Configurar a Estrutura de Política Modular do Firewall Threat Defense

Contents

Introdução

Este documento descreve o Firewall Threat Defense (FTD) Modular Policy Framework (MPF)

Pré-requisitos

Requisitos

Não há requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco Secure Firewall 3130 Threat Defense Versão 10.0.0 (Build 140)
- Firewall Management Center (FMC) versão 10.0.0 (Build 140)

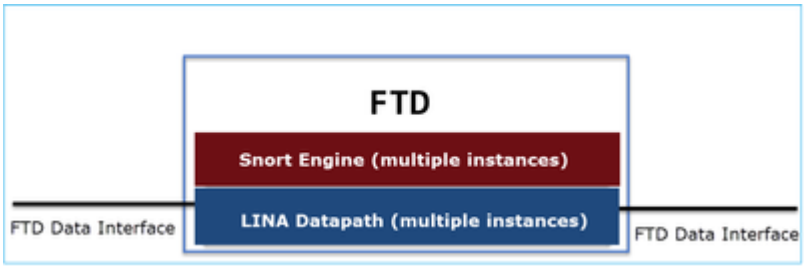
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Visão Geral do Plano de Dados do FTD

O FTD é uma imagem de software unificada que consiste em dois mecanismos principais:

- Datapath (também conhecido como LINA)
- Mecanismo Snort



O caminho de dados LINA e o Snort Engine são as partes principais do plano de dados do FTD.

Ingredientes MPF

O MPF usa estes componentes:

- class-map corresponde ao tráfego interessante.
- policy-map aplica ações ao tráfego interessante correspondido pelo class-map.
- service-policy aplica o policy-map globalmente (em todas as interfaces) ou em uma interface específica.

Direcionalidade do recurso

Em relação à direcionalidade dos recursos, consulte o guia de configuração do ASA:

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

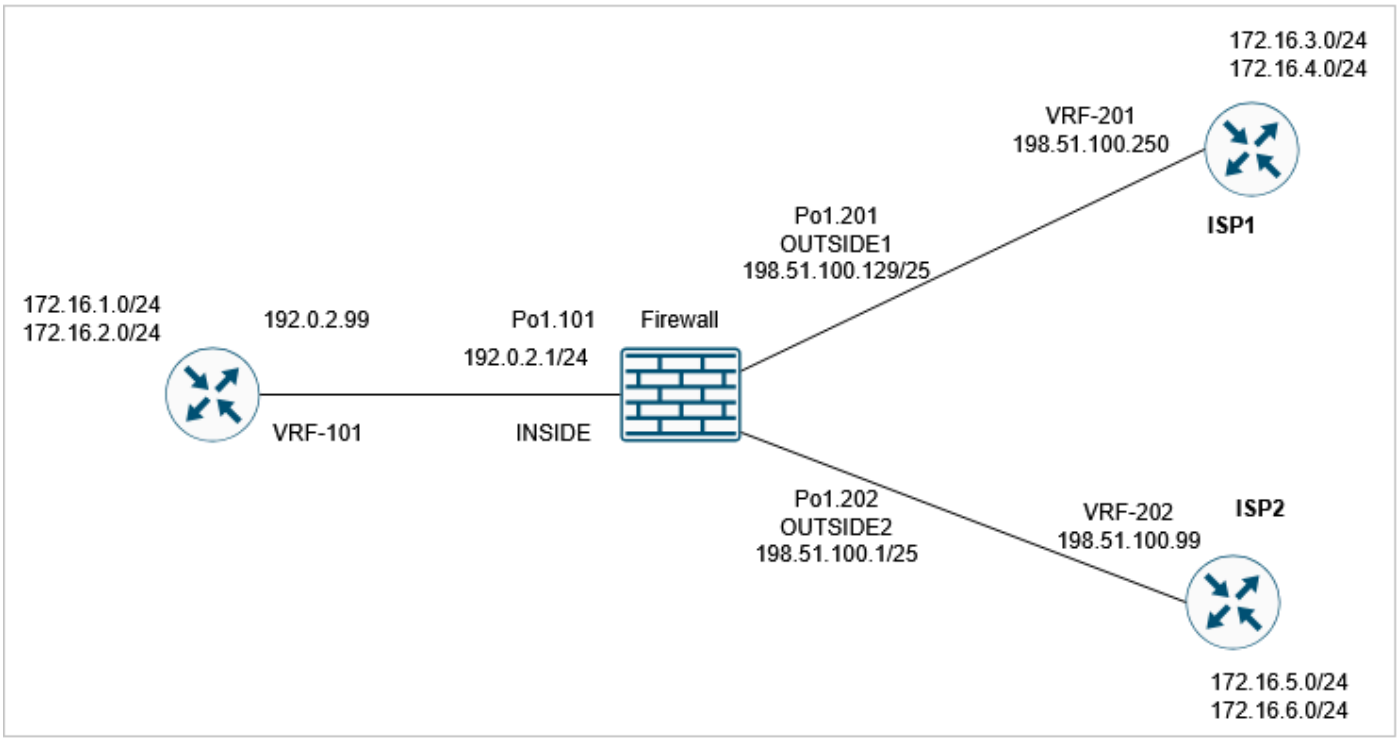
Os recursos relacionados ao FTD são destacados:

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

Topologia



A configuração padrão do 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
```

Tarefa 1. Desabilitar a inspeção do SIP globalmente no FTD

O requisito nesta tarefa é desativar a inspeção SIP no mecanismo LINA do FTD. Um motivo pode ser um requisito de política ou um defeito de software relacionado ao SIP que afeta o tráfego de trânsito.

Solução

Antes de desativar a inspeção SIP, confirme primeiro que ela é aplicada ao tráfego de trânsito:

<#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

Há duas maneiras de desabilitar globalmente a inspeção SIP:

Solução 1: Desabilitar SIP da CLI do FTD

<#root>

>

configure inspection sip disable

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

7818 bytes copied in 0.250 secs
[OK]

Verificação

<#root>

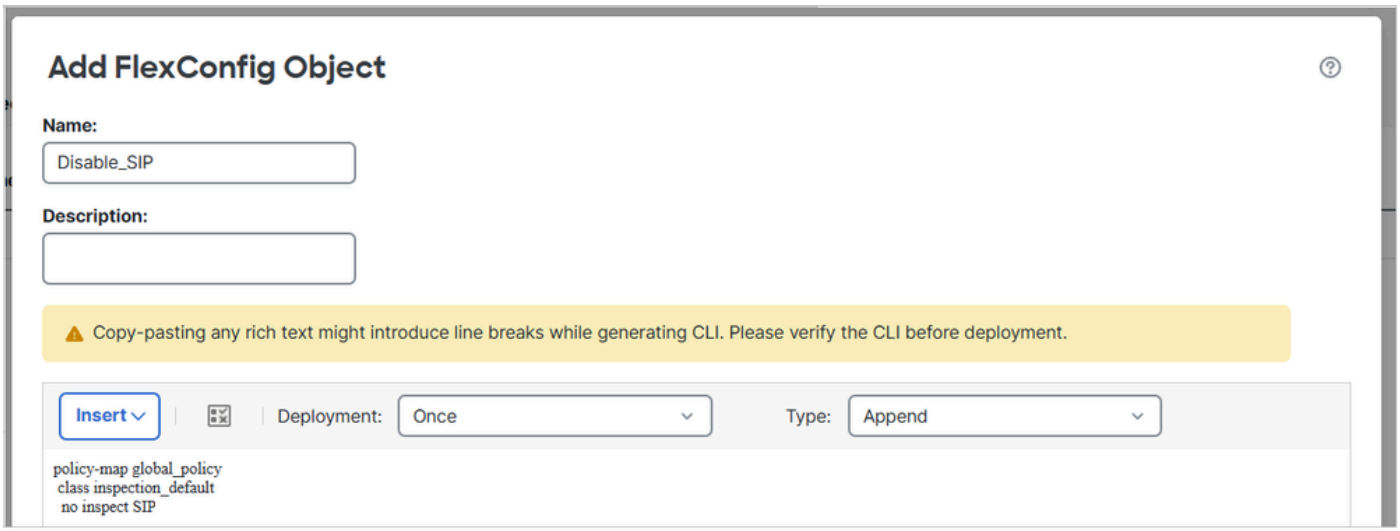
>

show running-config policy-map | include sip

>

Solução 2: Desabilitar SIP usando FlexConfig

No FMC, navegue até Devices > FlexConfig e crie um objeto FlexConfig:




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

Aplicar Use a política FlexConfig e selecione Preview Config para visualizá-la:

Finalmente, Implante a política.

Verificação

<#root>

```
firewall#
```

```
show run policy-map | include sip

firewall#
```

Observação - Você precisa limpar a conexão SIP existente da tabela de conexão LINA para que as conexões sejam restabelecidas sem inspeção de SIP. Você pode usar este comando para verificar as conexões SIP existentes:

```
<#root>

firewall#

show conn port 5060
```

Tarefa 2. Desabilitar a inspeção SIP para hosts específicos

Nesta tarefa, o requisito é desabilitar a inspeção de SIP para o tráfego entre essas redes:

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

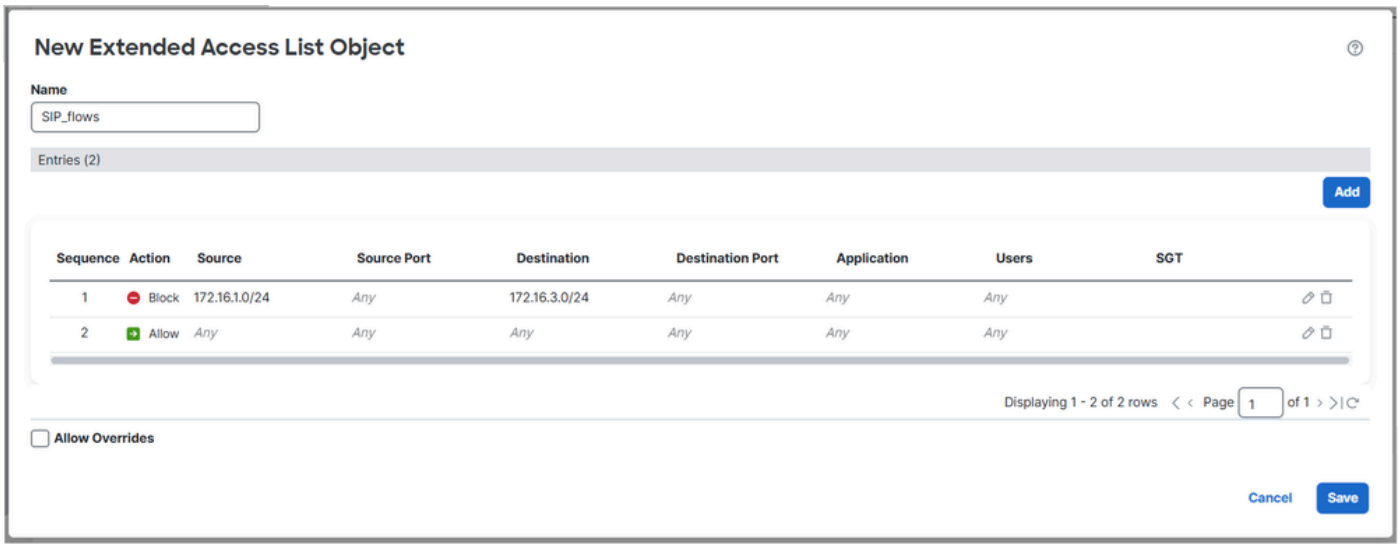
Um motivo para fazer isso pode ser um defeito de software relacionado ao SIP que afeta o tráfego de trânsito

Solução

Use o FlexConfig.

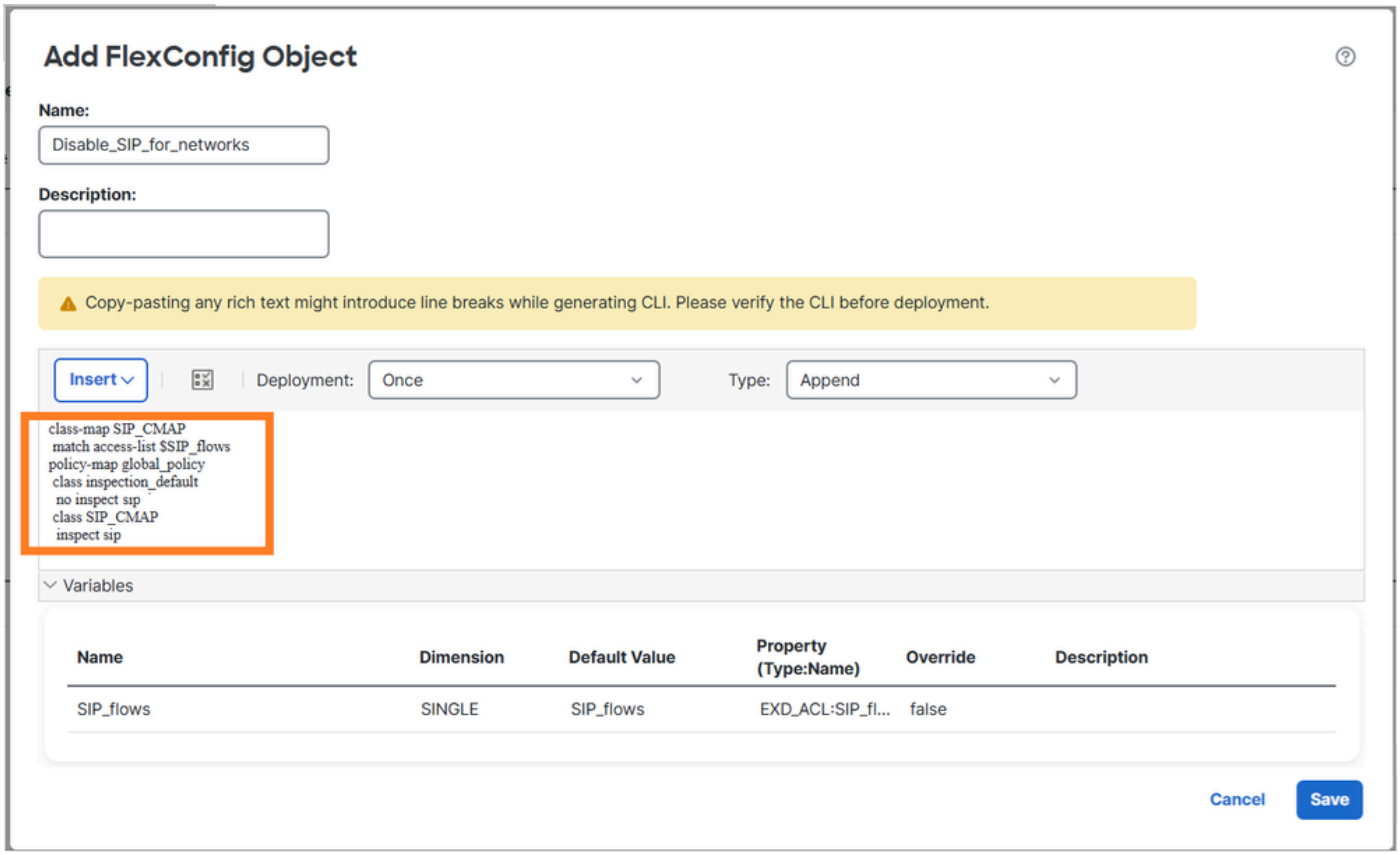
Passo 1

Navegue até Objetos > Lista de acesso > Estendida e crie uma lista de acesso estendida que corresponda ao tráfego interessante. Você deve usar a ação Bloquear desde o objetivo para excluir o tráfego específico. Além disso, adicione uma regra de permissão para corresponder ao restante do tráfego:



Passo 2

Crie um objeto FlexConfig com um mapa de classe que corresponda à lista de controle de acesso (ACL) do SIP e aplique-o à global_policy:



O 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

Ao configurar a ACL permit , tente ser o mais específico possível (por exemplo, coloque portas de protocolo) para evitar qualquer impacto potencial na CPU. O exemplo nesta tarefa não especifica portas de protocolo e pode ser evitado na produção.

Verificação 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
```

Verificação 2

O tráfego que não é inspecionado pela inspeção de SIP tem 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
...
```

O tráfego inspecionado pela inspeção de SIP tem 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,
...

Verificação 3

O contador de inspeção "sip" aumenta quando um pacote é inspecionado pelo 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


...
```

Tarefa 3. Configurar o desvio de estado TCP para hosts específicos

Nesta tarefa, o requisito é habilitar o desvio de estado TCP para o tráfego entre estas redes:

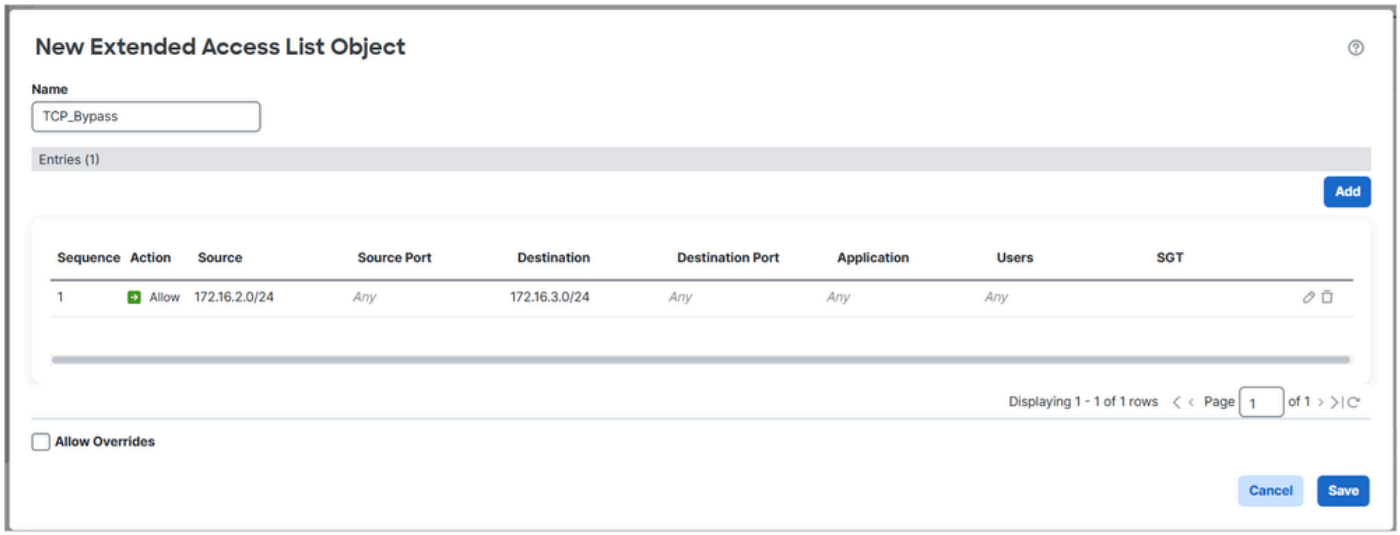
- SRC: 172.16.2.0/24
- DST: 172.16.3.0/24

Em geral, não é recomendável usar o desvio de estado TCP, mas ele pode ser usado como uma solução temporária para lidar com fluxos assimétricos.

Solução 1

Passo 1

Crie uma ACL estendida que corresponda ao tráfego interessante:

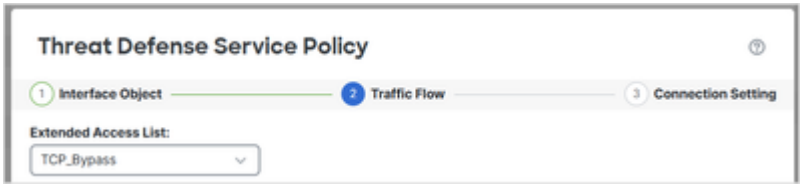


Passo 2

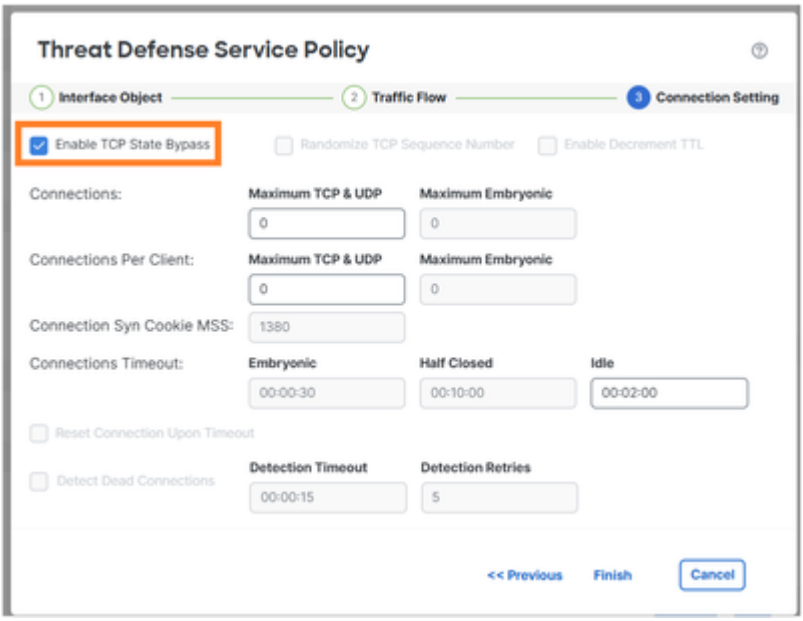
Edite a ACP (Política de Controle de Acesso) atribuída ao FTD, selecione a guia Configurações Avançadas e edite a Política do Serviço de Defesa contra Ameaças. Selecione Adicionar Regra e Próximo.

Etapa 3

Selecione a ACL estendida:



Passo 4



Etapa 5

Selecione Concluir, OK, Salvar e Implantar.

O 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
```

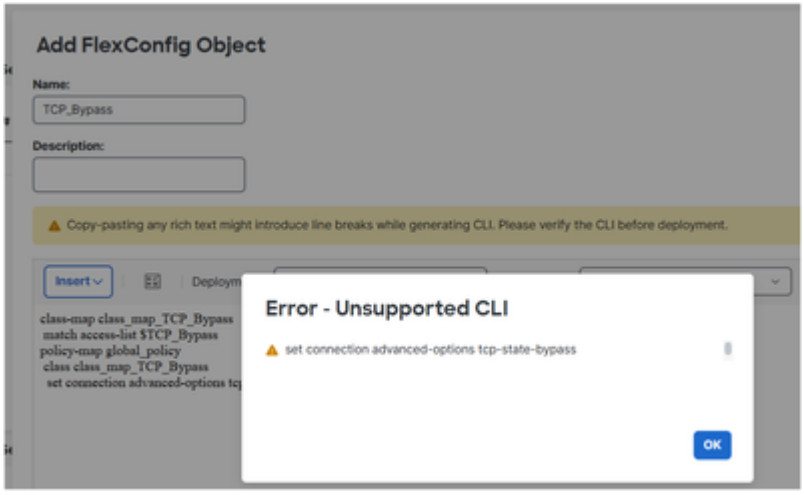
class class_map_TCP_Bypass

```
  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
```

Note: Em versões anteriores do FMC, como a 6.x, você pode usar o FlexConfig para configurar o desvio de estado do TCP. Em versões mais recentes, isso não é suportado:



Verificação

<#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:
```

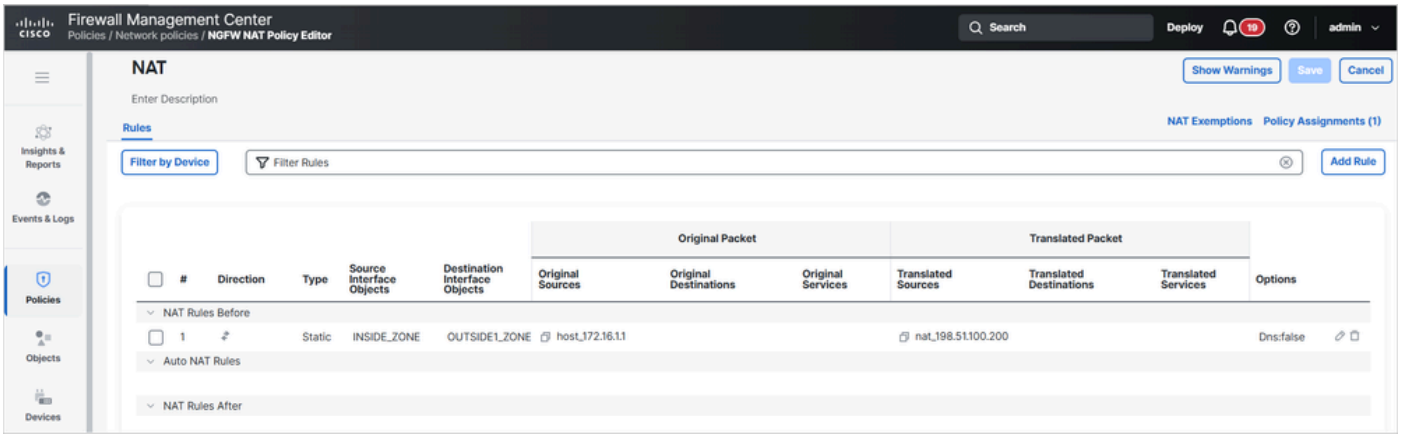
```
class-map class_map_TCP_Bypass
```

```
 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
...
```

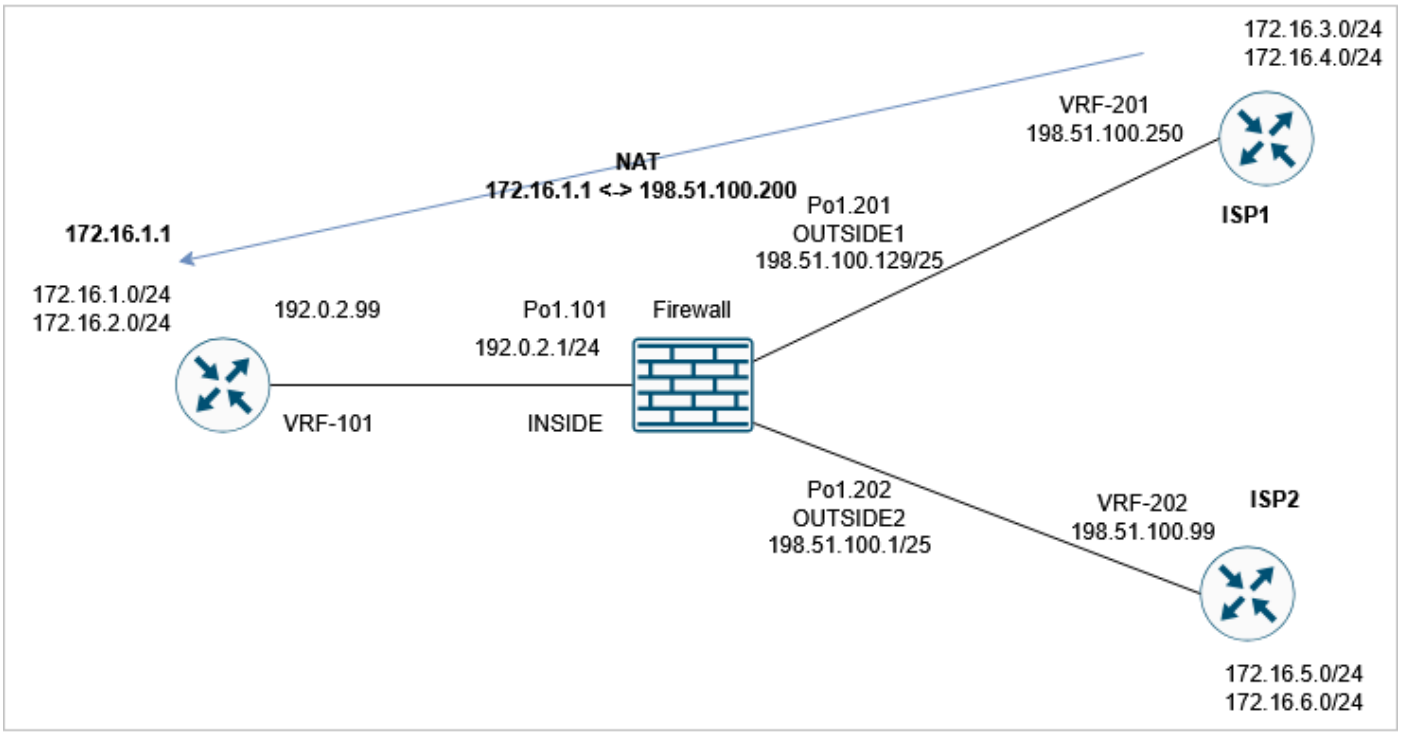
Tarefa 4. Modificações na saída do traceroute

Pré-requisito

Configure o NAT estático no FTD para que o IP 172.16.1.1 localizado atrás da interface INSIDE apareça como 198.51.100.200 nos hosts OUTSIDE1:



Em seguida, execute um traceroute de ISP1 para 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 *
```

Requisitos

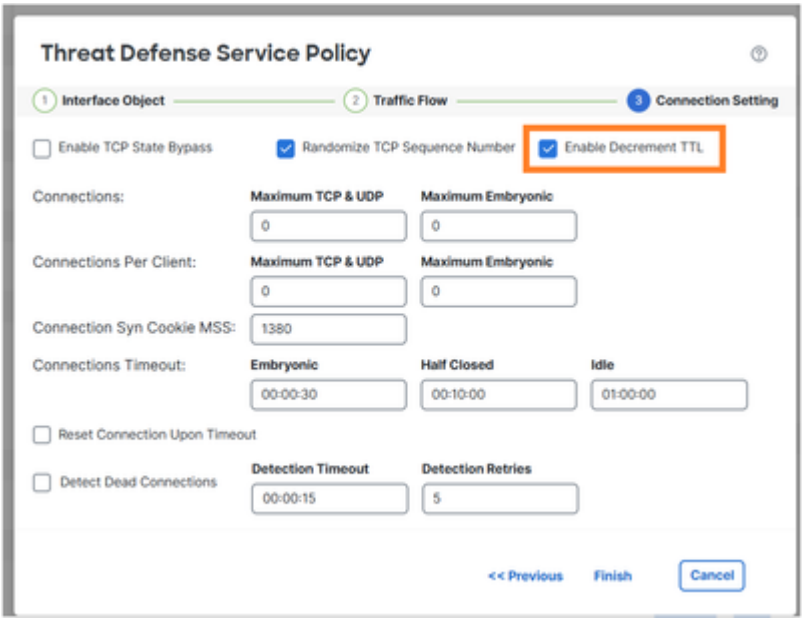
Modifique a configuração de FTD para que o traceroute corresponda a esta saída:

<#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 *
```

Solução

A solução inclui duas etapas de configuração:
1. Diminuir o TTL:

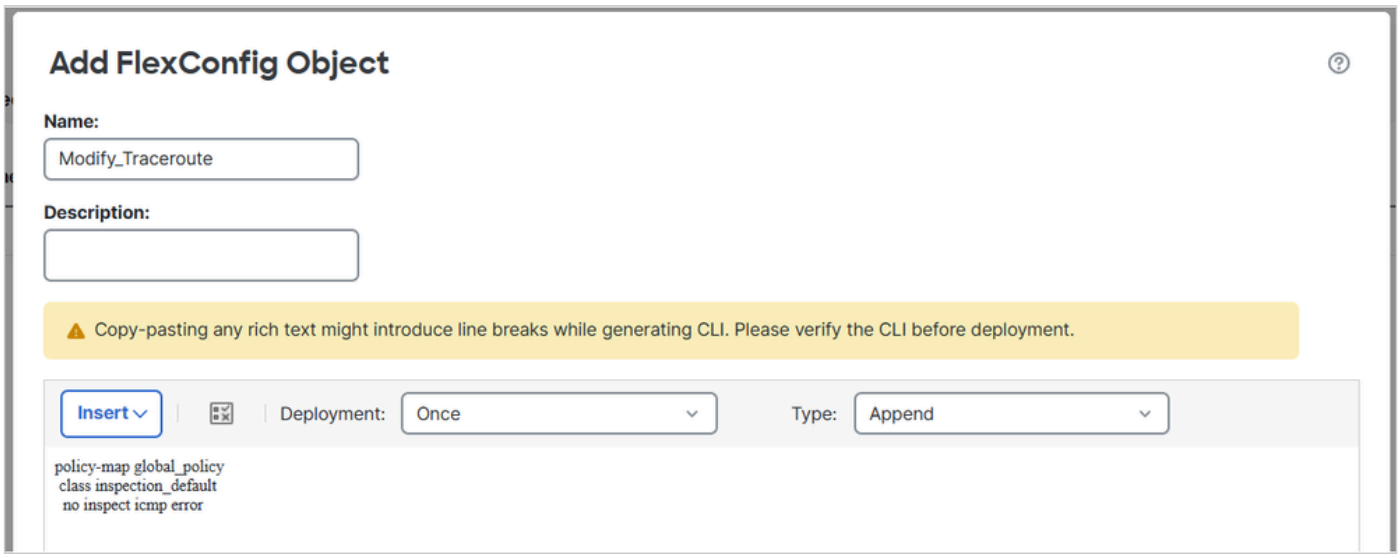


Após essa alteração, o traceroute revela o salto do firewall:

<#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. Desativar a inspeção de erros do ICMP:




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

Verificação

O traceroute mostra o endereço IP NAT convertido do host remoto e o endereço IP da interface 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 *
```

Tarefa 5. Definir tempos limite da conexão

Requisitos

Altere o tempo limite para 1 semana para este fluxo:

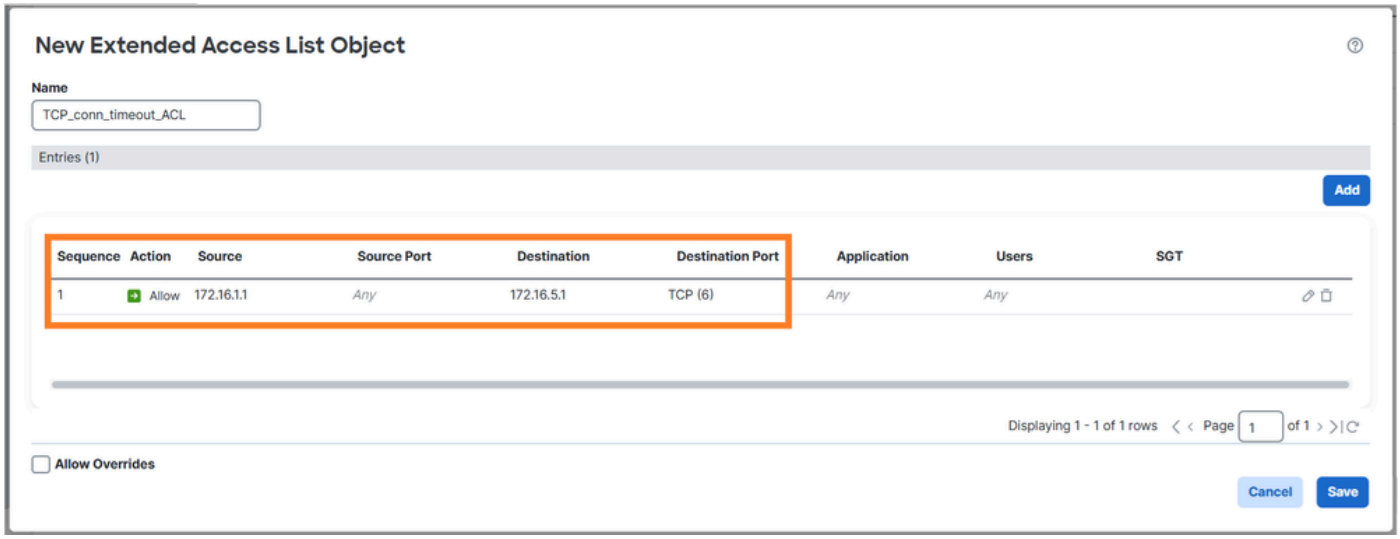
- Protocolo: TCP
- SRC: 172.16.1.1
- DST: 172.16.5.1

Solução

Para definir o tempo limite por fluxo, você precisa usar a Política de serviço.

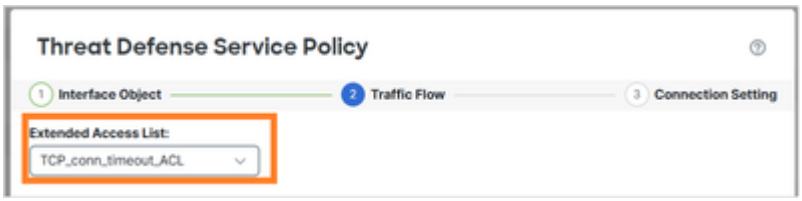
Passo 1

Navegue até Objetos > Lista de acesso e crie uma ACL estendida que corresponda ao tráfego interessante:

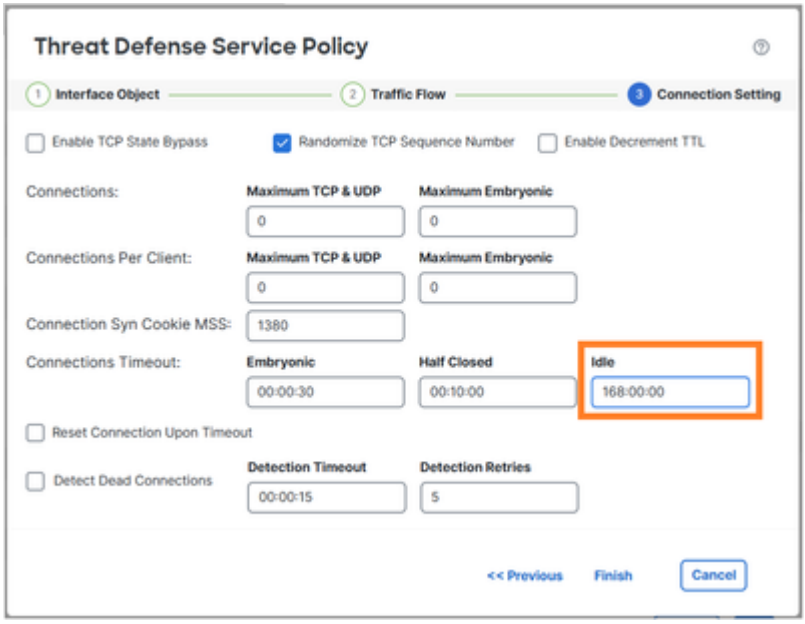


Passo 2

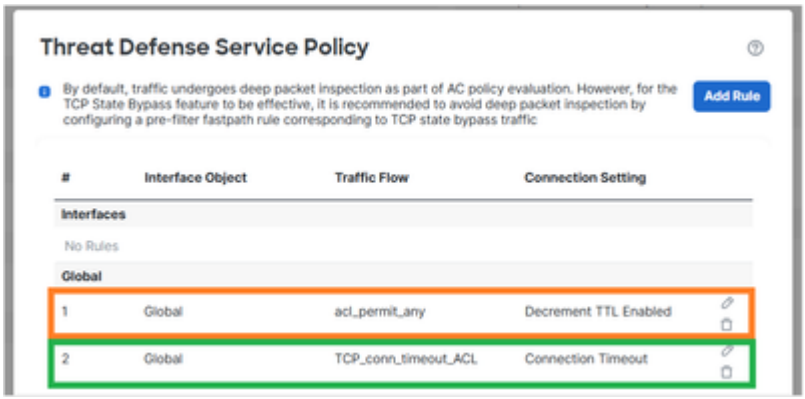
Configure uma política MPF que use a ACL criada na etapa 1:



Defina o tempo limite de ociosidade da conexão:



Remova a regra da tarefa anterior, já que ela se sobrepõe ao novo requisito:



Verificação

A configuração do mapa de políticas implantado:

<#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
```

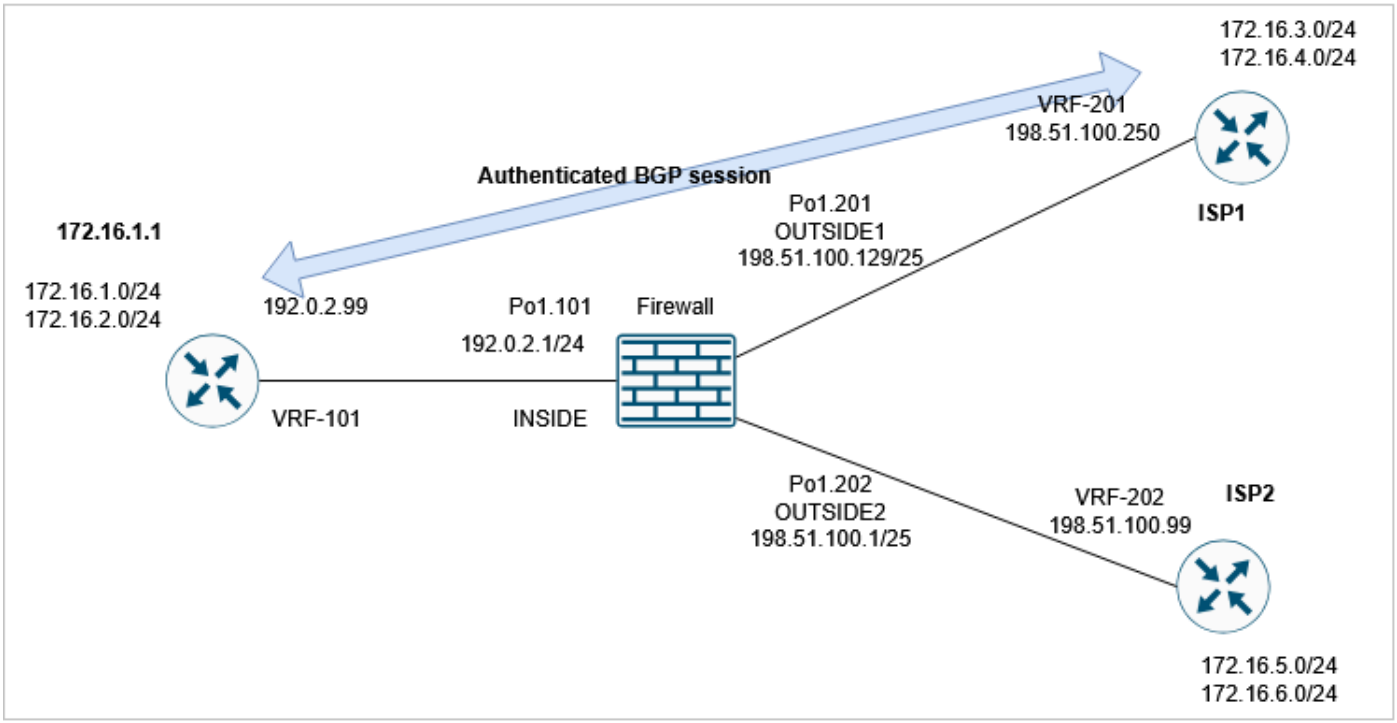
Inicie uma nova conexão TCP de 172.16.1.1 a 172.16.5.1 e verifique a tabela de conexão do FTD:

```
<#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
```

Tarefa 6. Autenticação BGP através de FTD

Pré-requisito

Configure uma sessão BGP através do FTD. A sessão BGP precisa usar a autenticação.



Verificação

Com a configuração FTD padrão, a sessão BGP não é estabelecida. No roteador, você pode 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)
```

No FTD, você vê que ambos os lados falham ao estabelecer a conexão BGP TCP (as flags de conexão indicam que somente os pacotes TCP SYN estão sendo recebidos):

<#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
```

Solução

Para permitir uma sessão BGP autenticada através do FTD, estas duas condições devem ser atendidas:

1. O TCP MD5 (opção 19) deve ser permitido através do FTD.
2. A aleatoriedade do número de sequência TCP deve ser desabilitada.

A opção TCP MD5 é permitida por padrão:

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
```

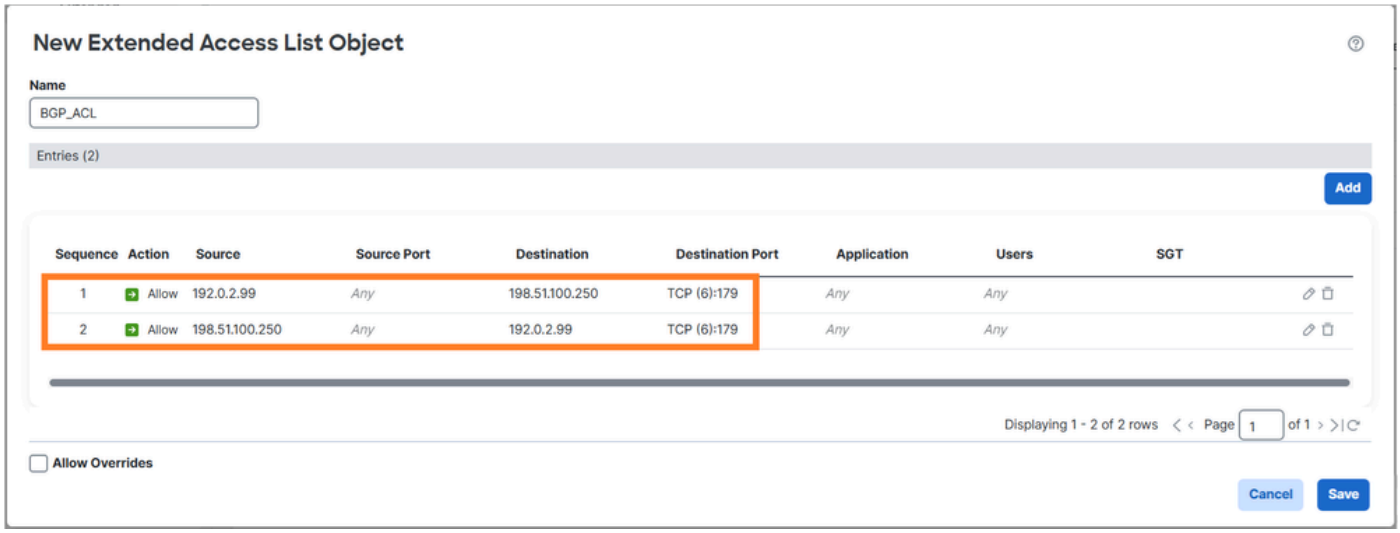
```
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  tcp-options timestamp allow
  tcp-options window-scale allow
  tcp-options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

  tcp-options md5 allow



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

Desabilite globalmente a aleatoriedade do Número de sequência inicial (ISN) do TCP:

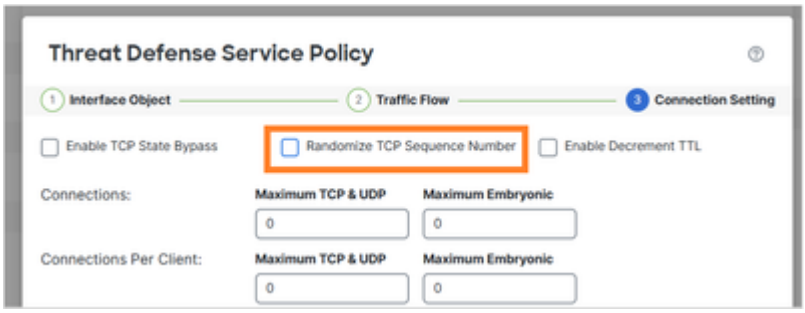
<#root>

```
>

configure tcp-randomization disable


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

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

ou (o método preferencial) crie uma lista de acesso estendida que corresponda à conexão BGP:



e desative a aleatoriedade do número de sequência TCP usando a Política do Threat Defense Service:



Verificação

A configuração do mapa de políticas implantado:

<#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
```

A sessão BGP é estabelecida através do 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: Você pode configurar uma regra prefilter fastpath para o tráfego BGP para evitar a inspeção Snort.

Tarefa 7. Detecção de Conexão Inativa (DCD)

Requisitos

Configure o DCD no FTD para o tráfego TCP destinado ao host 172.16.3.1.

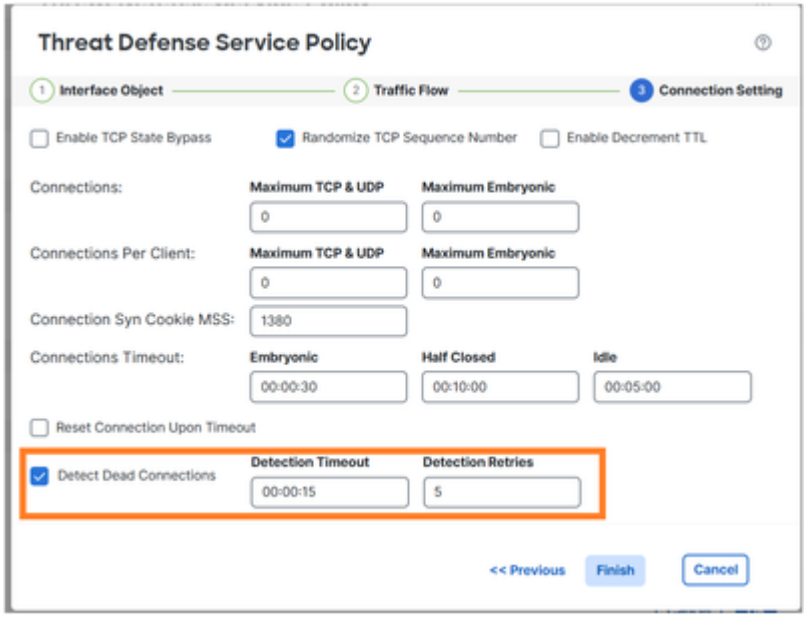
Solução

O DCD está documentado em:

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 até Objects > Access-List e crie uma lista de acesso que corresponda ao tráfego significativo.

2. Edite o ACP atribuído ao firewall, navegue até as opções Avançadas e selecione Threat Defense Service Policy para ativar o DCD:



A configuração implantada:

```
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
```

Como funciona

Configure capturas FTD para ver a operação de back-end:

```
<#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
```

Estabeleça uma conexão TCP através do 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, não há pacotes DCD mostrados nas capturas de 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
```

Quando uma conexão ociosa atinge o timeout de ociosidade, o FTD envia mensagens TCP ACK falsificadas para a origem e o 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, 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

Se ambos responderem, ele reinicializará o temporizador de inatividade:

<#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
```

Note: O DCD não funciona em conexões descarregadas (flag 'o').

Informações Relacionadas

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

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.