تكوين إطار عمل سياسة نمطي للدفاع عن تهديد جدار الحماية

المحتويات

المقدمة

يصف هذا المستند إطار السياسات النمطية للدفاع عن تهديد جدار الحماية (FTD)

المتطلبات الأساسية

المتطلبات

هناك متطلب خاص لهذا الوثيقة.

المكونات المستخدمة

تستند المعلومات الواردة في هذه المستند إلى إصدارات البرامج والمكونات المادية التالية:

- Cisco Secure Firewall 3130 Threat Defense، الإصدار 10.0.0 (Build 140)
- مركز إدارة جدار الحماية (FMC)، الإصدار 10.0.0 (Build 140)

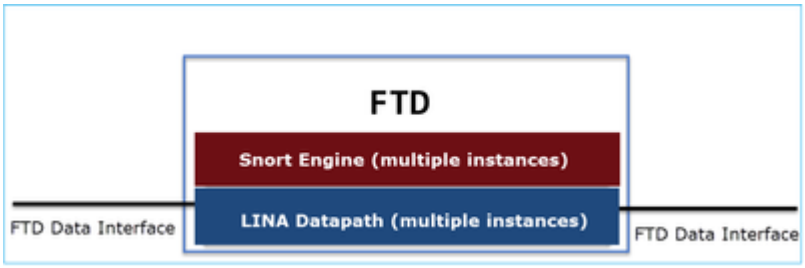
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

نظرة عامة على مستوى بيانات FTD

FTD عبارة عن صورة برنامج موحّد تتكون من محركين رئيسيين:

- Datapath (المعروف أيضا باسم LINA)
- محرك Snort



إن Lina Datapath و Snort Engine هما الجزءان الرئيسيان لمستوى بيانات FTD.

مكونات MPF

تستخدم MPF المكونات التالية:

- تطابق خريطة الفئة حركة المرور المثيرة للاهتمام.
- تطبق خريطة السياسة إجراءات على حركة المرور المثيرة التي تتطابق مع خريطة الفئة.
- يطبق Service-Policy خريطة السياسة بشكل عام (على جميع الواجهات) أو على واجهة معينة.

إتجاه الميزات

فيما يتعلق بتوجيه الميزات، راجع دليل تكوين ASA:

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

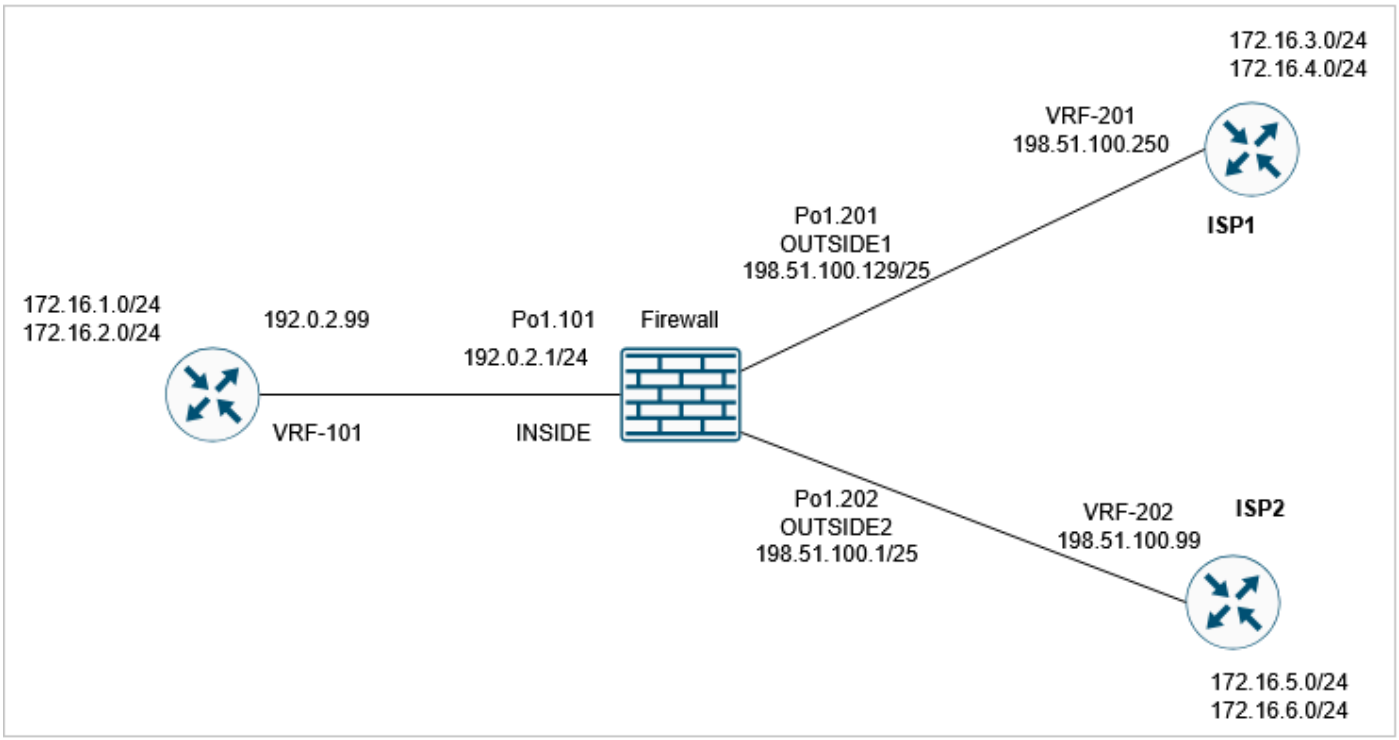
يتم تمييز الميزات المتعلقة ب FTD:

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

التكوين

المخطط



تكوين MPF الافتراضي (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
```

المهمة 1. تعطيل فحص SIP بشكل عام على FTD

الطلب في هذه المهمة هو تعطيل فحص SIP في محرك FTD LINA. أحد الأسباب يمكن أن يكون متطلب نهج أو عيب برنامج مرتبط ب SIP يؤثر على حركة مرور النقل.

الحل

قبل تعطيل فحص SIP، تأكد أو الم من تطبيقه على حركة مرور النقل:

<#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

هناك طريقتان لتعطيل فحص SIP بشكل عام:

الحل 1: تعطيل SIP من FTD CLISH

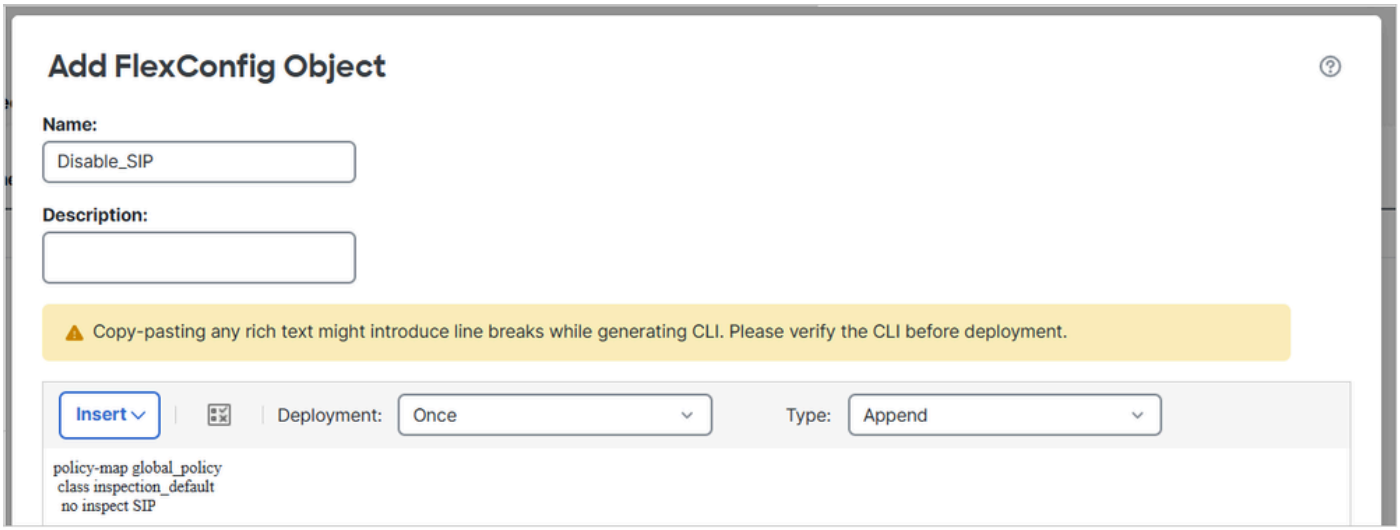
```
<#root>

>

configure inspection sip disable

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

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

التحقق

```
<#root>

>

show running-config policy-map | include sip

>
```

الحل 2: تعطيل SIP باستخدام FlexConfig

على FMC، انتقل إلى الأجهزة > FlexConfig وأنشئ كائن FlexConfig:



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

تطبيق نهج FlexConfig وتحديد Preview Config لمعاينته:

أخيرا، قم بنشر السياسة.

التحقق

<#root>

```
firewall#
```

show run policy-map | include sip

```
firewall#
```

ملاحظة - يلزمك مسح اتصال SIP الحالي من جدول اتصال LINA حتى يتم إعادة إنشاء الاتصالات بدون فحص SIP. يمكنك استخدام هذا الأمر للتحقق من اتصالات SIP الموجودة:

<#root>

```
firewall#
```

```
show conn port 5060
```

المهمة 2. تعطيل فحص SIP لمضيفين محددين

في هذه المهمة يكون المتطلب تعطيل فحص SIP لحركة المرور بين هذه الشبكات:

- س.ر: 172.16.1.0/24
- د.ت.: 172.16.3.0/24

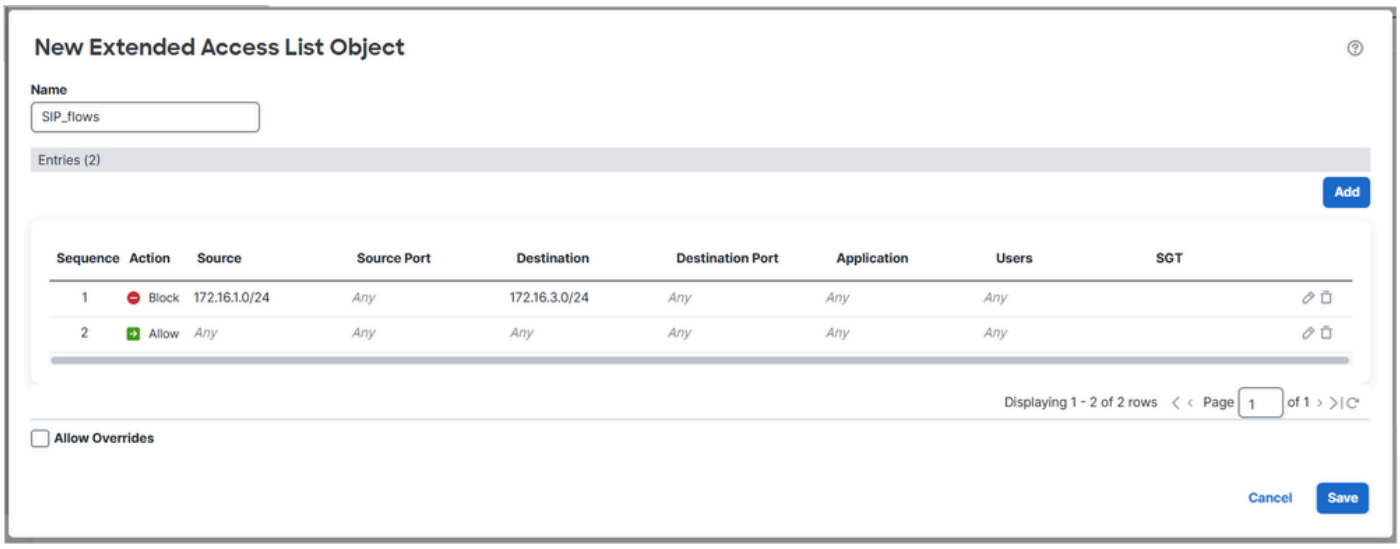
قد يكون أحد أسباب القيام بذلك هو حدوث عيب في البرنامج يتعلق ب SIP ويؤثر على حركة مرور النقل

الحل

إستخدام FlexConfig.

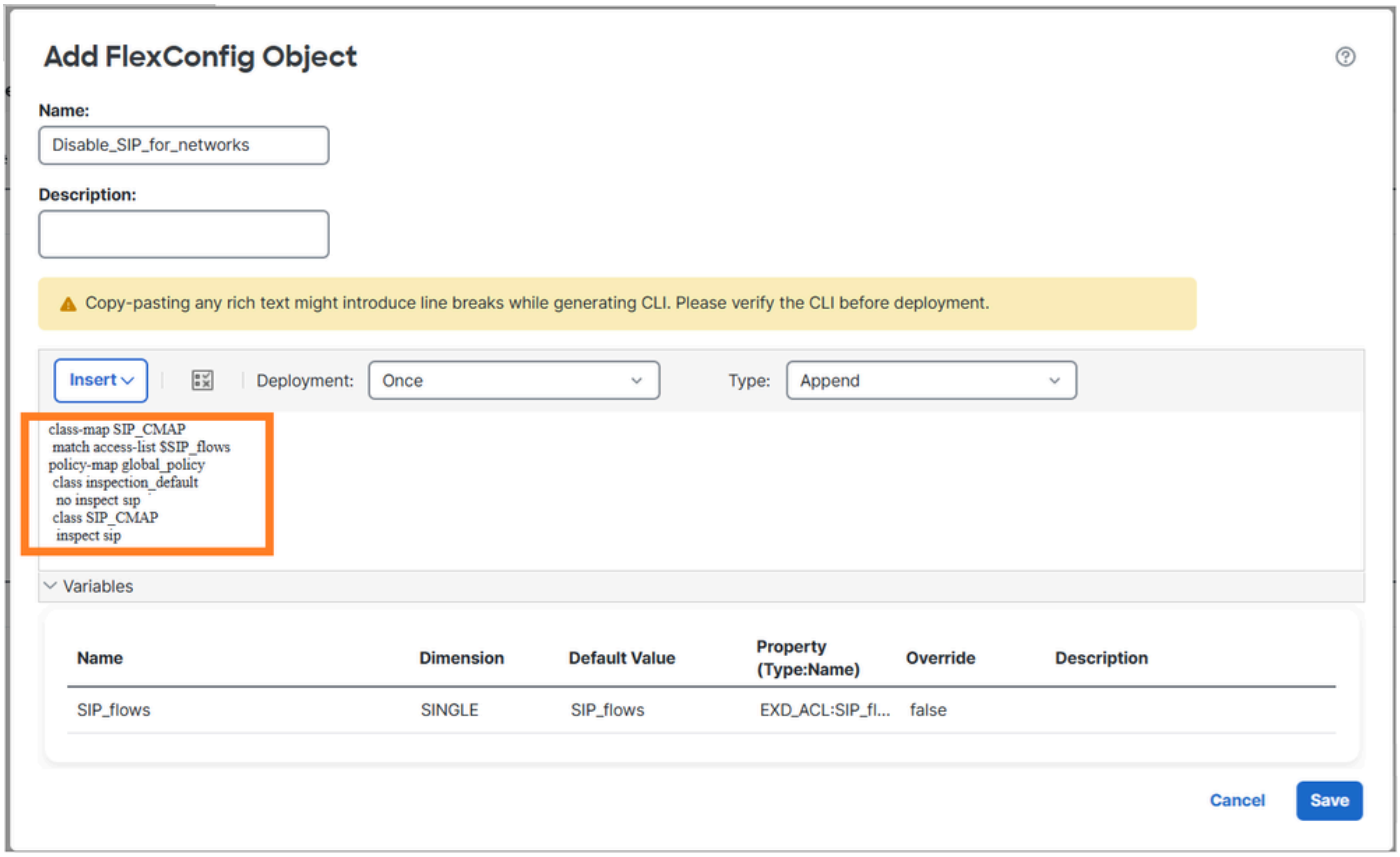
الخطوة 1

انتقل إلى كائنات > قائمة الوصول > موسع وأنشئ قائمة وصول موسعة تطابق حركة المرور المثيرة للاهتمام. يجب إستخدام إجراء الحظر منذ الهدف لاستبعاد حركة المرور المحددة. بالإضافة إلى ذلك، أضف قاعدة السماح لمطابقة بقية حركة المرور:



الخطوة 2

قم بإنشاء كائن FlexConfig باستخدام خريطة الفئة التي تطابق قائمة التحكم في الوصول (ACL) لبروتوكول SIP وتطبيقها في global_policy:



كائن FlexConfig الذي تم تكوينه:

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

ملاحظة

عند تكوين قائمة التحكم في الوصول (ACL) المسموح بها حاول أن تكون محددة قدر الإمكان (على سبيل المثال، وضع منافذ البروتوكول) لتجنب أي تأثير محتمل لوحدة المعالجة المركزية (CPU). لا يحدد المثال في هذه المهمة منافذ البروتوكول ويمكن تجنبه في الإنتاج.

التحقق 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
```

التحقق 2

تحتوي حركة المرور التي لم يتم فحصها بواسطة فحص SIP على 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
...
```

تحتوي حركة المرور التي يتم فحصها بواسطة فحص SIP على 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,
                                                                                                 ...
```

التحقق 3

يزداد عداد فحص "sip" عندما يتم فحص حزمة بواسطة جدار الحماية:

<#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
```

...

المهمة 3. تكوين تجاوز حالة TCP لمضيفين محددين

في هذه المهمة، تتمثل المتطلبات في تمكين تجاوز حالة TCP لحركة المرور بين هذه الشبكات:

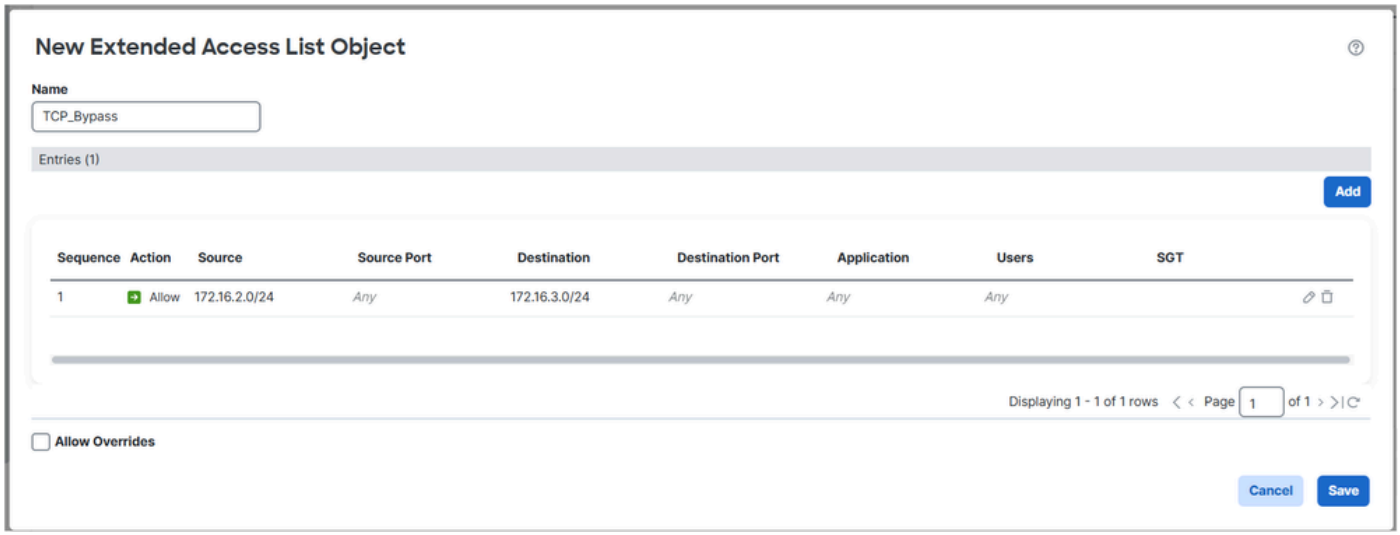
- ر.س: 172.16.2.0/24
- د.ت.: 172.16.3.0/24

تقوم بشكل عام، لا يوصى باستخدام تجاوز حالة TCP، ولكن يمكن استخدامه كحل بديل لمعالجة التدفقات غير المتماثلة.

الحل 1

الخطوة 1

إنشاء قائمة تحكم في الوصول (ACL) موسعة تطابق حركة المرور المثيرة:

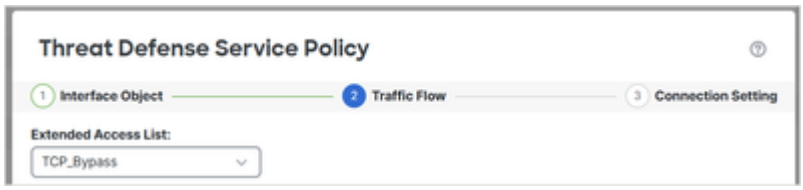


الخطوة 2

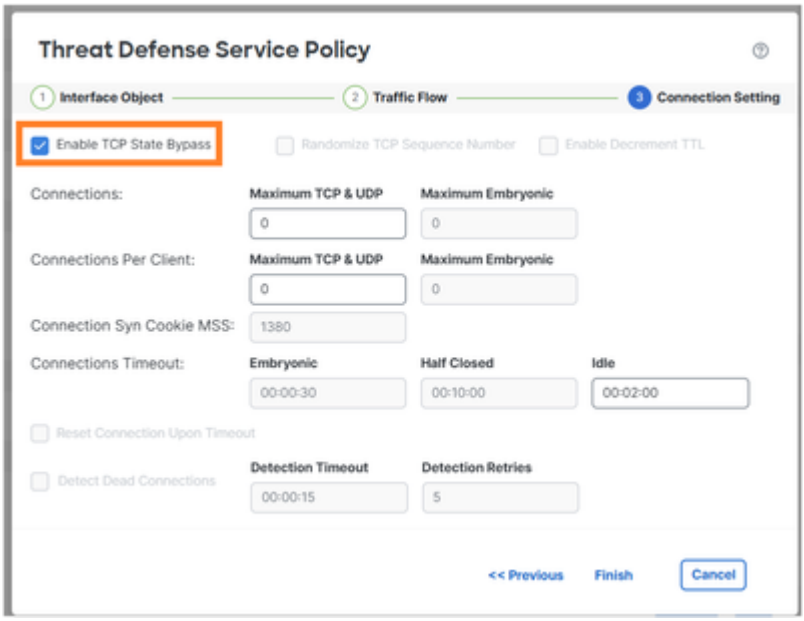
قم بتحرير نهج التحكم بالوصول (ACP) المعين لـ FTD، وحدد علامة التبويب إعدادات متقدمة وتحرير نهج خدمة الدفاع عن التهديدات. حدد إضافة قاعدة والتالي.

الخطوة 3

حدد قائمة التحكم في الوصول (ACL) الموسعة:



الخطوة 4



الخطوة 5

حدد إنهاء، موافق، حفظ ونشر.

النتيجة:

<#root>

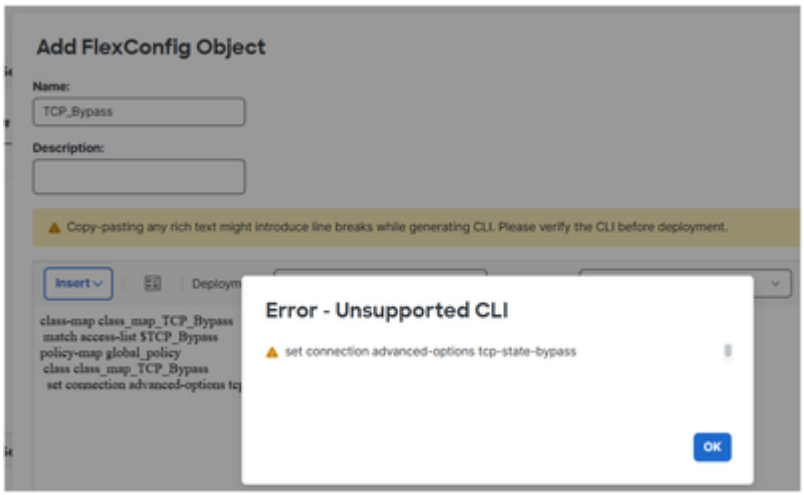
```
firewall#

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
```

ملاحظة: في إصدارات FMC السابقة مثل 6.x، يمكنك إستخدام FlexConfig لتكوين تجاوز حالة TCP. في الإصدارات الأحدث، هذا غير مدعوم:



التحقق

<#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

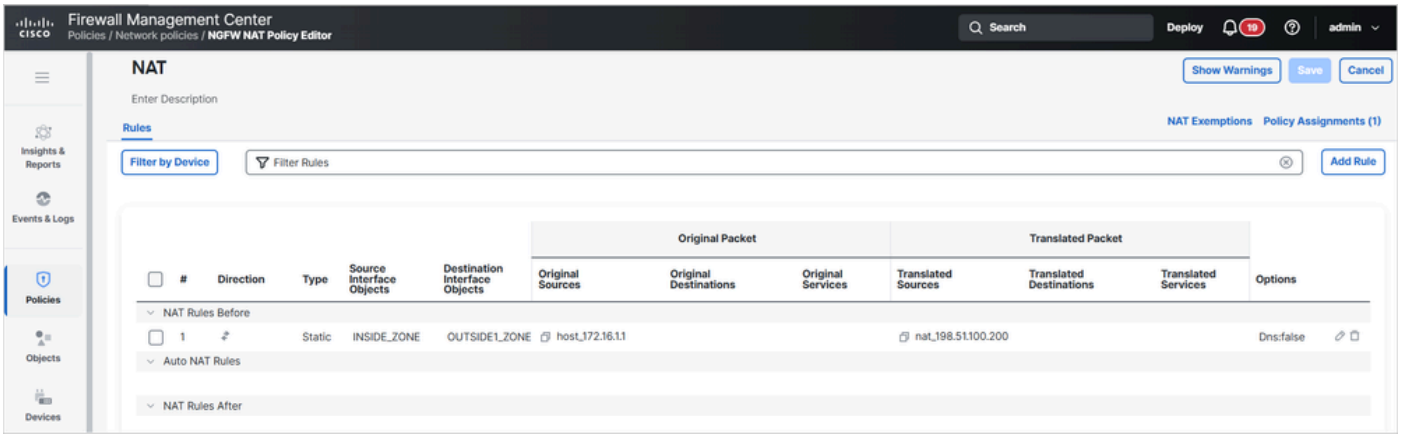
dst ip/id=172.16.3.0, mask=255.255.255.0, port=0, tag=any,

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

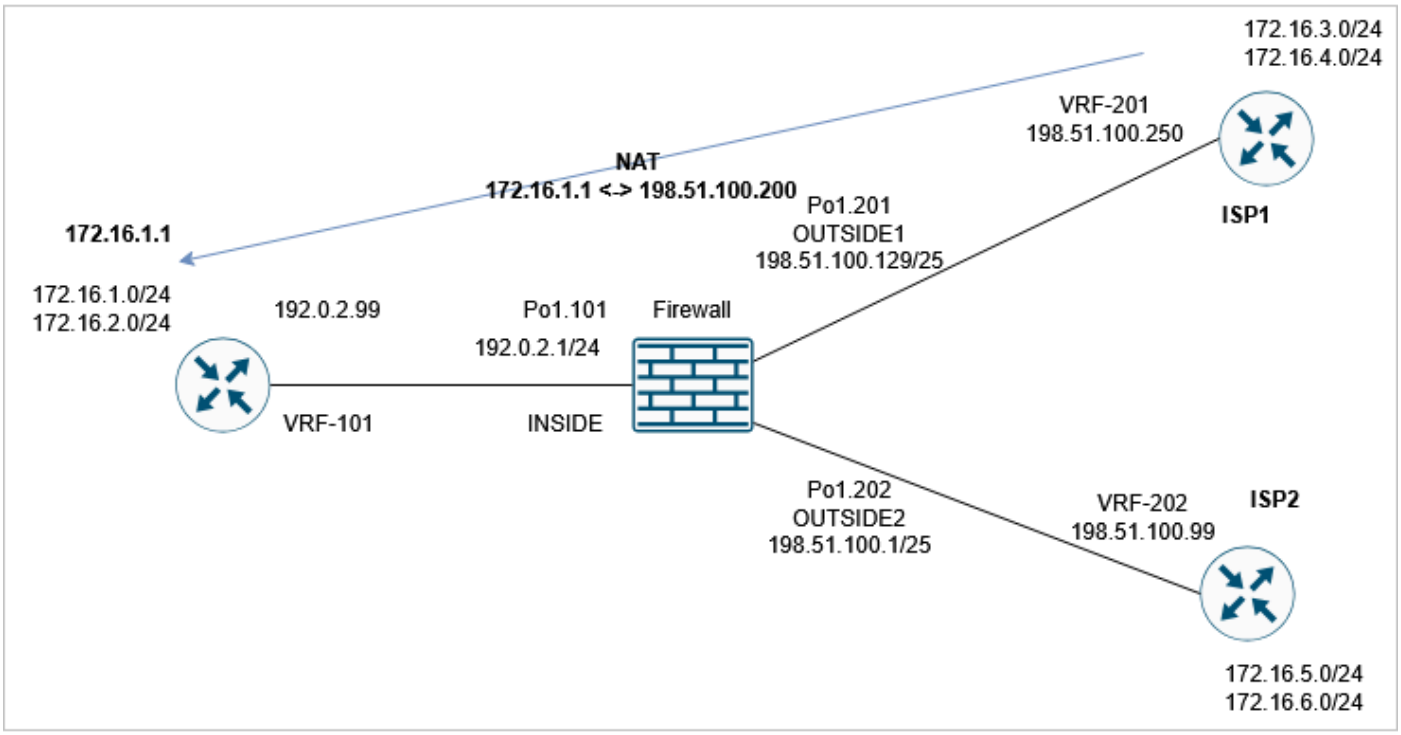
المهمة 4. تعديل مخرجات Traceroute

المتطلبات الأساسية

شكلت NAT ساكن إستاتيكي على FTD لذلك IP 172.16.1.1 يتواجد خلف قارن يظهر
198.51.100.200 على خارج1 مضيف:



بعد ذلك، قم بتشغيل traceroute من ISP1 إلى 198.51.100.200 (المضيف 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 *
```

المتطلبات

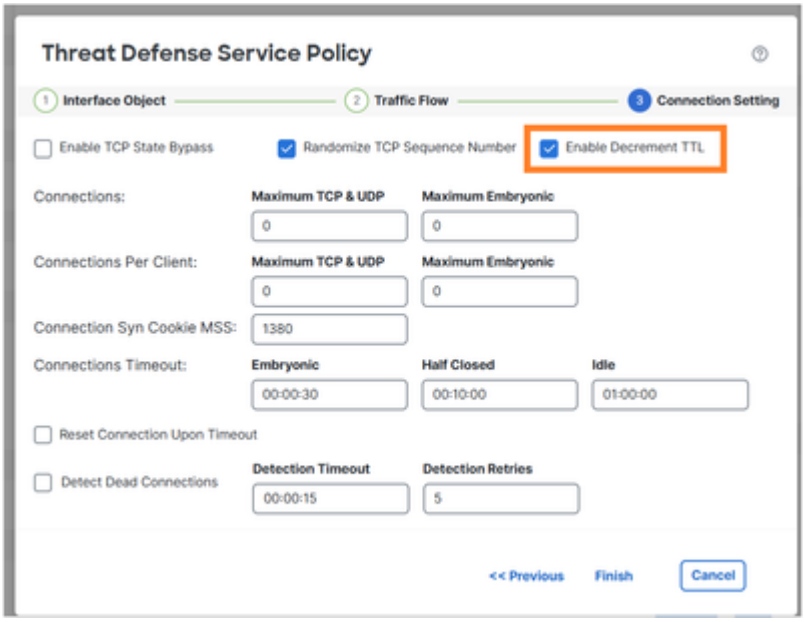
قم بتعديل تكوين FTD حتى تتطابق traceroute مع هذا الإخراج:

<#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 *
```

الحل

يتضمن الحل خطوتين للتكوين:
1. تقليل مدة البقاء (TTL):

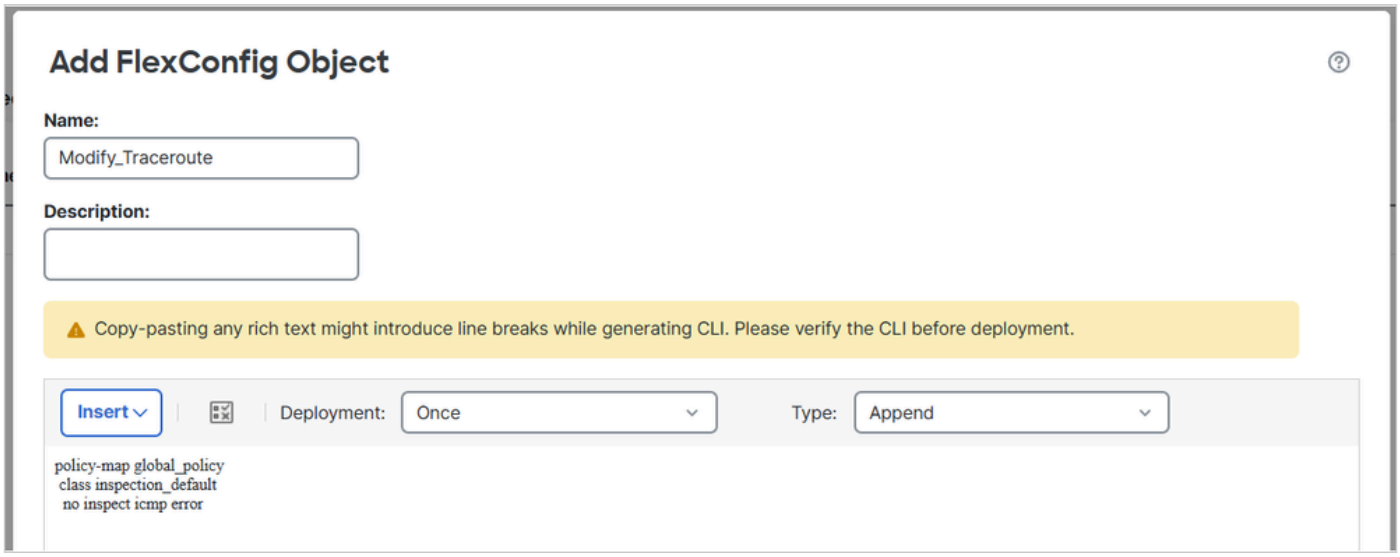


بعد هذا تغيير، يكشف ال traceroute جدار مانع للحريق:

<#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. تعطيل فحص خطأ ICMP:




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

التحقق

يبدي ال traceroute ال يترجم nat عنوان من المضيف بعيد والل FTD قارن عنوان:

<#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 *

المهمة 5. تعيين مهلات الاتصال

المتطلبات

تغيير المهلة إلى 1 أسبوع لهذا التدفق:

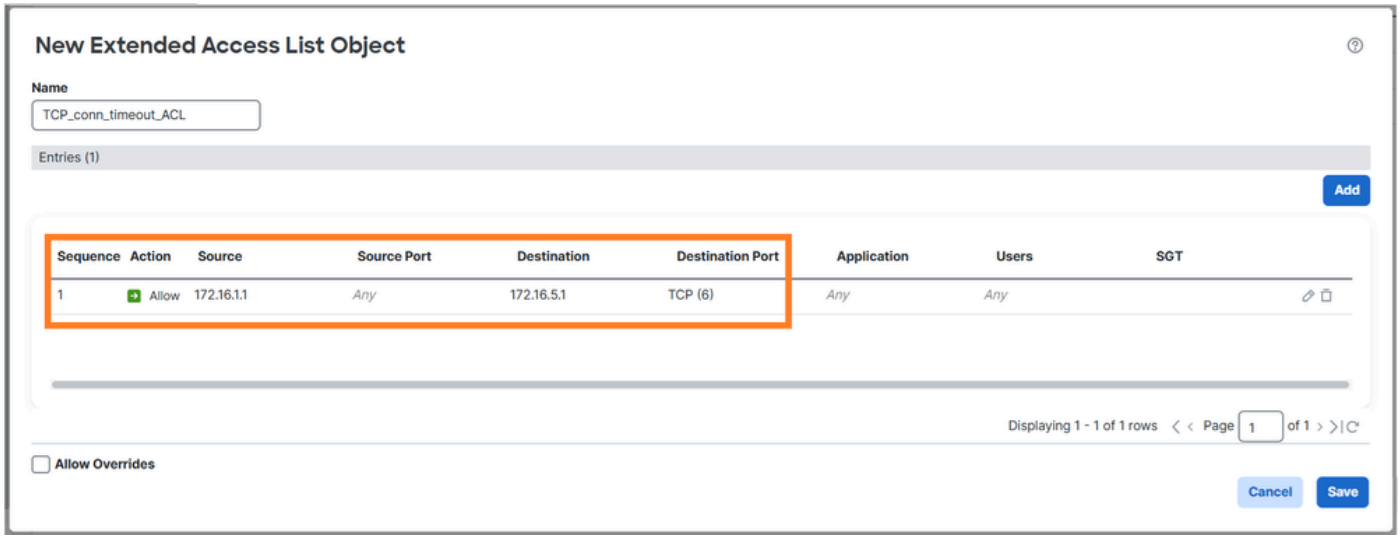
- البروتوكول: TCP
- س.ر: 172.16.1.1
- د.ت.: 172.16.5.1

الحل

لتعيين المهلة لكل تدفق تحتاج إلى إستخدام نهج الخدمة.

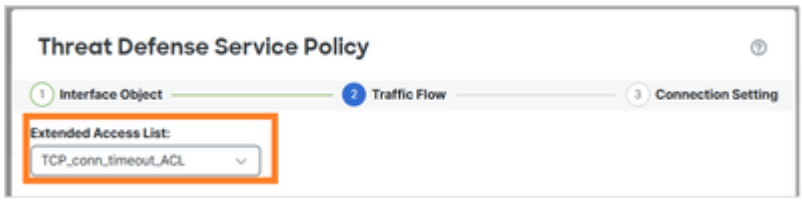
الخطوة 1

انتقل إلى كائنات > قائمة الوصول وأنشئ قائمة تحكم في الوصول (ACL) موسعة تطابق حركة المرور المفيدة:

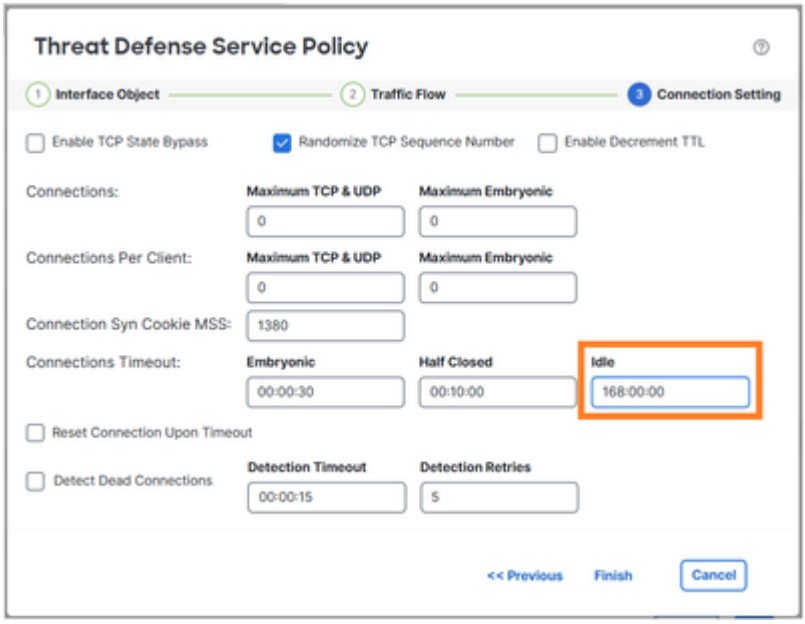


الخطوة 2

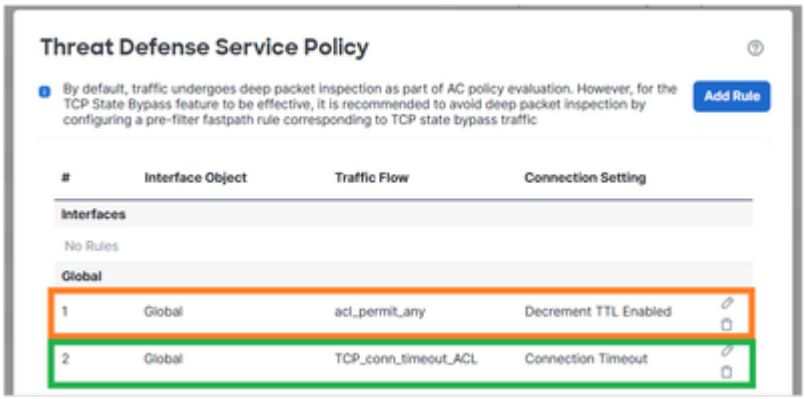
تكوين نهج MPF يستخدم قائمة التحكم في الوصول (ACL) التي تم إنشاؤها في الخطوة 1:



تعيين مهلة خمول الاتصال:



إزالة القاعدة من المهمة السابقة لأنها تتداخل مع المتطلب الجديد:



التحقق

تكوين خريطة السياسة المنشور:

<#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
```

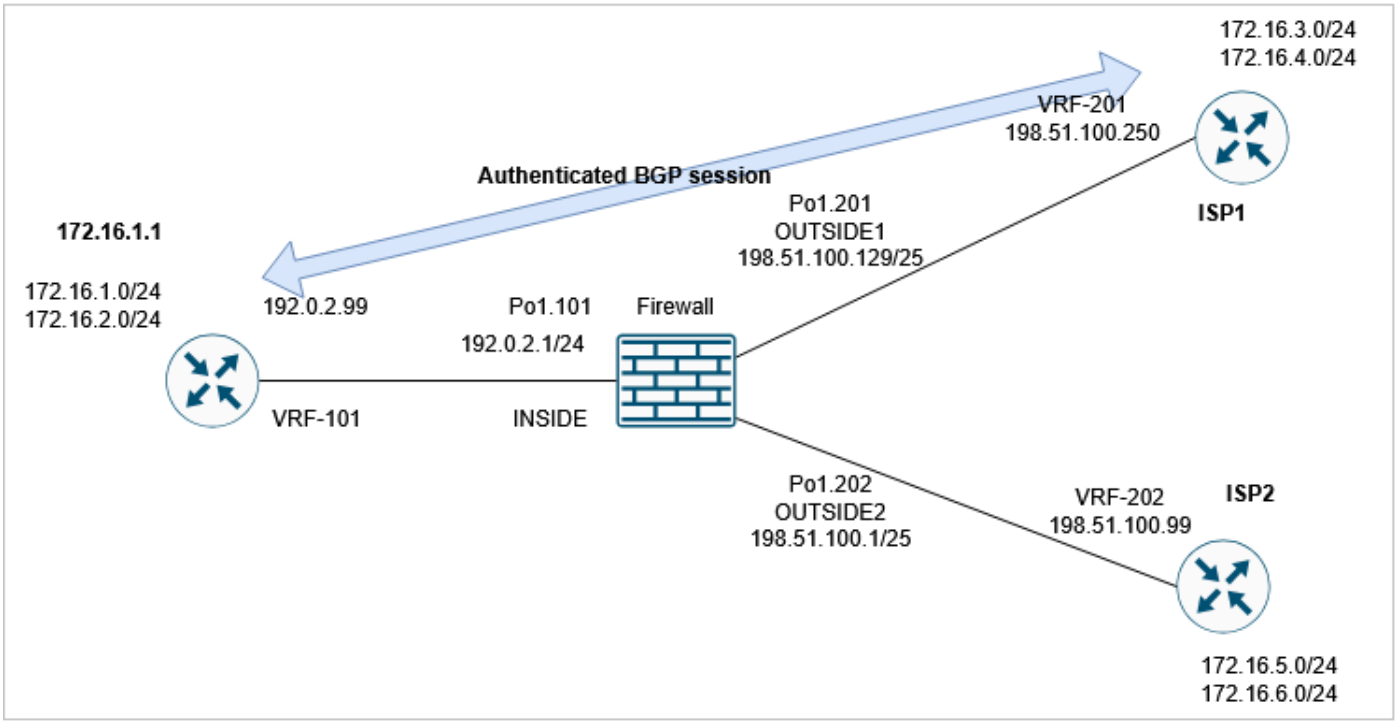
FTD: ب صاخلا لاتصالا لودج ددحو 172.16.5.1 ىلإ 172.16.1.1 نم ديدج TCP لاتصا أدبا

```
<#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
```

FTD لالخ نم BGP ةقداصم .6 ةمهملا

المتطلبات الأساسية

قم بتكوين جلسة BGP من خلال FTD. يجب أن تستخدم جلسة BGP المصادقة.



التحقق

باستخدام تكوين FTD الافتراضي، لم يتم إنشاء جلسة BGP. على الموجه، يمكنك مشاهدة:

<#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)

على FTD أنت ترى أن الجانب الذي يخلق BGP TCP توصيل (التوصيل يشير إلى أن إستلمت) يكون ربط TCP syn فقط:

<#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
```

الحل

للسماح بجلسة BGP مصدق عليها من خلال FTD يجب استيفاء الشرطين التاليين:

1. يجب السماح ل TCP MD5 (الخيار 19) من خلال FTD.
2. يجب تعطيل تعيين رقم تسلسل TCP عشوائيا.

يتم السماح بخيار TCP MD5 بشكل افتراضي:

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>

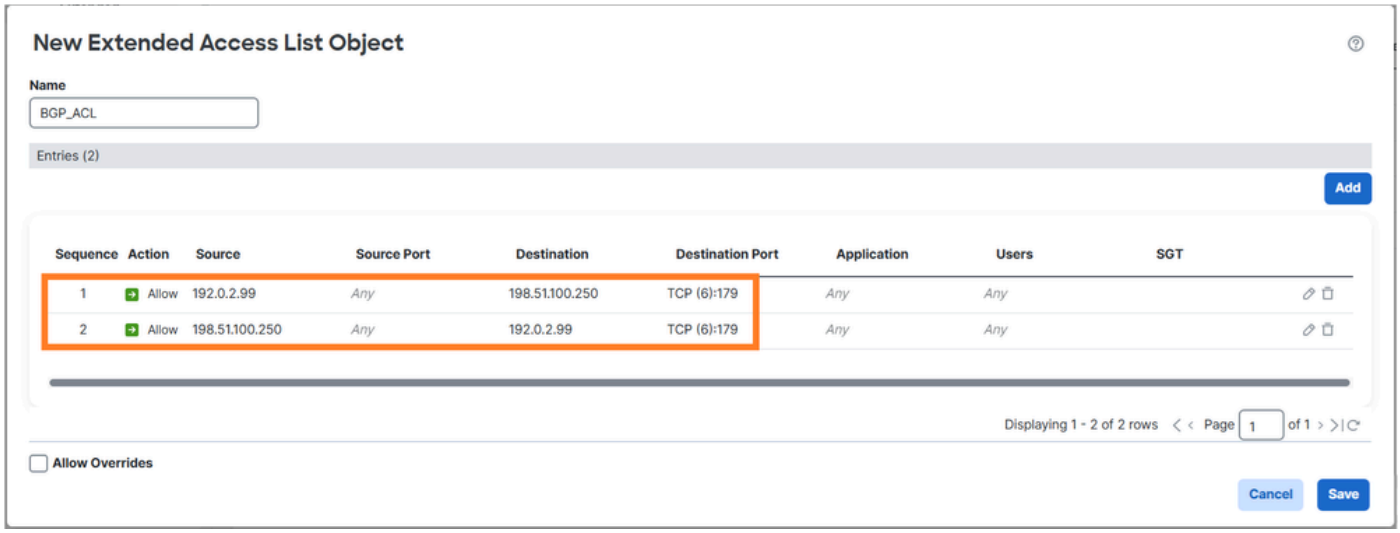
```
firewall#

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
```

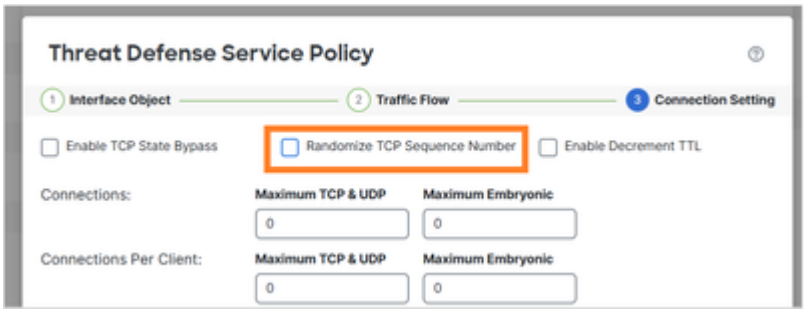
تعطيل عشوائي لرقم التسلسل الأولي (IS) ل TCP بشكل عام:

```
<#root>

                                                                    >

                                                  configure tcp-randomization disable


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

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

أو (الطريقة المفضلة) تقوم بإنشاء قائمة وصول موسعة تطابق اتصال BGP:



وتعطيل ترقيم تسلسل TCP العشوائي باستخدام نهج خدمة الدفاع عن التهديد:



التحقق

تكوين خريطة السياسة المنشور:

<#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
```

يتم إنشاء جلسة BGP من خلال 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
```

تلميح: يمكنك تكوين قاعدة مسار سريع ل PreFilter لحركة مرور BGP لتجنب فحص الشرخ.

المهمة 7. اكتشاف الاتصال غير المحقق (DCD)

المتطلبات

قم بتكوين DCD على FTD لحركة مرور TCP الموجهة إلى المضيف 172.16.3.1.

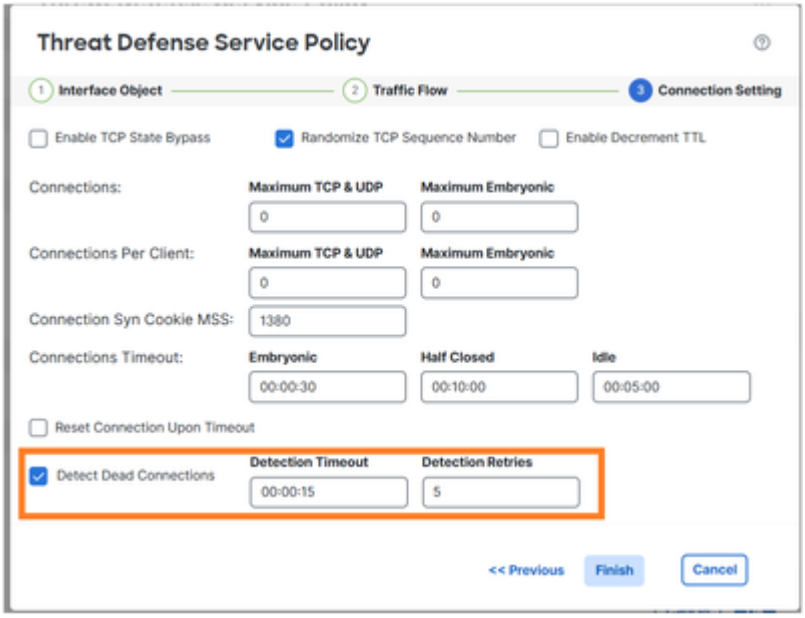
الحل

تم توثيق DCD على:

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. انتقل إلى كائنات > قائمة الوصول وأنشئ قائمة وصول تطابق حركة المرور المفيدة.

2. قم بتحرير قائمة التحكم في الوصول (ACP) المخصصة لجدار الحماية لديك والتنقل إلى الخيارات المتقدمة وحدد نهج خدمة الدفاع عن التهديدات لتمكين DCD:



التكوين الذي تم نشره:

```
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
```

كيف يعمل

تكوين لقطات FTD لرؤية عملية النهاية الخلفية:

```
<#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
```

إنشاء اتصال TCP من خلال جدار الحماية:

```
<#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
```

في البداية، لا توجد حزم DCD ظاهرة في مجموعات جدار الحماية:

```
<#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
```

عندما يصل اتصال خامل إلى مهلة الخمول، يرسل FTD رسائل TCP ACK المنتحلة إلى المصدر والوجهة:

<#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

إذا در كالهام، فإنه يعيد ضبط المؤقت الخامل:

<#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
```

ملاحظة: لا تعمل شاشة DCD على الاتصالات التي تم إلغاء تحميلها (علامة 'O').

معلومات ذات صلة

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

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).