يعرض مركز إدارة FirePOWER بعض أحداث اتصال TCP في الإتجاه الخاطئ

المحتويات

المقدمة

يصف هذا المستند أسباب ظهور خطوات تخفيف "مركز إدارة FirePOWER (FMC)" التي تعرض أحداث اتصال TCP في الإتجاه العكسي حيث يكون عنوان IP الخاص بالمنشئ هو عنوان IP الخاص بخادم اتصال TCP بينما يمثل عنوان IP الخاص بالمستجيب الخاص باتصال TCP.

ملاحظة: هناك أسباب متعددة لتكرار مثل هذه الأحداث. وتوضح هذه الوثائق السبب الأكثر شيوعا لهذا العرض.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- تقنية FirePOWER
- معرفة أساسية بأجهزة الأمان المعدلة (ASA)
- فهم آلية توقيت بروتوكول التحكم في الإرسال (TCP)

المكونات المستخدمة

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

- الدفاع ضد تهديد ASA 5516-X، ASA 5508-X، ASA Firepower (5506X/5506H-X/5506W-X) الذي يعمل بإصدار البرنامج 6.0.1 والإصدارات الأحدث
- الدفاع ضد تهديد ASA 5585-X، ASA 5555-X، ASA 5545-X، ASA 5525-X، ASA FirePOWER (5512-X،5515-X) الذي يعمل ببرنامج صيغة 6.0.1 ومتأخر (FP9300، FP4100
- ASA مع وحدات FirePOWER النمطية (ASA 5516-X، ASA 5508-X، 5506X/5506H-X/5506W-X) التي تشغل إصدارات البرامج 6.0.0 والإصدارات الأحدث

- مركز إدارة Firepower (FMC)، الإصدار 6.0.0 والإصدارات الأحدث

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

الخلفية

في اتصال TCP، يشير **العميل** إلى IP الذي يرسل الحزمة الأولية. يقوم مركز إدارة FirePOWER بإنشاء حدث اتصال عندما يرى الجهاز المدار (المستشعر أو FTD) حزمة TCP الأولية للاتصال.

تحتوي الأجهزة التي تتعقب حالة اتصال TCP على **مهلة خاملة** معرفة للتأكد من أن الاتصالات التي لا يتم إغلاقها بشكل خاطئ بواسطة نقاط النهاية لا تستهلك الذاكرة المتاحة لفترات طويلة من الوقت. مهلة الخمول الافتراضية لاتصالات TCP التي تم إنشاؤها على FirePOWER هي **ثلاث دقائق**. لم يتم تعقب اتصال TCP الذي ظل خاملا لمدة ثلاث دقائق أو أكثر بواسطة مستشعر FirePOWER IPS.

يتم التعامل مع الحزمة التالية بعد المهلة كتدفق TCP جديد ويتم إتخاذ قرار إعادة التوجيه وفقا للقاعدة التي تطابق هذه الحزمة.عندما تكون الحزمة من الخادم، يتم تسجيل IP الخاص بالخادم كبادئ لهذا التدفق الجديد. عند تمكين التسجيل للقاعدة، يتم إنشاء حدث اتصال على مركز إدارة FirePOWER.

ملاحظة: وفقا لسياسات تم تكوينها، يختلف قرار إعادة التوجيه للحزمة التي تأتي بعد انتهاء المهلة عن القرار الخاص بحزمة TCP الأولية. إذا كان الإجراء الافتراضي الذي تم تكوينه هو "حظر"، يتم إسقاط الحزمة.

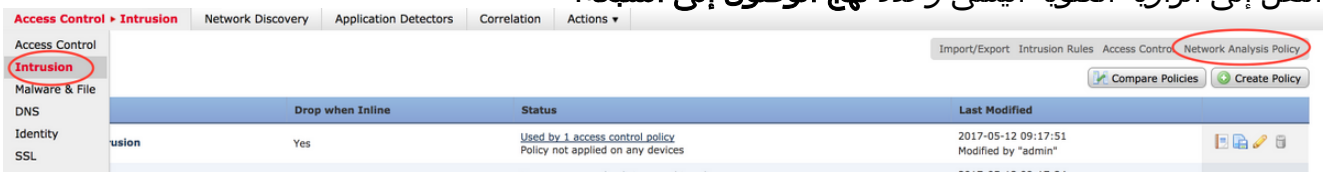
والمثال على هذا العرض هو بحسب لقطة الشاشة أدناه:

First Packet	Last Packet	Action	Reason	Initiator IP	Initiator Country	Responder IP	Responder Country	Ingress Security Zone	Egress Security Zone	Source Port / ICMP Type	Destination Port / ICMP Code
2017-05-12 17:48:05		Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
2017-05-12 17:39:13		Allow		192.168.38.30		10.32.38.30				44705 / tcp	443 (https) / tcp

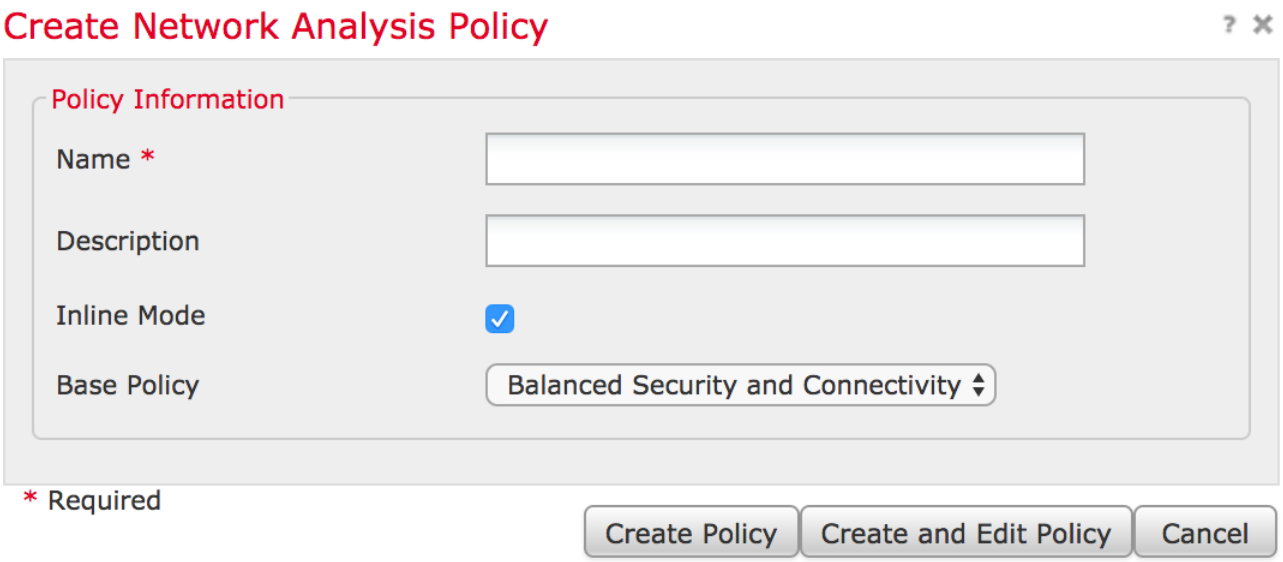
الحل

يتم تخفيف المشكلة المذكورة أعلاه عن طريق زيادة **مهلة** إتصالات TCP. ومن أجل تغيير المهلة،

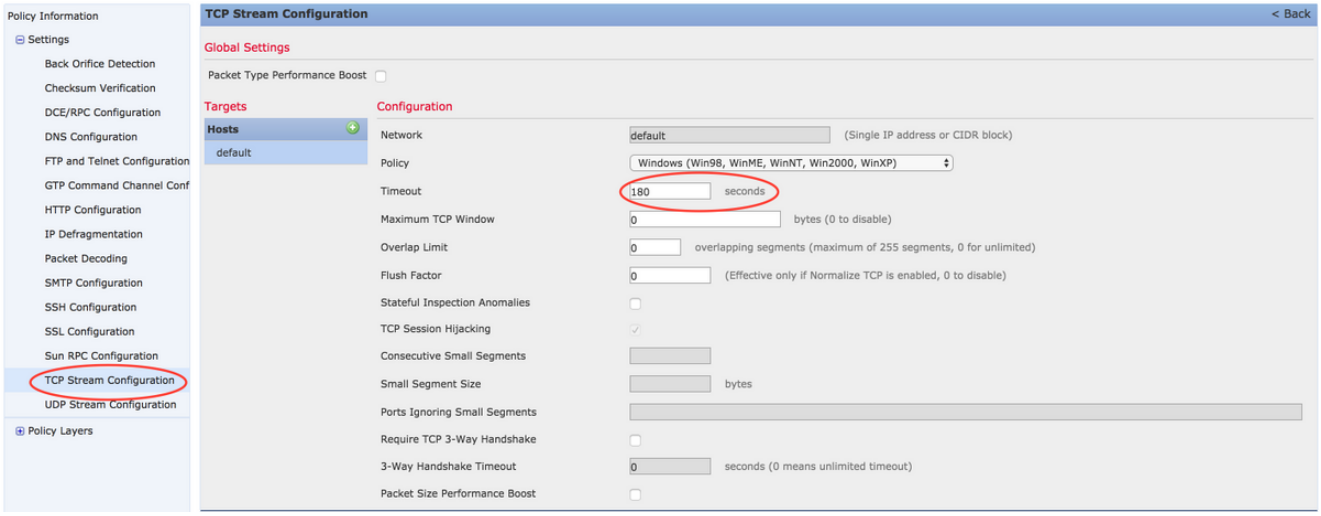
1. انتقل إلى **السياسات > التحكم في الوصول > التطفل**.
2. انتقل إلى الزاوية العلوية اليمنى وحدد **نهج الوصول إلى الشبكة**.



3. حدد **إنشاء نهج** ، أختر اسما وانقر فوق **إنشاء نهج وتحريره**. لا تقم بتعديل **النهج الأساسي**.

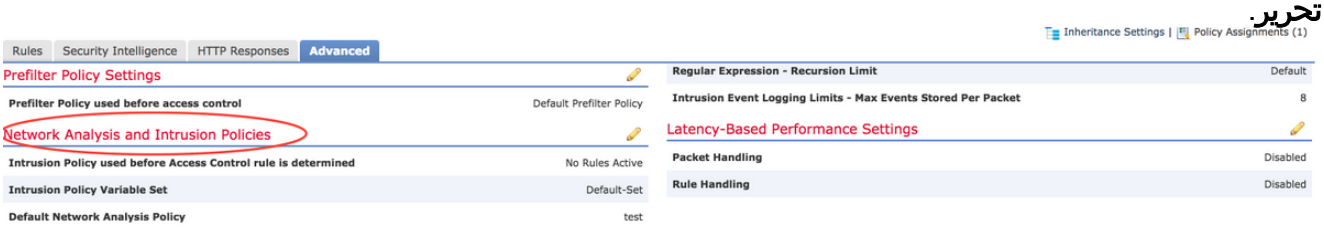


4. مددت **العملية إعداد** خيار واخترت **TCP دفق تشكيل**.
5. انتقل إلى قسم التكوين وغير قيمة **المهلة** حسب الرغبة.



6. انتقل إلى **السياسات > التحكم في الوصول > التحكم في الوصول**.
7. حدد الخيار **تحرير** لتحرير السياسة المطبقة على الجهاز المدار ذي الصلة أو إنشاء سياسة جديدة.

8. حدد علامة التبويب **خيارات متقدمة** في نهج الوصول.
9. حدد موقع قسم **تحليل الشبكة ونهج الاقتحام** وانقر على أيقونة **تحرير**.



10. من القائمة المنسدلة **لنهج تحليل الشبكة الافتراضي**، أختر النهج الذي تم إنشاؤه في الخطوة 2.
11. انقر فوق **موافق** و**حفظ** التغييرات.
12. انقر فوق خيار **النشر** لنشر السياسات على الأجهزة المرتبطة المرتبطة.

تحذير: من المتوقع أن تؤدي زيادة المهلة إلى زيادة إستخدام الذاكرة، ويتعين على FirePOWER تعقب التدفقات التي لا يتم إغلاقها بواسطة نقاط النهاية لفترة أطول. تختلف الزيادة الفعلية في إستخدام الذاكرة لكل

شبكة فريدة لأنها تعتمد على المدة التي تحافظ فيها تطبيقات الشبكة على إتصالات TCP في وضع الخمول.

القرار

يختلف الاختبار المعياري لكل شبكة للمهلة الخاملة لاتصالات TCP. يعتمد ذلك تماما على التطبيقات المستخدمة. يجب إنشاء قيمة مثالية من خلال ملاحظة المدة التي تبقي فيها تطبيقات الشبكة إتصالات TCP في وضع الخمول. بالنسبة للمشكلات المتعلقة بوحدة خدمة FirePOWER على جهاز ASA من Cisco، فعندما لا يمكن إستنتاج قيمة مثالية، يمكن ضبط المهلة من خلال زيادتها في خطوات تصل إلى قيمة المهلة الخاصة ب ASA.

معلومات ذات صلة

- دليل البدء السريع للدفاع عن تهديد FirePOWER من Cisco ل ASA
- الدعم التقني والمستندات - Cisco Systems
- دليل البدء السريع ل ASA Firepower

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).