

ثادحأ ضعب FirePOWER ةرادإ زكرم ضرعي ئطاخلا هاجتإلا يف TCP لاصتا

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الخلفية](#)
- [الحل](#)
- [القرار](#)
- [معلومات ذات صلة](#)

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

• مركز إدارة (FMC Firepower)، 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 خاملاً لمدة ثلاث دقائق أو أكثر بواسطة مستشعر FirePOWER IPS.

يتم التعامل مع الحزمة التالية بعد المهلة كتدفق TCP جديد ويتم اتخاذ قرار إعادة توجيهه وفقاً 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: وفقاً لسياسات تم تكوينها، يختلف قرار إعادة توجيه الحزمة التي تأتي بعد انتهاء المهلة عن القرار الخاص بحزمة TCP الأولية. إذا كان الإجراء الافتراضي الذي تم تكوينه هو "حظر"، يتم إسقاط الحزمة.

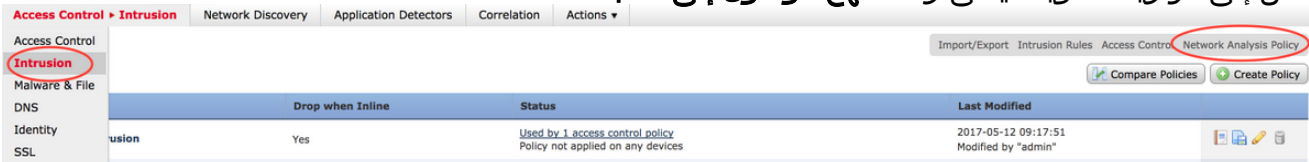
والمثال على هذا العرض هو بحسب لقطة الشاشة أدناه:

	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
↓	<input type="checkbox"/>	2017-05-12 17:48:05	Block		10.32.38.30		192.168.38.30				443 (https) / tcp	44705 / tcp
↓	<input type="checkbox"/>	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 ، أختار اسما وانقر فوق إنشاء نهج وتحريره. لا تقوم بتعديل النهج الأساسي.

Create Network Analysis Policy



Policy Information

Name *

Description

Inline Mode

Base Policy

* Required

Create Policy

Create and Edit Policy

Cancel

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

TCP Stream Configuration

Global Settings

Packet Type Performance Boost

Targets

Hosts (Single IP address or CIDR block)

Policy

Timeout seconds

Maximum TCP Window bytes (0 to disable)

Overlap Limit overlapping segments (maximum of 255 segments, 0 for unlimited)

Flush Factor (Effective only if Normalize TCP is enabled, 0 to disable)

Stateful Inspection Anomalies

TCP Session Hijacking

Consecutive Small Segments

Small Segment Size bytes

Ports Ignoring Small Segments

Require TCP 3-Way Handshake

3-Way Handshake Timeout seconds (0 means unlimited timeout)

Packet Size Performance Boost

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.

Access Control > Access Control

Network Discovery Application Detectors Correlation Actions

Object Management Intrusion Network Analysis Policy DNS Import/Export

Access Control

Intrusion

Malware & File

New Policy

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

Rules Security Intelligence HTTP Responses Advanced

Regular Expression - Recursion Limit Default

Intrusion Event Logging Limits - Max Events Stored Per Packet 8

Latency-Based Performance Settings

Packet Handling Disabled

Rule Handling Disabled

Default Network Analysis Policy test

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

تحذير: من المتوقع أن تؤدي زيادة المهلة إلى زيادة استخدام الذاكرة، ويتعين على FirePOWER تعقب التدفقات التي لا يتم إغلاقها بواسطة نقاط النهاية لفترة أطول. تختلف الزيادة الفعلية في استخدام 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 تبقى 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](#)

ةمچرتل هذه لوج

ةللأل تاينقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاءنأ عيچ ي ف ني مدخت سمل معد يوتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصفأ نأ ةظحال م يچري. ةصاخل مه تلغ بل
Cisco ي لخت. فرتحم مچرت م اهم دقي ي تلل ةي فارتحال ةمچرتل عم لالحل وه
ىل إأمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقदन ع اهتيل وئسس م
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل