Konfigurieren des modularen Firewall-Bedrohungsschutz-Richtlinien-Frameworks

Inhalt

Einleitung

Dieses Dokument beschreibt das modulare Richtlinien-Framework (MPF) für Firewall Threat Defense (FTD).

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine spezifischen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

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

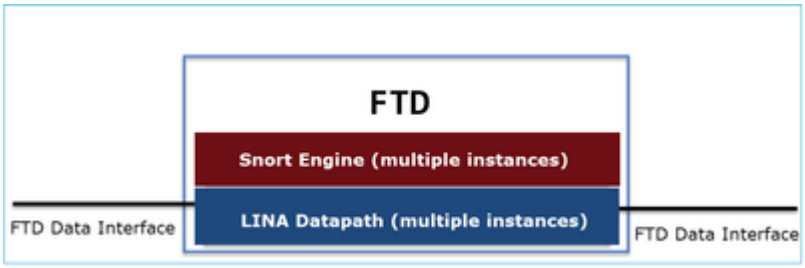
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

FTD-Datenebene - Übersicht

FTD ist ein einheitliches Software-Image, das aus zwei Haupt-Engines besteht:

- Datapath (auch als LINA bezeichnet)
- Snort-Engine



Der LINA Datapath und die Snort Engine sind die Hauptkomponenten der Datenebene der FTD.

MPF-Inhaltsstoffe

MPF verwendet folgende Komponenten:

- class-map entspricht dem interessanten Datenverkehr.
- policy-map wendet Aktionen auf den interessanten Datenverkehr an, dem die

Klassenzuordnung entspricht.
- service-policy wendet die Richtlinienzuweisung global (auf allen Schnittstellen) oder auf eine bestimmte Schnittstelle an.

Richtungsabhängigkeit der Funktionen

Informationen zur Richtungsgenauigkeit von Funktionen finden Sie im ASA-Konfigurationsleitfaden:

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

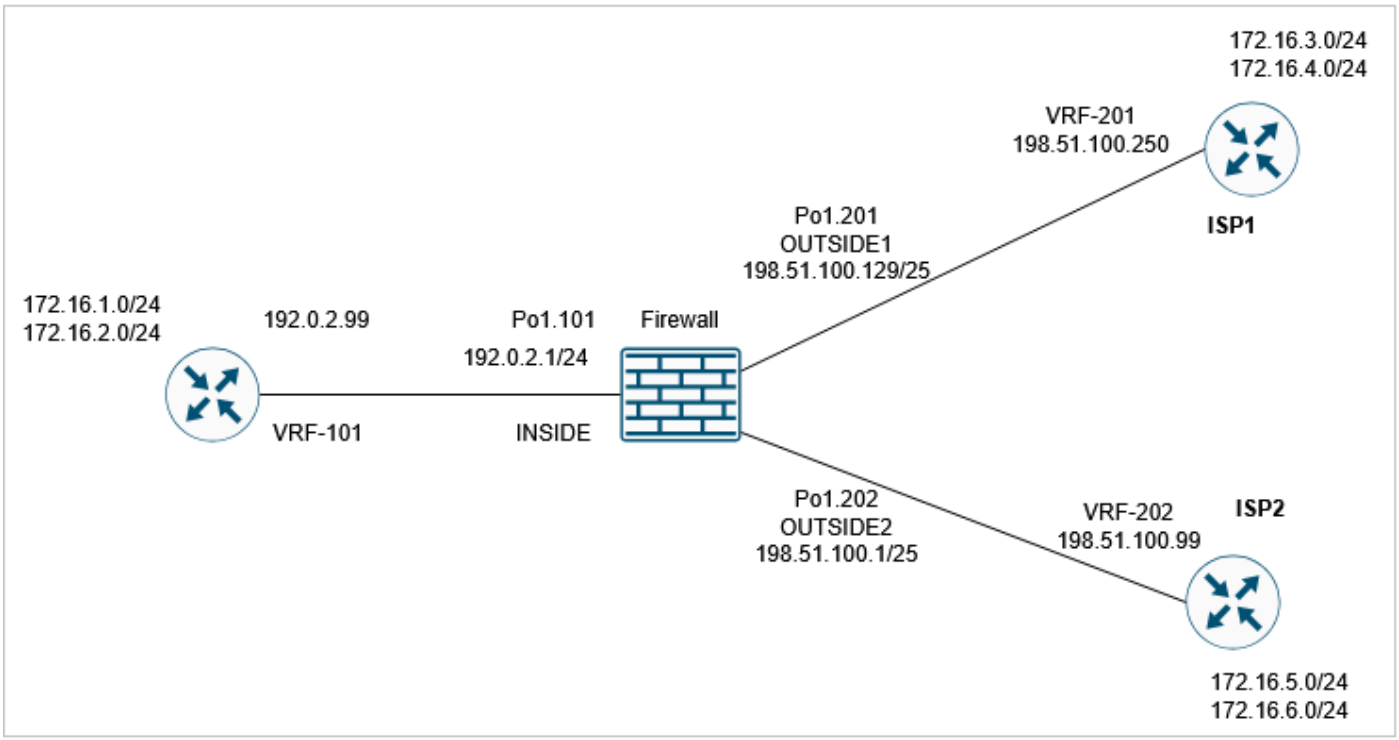
Die mit der FTD verbundenen Funktionen werden hervorgehoben:

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

Konfigurieren

Topologie



Die MPF-Standardkonfiguration (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
```

Aufgabe 1: Globale SIP-Inspektion auf FTD deaktivieren

Die Anforderung bei dieser Aufgabe besteht darin, die SIP-Inspektion in der FTD LINA-Engine zu deaktivieren. Ein Grund hierfür kann eine Richtlinienanforderung oder ein Softwarefehler sein, der sich auf das SIP bezieht und sich auf den Transitverkehr auswirkt.

Lösung

Bevor Sie die SIP-Inspektion deaktivieren, stellen Sie sicher, dass sie für den Transitverkehr gilt:

<#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

Es gibt zwei Möglichkeiten, die SIP-Inspektion global zu deaktivieren:

Lösung 1: Deaktivieren von SIP von FTD CLISH CLI

<#root>

>

configure inspection sip disable

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

7818 bytes copied in 0.250 secs
[OK]

Verifizierung

<#root>

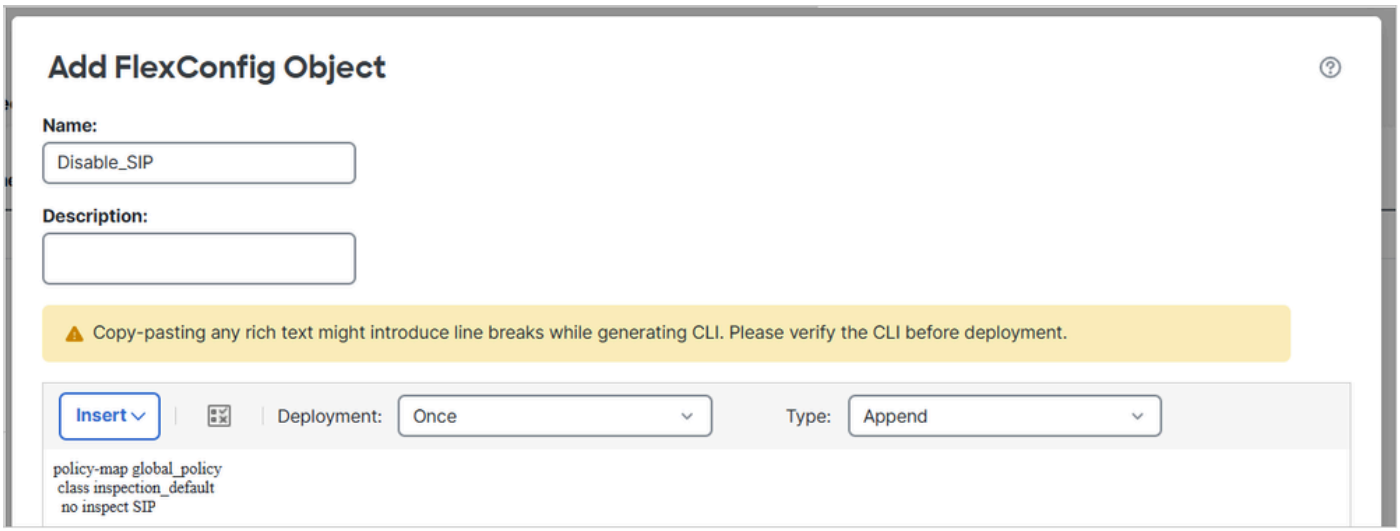
>

show running-config policy-map | include sip

>

Lösung 2: SIP mit FlexConfig deaktivieren

Navigieren Sie auf FMC zu Devices > FlexConfig, und erstellen Sie ein FlexConfig-Objekt:




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

Anwenden Wählen Sie die FlexConfig-Richtlinie aus, und wählen Sie Preview Config aus, um eine Vorschau anzuzeigen:

Stellen Sie abschließend die Richtlinie bereit.

Verifizierung

<#root>

```
firewall#

show run policy-map | include sip

firewall#
```

Hinweis - Sie müssen die vorhandene SIP-Verbindung aus der LINA-Verbindungstabelle löschen, damit die Verbindungen ohne SIP-Inspektion wiederhergestellt werden. Mit diesem Befehl können Sie die vorhandenen SIP-Verbindungen überprüfen:

<#root>

```
firewall#

show conn port 5060
```

Aufgabe 2: Deaktivieren der SIP-Inspektion für bestimmte Hosts

Bei dieser Aufgabe muss die SIP-Überprüfung für den Datenverkehr zwischen diesen Netzwerken deaktiviert werden:

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

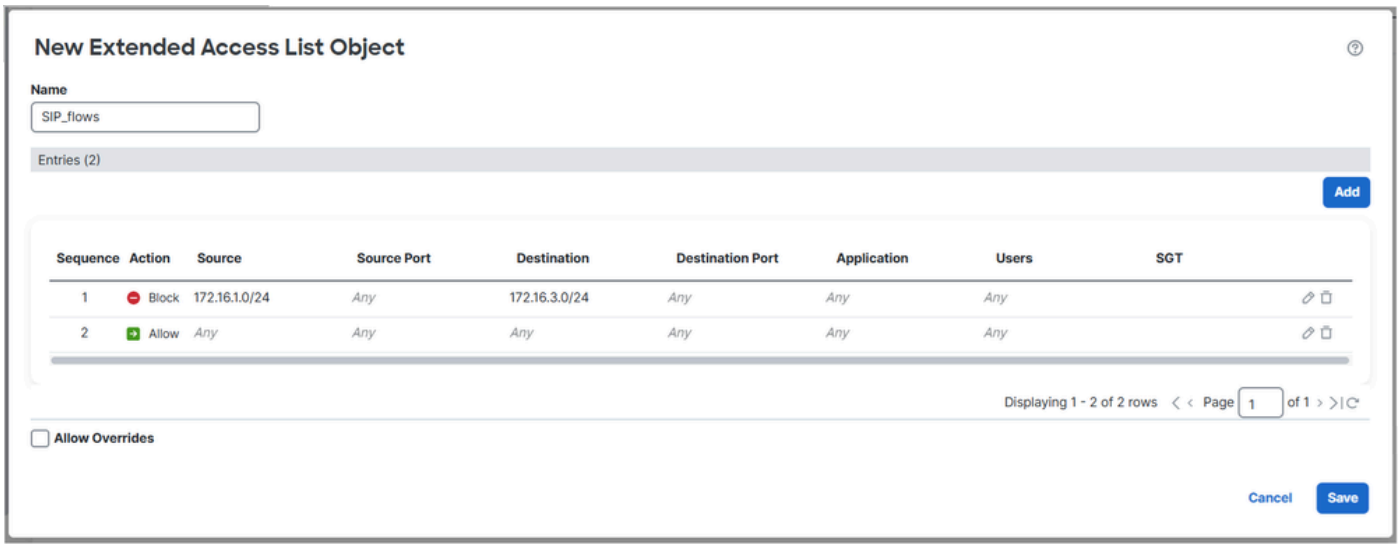
Ein Grund hierfür kann ein mit SIP in Zusammenhang stehender Softwarefehler sein, der sich auf den Transitverkehr auswirkt

Lösung

FlexConfig verwenden.

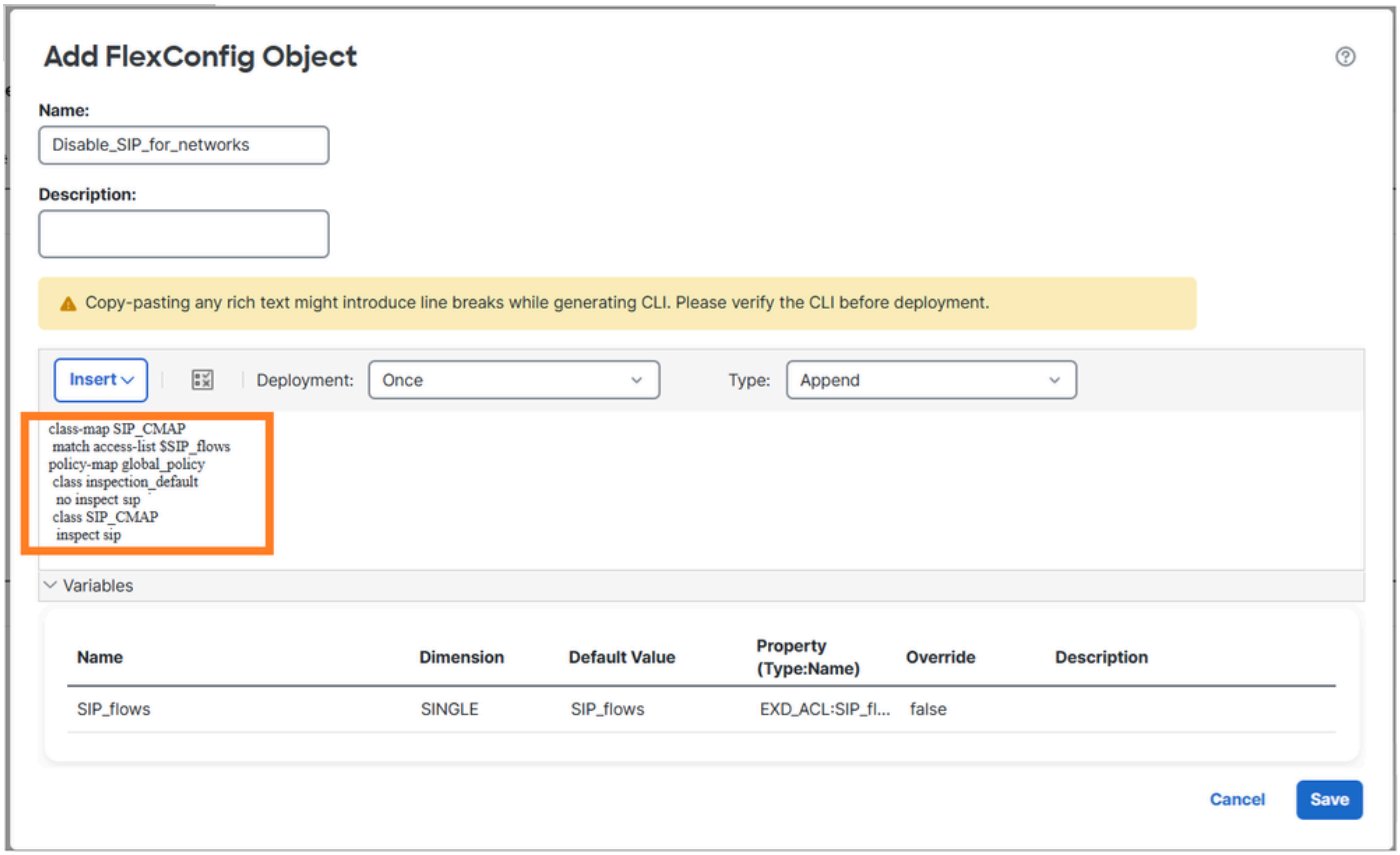
Schritt 1

Navigieren Sie zu Objekte > Zugriffsliste > Erweitert, und erstellen Sie eine erweiterte Zugriffsliste, die mit dem interessanten Datenverkehr übereinstimmt. Sie müssen die Aktion Blockieren seit dem Ziel verwenden, den spezifischen Datenverkehr auszuschließen. Fügen Sie außerdem eine Zulassungsregel hinzu, die mit dem restlichen Datenverkehr übereinstimmt:



Schritt 2

Erstellen Sie ein FlexConfig-Objekt mit einer Klassenzuordnung, die mit der SIP-Zugriffskontrollliste (ACL) übereinstimmt, und wenden Sie es auf die global_policy-Richtlinie an:



Das konfigurierte FlexConfig-Objekt:

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

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

Hinweis

Versuchen Sie bei der Konfiguration der permit-ACL, so spezifisch wie möglich zu sein (z. B. Protokollports), um mögliche Auswirkungen auf die CPU zu vermeiden. Im Beispiel dieser Aufgabe werden keine Protokoll-Ports angegeben. Dies kann in der Produktion vermieden werden.

Überprüfung 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
```

Überprüfung 2

Datenverkehr, der nicht von der SIP-Überprüfung überprüft wird, hat 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
...
```

Von der SIP-Überprüfung überprüfter Datenverkehr hat 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,
...
```

Überprüfung 3

Der Zähler "sip" inspect erhöht sich, wenn ein Paket von der Firewall geprüft wird:

<#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

...
```

Aufgabe 3: Konfigurieren der TCP-Zustandsumgehung für bestimmte Hosts

Bei dieser Aufgabe muss die TCP-Zustandsumgehung für den Datenverkehr zwischen diesen Netzwerken aktiviert werden:

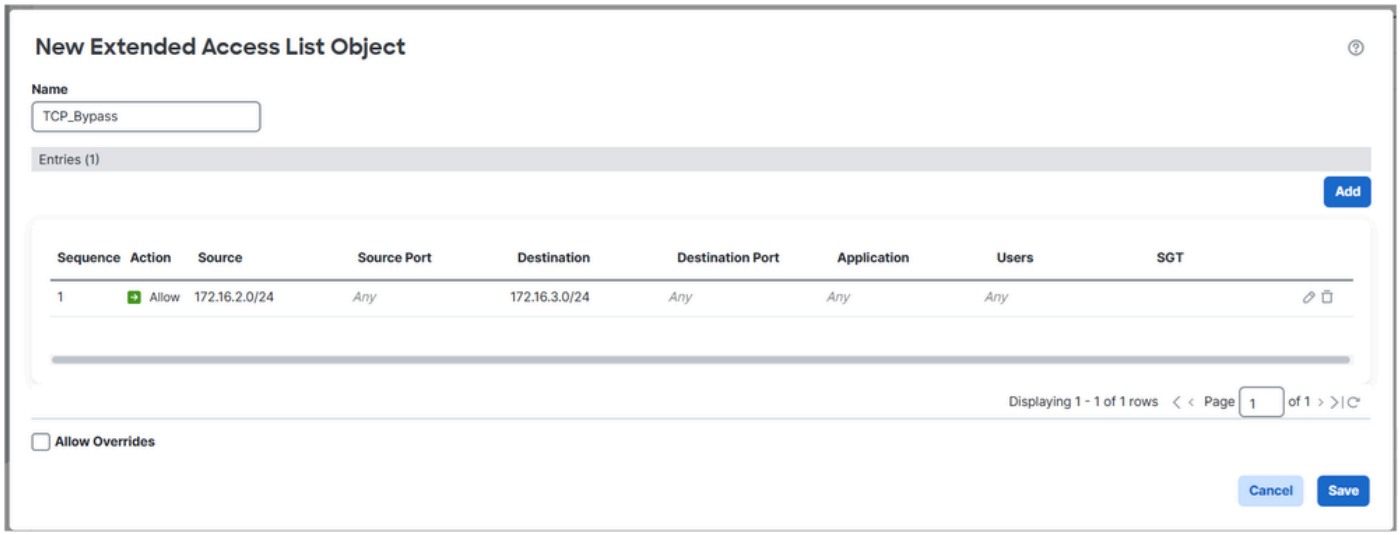
- SRC: 172.16.2.0/24
- DST: 172.16.3.0/24

Im Allgemeinen wird die Verwendung von TCP-Stati-Bypass nicht empfohlen, kann jedoch als vorübergehende Umgehung für asymmetrische Datenflüsse verwendet werden.

Lösung 1

Schritt 1

Erstellen Sie eine erweiterte ACL, die dem interessanten Datenverkehr entspricht:

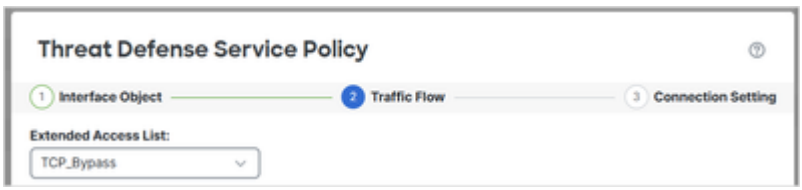


Schritt 2

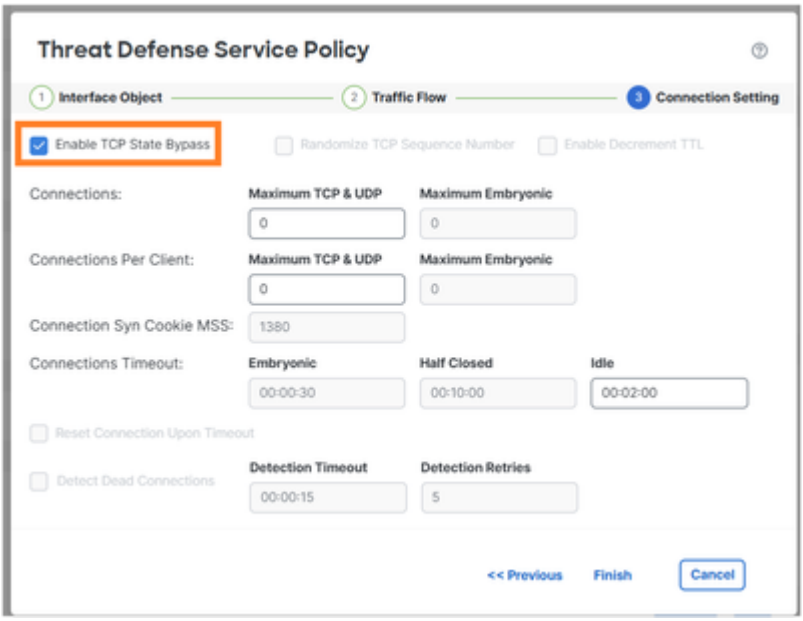
Bearbeiten Sie die dem FTD zugewiesene Zugriffskontrollrichtlinie (ACP), wählen Sie die Registerkarte Erweiterte Einstellungen aus, und bearbeiten Sie die Richtlinie für den Bedrohungsschutz. Wählen Sie Regel hinzufügen und Weiter aus.

Schritt 3

Wählen Sie die erweiterte ACL aus:



Schritt 4



Schritt 5

Wählen Sie Fertig stellen, OK, Speichern und Bereitstellen.

Ergebnis:

<#root>

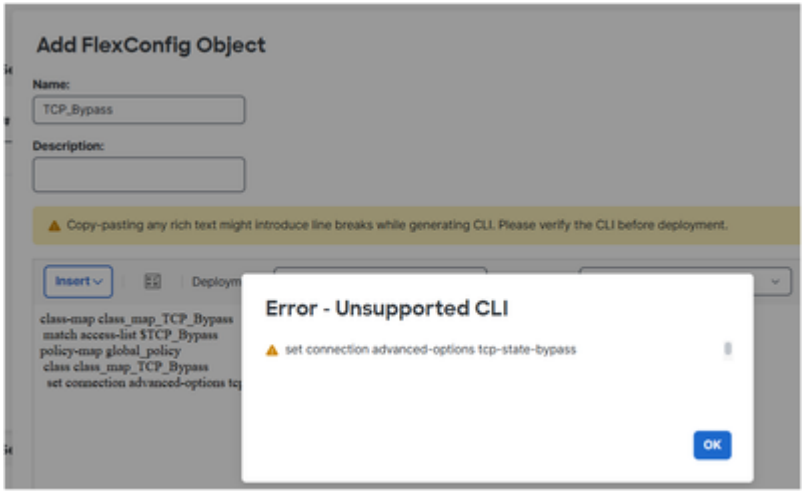
```
firewall#

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
```

Anmerkung: In früheren FMC-Versionen wie 6.x können Sie FlexConfig verwenden, um die TCP-Zustandsumgehung zu konfigurieren. In neueren Versionen wird dies nicht unterstützt:



Verifizierung

<#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:
```

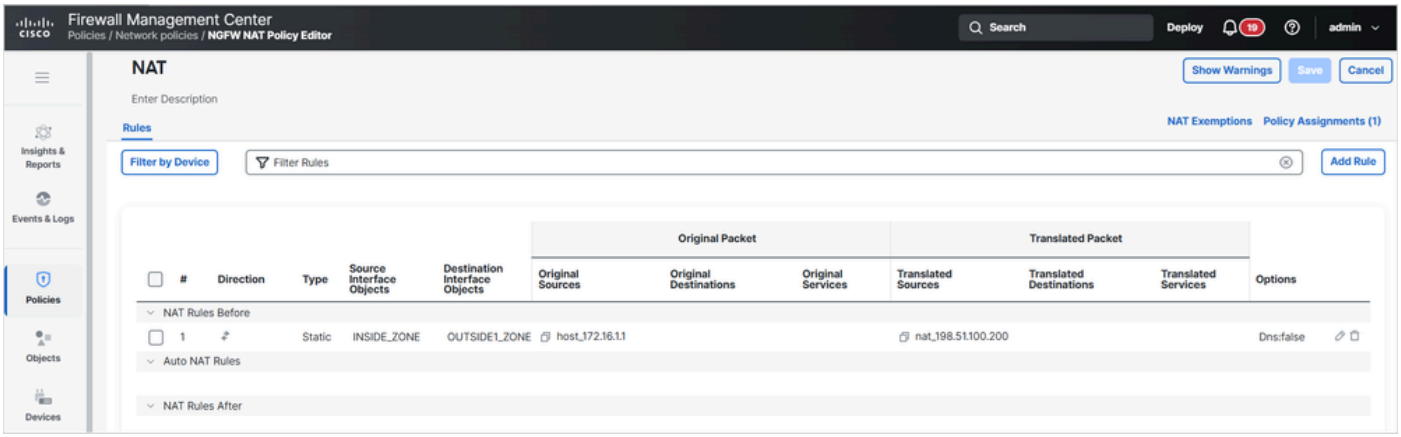
```
class-map class_map_TCP_Bypass
```

```
 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
...
```

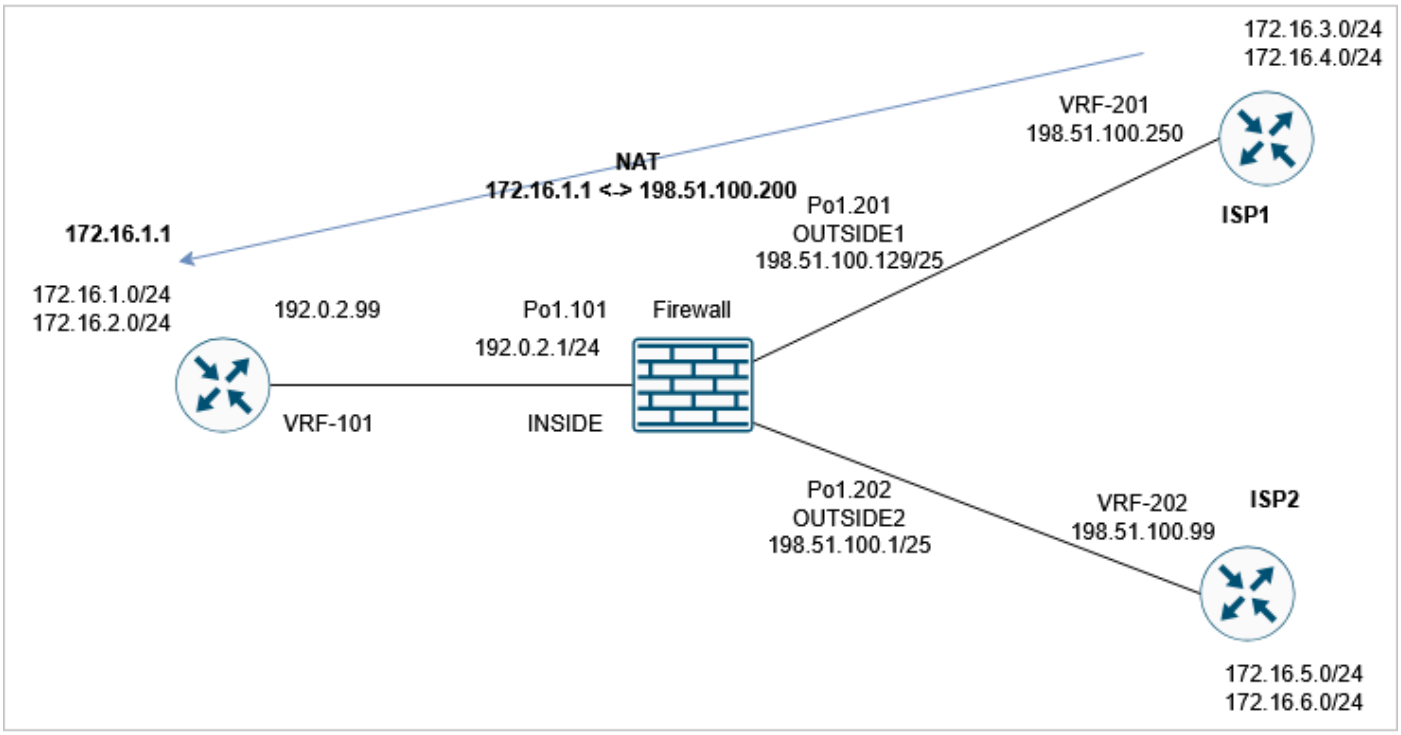
Aufgabe 4: Änderung der Traceroute-Ausgabe

Voraussetzung

Konfigurieren Sie statische NAT auf FTD, sodass die IP 172.16.1.1 hinter der INSIDE-Schnittstelle auf OUTSIDE1-Hosts als 198.51.100.200 angezeigt wird:



Führen Sie dann eine Traceroute von ISP1 zu 198.51.100.200 (Host 172.16.1.1) aus:



<#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 *
```

Anforderung

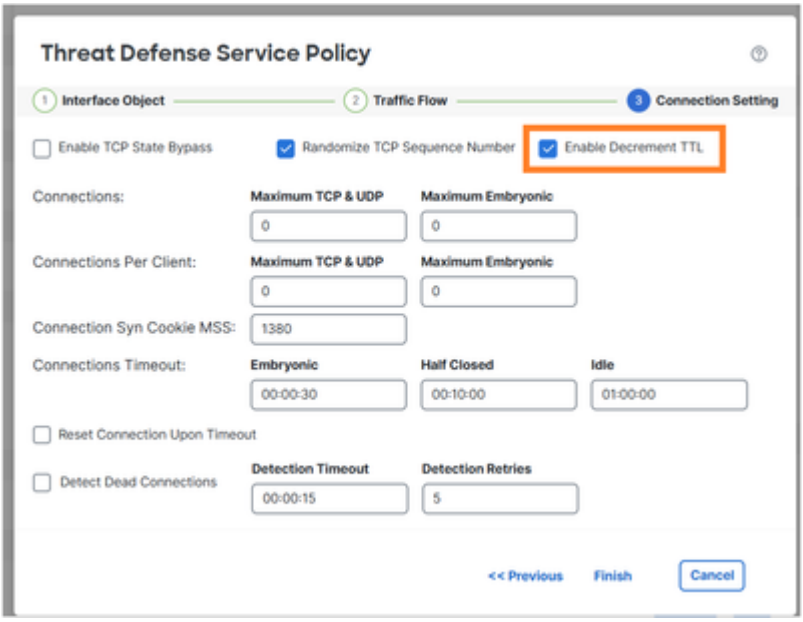
Ändern Sie die FTD-Konfiguration so, dass die Traceroute dieser Ausgabe entspricht:

<#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 *
```

Lösung

Die Lösung umfasst zwei Konfigurationsschritte:
1. Die TTL wird dekretiert:

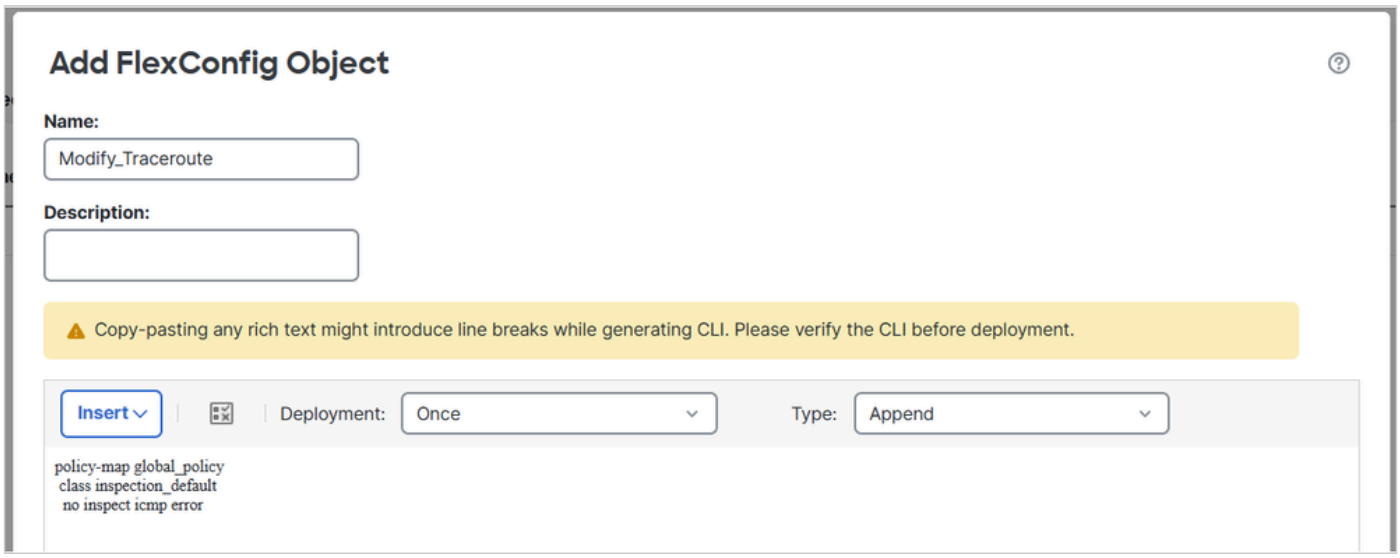


Nach dieser Änderung wird der Firewall-Hop auf der Traceroute angezeigt:

<#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. ICMP-Fehlerüberprüfung deaktivieren:




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

Verifizierung

Die Traceroute zeigt die übersetzte NAT-IP-Adresse des Remote-Hosts und die FTD-Schnittstellen-IP-Adresse an:

<#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 *
```

Aufgabe 5: Verbindungszeitüberschreitungen festlegen

Anforderung

Ändern Sie die Zeitüberschreitung für diesen Fluss auf 1 Woche:

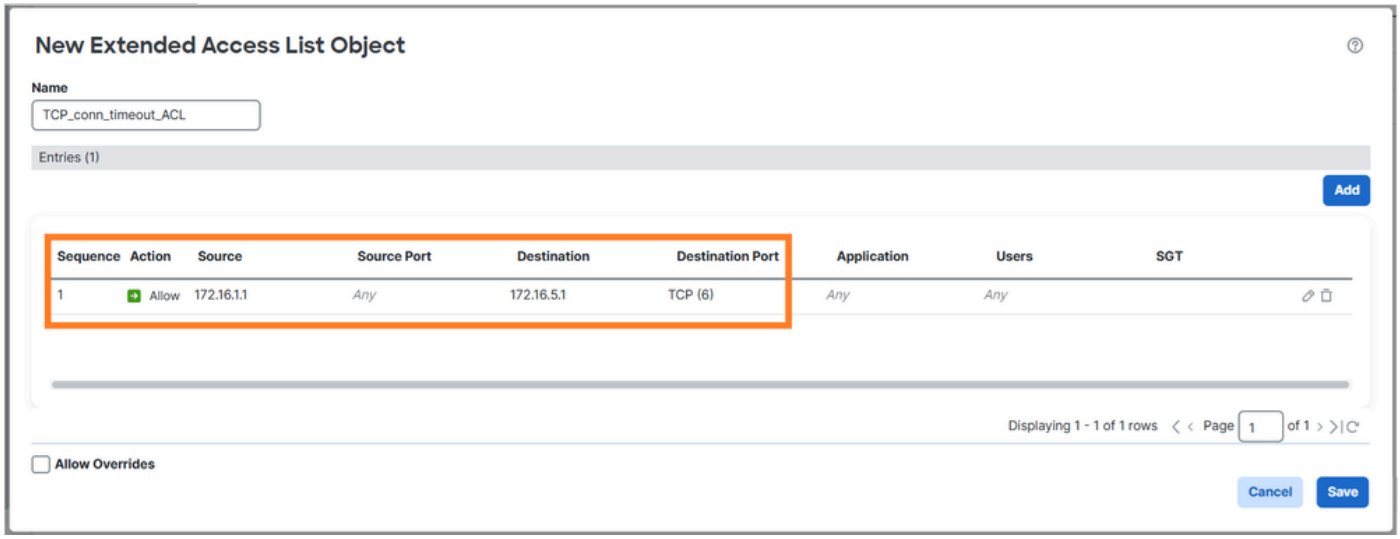
- Protokolle: TCP
- SRC: 172.16.1.1
- DST: 172.16.5.1

Lösung

Um ein Timeout für jeden Fluss festzulegen, müssen Sie die Servicerichtlinie verwenden.

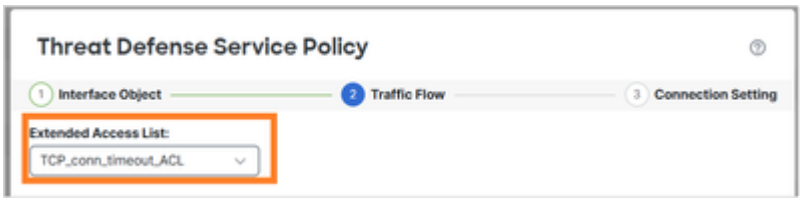
Schritt 1

Navigieren Sie zu Objekte > Zugriffsliste, und erstellen Sie eine erweiterte Zugriffskontrollliste, die dem entsprechenden Datenverkehr entspricht:

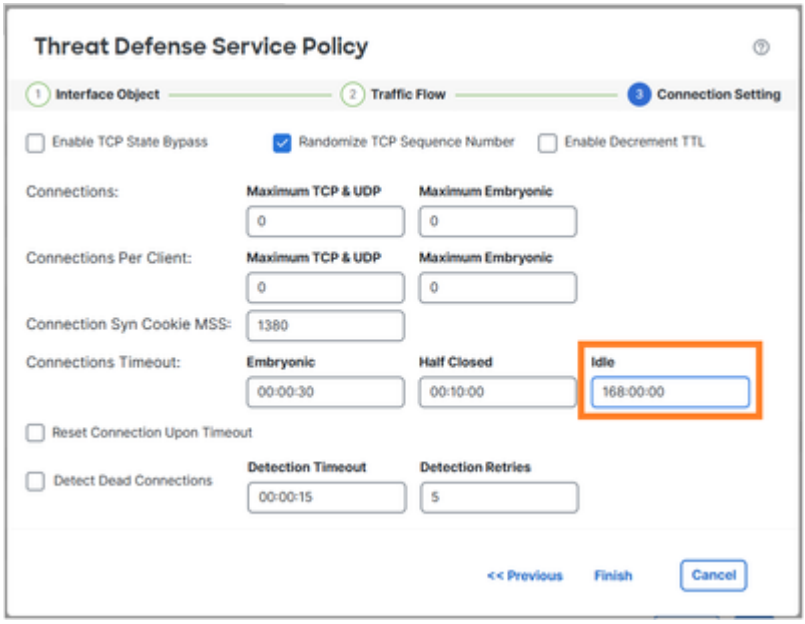


Schritt 2

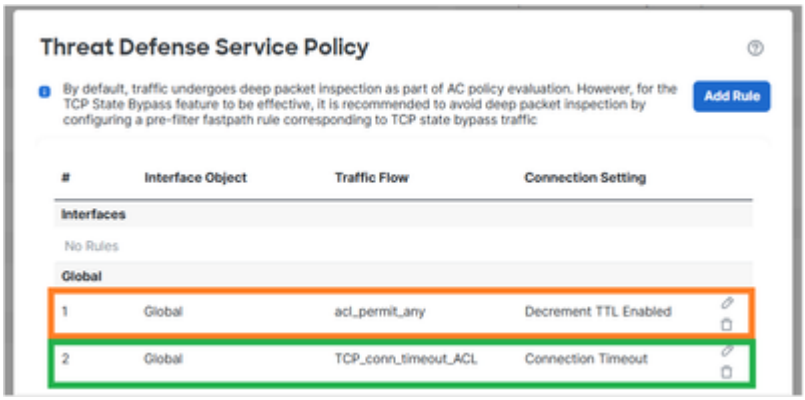
Konfigurieren Sie eine MPF-Richtlinie, die die in Schritt 1 erstellte ACL verwendet:



Timeout für Verbindungsleerlauf festlegen:



Entfernen Sie die Regel aus der vorherigen Aufgabe, da sie sich mit der neuen Anforderung überschneidet:



Verifizierung

Konfiguration der bereitgestellten Richtlinienzuweisung:

<#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
```

Starten Sie eine neue TCP-Verbindung von 172.16.1.1 zu 172.16.5.1, und überprüfen Sie die Verbindungstabelle des FTD:

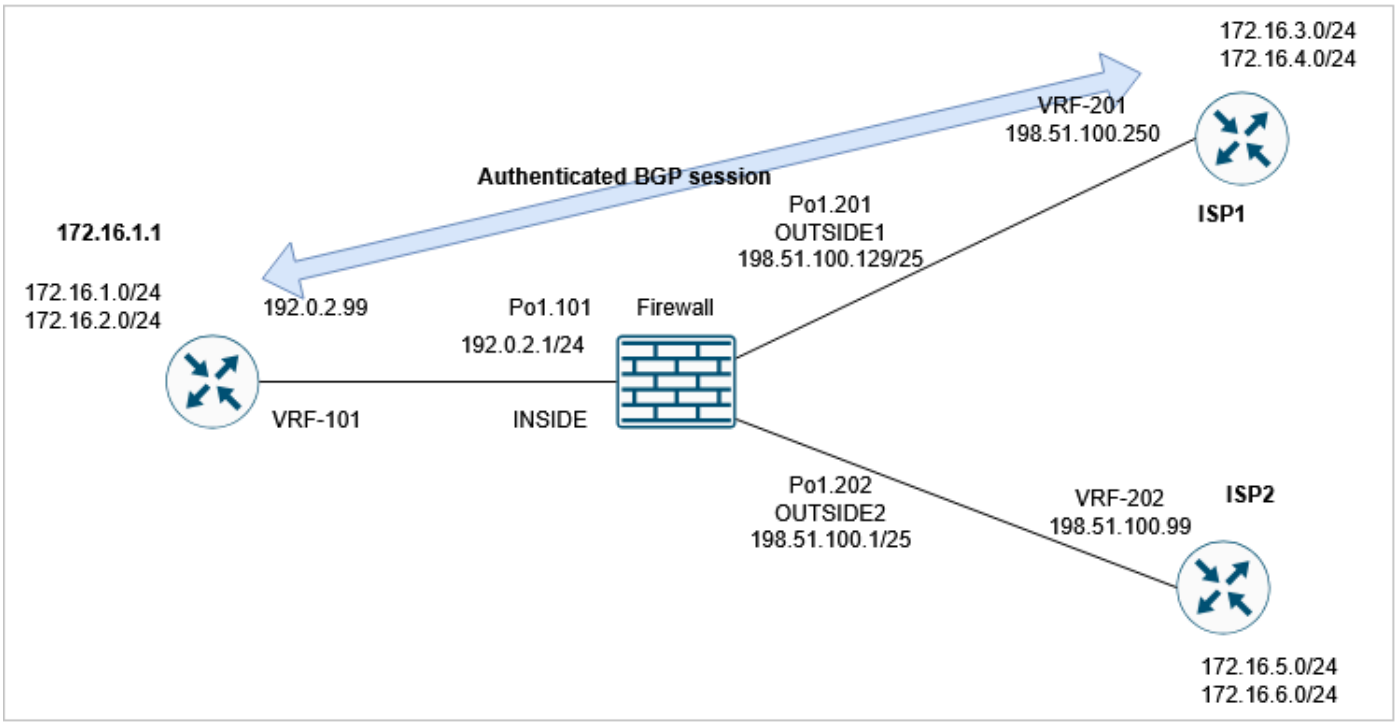
<#root>

```
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
```

Aufgabe 6: BGP-Authentifizierung über FTD

Voraussetzung

Konfigurieren Sie eine BGP-Sitzung über die FTD. Die BGP-Sitzung muss eine Authentifizierung verwenden.



Verifizierung

Mit der FTD-Standardkonfiguration wird die BGP-Sitzung nicht eingerichtet. Der Router zeigt Folgendes:

<#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)
```

Auf der FTD sehen Sie, dass beide Seiten die BGP TCP-Verbindung nicht herstellen können (die Verbindungsflags weisen darauf hin, dass nur TCP SYN-Pakete empfangen werden):

<#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
```

Lösung

Damit eine authentifizierte BGP-Sitzung über die FTD möglich ist, müssen die folgenden beiden Bedingungen erfüllt sein:

1. TCP MD5 (Option 19) muss über FTD zugelassen werden.
2. Die Randomisierung der TCP-Sequenznummer muss deaktiviert werden.

Die MD5-TCP-Option ist standardmäßig zulässig:

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
```

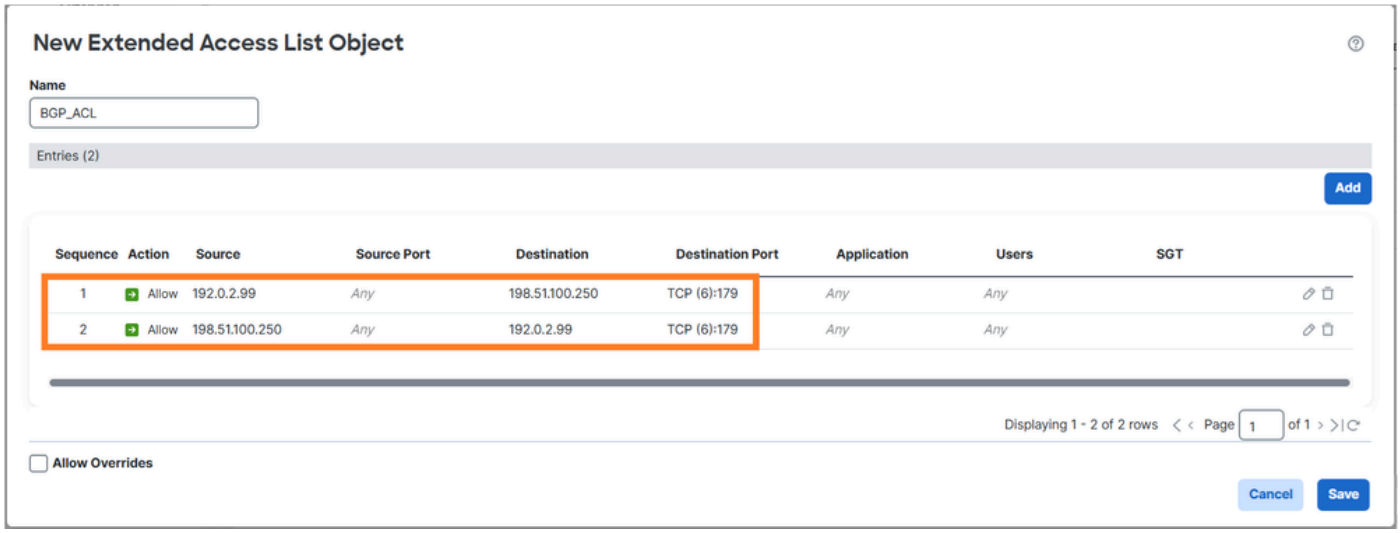
```
  no checksum-verification
  exceed-mss allow
  queue-limit 0 timeout 4
  reserved-bits allow
  syn-data allow
  synack-data drop
  invalid-ack drop
  seq-past-window drop
  tcp-options range 6 7 allow
  tcp-options range 9 18 allow
  tcp-options range 20 255 allow
  tcp-options selective-ack allow
  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
```

Zufällige TCP-Startsequenznummer (ISN) global deaktivieren:

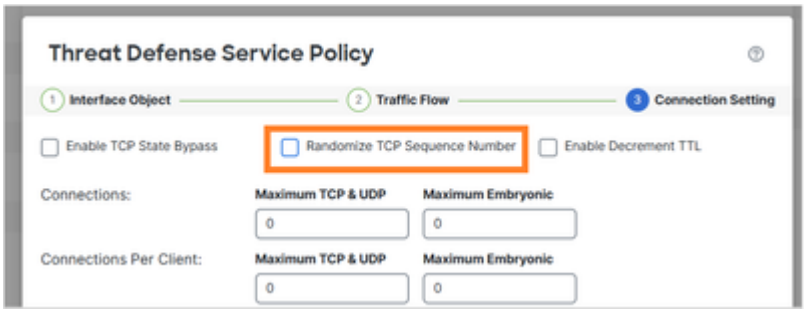
<#root>

```
>

configure tcp-randomization disable


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

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

oder (die bevorzugte Methode) eine erweiterte Zugriffsliste erstellen, die mit der BGP-Verbindung übereinstimmt:



und deaktivieren Sie die Zufälligkeit der TCP-Sequenznummer mithilfe der Richtlinie für den Bedrohungsschutz:



Verifizierung

Konfiguration der bereitgestellten Richtlinienzuweisung:

<#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
```

Die BGP-Sitzung wird über FTD eingerichtet:

<#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
```

Tipp: Sie können eine FastPath-Vorfilterregel für den BGP-Datenverkehr konfigurieren, um eine Snort-Überprüfung zu vermeiden.

Aufgabe 7: Dead Connection Detection (DCD)

Anforderung

Konfigurieren Sie DCD auf FTD für TCP-Datenverkehr, der für den Host 172.16.3.1 bestimmt ist.

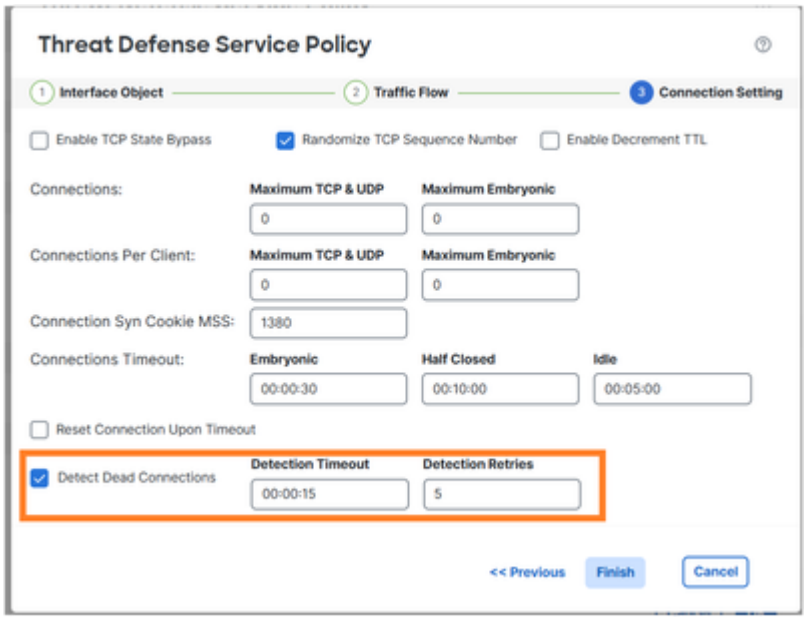
Lösung

DCD ist dokumentiert unter:

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. Navigieren Sie zu Objekte > Zugriffsliste, und erstellen Sie eine Zugriffsliste, die mit dem interessanten Datenverkehr übereinstimmt.

2. Bearbeiten Sie die Ihrer Firewall zugewiesenen ACPs, navigieren Sie zu den erweiterten Optionen, und wählen Sie Threat Defense Service Policy aus, um DCD zu aktivieren:



Die bereitgestellte Konfiguration:

```
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
```

So funktioniert es

Konfigurieren Sie FTD-Erfassungen, um den Backend-Vorgang anzuzeigen:

<#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
```

Stellen Sie eine TCP-Verbindung über die Firewall her:

<#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
```

Zunächst werden in den Firewall-Erfassungen keine DCD-Pakete angezeigt:

```
<#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
```

Wenn eine inaktive Verbindung den Timeout für inaktive Verbindungen erreicht, sendet die FTD gefälschte TCP ACK-Nachrichten an die Quelle und das Ziel:

```
<#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

Wenn beide antworten, wird der Leerlauf-Timer zurückgesetzt:

<#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
```

Anmerkung: DCD funktioniert nicht bei ausgelagerten Verbindungen ("o"-Flag).

Zugehörige Informationen

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.