تكوين واجهات الدفاع ضد تهديد Firepower في الوضع الموجه

المحتويات

المقدمة

يصف هذا المستند تكوين واجهة زوج مضمنة على جهاز الدفاع عن تهديد FirePOWER (FTD) والتحقق منها وتشغيلها.

المتطلبات الأساسية

المتطلبات

هناك ما من متطلب خاص ل هذا وثيقة.

المكونات المستخدمة

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

- ASA5512-X - رمز FTD 6.1.0.x
- مركز إدارة Firepower (FMC) - الرمز 6.1.0.x

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.

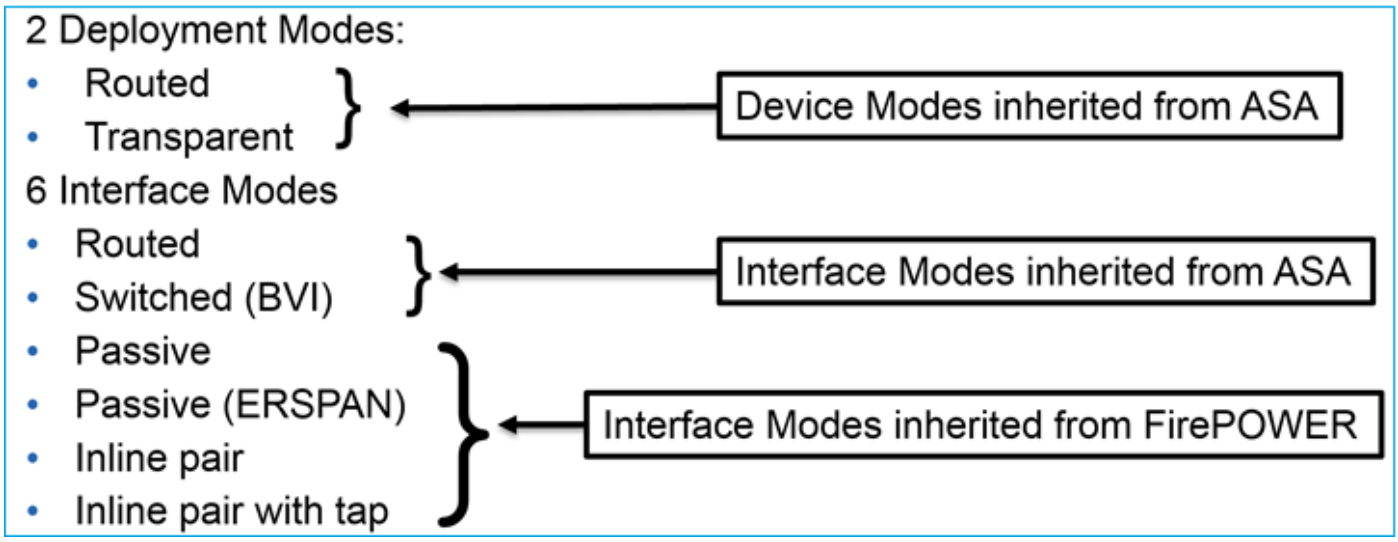
المنتجات ذات الصلة

هذا وثيقة يستطيع أيضا كنت استعملت مع هذا جهاز وبرمجية صيغة:

- ASA5506-X, ASA5506W-X, ASA5506H-X, ASA5508-X, ASA5516-X
- ASA5512-X, ASA5515-X, ASA5525-X, ASA5545-X, ASA5555-X
- FPR2100 و FPR4100 و FPR9300
- VMware (ESXi)، خدمات أمازون ويب (AWS)، الجهاز الافتراضي المستند إلى Kernel (KVM)
- رمز برنامج FTD الإصدار 6.2.x والإصدارات الأحدث

معلومات أساسية

يوفر الدفاع ضد تهديد Firepower (FTD) وضعي نشر وستة أوضاع واجهة كما هو موضح في هذه الصورة:



ملاحظة: يمكنك مزج أوضاع الواجهة على جهاز FTD واحد.

نظرة عامة عالية المستوى على مختلف أوضاع نشر برنامج الإرسال فائق السرعة (FTD) والواجهة:

نمط واجهة FTD	وضع نشر FTD	الوصف	يمكن إسقاط حركة المرور

مجوّم	مجوّم	فحص محرك LINA بالكامل ومحرك الشخر	نعم
محول	شفاف	فحص محرك LINA بالكامل ومحرك الشخر	نعم
زوج مضمن	موجه أو شفاف	محرك LINA الجزئي وفحوصات محرك الزخر بالكامل	نعم
زوج مضمن مع TAP	موجه أو شفاف	محرك LINA الجزئي وفحوصات محرك الزخر بالكامل	ال
خامل	موجه أو شفاف	محرك LINA الجزئي وفحوصات محرك الزخر بالكامل	ال
خامل (ERSPAN)	مجوّم	محرك LINA الجزئي وفحوصات محرك الزخر بالكامل	ال

التكوين

الرسم التخطيطي للشبكة

تكوين واجهة موجهة وواجهة فرعية

تكوين الواجهة الفرعية G0/0.201 والواجهة G0/1 وفقا لهذه المتطلبات:

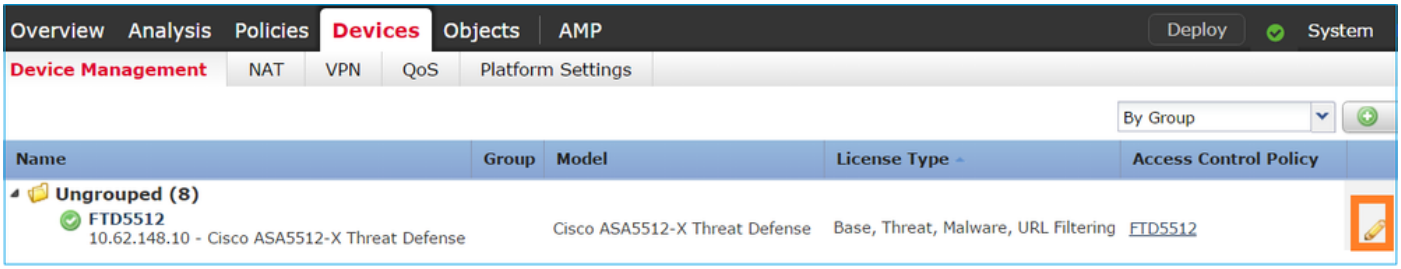
الواجهة	G0/0.201	G0/1
الاسم	داخل	خارج
المنطقة الأمنية	Inside_zone	Outside_Zone

الوصف	داخلي	خارجي
معرف الواجهة الفرعية	201	-
VLAN ID	201	-
IPv4	192.168.201.1/24	192.168.202.1/24
الإرسال ثنائي الإتجاه/السرعة	تلقائي	تلقائي

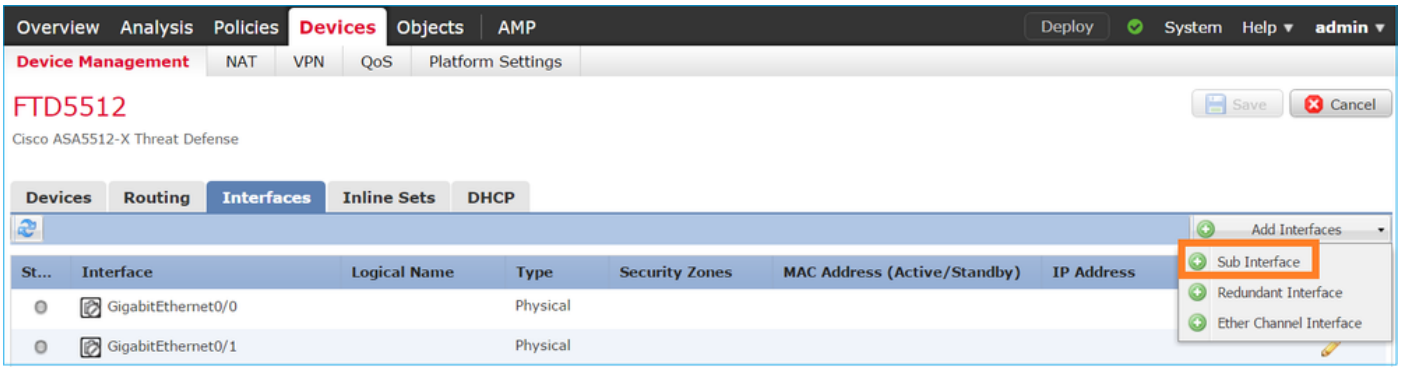
الحل

الخطوة 1. تكوين الواجهة المنطقية

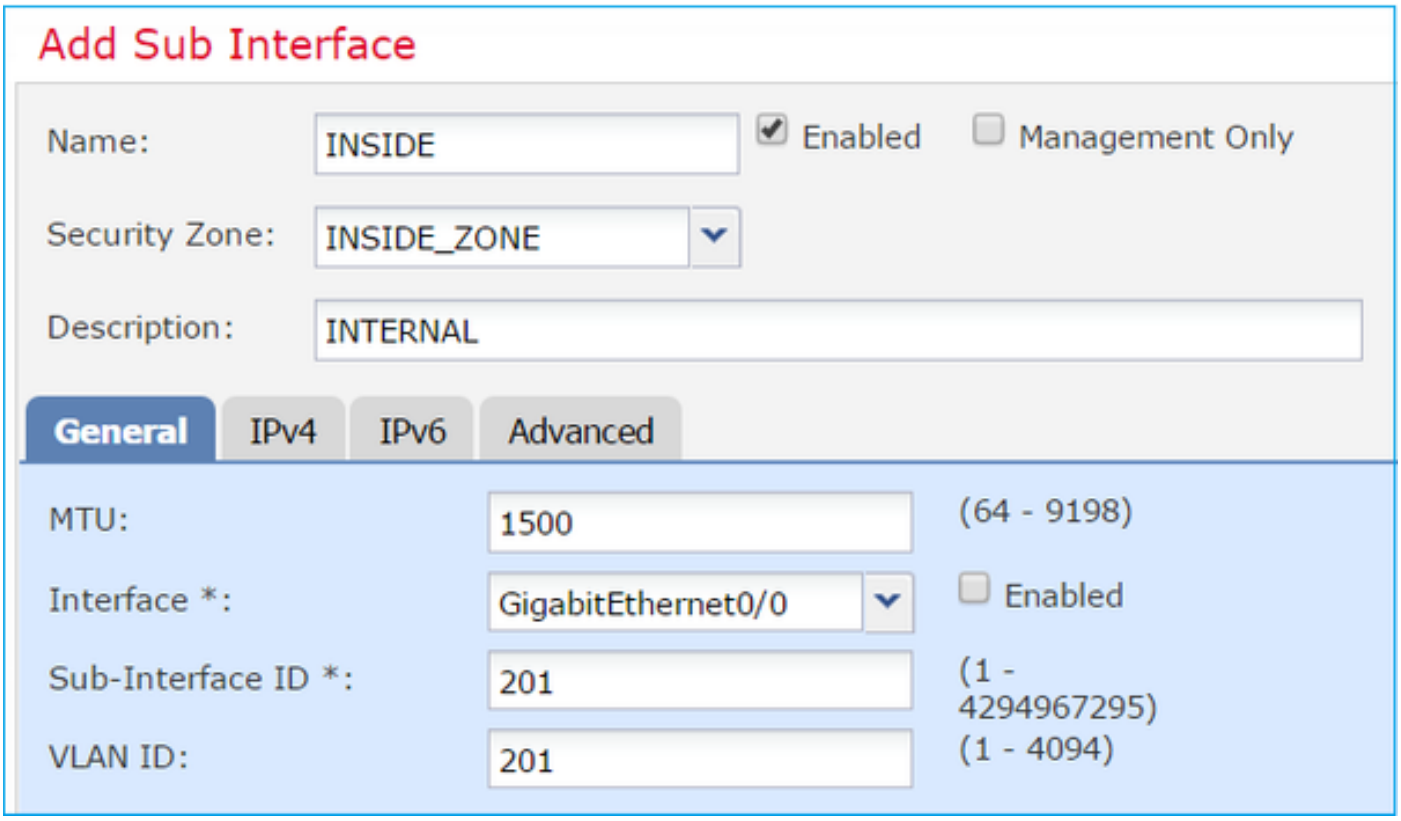
انتقل إلى الأجهزة > إدارة الأجهزة، وحدد الجهاز المناسب، ثم حدد أيقونة تحرير:



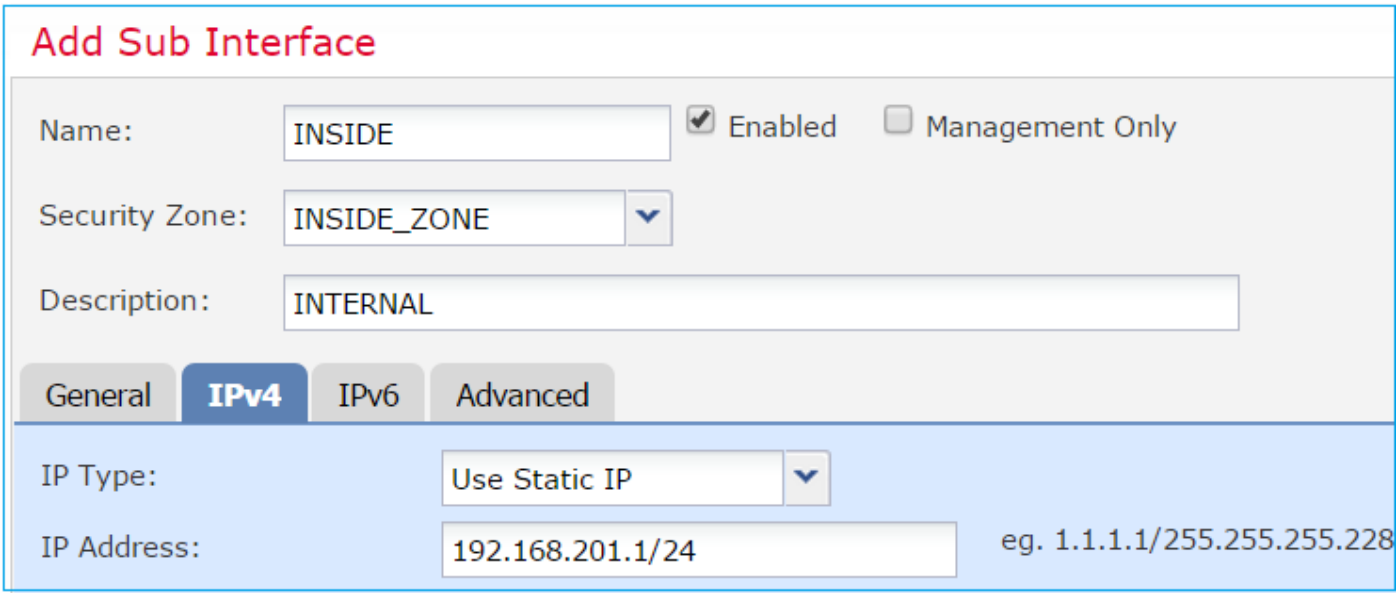
حدد إضافة واجهات > الواجهة الفرعية:



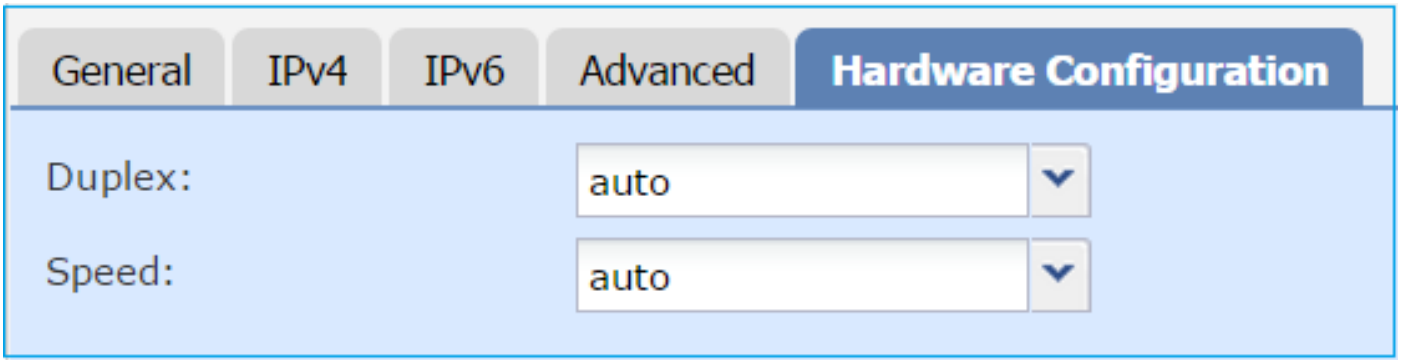
تكوين إعدادات الواجهة الفرعية حسب المتطلبات:



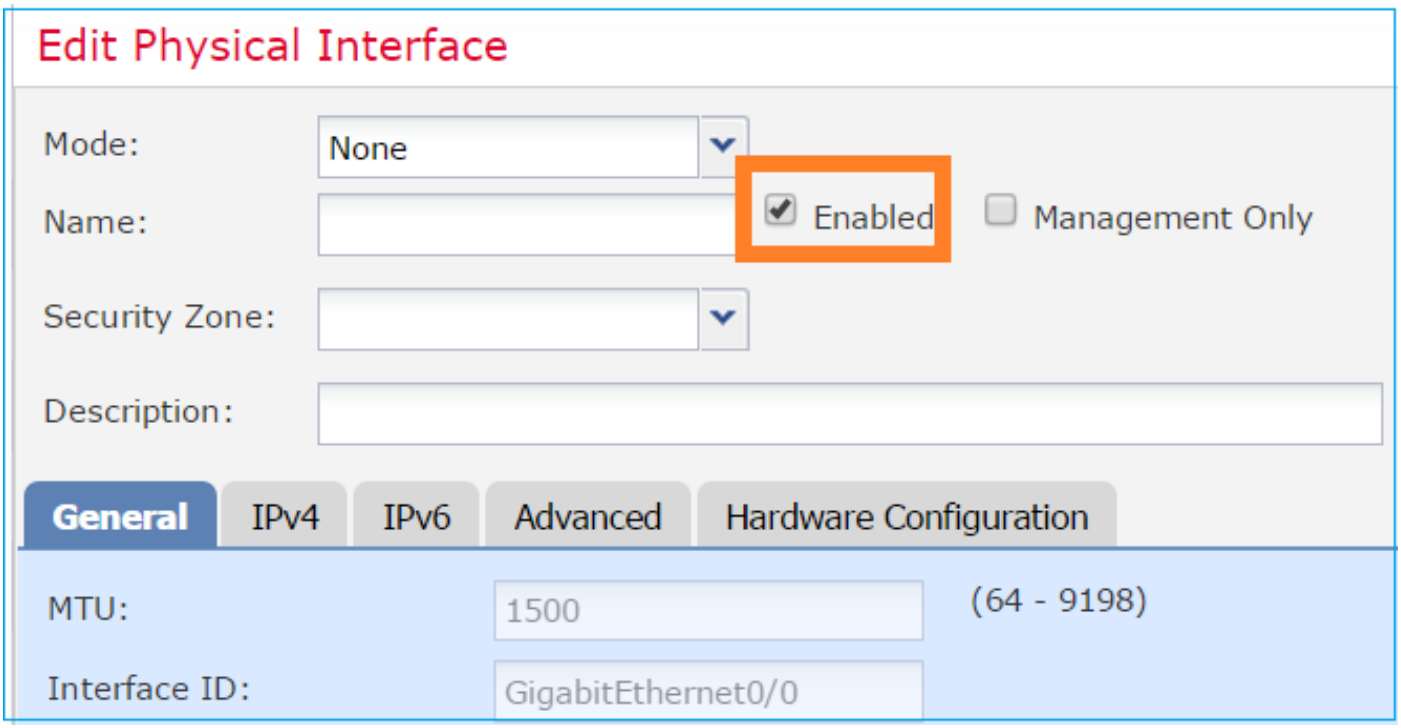
إعدادات IP للواجهة:



تحت الواجهة الفعلية (GigabitEthernet0/0) حدد إعدادات السرعة والإرسال ثنائي الإتجاه:

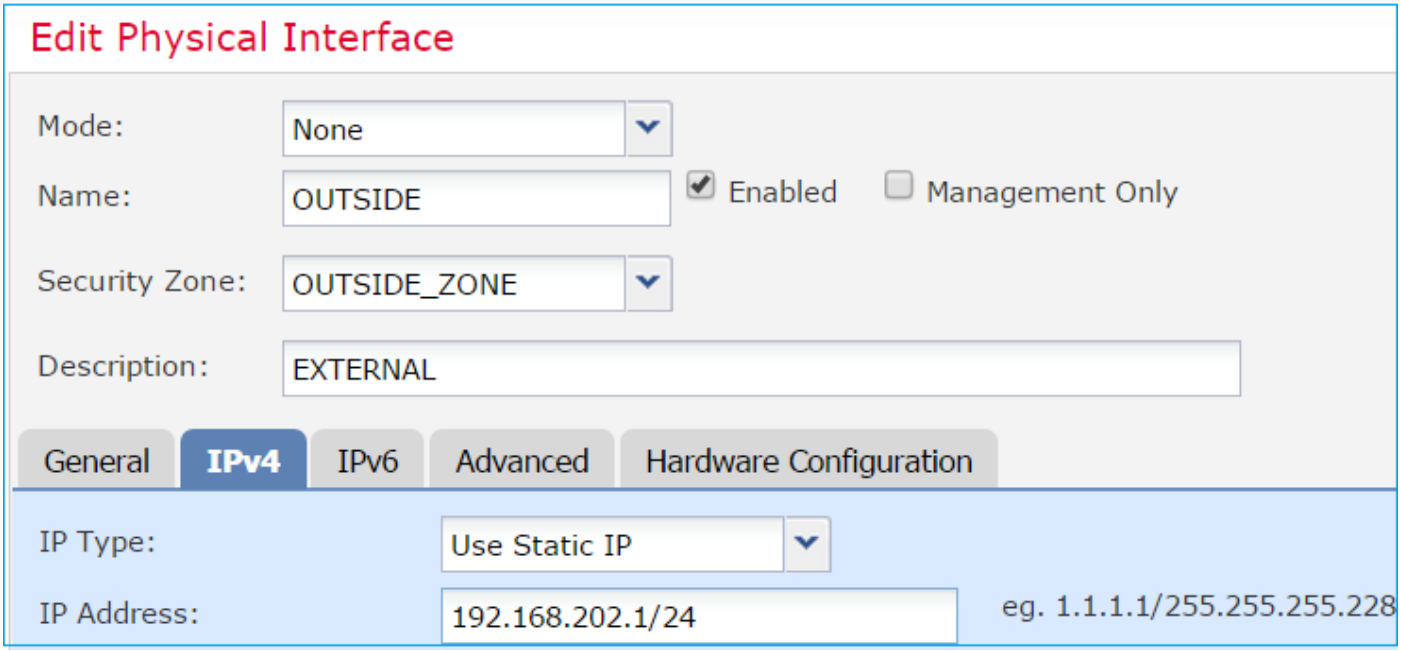


مكنت القارن طبيعي (G0/0 في هذه الحالة):



الخطوة 2. تكوين الواجهة المادية

قم بتحرير الواجهة المادية GigabitEthernet0/1 وفقا للمتطلبات:

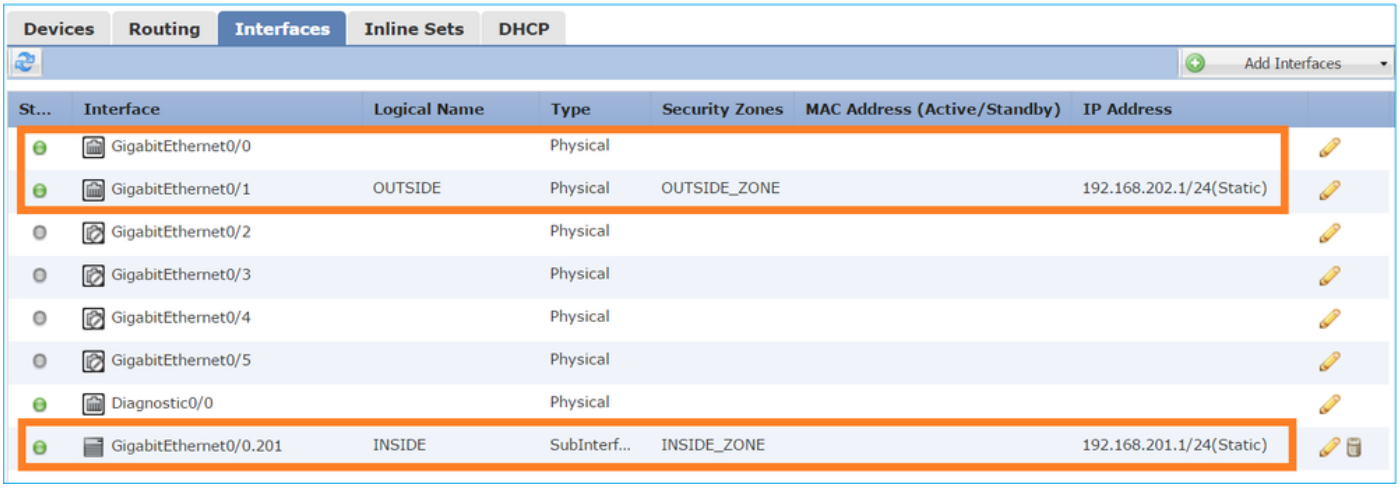


- للواجهة الموجهة يكون الوضع: none
- الاسم مكافئ لاسم واجهة ASA IF
- على FTD، تحتوي جميع الواجهات على مستوى الأمان = 0
- ال يتم تطبيق حركة مرور نفس الأمان على FTD. يسمح بحركة المرور بين واجهات FTD (بين) و(بين) بشكل افتراضي

حدد حفظ ونشر.

التحقق

من واجهة المستخدم الرسومية (GUI) لوحدة التحكم FMC:

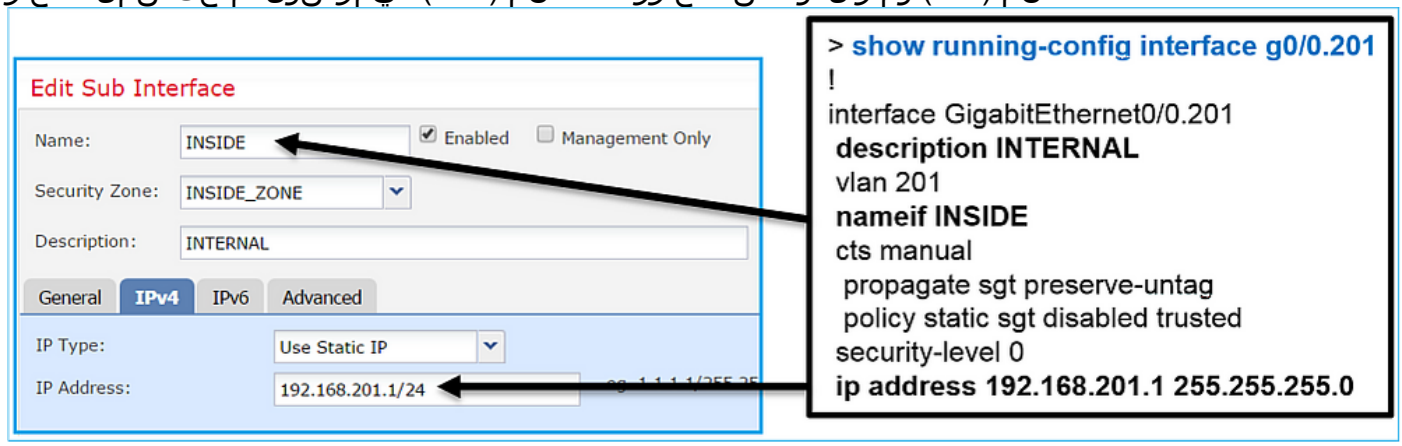


من واجهة سطر الأوامر في برنامج FTD:

```
<#root>

>

show interface ip brief

Interface                  IP-Address      OK? Method Status                Protocol
GigabitEthernet0/0         unassigned      YES unset  up                    up

GigabitEthernet0/0.201     192.168.201.1   YES manual up                    up
GigabitEthernet0/1         192.168.202.1   YES manual up                    up

GigabitEthernet0/2         unassigned      YES unset  administratively down down
GigabitEthernet0/3         unassigned      YES unset  administratively down down
GigabitEthernet0/4         unassigned      YES unset  administratively down down
GigabitEthernet0/5         unassigned      YES unset  administratively down down
Internal-Control0/0        127.0.1.1       YES unset  up                    up
Internal-Data0/0           unassigned      YES unset  up                    up
Internal-Data0/1           unassigned      YES unset  up                    up
Internal-Data0/2           169.254.1.1     YES unset  up                    up
Management0/0              unassigned      YES unset  up                    up
```

```
<#root>

>

show ip

System IP Addresses:
Interface                  Name                IP address      Subnet mask     Method
GigabitEthernet0/0.201     INSIDE              192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1         OUTSIDE             192.168.202.1   255.255.255.0   manual
Current IP Addresses:
Interface                  Name                IP address      Subnet mask     Method

GigabitEthernet0/0.201     INSIDE              192.168.201.1   255.255.255.0   manual
GigabitEthernet0/1         OUTSIDE             192.168.202.1   255.255.255.0   manual
```

واجهة المستخدم الرسومية (GUI) من FMC وواجهة سطر الأوامر (CLI) من FTD:




```
<#root>

>
```

show interface g0/0.201

Interface GigabitEthernet0/0.201

"

INSIDE

",

is up, line protocol is up

  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

VLAN identifier 201

Description: INTERNAL

        MAC address a89d.21ce.fdea, MTU 1500

IP address 192.168.201.1, subnet mask 255.255.255.0

  Traffic Statistics for "INSIDE":
        1 packets input, 28 bytes
        1 packets output, 28 bytes
        0 packets dropped
>

show interface g0/1

Interface GigabitEthernet0/1 "OUTSIDE", is up, line protocol is up

  Hardware is i82574L rev00, BW 1000 Mbps, DLY 10 usec

Auto-Duplex(Full-duplex), Auto-Speed(1000 Mbps)

        Input flow control is unsupported, output flow control is off

Description: EXTERNAL

        MAC address a89d.21ce.fde7, MTU 1500

IP address 192.168.202.1, subnet mask 255.255.255.0

        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 pause input, 0 resume input
        0 L2 decode drops
        1 packets output, 64 bytes, 0 underruns
        0 pause output, 0 resume output
        0 output errors, 0 collisions, 12 interface resets
        0 late collisions, 0 deferred
        0 input reset drops, 0 output reset drops
        input queue (blocks free curr/low): hardware (511/511)
        output queue (blocks free curr/low): hardware (511/511)
  Traffic Statistics for "OUTSIDE":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec, 0 bytes/sec

```
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec
>
```

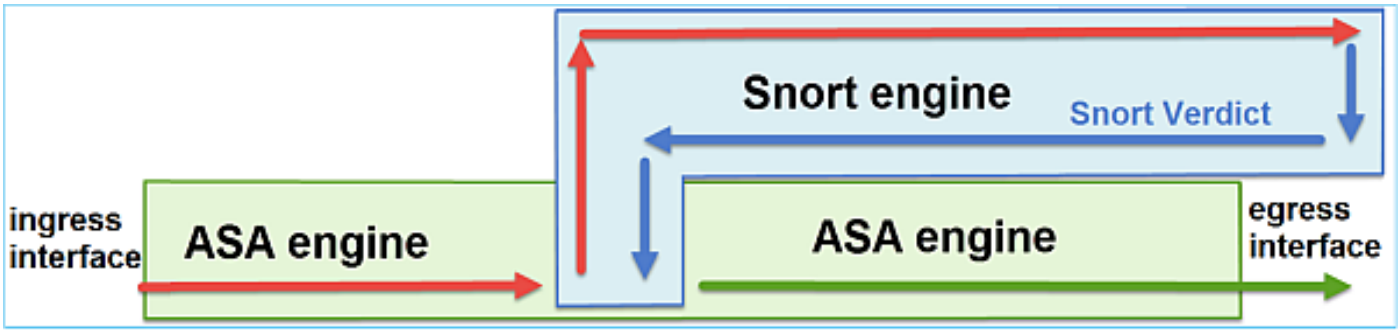
عملية FTD للواجهة الموجهة

تحقق من تدفق حزمة FTD عندما تكون الواجهات الموجهة قيد الاستخدام.

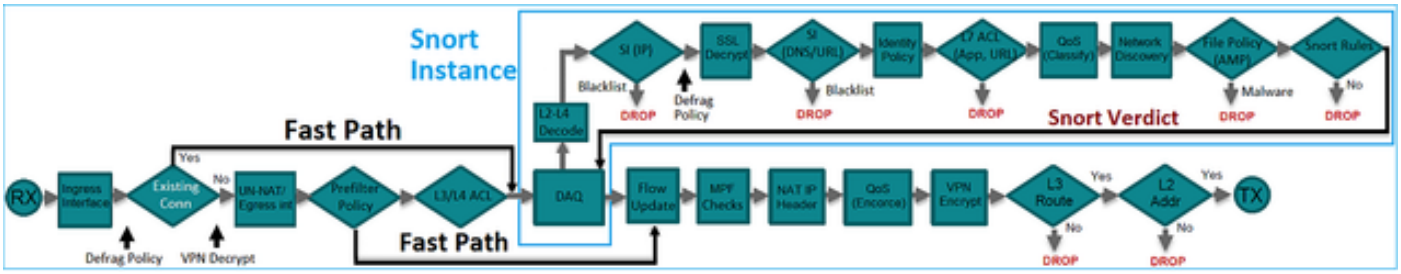
الحل

نظرة عامة على بنية FTD

نظرة عامة عالية المستوى على مستوى بيانات FTD:



تظهر هذه الصورة بعض التحققات التي تحدث داخل كل محرك:



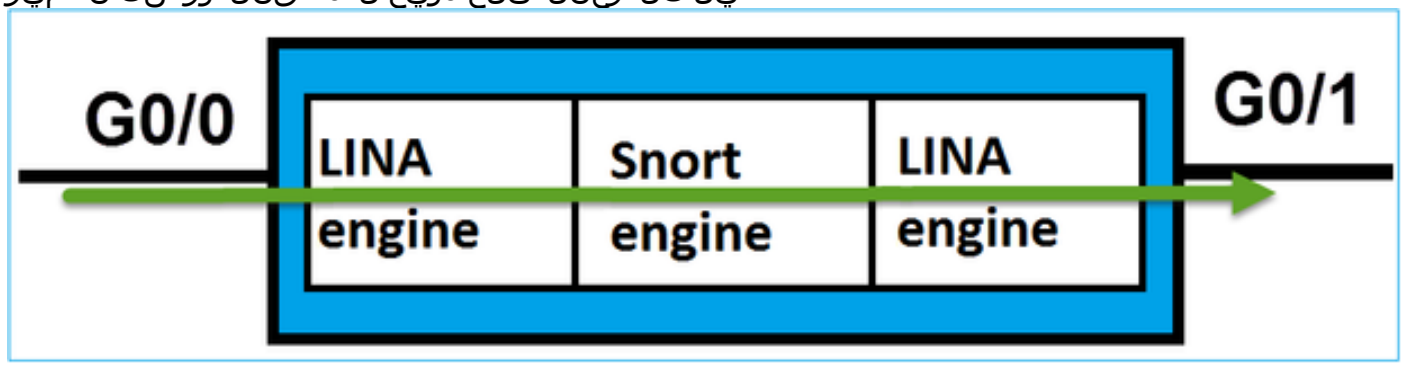
النقاط الرئيسية

- تتوافق التحقيقات السفلى مع مسار بيانات محرك FTD LINA
- التحقيقات الموجودة داخل المربع الأزرق ترادف مثيل محرك FTD snort

نظرة عامة على الواجهة الموجهة ل FTD

- متوفر فقط في النشر الموجه
- نشر جدار الحماية التقليدي من المستوى الثالث
- واجهة واحدة أو أكثر من الواجهات القابلة للتوجيه المادية أو المنطقية (VLAN)
- يتيح تكوين ميزات مثل NAT أو بروتوكولات التوجيه الديناميكية
- تتم إعادة توجيه الحزم استنادا إلى بحث المسار ويتم حل الخطوة التالية استنادا إلى بحث ARP
- حركة المرور الفعلية يمكن إسقاطها
- يتم تطبيق فحوصات محرك LINA الكاملة مع فحوصات محرك الشخ الكامل

ويمكن تصور النقطة الأخيرة على النحو التالي:



التحقق من الصحة

تعقب حزمة على واجهة FTD الموجهة

الرسم التخطيطي للشبكة

أستخدم تطبيق Packet-tracer مع المعلمات التالية للاطلاع على السياسات المطبقة:

واجهة الإدخال	داخل

البروتوكول/الخدمة	منفذ TCP رقم 80
IP المصدر	192.168.201.100
IP الوجهة	192.168.202.100

الحل

عند إستخدام واجهة موجهة تتم معالجة الحزمة بطريقة مشابهة للواجهة التقليدية الموجهة (MPF) و NAT يتم إجراء عمليات التحقق مثل بحث المسار وإطار السياسات النمطية ASA. وإلى ذلك في مسار بيانات محرك LINA. وامإ (ARP) العنواني لحل العلوكوتورب والبحث في محرك LINA. بالإضافة إلى ذلك، إذا كانت سياسة التحكم في الوصول تتطلب ذلك، يتم فحص الحزمة بواسطة محرك الشرخ (أحد مثيلات الشرخ) حيث يتم إنشاء الحكم وإعادته إلى محرك LINA:

<#root>

>

packet-tracer input INSIDE tcp 192.168.201.100 11111 192.168.202.100 80

Phase: 1

Type: ROUTE-LOOKUP

Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:

found next-hop 192.168.202.100 using egress ifc OUTSIDE

Phase: 2

Type: ACCESS-LIST

Subtype: log
Result: ALLOW
Config:

access-group CSM_FW_ACL_ global
access-list CSM_FW_ACL_ advanced permit ip any any rule-id 268437505
access-list CSM_FW_ACL_ remark rule-id 268437505: ACCESS POLICY: FTD5512 - Default/1
access-list CSM_FW_ACL_ remark rule-id 268437505: L4 RULE: DEFAULT ACTION RULE

Additional Information:

This packet will be sent to snort for additional processing where a verdict will be reached

Phase: 3

Type: CONN-SETTINGS

Subtype:
Result: ALLOW
Config:

class-map class-default

match any

policy-map global_policy

class class-default

set connection advanced-options UM_STATIC_TCP_MAP

service-policy global_policy global

Additional Information:

Phase: 4

Type: NAT

Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:

```
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:

Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 11336, packet dispatched to next module


Result:


input-interface: INSIDE


input-status: up
input-line-status: up

output-interface: OUTSIDE


output-status: up
output-line-status: up
Action: allow

>
```

ملاحظة: في المرحلة 4، يتم التحقق من الحزمة مقابل خريطة TCP المسماة UM_STATIC_TCP_MAP. هذه هي خريطة TCP الافتراضية على FTD.

```
<#root>

firepower#

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 clear
  ttl-evasion-protection
  urgent-flag allow
  window-variation allow-connection
!
>
```

معلومات ذات صلة

- دليل تكوين Firepower Threat Defense من Cisco لأجهزة الأمان Firepower، الإصدار 6.1
- تثبيت الدفاع ضد التهديد FirePOWER وترقيته على أجهزة ASA 55xx-X
- الدفاع ضد التهديد جدار الحماية الآمن من Cisco
- الدعم الفني والتنزيلات من Cisco

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).