تكوين syslog المدرك ل VRF على FTD

المحتويات

المقدمة

المتطلبات الأساسية

المتطلبات

المكونات المستخدمة

معلومات أساسية

دعم نظام التشغيل SNORT3 ونظام Multi-Instance/Context ونظام HA/Cluster

التكوين

الرسم التخطيطي للشبكة

التكوينات

التكوين في FMC

تكوين الموجه الظاهري

المتطلبات الأساسية لتكوين خادم FTP في FMC

التكوين

التحقق من الصحة

قبل 7.4.1

Post 7.4.1

التحقق من خادم FTP

قبل 7.4.1

Post 7.4.1

المقدمة

يصف هذا المستند خطوات التكوين ل syslog المدرك ل VRF على FTD.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- Syslog
- Firepower Threat Defense (FTD)

المكونات المستخدمة

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

- Secure Firewall Management Center (FMCv) الإصدار 7.4.2
- Secure Firewall Threat Defense Virtual (FTDv) v7.4.2

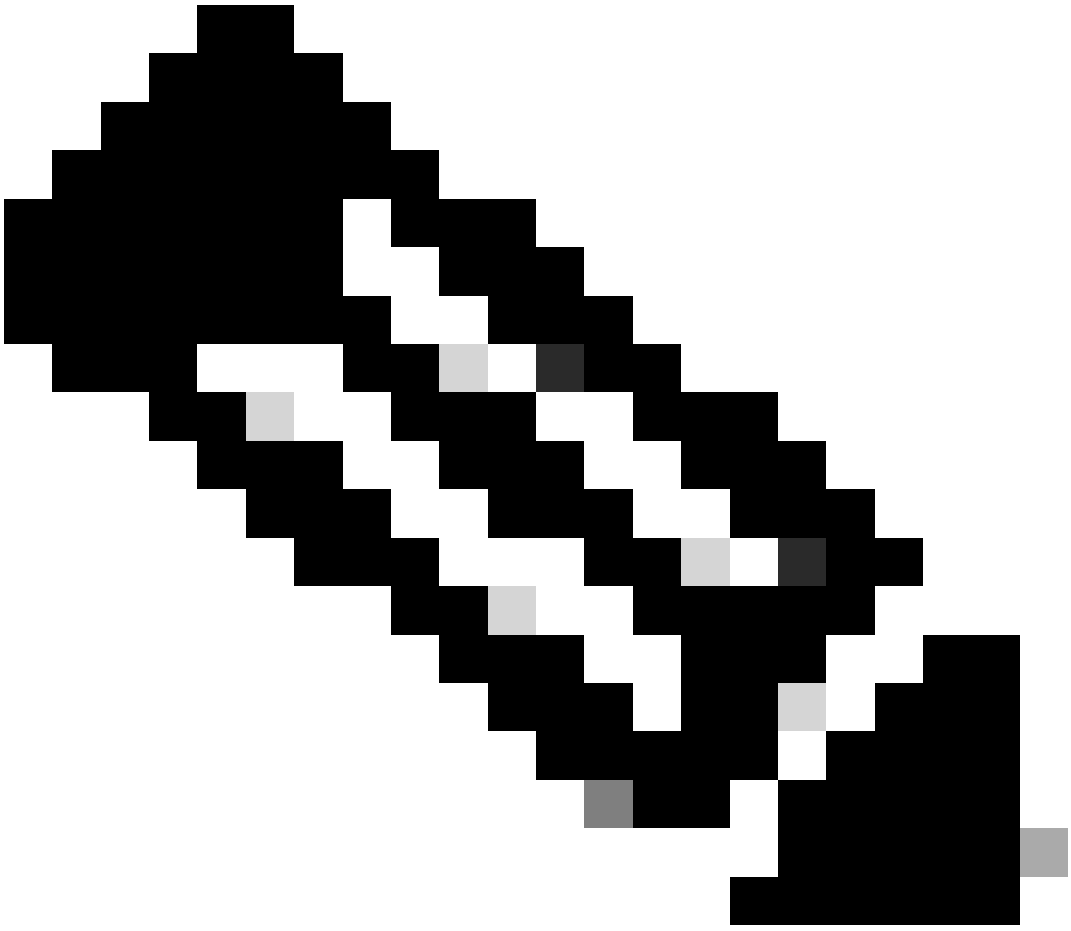
تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الحد الأدنى للبرامج والأجهزة الأساسية

- التطبيق والحد الأدنى للإصدار: Secure Firewall 7.4.1
- الأنظمة الأساسية المدارة والإصدار المدعوم: كل ما يدعم FTD 7.4.1
- المديرون:
  1) واجهة برمجة تطبيقات FMC على الخادم + واجهة برمجة تطبيقات REST الخاصة بوحدة التحكم FMC
  2) وحدة التحكم في إدارة اللوحة الأساسية (FMC) التي يتم تسليمها عبر السحابة
  3) FDM + REST API

دعم نظام التشغيل SNORT3 ونظام Multi-Instance/Context ونظام HA/Cluster

---



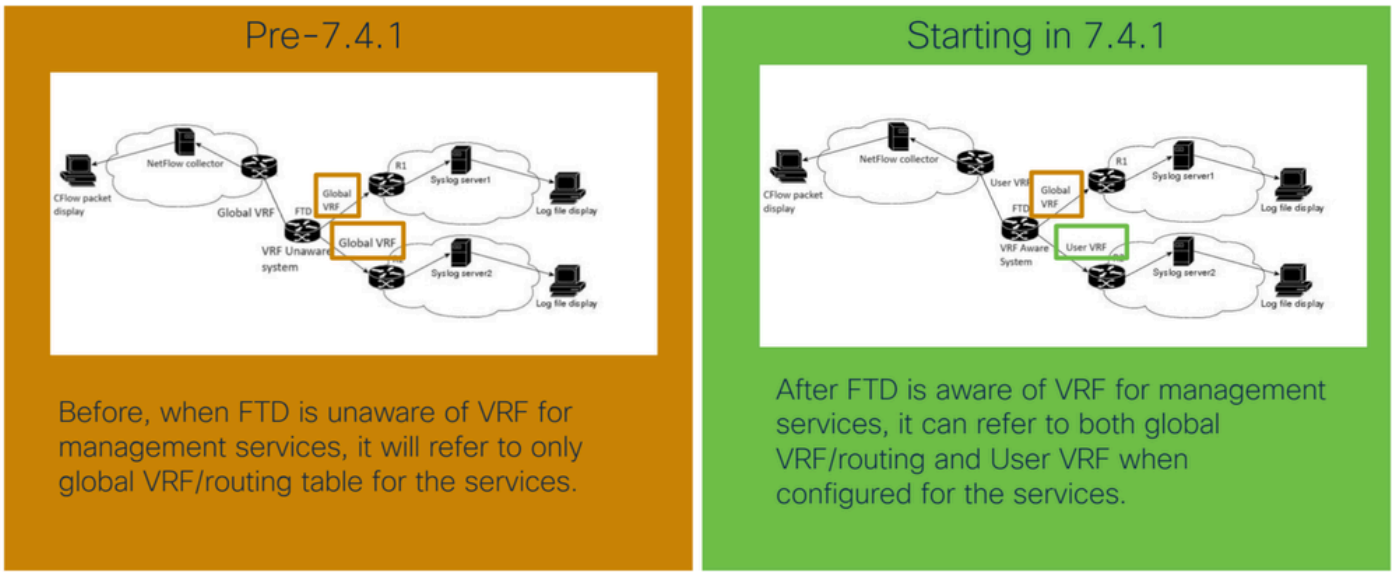
ملاحظة: يعمل عميل syslog الخاص بالإصدار الرابع من برنامج Cisco Secure Client مع كل من خوادم syslog الخاصة بالإصدار الرابع من بروتوكول الإنترنت

(IPv4) و IPv6. الـ يتم دعم IPv6 حتى الآن في خادم Syslog FTP.

- مدعم مع Multi-instance.
- مدعوم بأجهزة HA.
- مدعوم على الأجهزة المجمعة.

التكوين

الرسم التخطيطي للشبكة



مقارنة الرسم التخطيطي للشبكة بين الطرازين السابق واللاحق 7. 4.

التكوينات

التوجيه وإعادة التوجيه الظاهري (VRF) هي تقنية تستخدم في الشبكة للسماح للمثيلات المتعددة لجدول التوجيه بالتعايش داخل الموجه نفسه، مما يوفر عزل الشبكة بين الشبكات الظاهرية المختلفة. كل حالة من حالات تردد الراديو (VRF) مستقلة عن الأخرى، ويتم الاحتفاظ بحركة المرور بينها منفصلة. Multi-VRF هي ميزة تتيح لمزودي الخدمة دعم شبكات VPN متعددة والخدمات، حتى إذا تداخل عناوين IP الخاصة بهم. وهو يستخدم واجهات الإدخال لتعيين المسارات لخدمات مختلفة وإنشاء جداول إعادة توجيه حزم افتراضية من خلال تعيين واجهات الطبقة 3 لكل VRF. تستخدم خدمات الإدارة (Syslog، NetFlow) VRF العام كإعداد افتراضي. يريد المستخدمون إستخدام VRF الخاص بالمستخدم لخدمات الإدارة بالإضافة إلى VRF العمومي لأن ليس كل واجهات التحميل يمكن الوصول إليها عبر VRF العام.

في هذا وثيقة، شامل + مستعمل VRF = multi-VRF

مكنت syslog لمستخدم VRF.

- يمكن أن تستخدم syslog خدمة ftp في سياق multi-VRF.

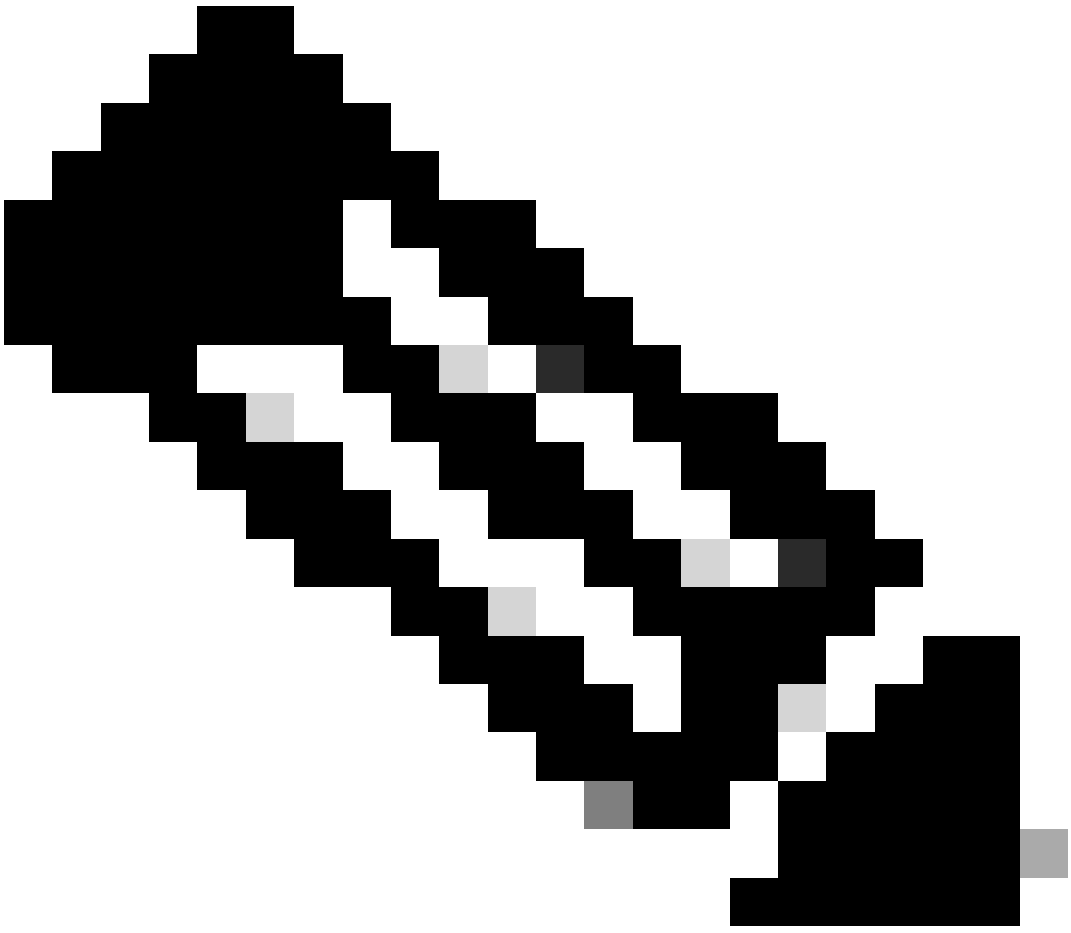
كيف يعمل

عندما يتم تكوين الواجهة باستخدام VRF للمستخدم، يحدث بحث المسار في مجال توجيه VRF، بدلا من مجال التوجيه العام الافتراضي.

- يتم دعم نوعين من تكوينات الخادم:

1. إرسال رسائل التسجيل إلى خوادم Syslog لمراقبة حركة مرور الشبكة واستكشاف أخطائها وإصلاحها.
2. إرسال محتوى التخزين المؤقت للسجل إلى خادم FTP كملف نصي

- تقوم Syslog بإرسال السجلات إلى خوادم UDP/TCP المقابلة داخل بروتوكول VRF هذا.
- بالنسبة لنظم التفاف المخزن المؤقت، يتم إرسال السجلات إلى خادم FTP الذي تم تكوينه داخل VRF هذا.

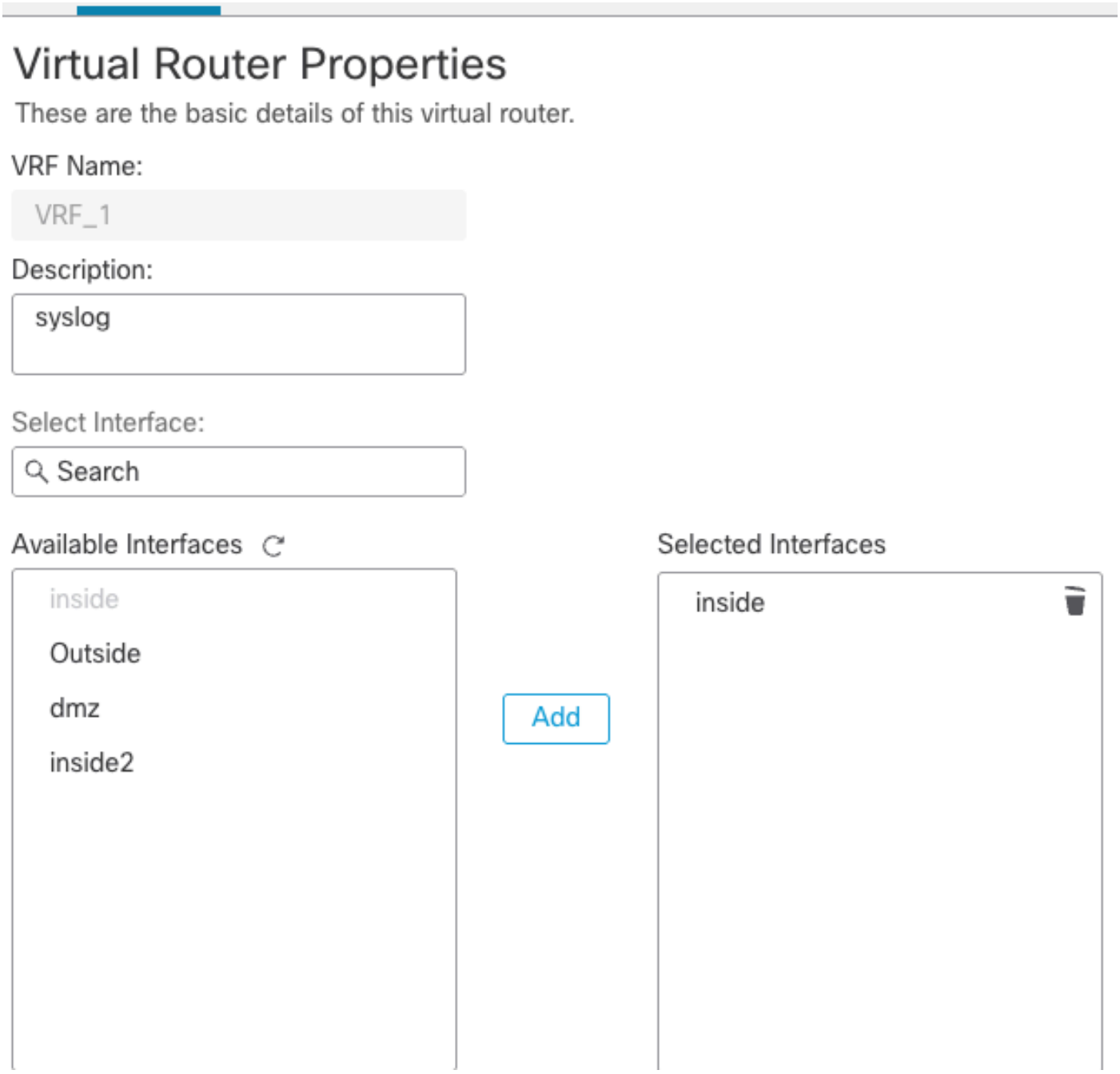


ملاحظة: Syslog لدان و FTP لدان يستطيع كنت جزء من VRFs مختلف.

تكوين الموجه الظاهري

الخطوة 1. إنشاء VRF

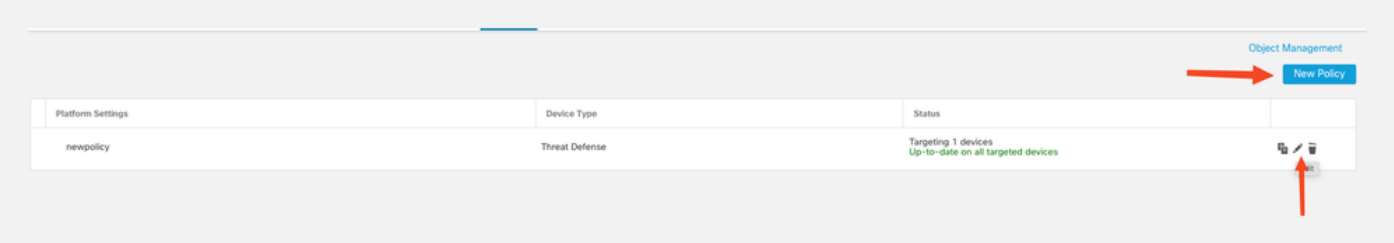
- سجل الدخول إلى FMC وانتقل إلى الجهاز > إدارة الأجهزة.
- حدد الجهاز وانقر على أيقونة القلم الرصاص لتحريره.
- انتقل إلى التوجيه> إدارة الموجه الظاهري > إضافة موجه ظاهري.
- دخلت الإسم في VRF إسم.
- حدد الواجهة وانقر إضافة وحفظ.



إضافة واجهة إلى VRF

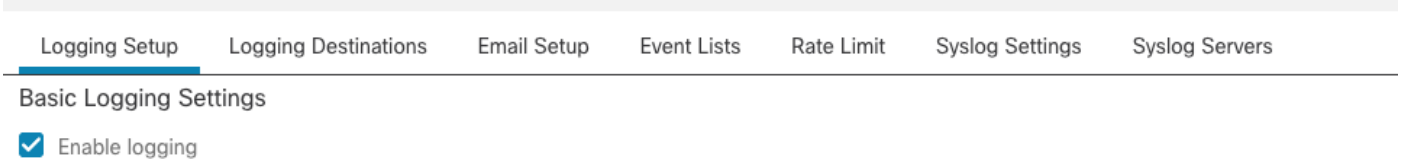
الخطوة 2. قم بتكوين إعداد التسجيل.

- انتقل إلى الأجهزة > إعدادات النظام الأساسي.
- إنشاء نهج جديد أو تحرير أيقونة القلم الرصاص في النهج الموجود.



إنشاء إعدادات النظام الأساسي

- حدد إعداد التسجيل وتمكين التسجيل.

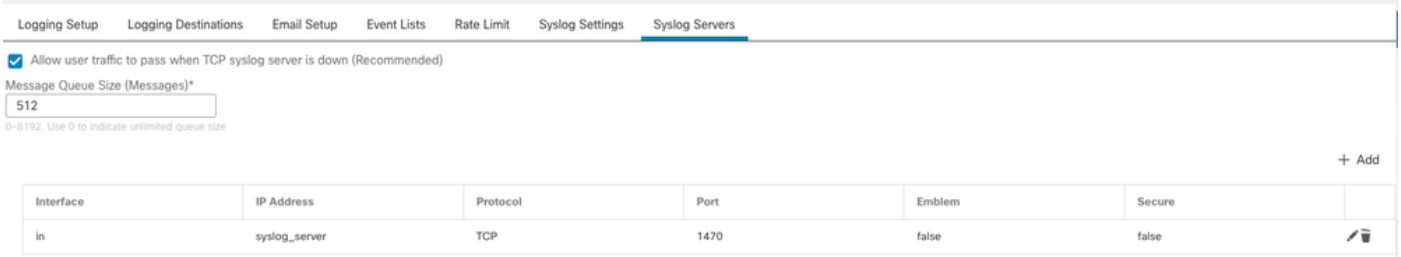


تمكين التسجيل

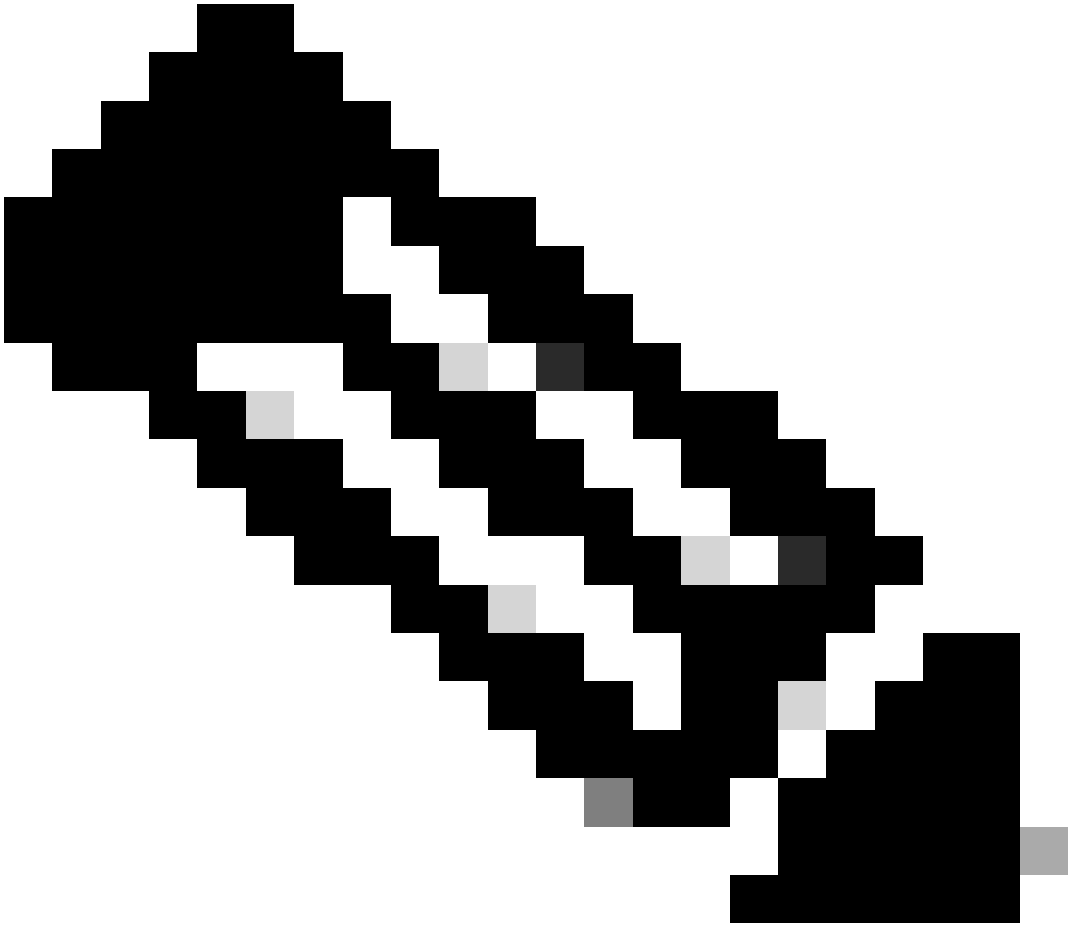
- حدد وجهة التسجيل وانقر فوق إضافة.
- ثبتت ال logging غاية ك syslog نادل.

تسجيل الوجهة كخوادم syslog

- حدد خوادم Syslog > إضافة.



إضافة خادم syslog باستخدام واجهة VRF الحساسة



ملاحظة: الواجهة الداخلية هي جزء من منطقة الأمان في.

- الواجهة التي تم تكوينها في الأمر logging host تكون الآن مدركة ل VRF.
- انقر فوق حفظ.

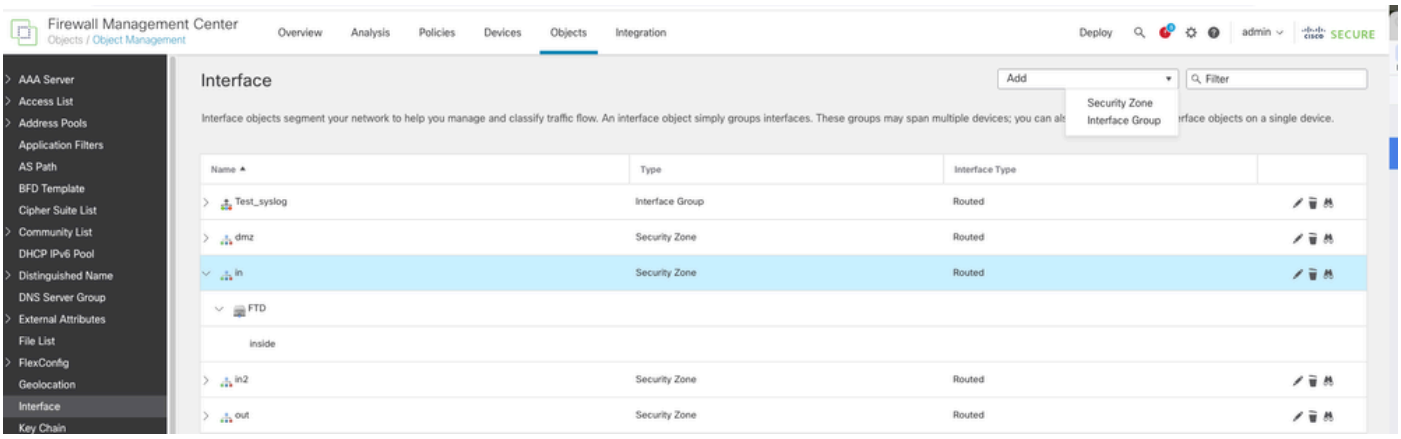
المتطلبات الأساسية لتكوين خادم FTP في FMC

- إستخدام كائن مجموعة الواجهة.
- يمكن أن يحتوي كائن مجموعة الواجهة على كل من User و VRF العمومي.

التكوين

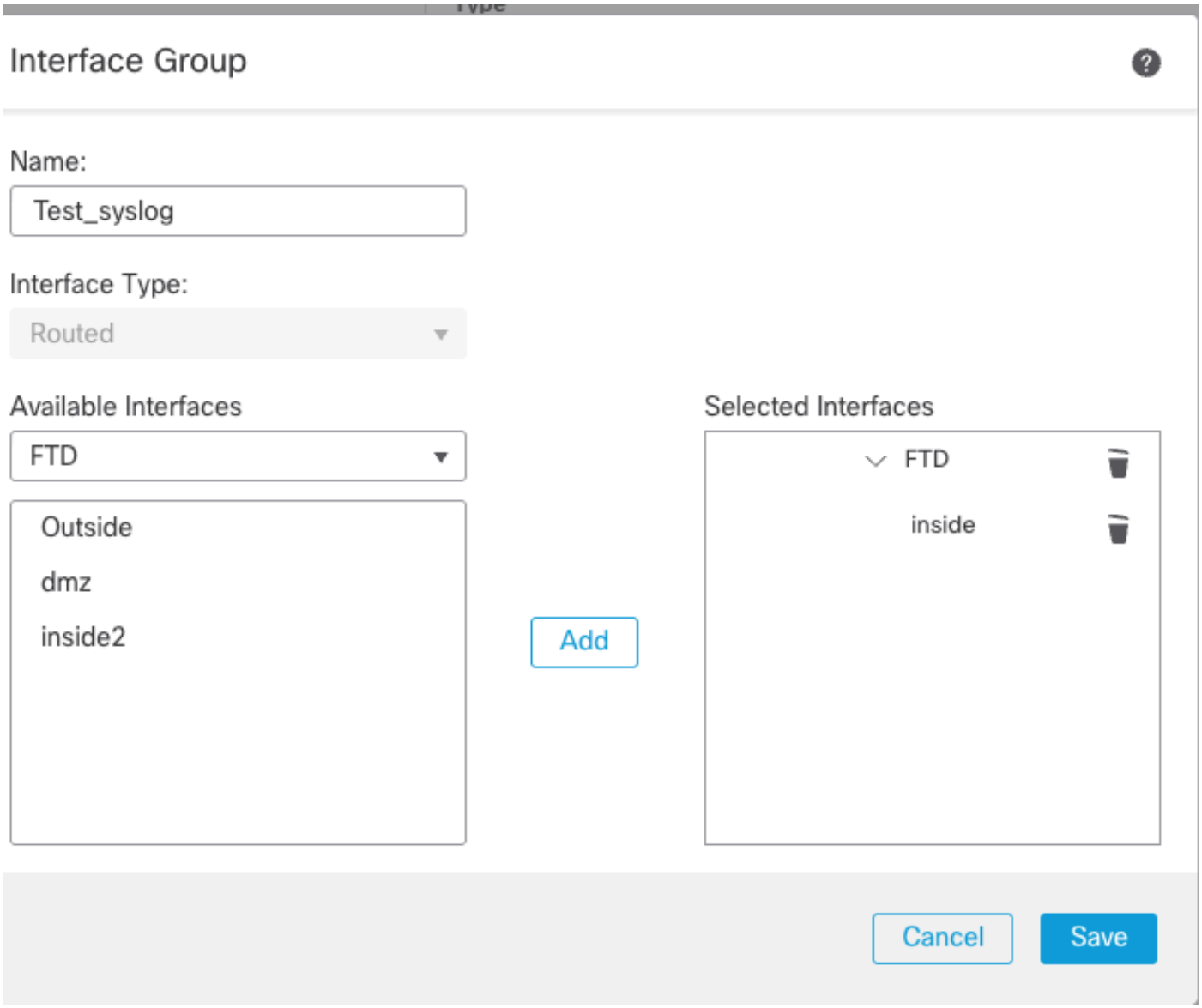
الخطوة 1.

- انتقل إلى كائن > إدارة الكائن > واجهة > إضافة > مجموعة واجهة.



اضافة مجموعة واجهة

- حدد الجهاز من القائمة المنسدلة وأضفت واجهة VRF.



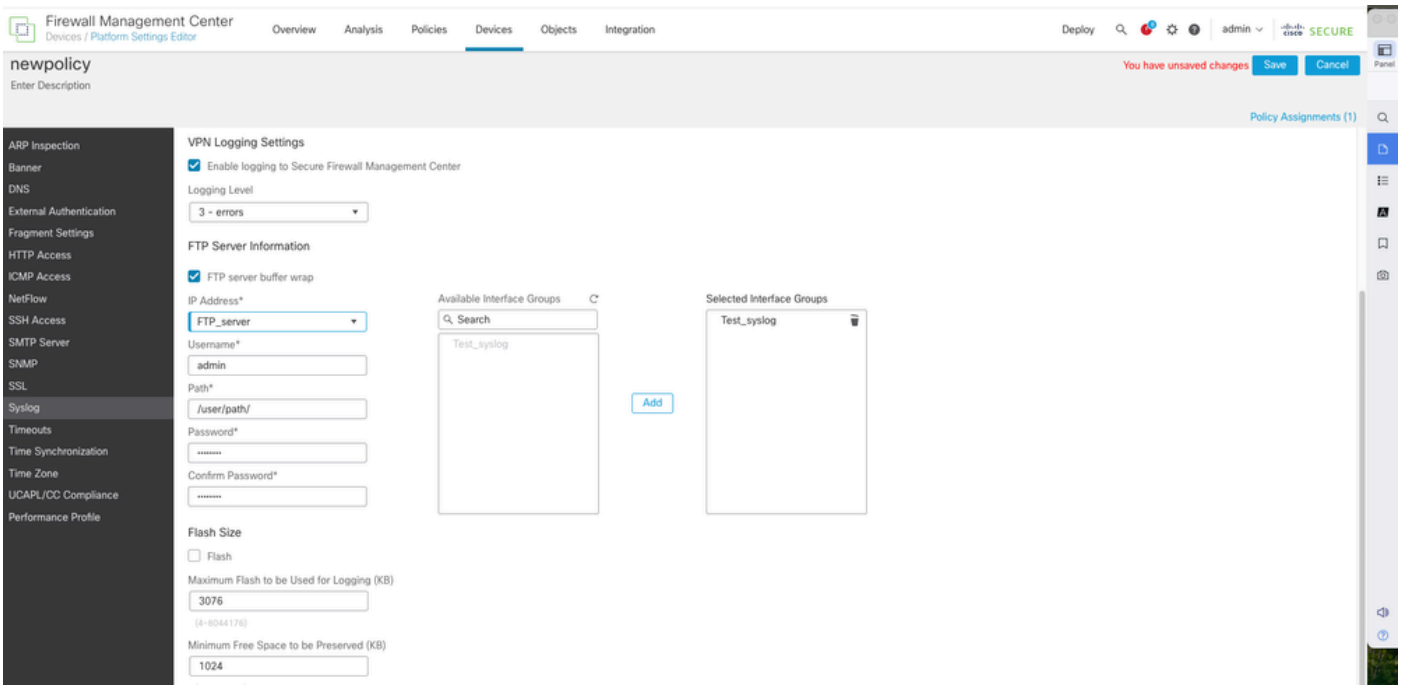
اضافة واجهة VRF Aware

الخطوة 2.

- انتقل إلى الأجهزة > إعدادات النظام الأساسي > Syslog > إعداد التسجيل. قم بتمكين

التفاف المخزن المؤقت لخادم FTP.

- انقر فوق حفظ.



تمكين خادم FTP باستخدام واجهة VRF Aware

التحقق من الصحة

ما قبل 7.4.1

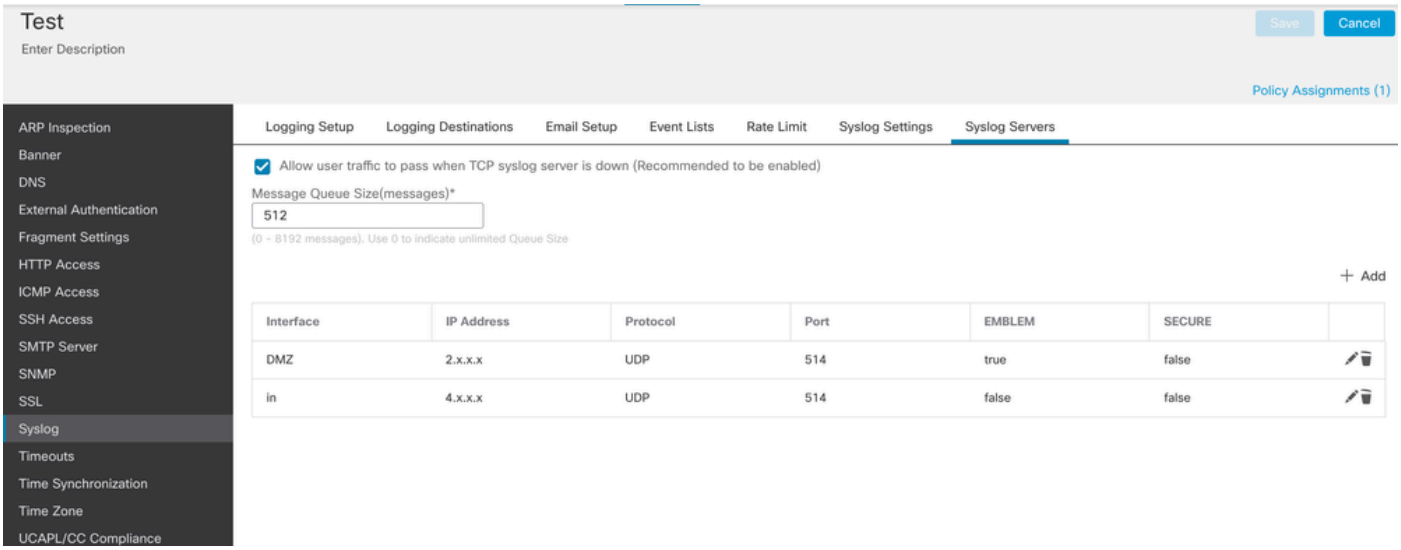
في هذا الاختبار، يبلغ إختبار FTD و FMC 7. 0. 5.

تم تكوين FTD باستخدام VRF وتم تخصيص واجهة DMZ لـ VRF.

تم تكوين واجهة DMZ باستخدام مضيف تسجيل خادم syslog.

وبالإضافة إلى ذلك، تم تكوين الواجهة الداخلية باستخدام إعداد syslog.

القارن داخلي جزء من VRF شامل.

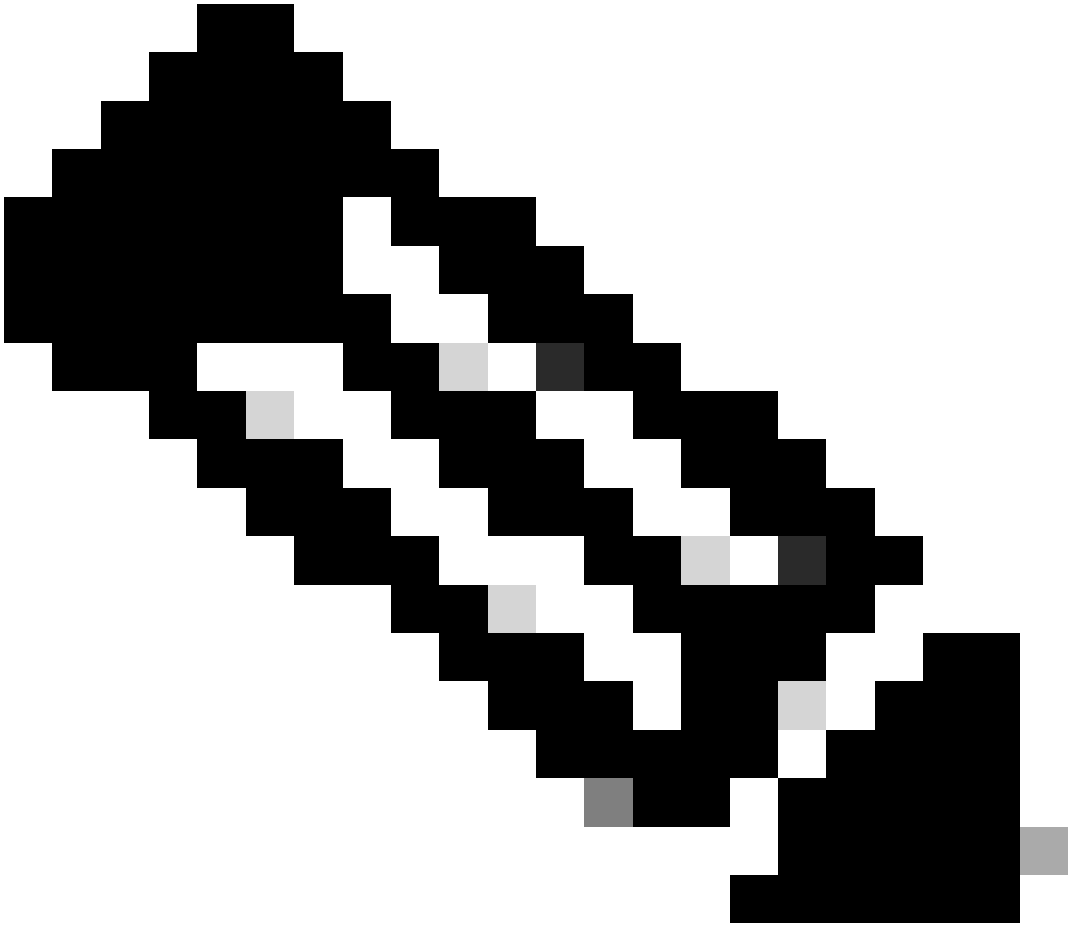


إعداد Syslog Server على 7.0.5 FMC

التحقّق من واجهة سطر الأوامر (CLI)

```
> show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, facility 20, 1193 messages logged
        Logging to inside 4.x.x.x, UDP TX:52
    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
        CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, 0 messages logged
```

```
> show vrf

Name            VRF ID          Description             Interfaces
VRF-1           1                                       dmz
```



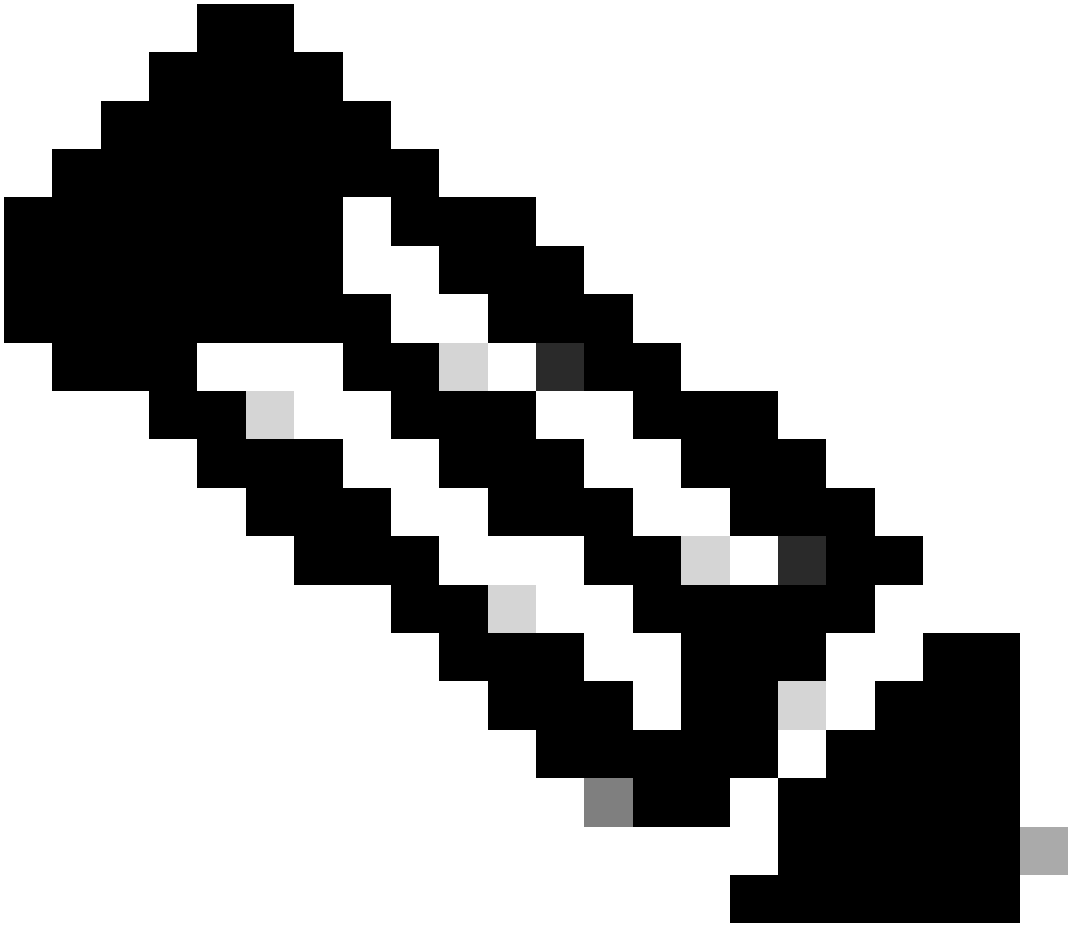
ملاحظة: الا يتوفر خادم Syslog ذي الوجهة 2.x.x.x في إعداد التسجيل ل FTD CLI. هذا جزء من VRF للمستخدم.
يتوفر خادم Syslog مع الوجهة 4.x.x.x على إعداد التسجيل ل FTD CLI. هذا جزء من VRF العالمي.

Post 7.4.1

التحقّق من واجهة سطر الأوامر (CLI)

```
ftd1# show vrf

Name                            VRF ID     Description     Interfaces
VRF_1                           1          syslog          inside



td1# show logging
```

```
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Hide Username logging: enabled
    Standby logging: disabled
    Debug-trace logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level informational, class auth, facility 20, 19284 messages logged
        Logging to inside 192.x.x.x tcp/1470 Not connected since Thu, 20 Mar 2025 01:53:17 UTC TX:0
            TCP SYSLOG_PKT_LOSS:0
            TCP [Channel Idx/Not Putable counts]: [0/0]
            TCP [Channel Idx/Not Putable counts]: [1/0]
            TCP [Channel Idx/Not Putable counts]: [2/0]
            TCP [Channel Idx/Not Putable counts]: [3/0]

    Global TCP syslog stats::
        NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 1584
        CHANNEL_FLAP_CNT: 1584, SYSLOG_PKT_LOSS: 0
        PARTIAL_REWRITE_CNT: 0
    Permit-hostdown logging: enabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
    FMC logging: list MANAGER_VPN_EVENT_LIST, class auth, 0 messages logged
```



ملاحظة: يستخدم مضيف خادم Syslog 192.x.x.x الواجهة الداخلية التي تم وضع VRF عليها.

التحقق من خادم FTP

ما قبل 7.4.1

- على FMC، لا يحتوي إعداد خادم FTP على خيار تحديد الواجهة التي تريد إستخدامها. يتوفر عنوان IP فقط لخيار خادم syslog.

Specify FTP Server Information

☑ FTP Server Buffer Wrap

IP Address*

Username*

Path*

Password*

Confirm*

Specify Flash Size

☐ Flash

Maximum Flash to be used by Logging(KB)

3076

(4-8044176)

Minimum free Space to be preserved(KB)

1024

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).