# FTD: كيفية تمكين تكوين تجاوز حالة TCP باستخدام سياسة FlexConfig

## المحتويات



## المقدمة

يوضح هذا المستند كيفية تنفيذ ميزة تجاوز حالة بروتوكول التحكم في الإرسال (TCP) باستخدام مركز إدارة FirePOWER (FMC) عبر تهديد FirePOWER (FTD) أجهزة الدفاع عن على سياسة FlexConfig في الإصدارات السابقة لـ 6.3.0.

## المتطلبات الأساسية

### المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة مركز إدارة FirePOWER.
- المعرفة الأساسية الخاصة بالدفاع ضد تهديد قوة النيران.
- فهم ميزة تجاوز حالة TCP.

### المكونات المستخدمة

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

- الدفاع ضد تهديد Firepower (FTD)، الإصدار 6.2.3.
- مركز إدارة Firepower (FMC)، الإصدار 6.2.3.

## معلومات أساسية

يعد تجاوز حالة TCP ميزة موروثة من جهاز الأمان القابل للتكيف (ASA) ويوفر المساعدة عند

أستكشاف أخطاء حركة المرور وإصلاحها التي يمكن إسقاطها إما من خلال ميزات تطبيع TCP وشروط التوجيه غير المتماثل وعمليات فحص معينة للتطبيقات.

هذه الميزة مدعومة بطبيعتها على إصدار بدء FMC 6.3.0. يوصى بحذف كائنات FlexConfig بعد الترقية ونقل هذا التكوين إلى FMC قبل النشر الأول. لمزيد من المعلومات حول كيفية تكوين تجاوز حالة TCP في الإصدار 6.3.0 أو إصدار أحدث، انتقل إلى دليل التكوين هذا.

يستخدم الدفاع عن تهديد Firepower أوامر تكوين ASA لتنفيذ بعض الميزات، ولكن ليس جميع الميزات. ال توجد مجموعة فريدة من أوامر تكوين الدفاع عن تهديد FirePOWER. وبدلا من ذلك، فإن النقطة من FlexConfig هي السماح لك بتكوين الميزات التي لم يتم دعمها مباشرة بعد من خلال نهج مركز إدارة Firepower وإعداداته.

> **ملاحظة**: يجب إستخدام تجاوز حالة TCP فقط لأغراض أستكشاف الأخطاء وإصلاحها أو عندما ال يمكن حل التوجيه غير المتماثل. يؤدي إستخدام هذه الميزة إلى تعطيل ميزات أمان متعددة وقد يؤدي إلى إرتفاع عدد الاتصالات إذا لم يتم تنفيذها بشكل صحيح.

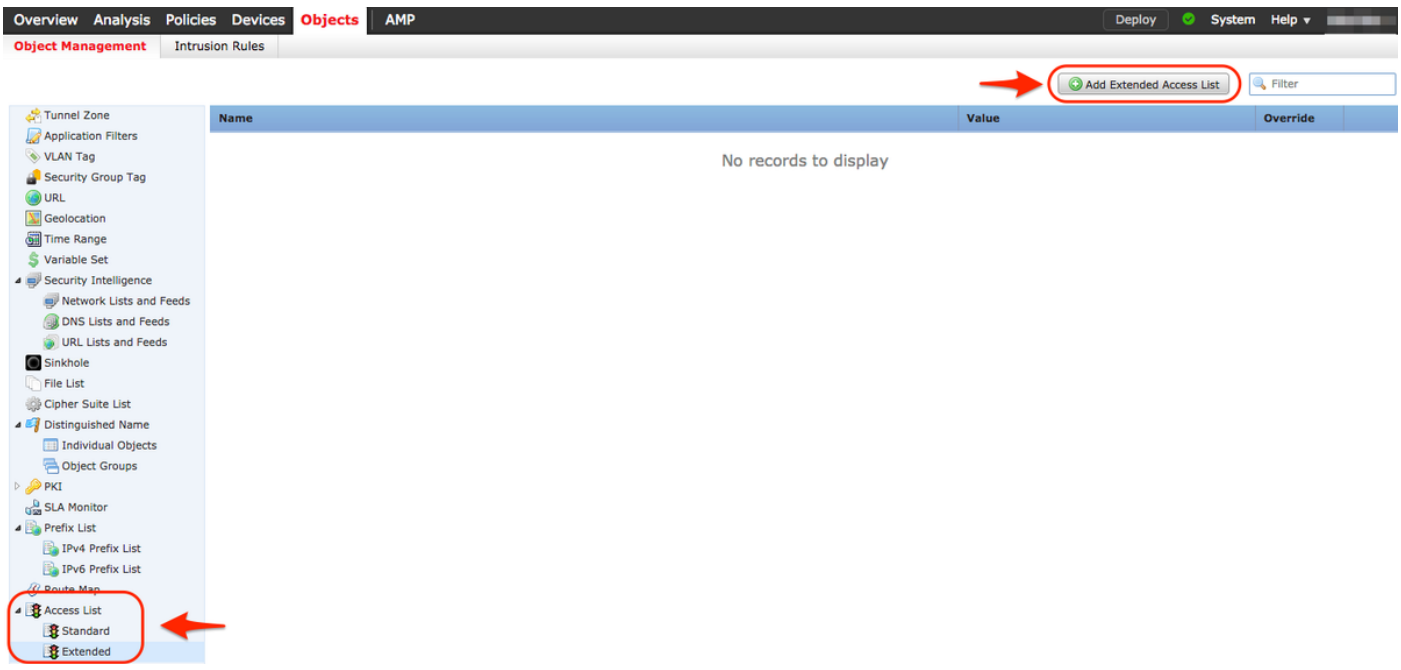
أحلت in order to عرفت كثير حول TCP دولة تجاوز سمة وأ تنفيذها في ASA، ال configure ال TCP دولة مجرى جانبي سمة على ال ASA 5500 sery والcisco ASA 5500 sery تشكيل مرشد.

# التكوين

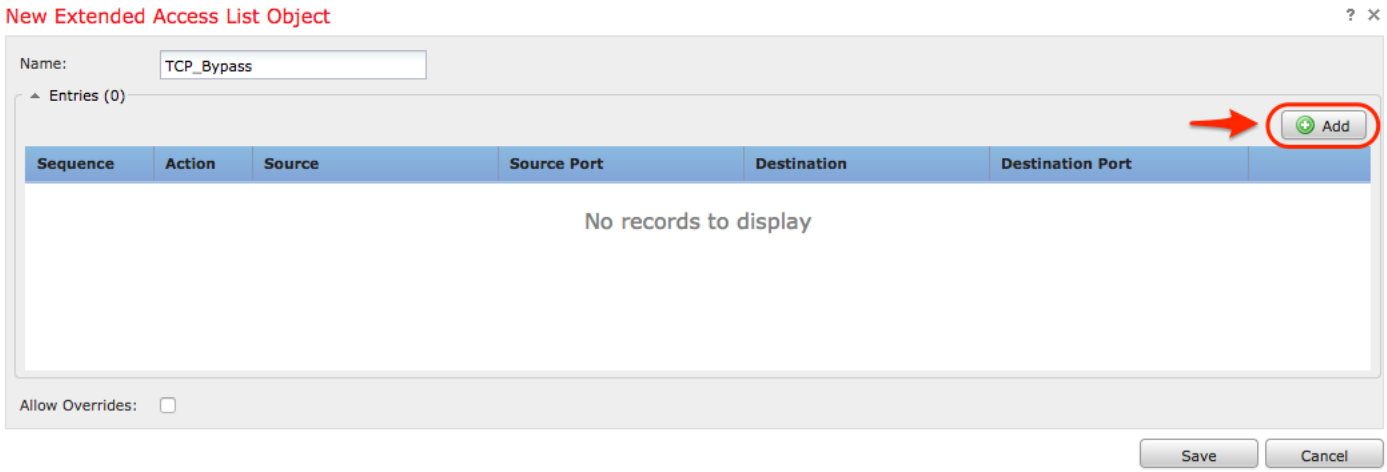
يصف هذا القسم كيفية تكوين تجاوز حالة TCP على FMC من خلال سياسة FlexConfig.

### الخطوة 1. تكوين كائن قائمة الوصول الموسعة

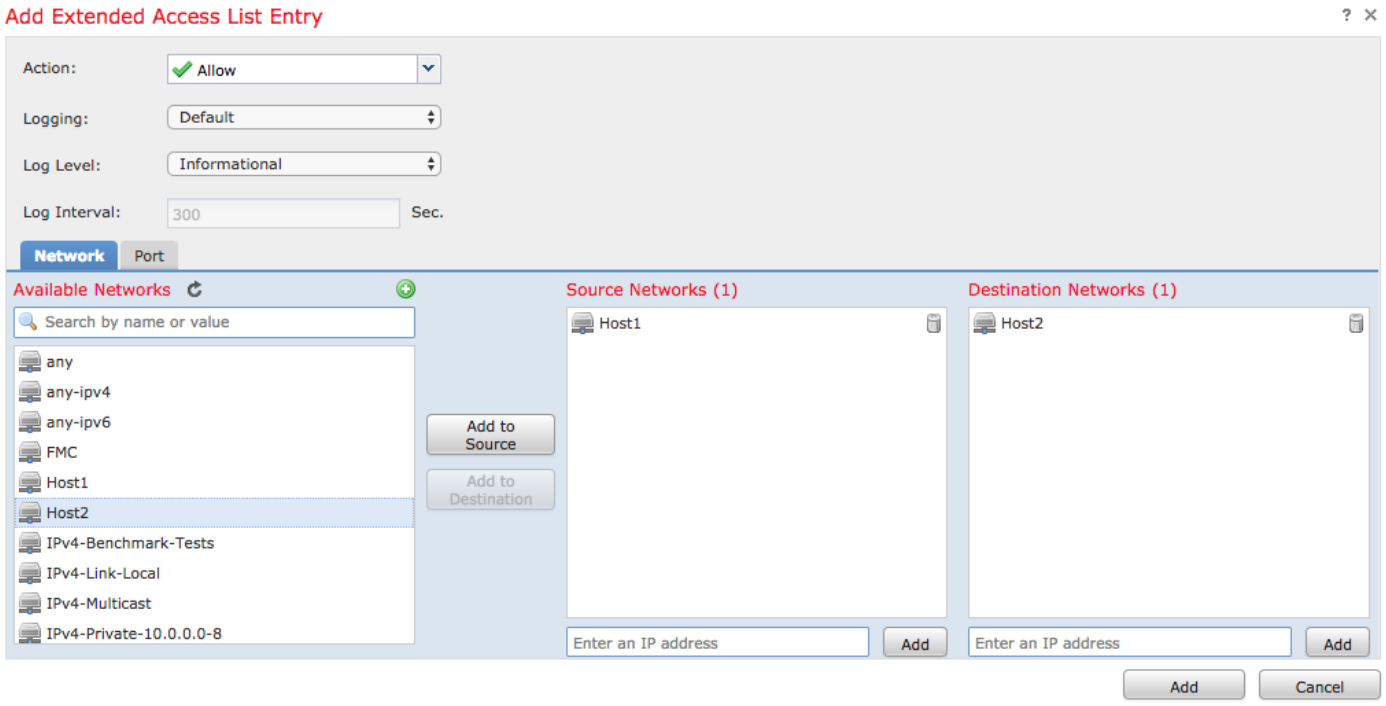
لإنشاء قائمة الوصول الموسعة على FMC، انتقل إلى **الكائنات >إدارة الكائنات**، وعلى القائمة اليسرى، تحت **قائمة الوصول** حدد **موسع. قائمة الوصول الموسعة ل ClickAdd.**



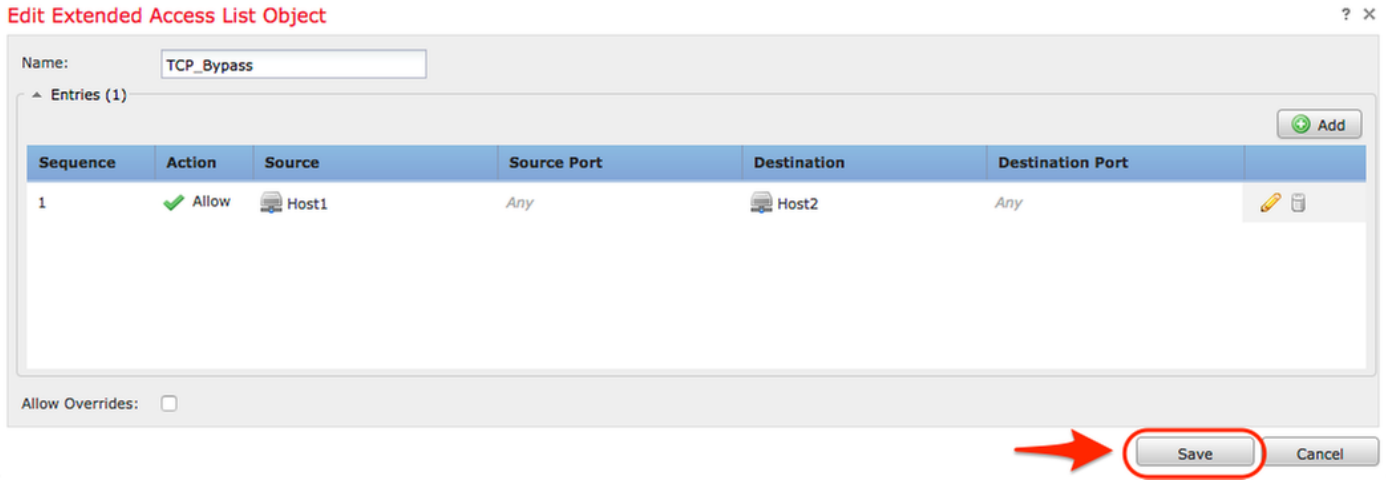

قم بتعبئة حقل "الاسم" بالقيمة المطلوبة. في هذا المثال، يكون الاسم **TCP_Bypass**. طقطقة **يضيف** زر.




يجب تكوين الإجراء الخاص بهذه القاعدة **على** أنه **'السماح'**. يمكن إستخدام شبكة معرفة بواسطة النظام أو يمكن إنشاء كائن شبكة جديد لكل مصدر ووجهة. في هذا المثال، تطابق قائمة الوصول حركة مرور IP من المضيف1 إلى المضيف2 حيث يكون هذا الاتصال لتطبيق تجاوز حالة TCP. يمكن إستخدام علامة تبويب المنفذ إختياري لمطابقة منفذ TCP أو UDP معين. انقر فوق الزر **إضافة** للمتابعة.

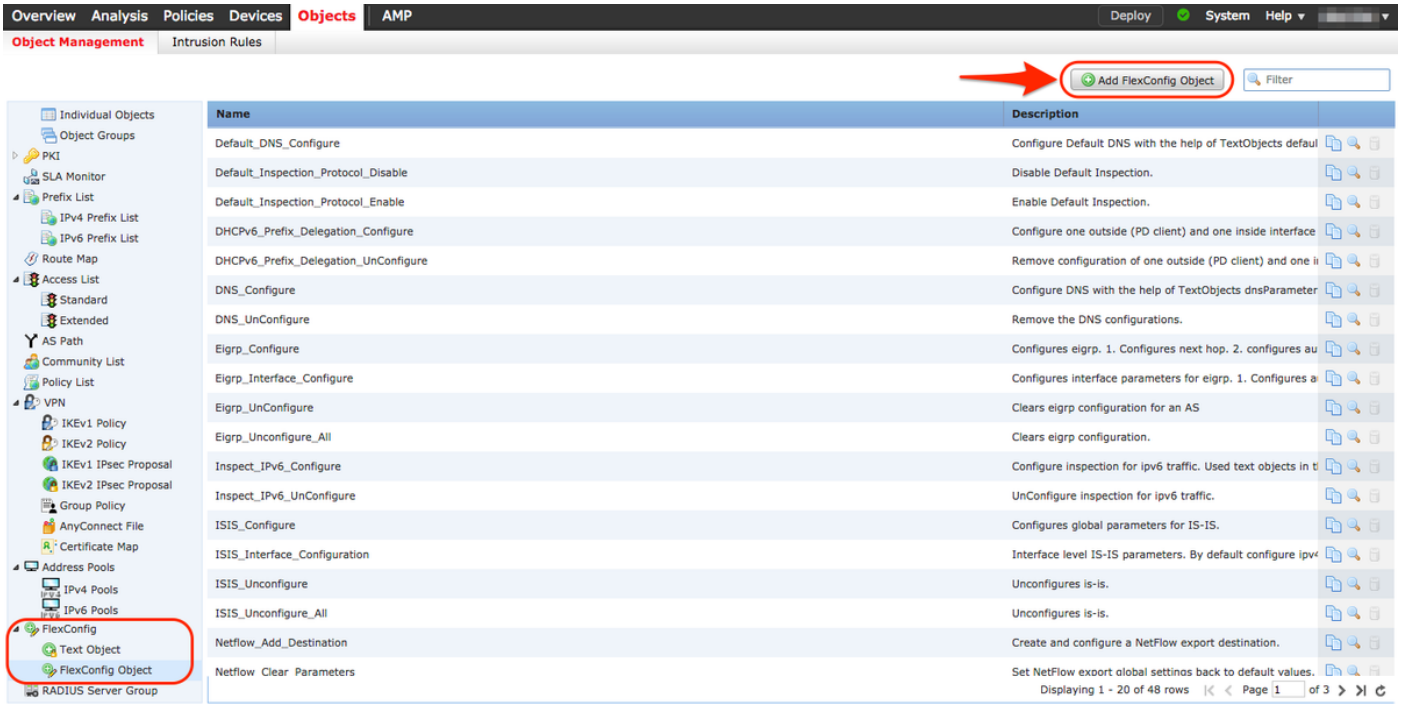



بمجرد تحديد الشبكات أو البيئات المضيفة المصدر والوجهة، انقر على **حفظ**.



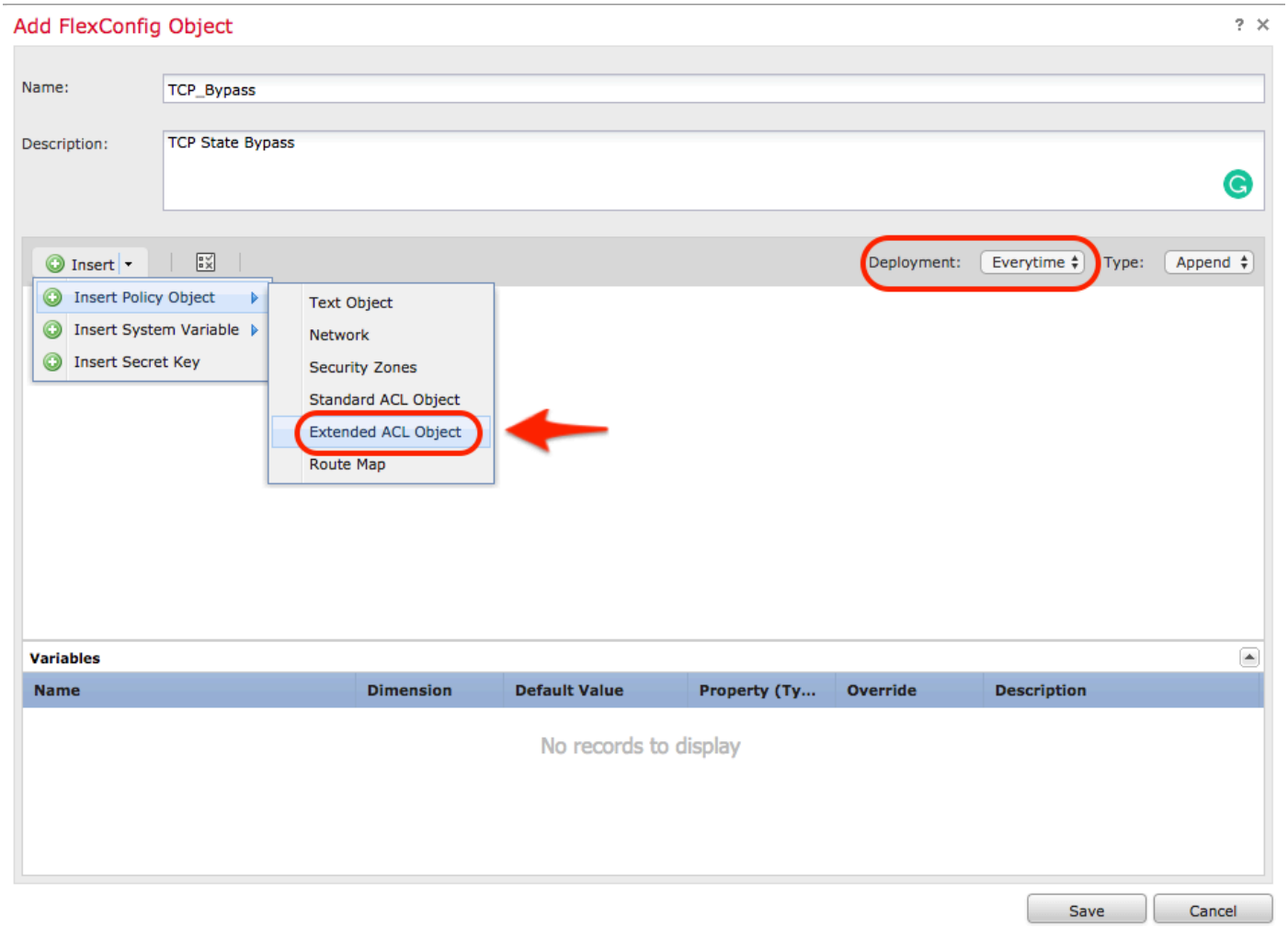
## الخطوة 2. تكوين كائن FlexConfig

انتقل إلى **الكائنات > إدارة الكائن > FlexConfig > FlexConfig Object** وانقر على زر **إضافة كائن FlexConfig**.




يسمى اسم الكائن لهذا المثال **TCP_Bypass** مثل قائمة الوصول. لا يلزم أن يتطابق هذا الاسم مع اسم قائمة الوصول.

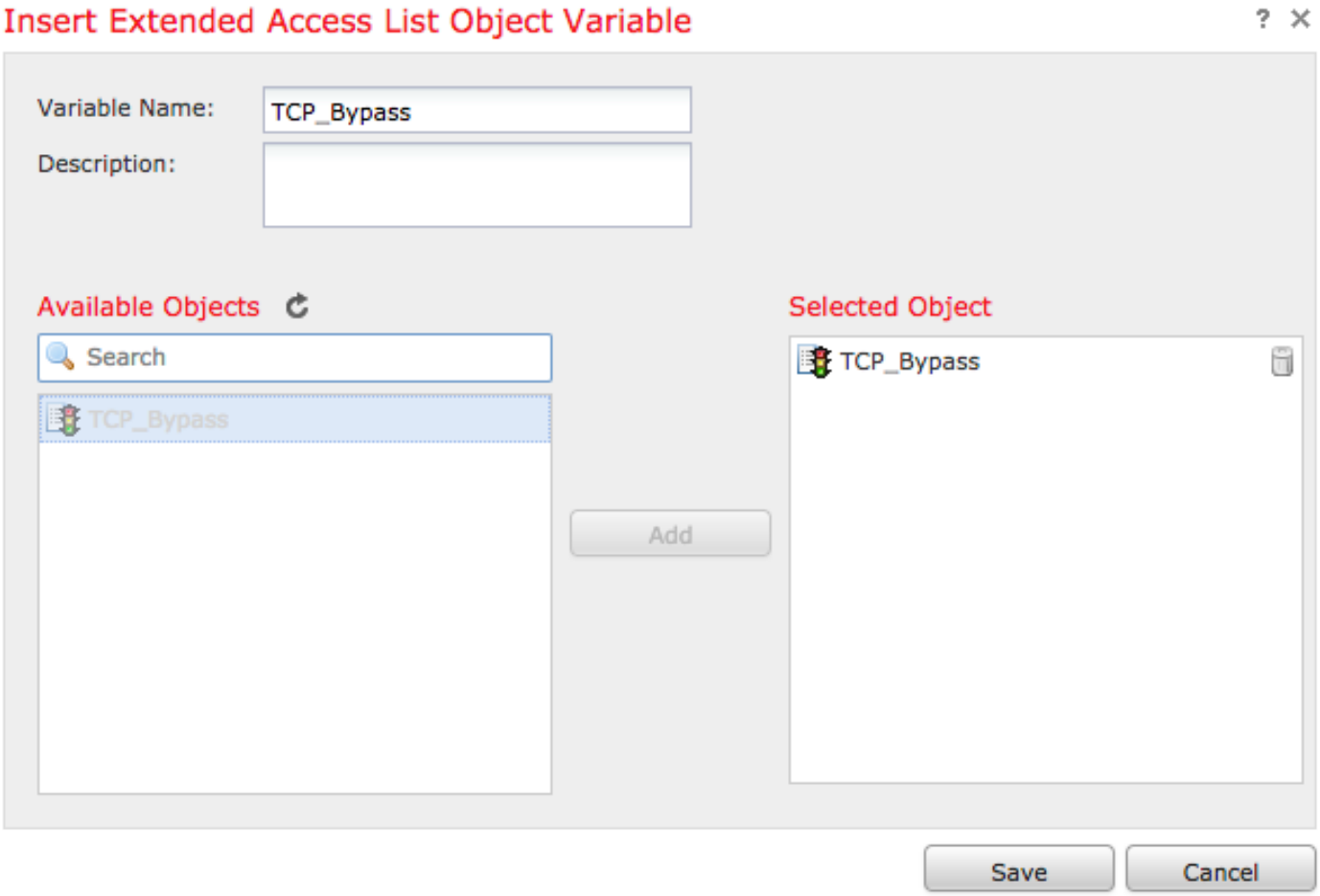
حدد **إدراج كائن نموذج > كائن قائمة التحكم في الوصول الموسعة.**




**ملاحظة**: تأكد من إختيار الخيار "كل مرة". وهذا يسمح بالحفاظ على هذا التكوين أثناء عمليات النشر والترقية الأخرى.

حدد قائمة الوصول التي تم إنشاؤها في الخطوة 1 من قسم **الكائنات المتاحة** وقم بتعيين اسم متغير. بعد ذلك، انقر فوق الزر **إضافة**. في هذا مثال، ال متغير إسم **TCP_Bypass**.

انقر فوق **حفظ**.

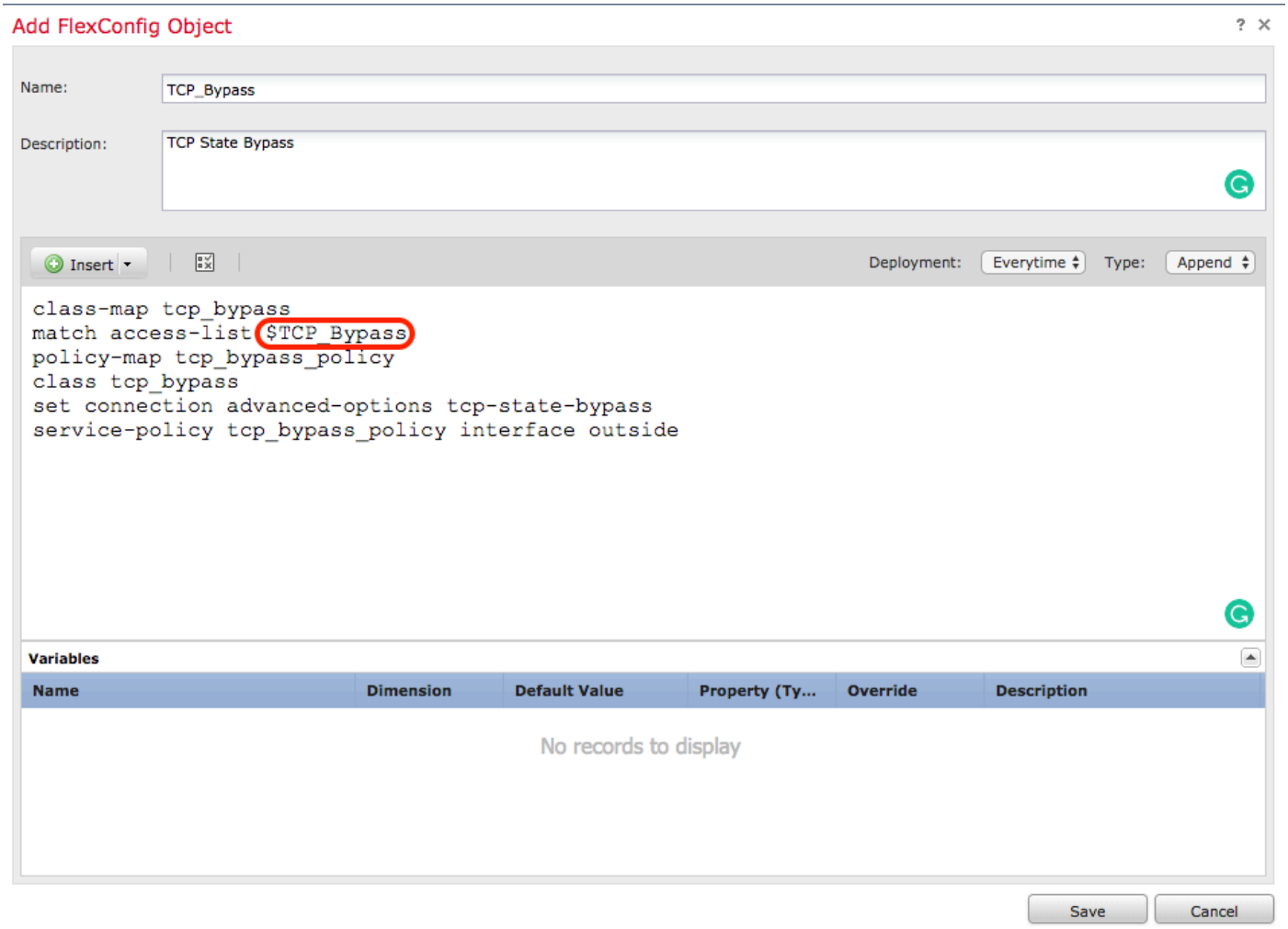



قم بإضافة خطوط التكوين التالية في الحقل الفارغ أسفل الزر **إدراج** وقم بتضمين match access-list. لاحظ أن رمز $ سابق لاسم المتغير. هذا يساعد على تعريف أن المتغير يتبعه. (**$TCP_Bypass**) في سطر تكوين *match access-list*. لاحظ المتغير الذي تم تعريفه مسبقا

```
class-map tcp_bypass
match access-list $TCP_Bypass
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
service-policy tcp_bypass_policy interface outside
```

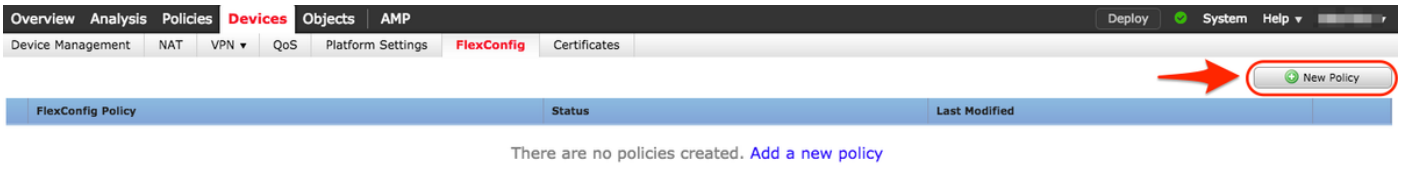
في هذا المثال، يتم إنشاء خريطة سياسة ويتم تطبيقها على الواجهة الخارجية. إذا كان يلزم تكوين تجاوز حالة TCP كجزء من سياسة الخدمة العالمية، يمكن تطبيق خريطة فئة tcp_bypass على global_policy.

انقر على **حفظ** عند الانتهاء.

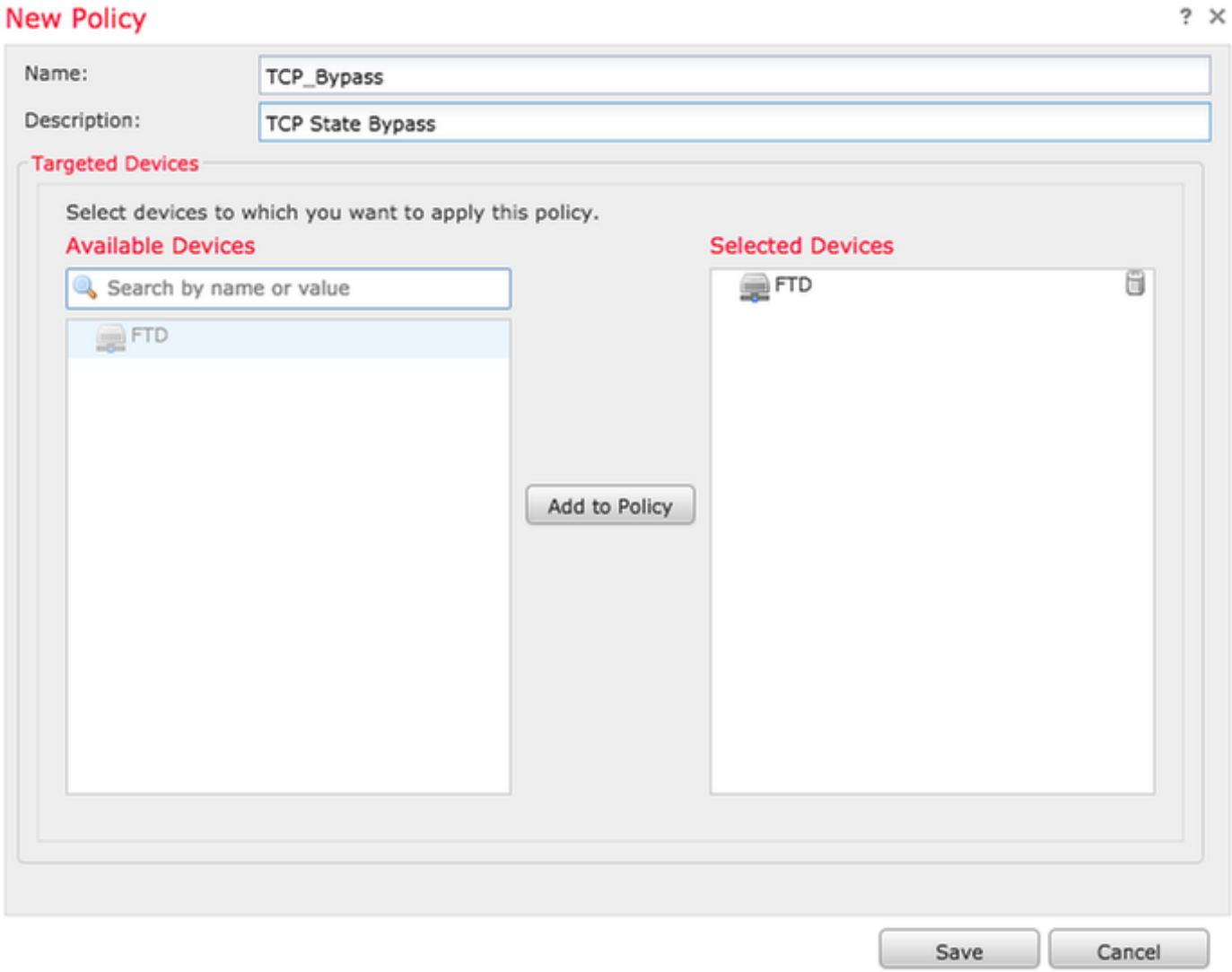



### الخطوة 3. تعيين سياسة FlexConfig إلى FTD

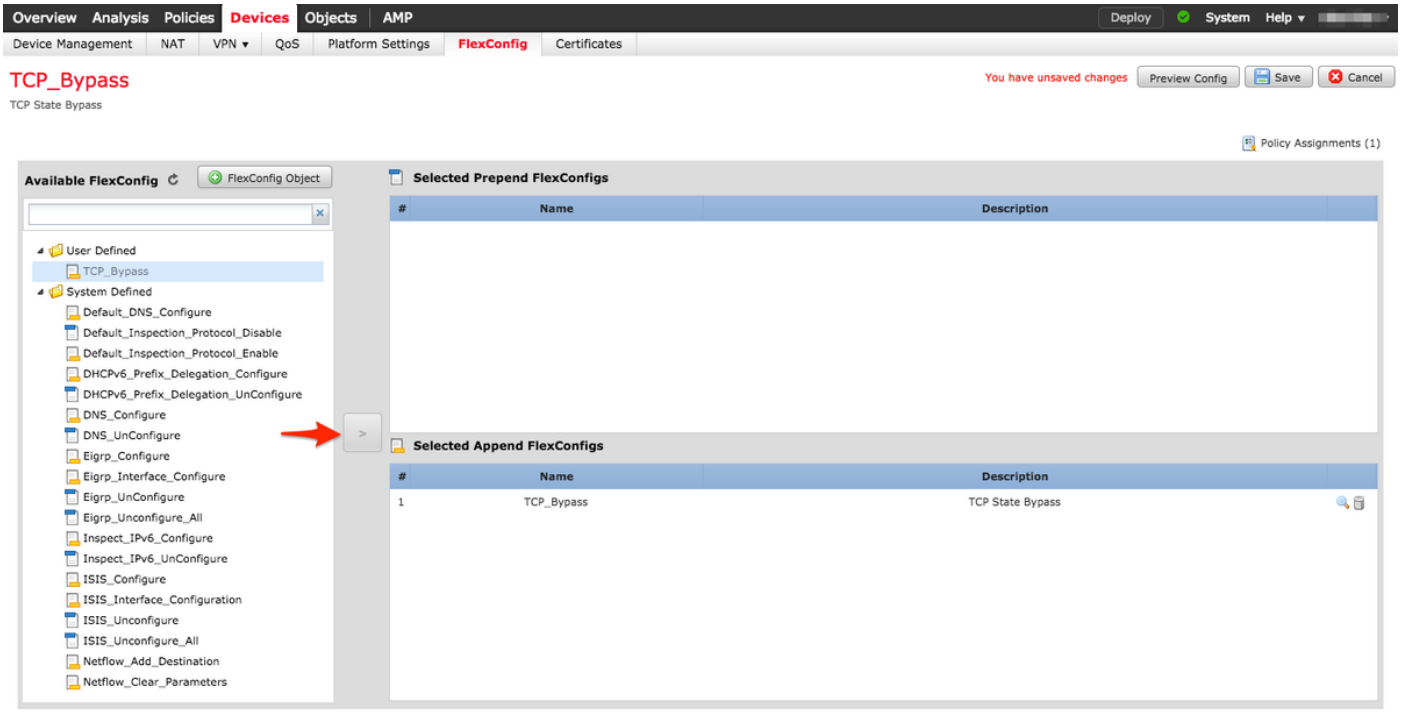
انتقل إلى **الأجهزة > FlexConfig** وأنشئ سياسة جديدة (ما لم يكن هناك نهج تم إنشاؤه بالفعل لغرض آخر وتم تعيينه إلى نفس FTD).في هذا المثال، يسمى نهج FelxConfig الجديد **TCP_Bypass**.



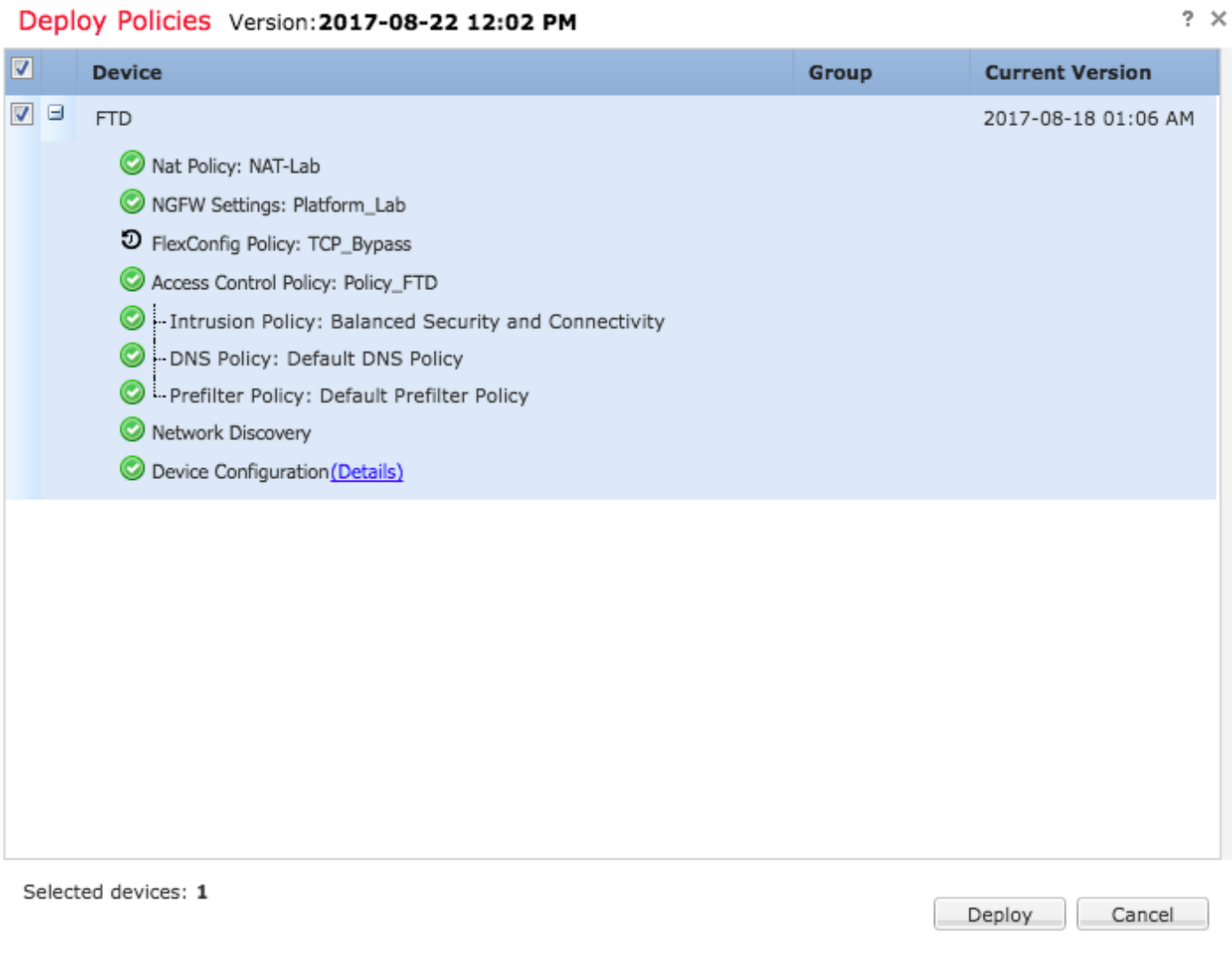

قم بتخصيص سياسة **TCP_Bypass** FlexConfig لجهاز FTD.




حدد كائن FlexConfig المسمى **TCP_Bypass** الذي تم إنشاؤه في الخطوة 2 تحت القسم **معرف من قبل المستخدم** وانقر فوق السهم لإضافة هذا الكائن إلى النهج.




حفظ التغييرات والنشر.




# التحقق

قم بالوصول إلى FTD من خلال SSH أو وحدة التحكم واستخدم الأمر **system support diagnostic-cli.**

```
> system support diagnostic-cli
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.
Type help or '?' for a list of available commands.

firepower# show access-list TCP_Bypass
access-list TCP_Bypass; 1 elements; name hash: 0xec2b41eb
access-list TCP_Bypass line 1 extended permit object-group ProxySG_ExtendedACL_34359739205
object Host1 object Host2 log informational interval 300 (hitcnt=0) 0x42940b0e
access-list TCP_Bypass line 1 extended permit ip host 1.1.1.1 host 1.1.1.2 log informational
interval 300 (hitcnt=0) 0x769561fc

firepower# show running-config class-map
!
class-map inspection_default
match default-inspection-traffic
class-map tcp_bypass
match access-list TCP_Bypass
!
firepower# show running-config 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 xdmcp
inspect sip
inspect netbios
inspect tftp
inspect icmp
inspect icmp error
inspect ip-options UM_STATIC_IP_OPTIONS_MAP
class class-default
set connection advanced-options UM_STATIC_TCP_MAP
policy-map tcp_bypass_policy
class tcp_bypass
set connection advanced-options tcp-state-bypass
!
```

# استكشاف الأخطاء وإصلاحها

لاستكشاف أخطاء هذه المميزة وإصلاحها، ينتج عن هذه الأوامر مساعدة.

**- show conn [detail]**
Shows connection information. Detailed information uses flags to indicate special connection characteristics.
For example, the “b” flag indicates traffic subject to TCP State Bypass

**- show service-policy**
Shows service policy statistics, including Dead Connection Detection (DCD) statistics

# روابط ذات صلة

https://www.cisco.com/c/en/us/td/docs/security/asa/asa91/configuration/firewall/asa_91_firewall_config/conns_connlimits.html

https://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/118995-configure-asa-00.html

https://www.cisco.com/c/en/us/td/docs/security/firepower/620/configuration/guide/fpmc-config-guide-v62/flexconfig_policies.html

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).