تكوين واجهة بيانات FTD ل Syslog عبر نفق VPN

المحتويات

المقدمة

يصف هذا وثيقة كيفية أن يشكل cisco FTD عطيات قارن كمصدر ل syslog يرسل عبر VPN نفق.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تكوين Syslog على Cisco Secure Firewall Threat Defense (FTD)
- عام Syslog
- مركز إدارة جدار الحماية الآمن (FMC) من Cisco

المكونات المستخدمة

أسست المعلومة في هذا وثيقة على هذا برمجية وجهاز صيغة:

- Cisco FTD، الإصدار 7.3.1
- Cisco FMC، الإصدار 7.3.1

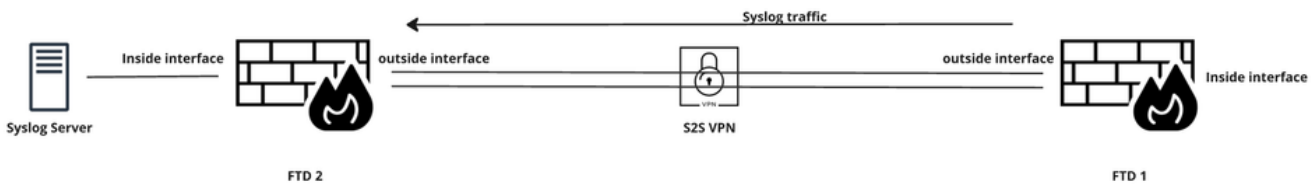
إخلاء المسؤولية: ال تكون الشبكات وعناوين IP المشار إليها في هذا المستند مرتبطة بأي مستخدمين فرديين أو مجموعات أو مؤسسات. تم إنشاء هذا التكوين حصريا للاستخدام في بيئة معملية.

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

يصف هذا وثيقة حل أن يستعمل واحد من المعطيات قارن من FTD كمصدر ل syslog أن يكون أرسلت عبر VPN نفق إلى syslog دان أن يكون يتواجد في موقع بعيد.

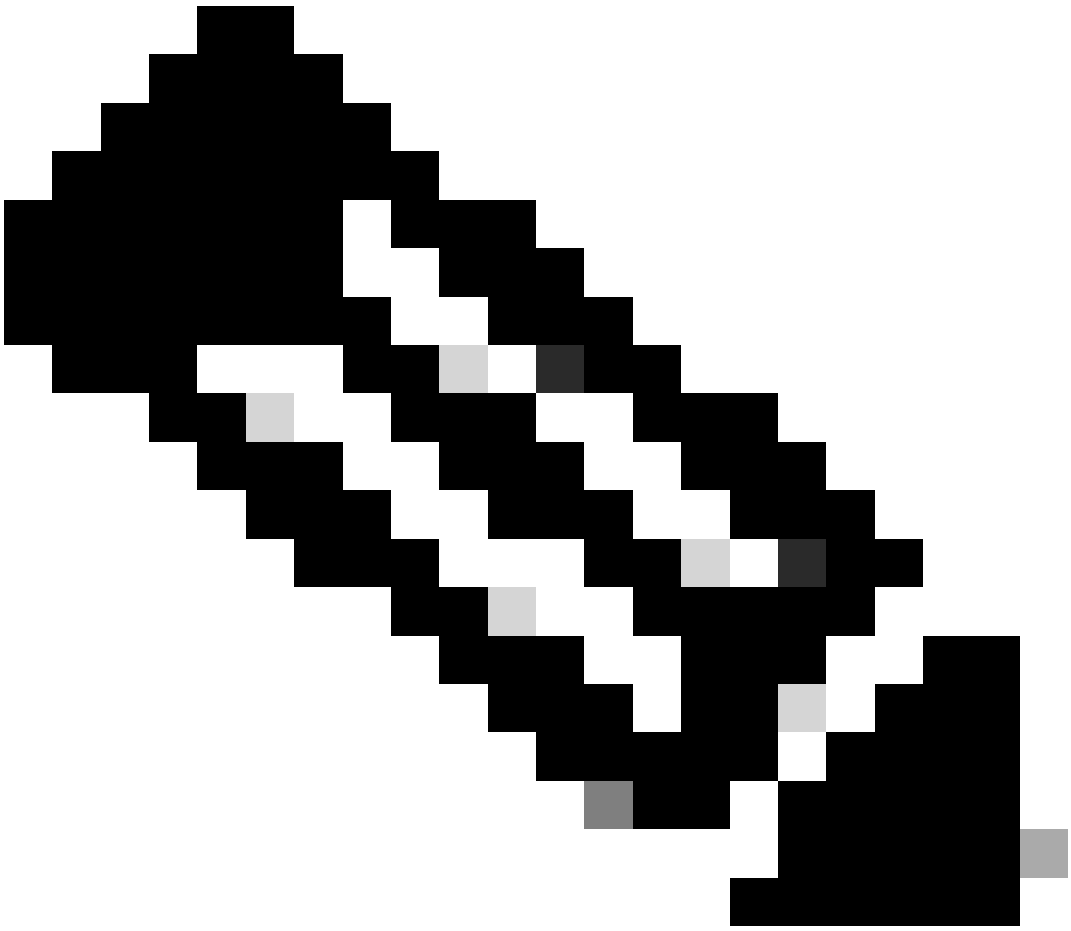
الرسم التخطيطي



الرسم التخطيطي للشبكة

لتحديد الواجهة التي يتم منها مصدر حركة مرور syslog التي يتم إرسالها عبر النفق، يمكنك تطبيق الأمر **management-access** عبر Flex Config.

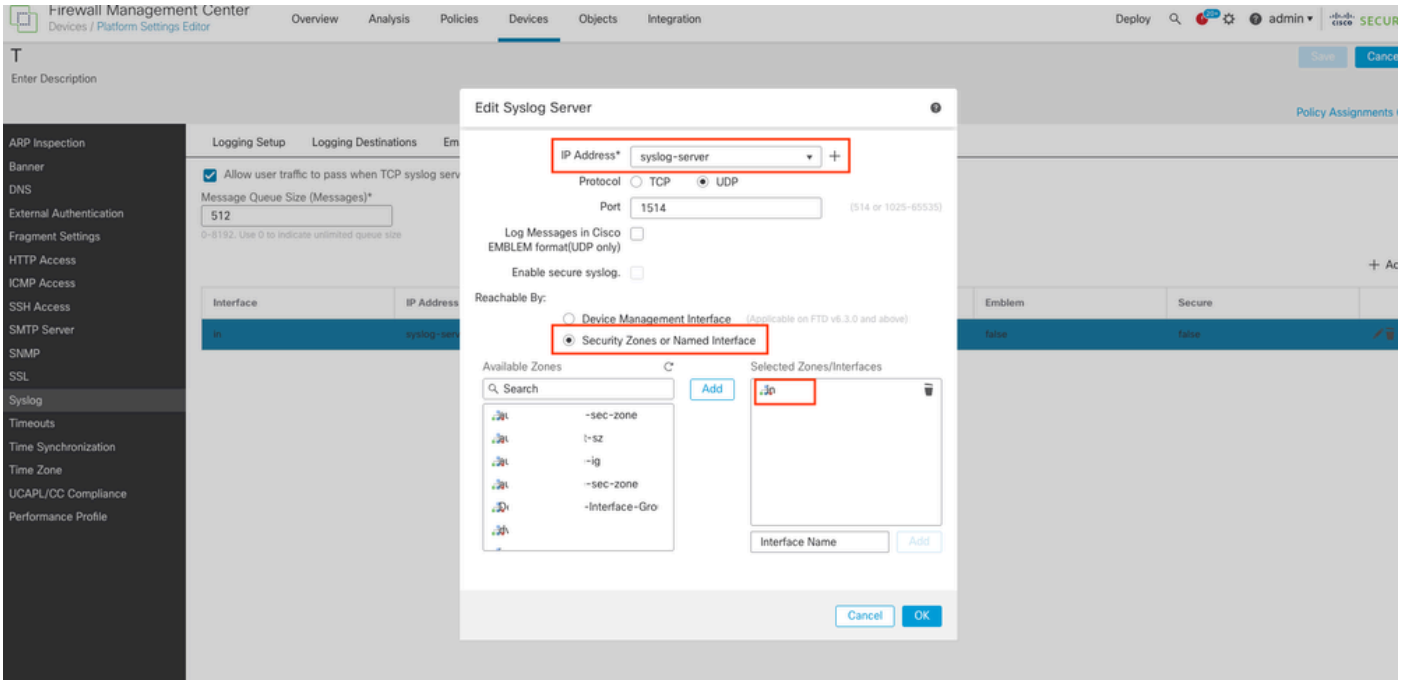
قفل نفق يسمح هذا الأمر فقط باستخدام واجهة الوصول إلى الإدارة كواجهة مصدر لرسائل Syslog التي يتم إرسالها من خلال نفق عبر VPN، ولكن أيضا بالاتصال بواجهة البيانات عبر SSH و Ping عند إستخدام عميل VPN لـ SSL VPN كامل النفق أو VPN قفل IPsec من موقع إلى موقع.



ملاحظة: يمكنك تحديد واجهة وصول-إدارة واحدة فقط.

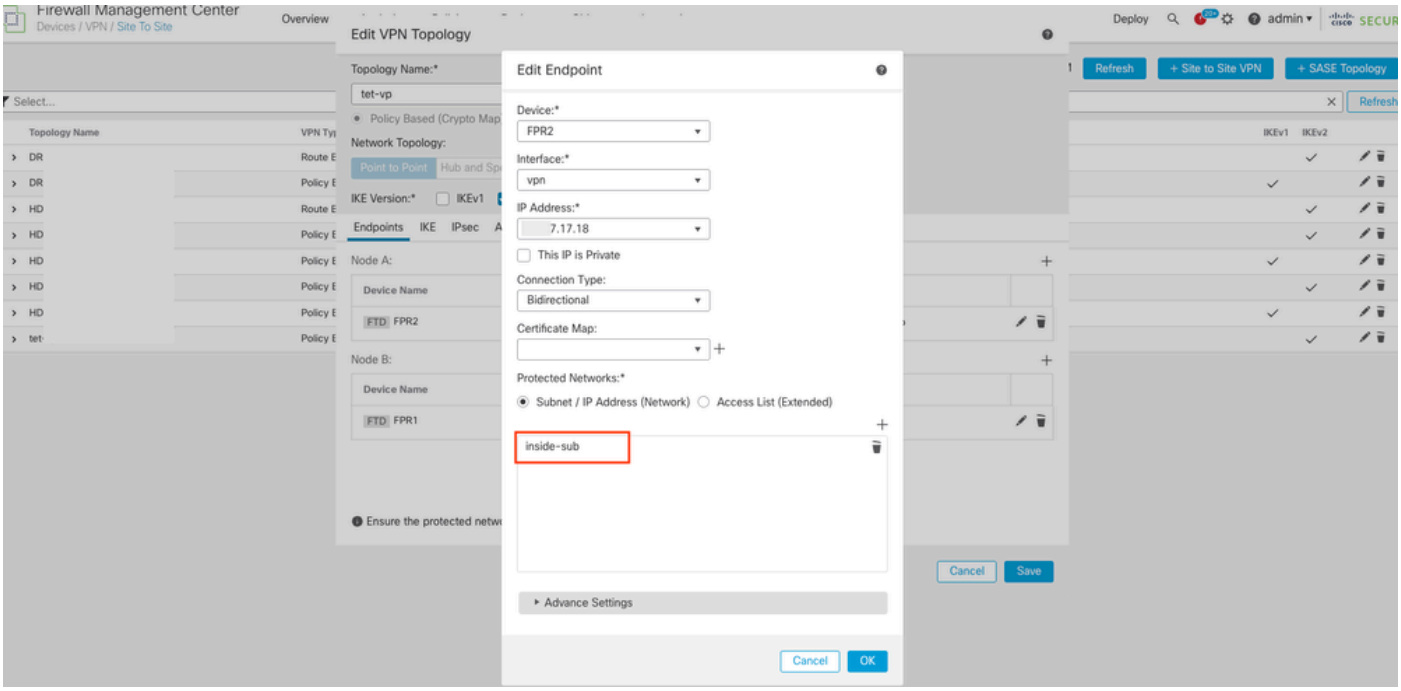
التكوين

1. قم بتكوين syslog ضمن الأجهزة > إعدادات النظام الأساسي لـ FTD. تأكد من تحديد منطقة الأمان أو خيار الواجهة المسماة بدلا من واجهة إدارة الأجهزة أثناء تكوين خادم syslog واختر واجهة الوصول-الإدارة لتحديد مصدر حركة مرور syslog.



تكوين خادم Syslog

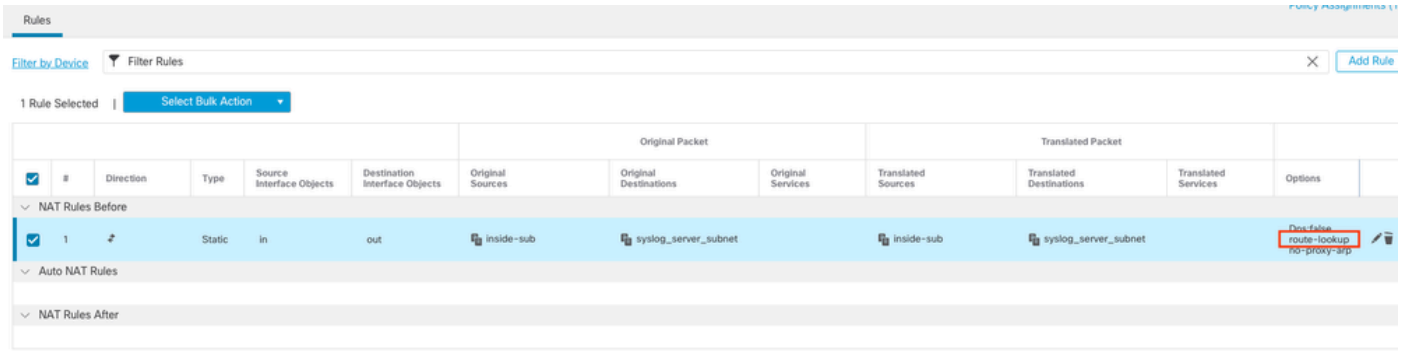
2. تأكد من إضافة شبكة واجهة الوصول إلى الإدارة ضمن الشبكات المحمية لنقطة نهاية VPN. (تحت الأجهزة > موقع إلى موقع > مخطط VPN > عقدة).



تكوين الشبكات المحمية

3. تأكد من تكوين NAT للهوية بين شبكة واجهة الإدارة-الوصول وشبكات VPN (تكوين شائع NAT لحركة مرور VPN). يجب تحديد خيار تنفيذ بحث المسار لواجهة الوجهة ضمن قسم متقدم من قاعدة NAT.

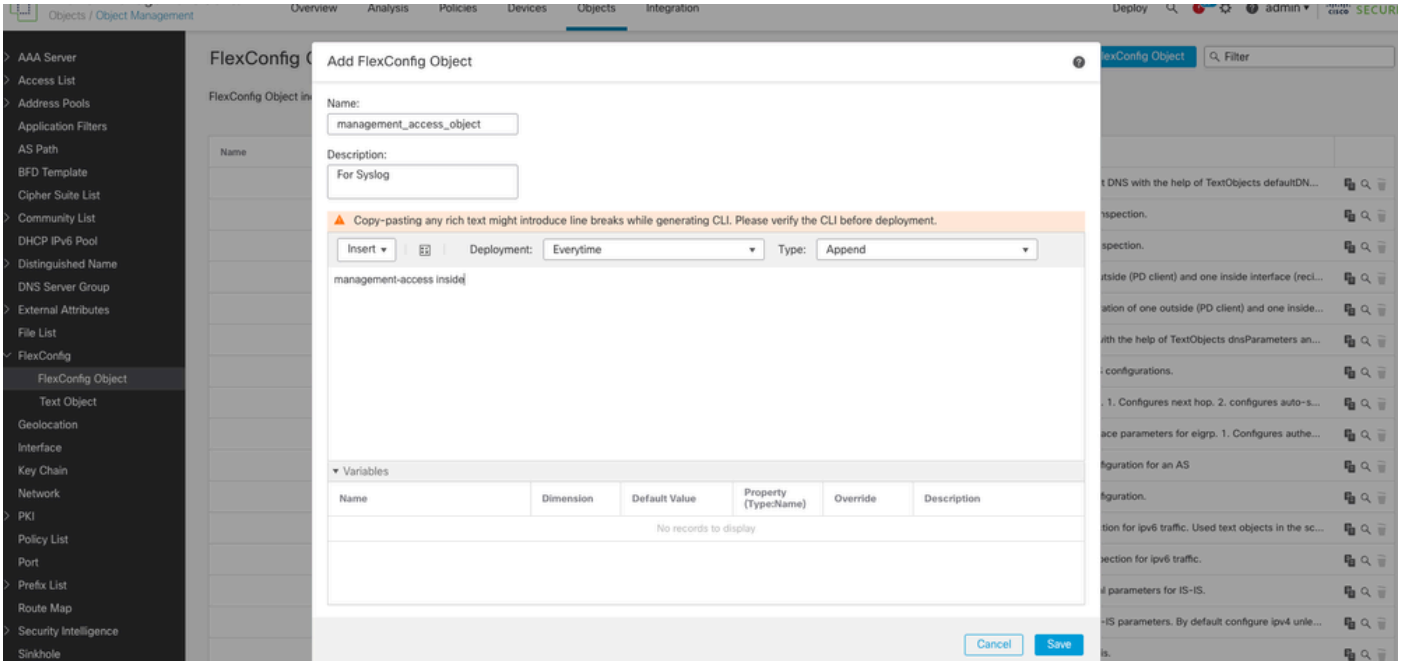
بدون بحث عن المسار، يرسل FTD حركة مرور البيانات من خلال الواجهة المحددة في تكوين nat، بغض النظر عن ما يقوله جدول التوجيه.



تشكيل هوية nat

4. يمكنك الآن تكوين management-access <interface name>(في هذا السيناريو management-access inside) تحت الكائنات > إدارة الكائن > كائن FlexConfig .

قم بتعيينها على نهج FlexConfig للجهاز المستهدف ونشر التكوين.



تكوين FlexConfig

التحقق من الصحة

تكوين الوصول إلى الإدارة:

```
<#root>

firepower#

show run | in management-access

management-access inside
```

تكوين Syslog:

<#root>

firepower#

show run logging

logging enable
logging timestamp
logging trap debugging
logging FMC MANAGER_VPN_EVENT_LIST

logging host inside 192.168.17.17 17/1514

logging debug-trace persistent
logging permit-hostdown
logging class vpn trap debugging

يتم إرسال حركة مرور Syslog عبر نفق VPN:

<#root>

FTD 2:
firepower#

show conn

36 in use, 46 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP vpn 192.168.17.17:1514 inside 10.17.17.18:514, idle 0:00:02, bytes 35898507, flags -

FTD 1:
firepower#

show conn

6 in use, 9 most used
Inspect Snort:
preserve-connection: 0 enabled, 0 in effect, 0 most enabled, 0 most in effect

UDP server 192.168.17.17:1514 vpn 10.17.17.18:514, idle 0:00:00, bytes 62309790, flags -

firepower#

show crypto ipsec sa

interface: vpn
Crypto map tag: CSM_vpn_map, seq num: 1, local addr: 17.xx.xx.18

access-list CSM_IPSEC_ACL_2 extended permit ip 10.17.17.0 255.255.255.0 192.168.17.0 255.255.255.0
Protected vrf (ivrf):

local ident (addr/mask/prot/port): (10.17.17.0/255.255.255.0/0/0)

----------> Inside interface subnet

```
remote ident (addr/mask/prot/port): (192.168.17.0/255.255.255.0/0/0)

------------> Syslog server subnet
current_peer: 17.xx.xx.17


#pkts encaps: 309957, #pkts encrypt: 309957, #pkts digest: 309957


#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 309957, #pkts comp failed: 0, #pkts decomp failed: 0
#pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
#PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
#TFC rcvd: 0, #TFC sent: 0
#Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
#send errors: 0, #recv errors: 0
```

معلومات ذات صلة

- تكوين التسجيل على FTD عبر FMC
- تكوين الموقع إلى شبكة VPN على FTD المدارة بواسطة FMC

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).