# حساب عدد عناصر قائمة الوصول (ACE) باستخدام FMC CLI

## المحتويات



## المقدمة

يوضح هذا المستند كيفية العثور على القاعدة التي يتم توسيعها في نهج التحكم في الوصول الخاص بك إلى عدد عناصر قائمة الوصول.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة تقنية FirePOWER
- معرفة حول تكوين سياسات التحكم في الوصول على FMC

### المكونات المستخدمة

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

- مركز إدارة جدار الحماية الآمن (FMC) من Cisco
- الدفاع ضد تهديد FirePOWER (FTD) من Cisco

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

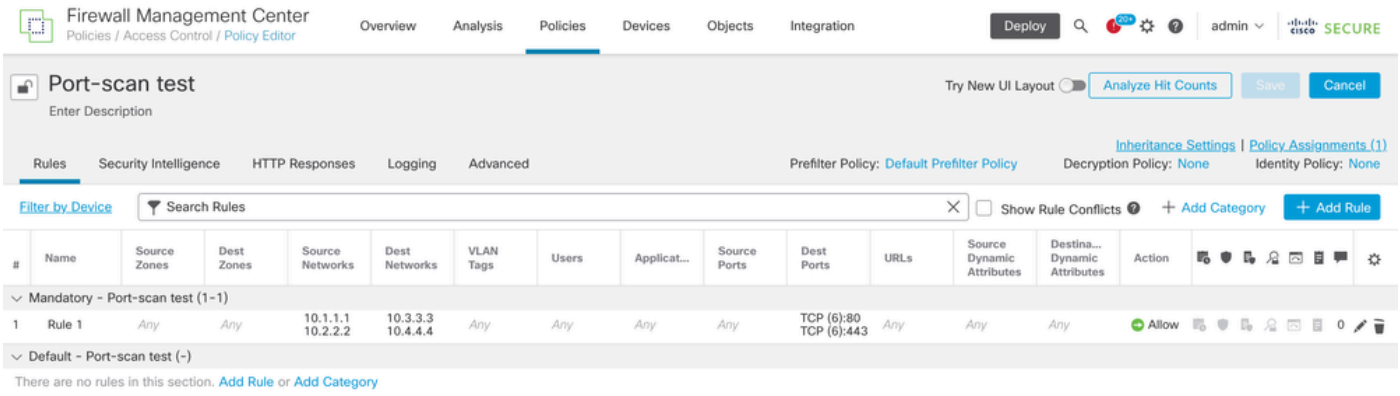
يتم إنشاء قاعدة التحكم بالوصول باستخدام مجموعة واحدة أو عدة مجموعات من هذه المعلمات:

- عنوان IP (المصدر والوجهة)
- المنافذ (المصدر والوجهة)
- URL (يوفر النظام الفئات وعناوين URL مخصصة)
- أجهزة اكتشاف التطبيقات
- شبكات VLAN
- المناطق

استنادا إلى مجموعة المعلمات المستخدمة في قاعدة الوصول، يتغير توسيع القاعدة على المستشعر. يسلط هذا المستند الضوء على تولیفات مختلفة من القواعد المتعلقة بوحدة إدارة الاتصالات الفيدرالية (FMC) والتوسعات المرتبطة بها على أجهزة الاستشعار.

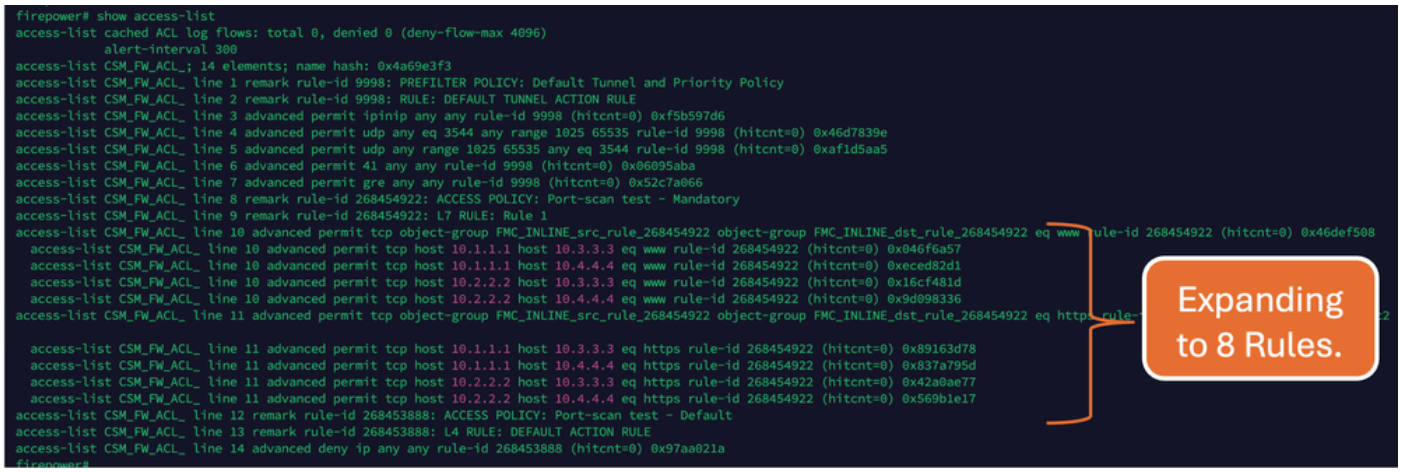
# كيفية حساب عدد عناصر قائمة الوصول (ACE) باستخدام FMC CLI

ضع في الاعتبار تكوين قاعدة وصول من وحدة التحكم في إدارة اللوحة الأساسية (FMC)، كما هو موضح في الصورة:




تكوين القاعدة في سياسة التحكم بالوصول

إذا رأيت هذه القاعدة في FTD CLI، تلاحظ أن هذه القاعدة توسعت في 8 قواعد.



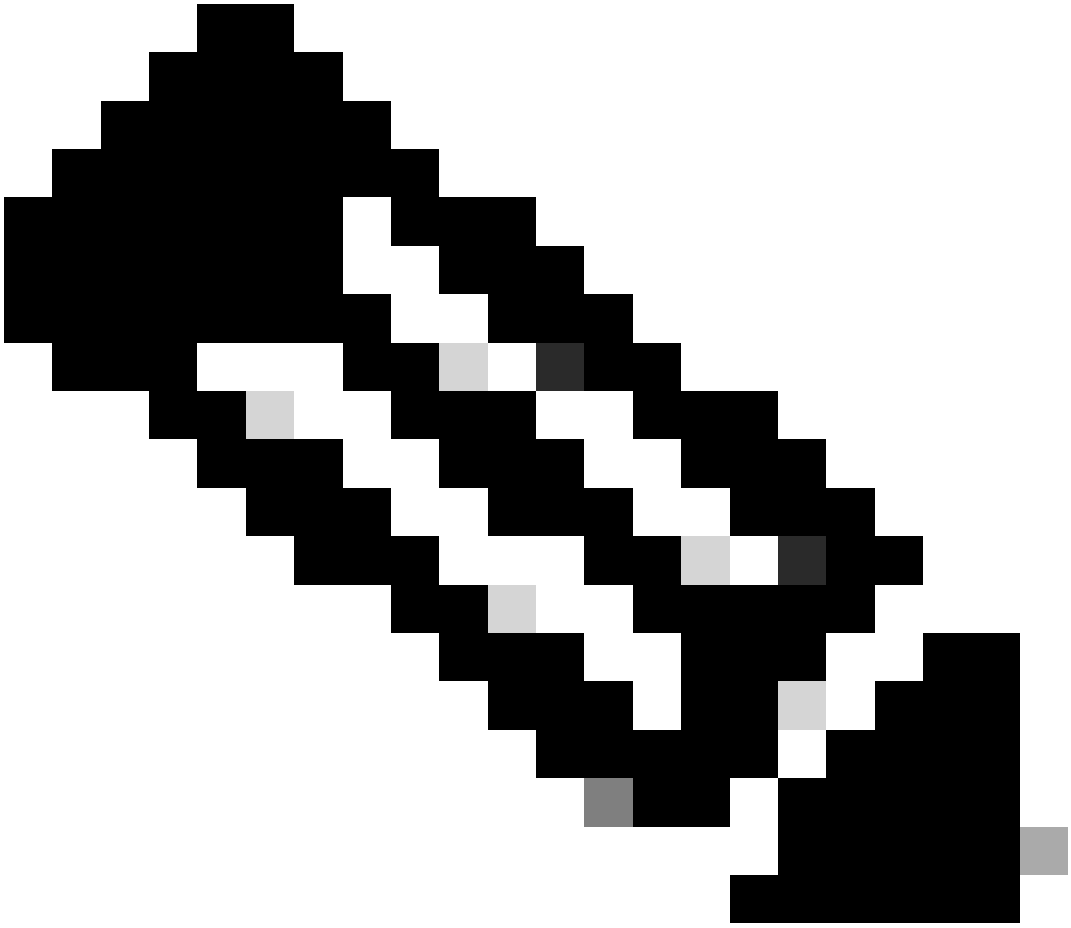

يمكنك التحقق من القاعدة التي تتوسع في عدد عناصر قائمة الوصول باستخدام الأمر perl في واجهة سطر الأوامر (CLI) الخاصة بوحدة التحكم في الوصول الموحدة:

<#root>

**perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl**

```
root@firepower:/Volume/home/admin# perl /var/opt/CSCOpx/bin/access_rule_expansion_count.pl

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer



  Enter FTD UUID or Name:

  > 10.70.73.44

------------------------------------------------------------------------------------------------------------

  Secure Firewall Management Center for VMware - v7.4.1 - (build 172)

  Access Control Rule Expansion Computer

  Device:

    UUID: 93cc359c-39be-11d4-9ae1-f2186cbddb11

    Name: 10.70.73.44

  Access Control Policy:

    UUID: 005056B9-F342-0ed3-0000-292057792375

    Name: Port-scan test

    Description:

  Intrusion Policies:
```

```
-----------------------------------------------------------------------------------------------

|  UUID                                    |  NAME                                              |

-----------------------------------------------------------------------------------------------

-----------------------------------------------------------------------------------------------

  Date: 2024-Jul-17 at 06:51:55 UTC

  NOTE: Computation is done on per rule basis. Count from shadow rules will not be applicable on device

  Run "Rule Conflict Detection" tool on AC Policy for specified device to detect and optimise such rules


-------------------------------------------------------------------------------------------------------
| UUID                                       | NAME                     |             COUNT
-------------------------------------------------------------------------------------------------------
| 005056B9-F342-0ed3-0000-000268454919       | Rule 1                   |               8
-------------------------------------------------------------------------------------------------------
|   TOTAL: 8
-------------------------------------------------------------------------------------------------------
| Access Rule Elements Count on FTD: 14
-------------------------------------------------------------------------------------------------------

>>> My JVM PID : 19417
```



ملاحظة: تعتمد عناصر قاعدة الوصول على FTD: 14. ويتضمن ذلك المجموعة الافتراضية من قواعد FTD (التصفية المسبقة) وقاعدة التحكم في الوصول الافتراضية أيضا.

---

يمكن رؤية قواعد التصفية المسبقة الافتراضية في FTD CLI:

```
firepower# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
            alert-interval 300
access-list CSM_FW_ACL_; 14 elements; name hash: 0x4a69e3f3
access-list CSM_FW_ACL_ line 1 remark rule-id 9998: PREFILTER POLICY: Default Tunnel and Priority Policy
access-list CSM_FW_ACL_ line 2 remark rule-id 9998: RULE: DEFAULT TUNNEL ACTION RULE
access-list CSM_FW_ACL_ line 3 advanced permit ipinip any any rule-id 9998 (hitcnt=0) 0xf5b597d6
access-list CSM_FW_ACL_ line 4 advanced permit udp any eq 3544 any range 1025 65535 rule-id 9998 (hitcnt=0) 0x46d7839e
access-list CSM_FW_ACL_ line 5 advanced permit udp any range 1025 65535 any eq 3544 rule-id 9998 (hitcnt=0) 0xaf1d5aa5
access-list CSM_FW_ACL_ line 6 advanced permit 41 any any rule-id 9998 (hitcnt=0) 0x06095aba
access-list CSM_FW_ACL_ line 7 advanced permit gre any any rule-id 9998 (hitcnt=0) 0x52c7a066
access-list CSM_FW_ACL_ line 8 remark rule-id 268454922: ACCESS POLICY: Port-scan test - Mandatory
access-list CSM_FW_ACL_ line 9 remark rule-id 268454922: L7 RULE: Rule 1
access-list CSM_FW_ACL_ line 10 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq www rule-id 268454922 (hitcnt=0) 0x46def508
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x046f6a57
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0xeced82d1
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq www rule-id 268454922 (hitcnt=0) 0x16cf481d
  access-list CSM_FW_ACL_ line 10 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq www rule-id 268454922 (hitcnt=0) 0x9d098336
access-list CSM_FW_ACL_ line 11 advanced permit tcp object-group FMC_INLINE_src_rule_268454922 object-group FMC_INLINE_dst_rule_268454922 eq https rule-id 268454922 (hitcnt=0) 0x548058c2

  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x89163d78
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.1.1.1 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x837a795d
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.3.3.3 eq https rule-id 268454922 (hitcnt=0) 0x42a0ae77
  access-list CSM_FW_ACL_ line 11 advanced permit tcp host 10.2.2.2 host 10.4.4.4 eq https rule-id 268454922 (hitcnt=0) 0x569b1e17
access-list CSM_FW_ACL_ line 12 remark rule-id 268453888: ACCESS POLICY: Port-scan test - Default
access-list CSM_FW_ACL_ line 13 remark rule-id 268453888: L4 RULE: DEFAULT ACTION RULE
access-list CSM_FW_ACL_ line 14 advanced deny ip any any rule-id 268453888 (hitcnt=0) 0x97aa021a
```

6 Default Pre-filter Rules.

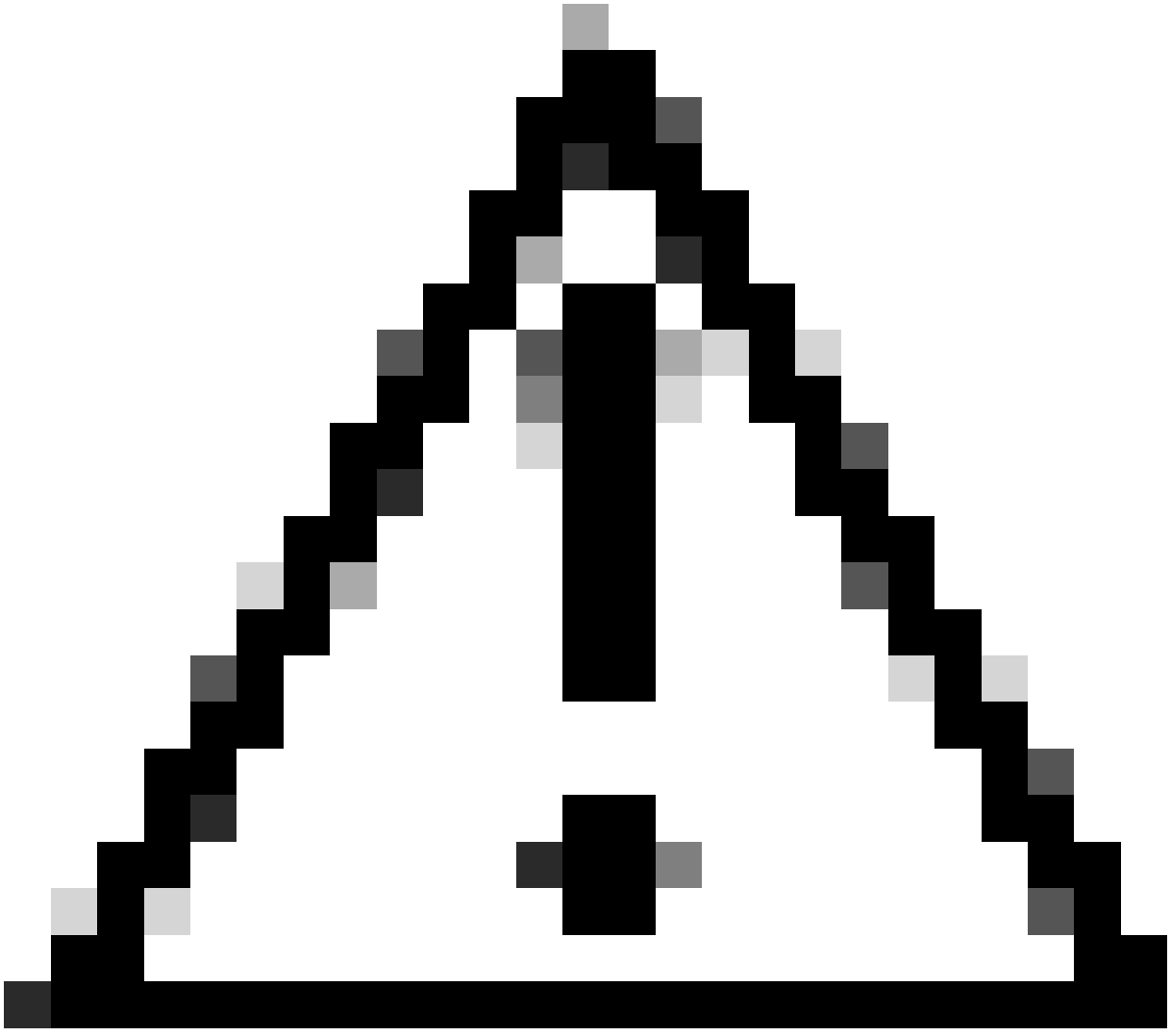
## تأثير High ACE

- يمكن مالحظة إرتفاع مستوى وحدة المعالجة المركزية.
- يمكن رؤية سعة الذاكرة العالية.
- يمكن مالحظة بطء الجهاز.
- فشل عمليات النشر/ وقت أطول للنشر.

## تحديد متى يتم تمكين بحث مجموعة الكائنات (OGS)

- يتجاوز عدد ACE حد ACE الخاص بالجهاز.
- وحدة المعالجة المركزية الخاصة بالجهاز ليست عالية بالفعل حيث أن تمكين OGS يفرض المزيد من الضغط على وحدة المعالجة المركزية الخاصة بالجهاز.
- قم بتمكينه أثناء ساعات عدم الإنتاج.

---



---

تحذير: الرجاء تمكين مجموعة الوصول إلى الالتزام بالمعاملات لمحرك قاعدة ASP من وضع واجهة سطر الأوامر (CLI) ل FTD قبل تمكين OGS. تم تكوين هذا الخيار لتجنب حالات سقوط حركة المرور أثناء عملية النشر وبعدها مباشرة أثناء تمكين OGS.

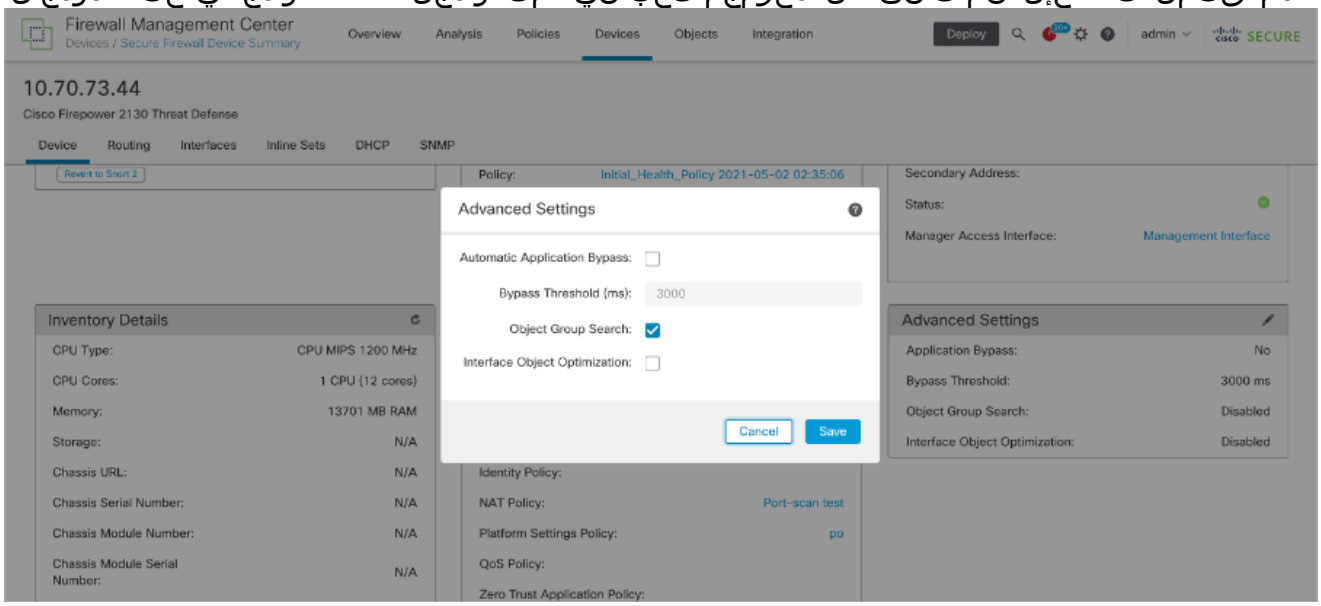
```
>
>
>
>
> asp rule-engine transactional-commit access-group
>
>
>
```

## تمكين البحث عن مجموعة كائنات

لم يتم تمكين OGS حاليا:

```
firepower#
firepower#
firepower#
firepower# show run object-group-search
firepower#
firepower#
firepower#
```

1. سجل الدخول إلى واجهة سطر الأوامر (CLI) لوحدة التحكم FMC. انتقل إلى الأجهزة > إدارة الأجهزة > تحديد جهاز FTD > الجهاز. تمكين بحث مجموعة الكائنات من الإعدادات المتقدمة:

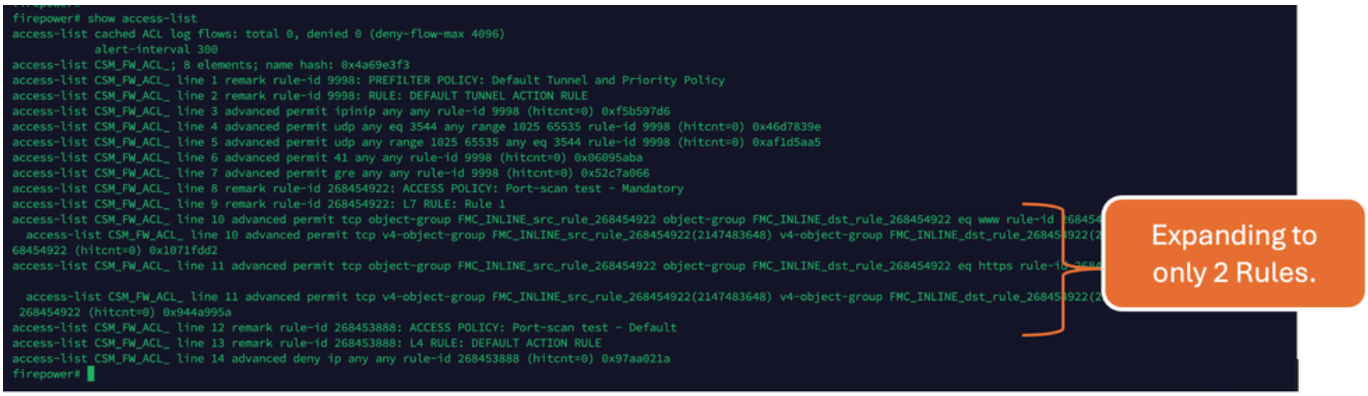


2. انقر فوق حفظ ونشر.

## التحقق من الصحة

قبل تمكين OGS:


بعد تمكين OGS:




## معلومات ذات صلة

لمزيد من المعلومات التفصيلية حول كيفية توسيع القواعد في FTD، راجع المستند [فهم توسيع القاعدة على أجهزة FirePOWER](#).

لمزيد من المعلومات حول بنية "برنامج الإرسال فائق السرعة (FTD)" واستكشاف الأخطاء وإصلاحها، ارجع إلى [الدفاع عن تهديد الطاقة النارية (FTD).](#)

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).