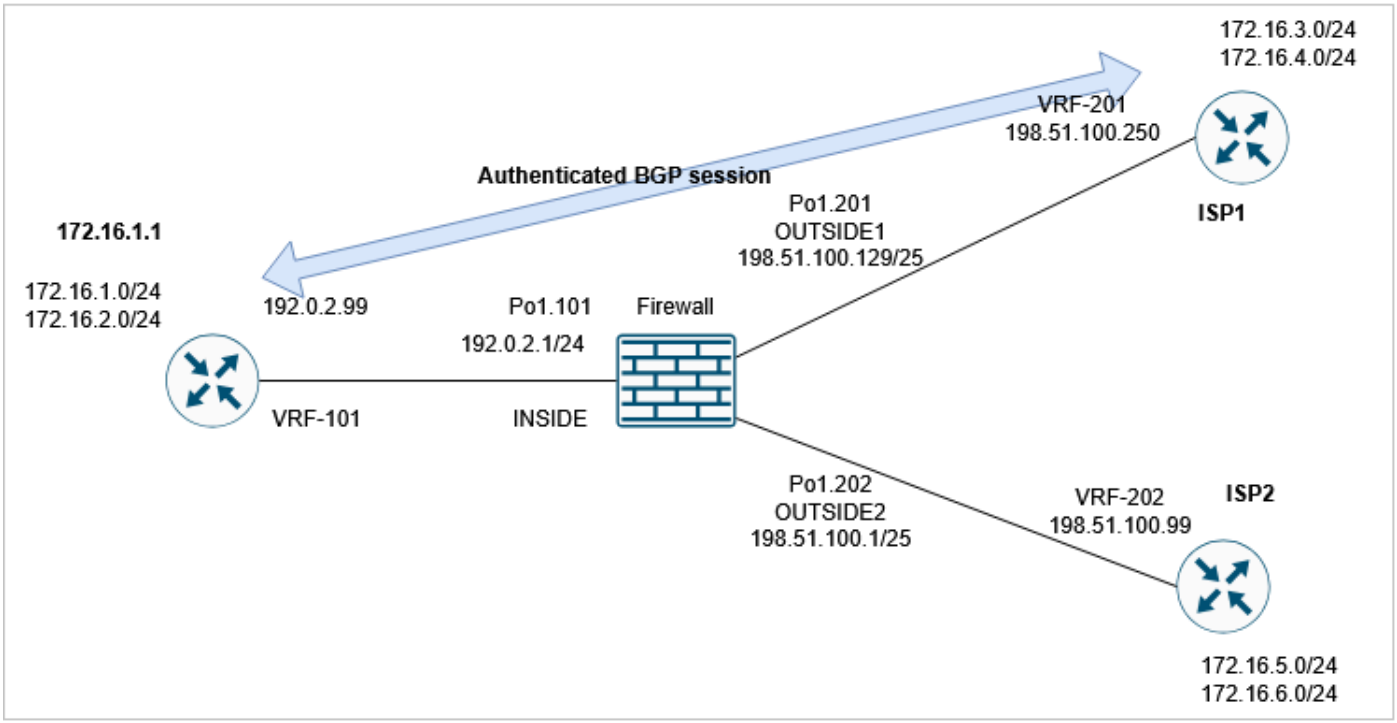
Inicie una nueva conexión TCP desde 172.16.1.1 a 172.16.5.1 y verifique la tabla de conexión del FTD:

```
<#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
```

Tarea 6. Autenticación BGP a través de FTD

Requisito previo

Configure una sesión BGP a través del FTD. La sesión BGP necesita utilizar la autenticación.



Verificación

Con la configuración de FTD predeterminada, la sesión BGP no se establece. En el router puede ver:

<#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)
```

En el FTD se observa que ambos lados no pueden establecer la conexión TCP BGP (los indicadores de conexión indican que sólo se reciben paquetes SYN TCP):

<#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
```

Solución

Para permitir una sesión BGP autenticada a través del FTD, deben cumplirse estas 2 condiciones:

1. Se debe permitir TCP MD5 (opción 19) a través del FTD.
2. La aleatorización de números de secuencia TCP debe estar deshabilitada.

La opción TCP MD5 está permitida de forma predeterminada:

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
```

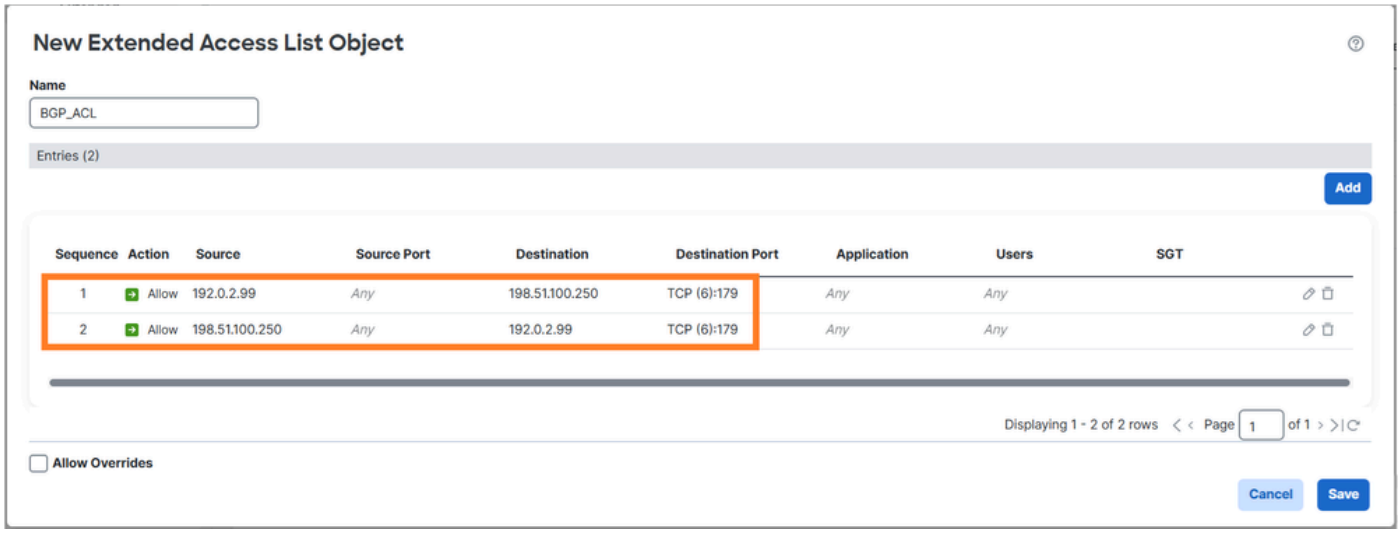
```
  queue-limit 0 timeout 4
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options mss allow

  tcp-options md5 allow



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

Desactivar de forma global la aleatorización del número de secuencia inicial (ISN) de TCP:

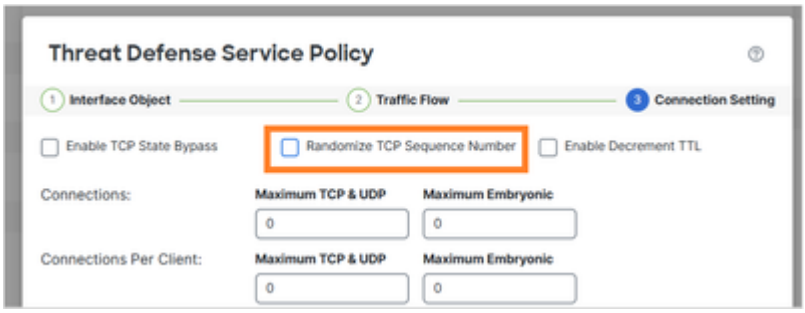
<#root>

```
>

configure tcp-randomization disable


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

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

o (el método preferido) crea una lista de acceso ampliada que coincide con la conexión BGP:



e inhabilite la aleatorización del número de secuencia TCP mediante la política del servicio Threat Defence:



Verificación

La configuración de policy-map implementada:

<#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
```

La sesión BGP se establece a través de 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
```

Consejo: Puede configurar una regla de ruta rápida de filtro previo para el tráfico BGP para evitar la inspección de Snort.

Tarea 7. Detección de conexiones inactivas (DCD)

Requisito

Configure DCD en FTD para el tráfico TCP destinado al host 172.16.3.1.

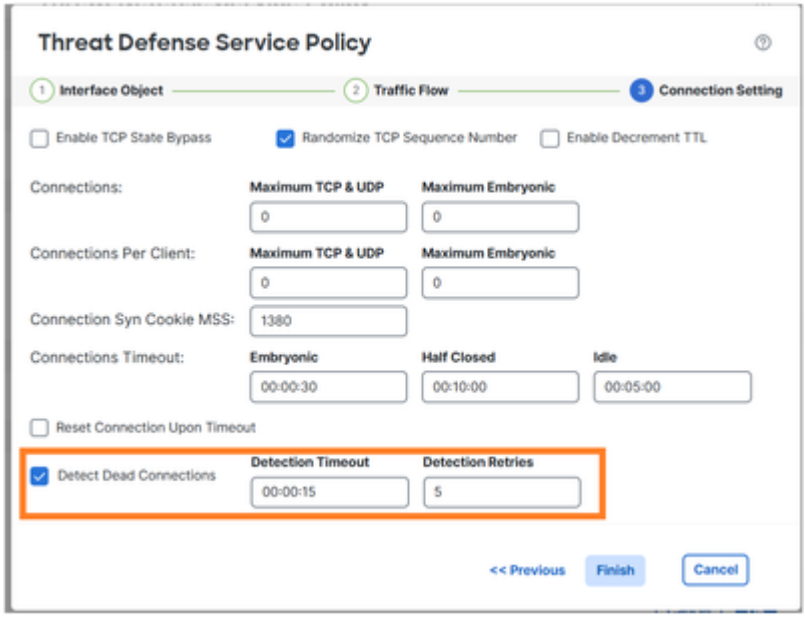
Solución

DCD está documentado en:

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. Navegue hasta Objetos > Lista de Acceso y cree una lista de acceso que coincida con el tráfico interesante.

2. Edite el ACP asignado a su firewall, navegue hasta Opciones avanzadas y seleccione Threat Defence Service Policy para habilitar DCD:



La configuración implementada:

```
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
```

Cómo funciona

Configure las capturas de FTD para ver la operación de backend:

<#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
```

Establezca una conexión TCP a través del 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
```

Inicialmente, no se muestran paquetes DCD en las capturas del firewall:

```
<#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
```

Cuando una conexión inactiva alcanza el tiempo de espera inactivo, el FTD envía mensajes TCP ACK falsos al origen y al destino:

```
<#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

Si ambos responden, restablece el temporizador de inactividad:

<#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
```

Nota: El DCD no funciona en conexiones descargadas (indicador 'o').

Información Relacionada

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).