قم بتمكين المعالج المسبق للتطبيع المضمن وفهم الفحص المسبق للطرح واللاحق للطرح

المحتويات

المقدمة

يوضح هذا المستند كيفية تمكين المعالج المسبق للتطبيع داخل الشركة ويساعدك على فهم أخطاء وتأثير خياري متقدمين للتطبيع داخل الشركة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بنظام Cisco Firepower والنسخ.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى مركز إدارة FireSIGHT من Cisco وأجهزة FirePOWER.

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 مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

يعمل التطبيع المضمن على تطبيع حركة مرور البيانات لتقليل فرصة أن المهاجم يمكن أن يتهرب من الكشف باستخدام عمليات النشر المضمن. تحدث التطبيع مباشرة بعد فك تشفير الحزمة وقبل أي معالجات مسبقة أخرى، ويبدأ من الطبقات الداخلية للحزمة إلى

الخارج. ال توقوم التطبيع المضمن بإنشاء أحداث، ولكنها توقوم بإعداد الحزم للاستخدام من قبل معالجات سابقة أخرى.

عند تطبيق سياسة إقتحام مع تمكين معالج التسوية المسبق المضمن، يقوم جهاز FirePOWER بإختبار هذين الشرطين لضمان إستخدامك لعملية نشر مضمنة:

- بالنسبة للإصدارات 5.4 والإصدارات الأحدث، يتم تمكين *الوضع المضمن* في نهج تحليل الشبكة (NAP)، كما يتم تكوين *ميزة طاقس إلى طاقس* عند تكوين *المدخل* أيضا في نهج التسلل إذا تم تعيين سياسة الإقتحام على إسقاط حركة المرور. بالنسبة للإصدارات 5.3 والإصدارات الأقدم، يتم تمكين خيار *الوكيل عند طاقس إلى طاقس* داخل *السطر* في نهج التسلل.

- يتم تطبيق النهج على مجموعة واجهة مضمنة (أو مضمنة مع فشل مفتوح).

لذلك، بالإضافة إلى تمكين المعالج المسبق للتطبيع الداخلي وتكوينه، يجب عليك أيضا التأكد من تلبية هذه المتطلبات، أو أن المعالج المسبق لن يقوم بتطبيع حركة المرور:

- يجب تعيين النهج الخاص بك إلى طاقس حركة مرور البيانات في عمليات النشر المضمنة.

- يجب تطبيق النهج الخاص بك على مجموعة أسطر مضمنة.

تمكين التطبيع المضمن

يوضح هذا القسم كيفية تمكين التطبيع الداخلي للإصدارات 5.4 والإصدارات الأحدث، وكذلك للإصدارات 5.3 والإصدارات الأقدم.

تمكين التطبيع الداخلي في الإصدارات 5.4 والإصدارات الأحدث

يتم تكوين معظم إعدادات المعالج المسبق في NAP للإصدارات 5.4 والإصدارات الأحدث. أكمل الخطوات التالية لتمكين التطبيع الداخلي في NAP:

1. قم بتسجيل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT.

2. انتقل إلى **السياسات > التحكم في الوصول**.

3. انقر فوق **نهج تحليل الشبكة** بالقرب من المنطقة العليا اليمنى من الصفحة.

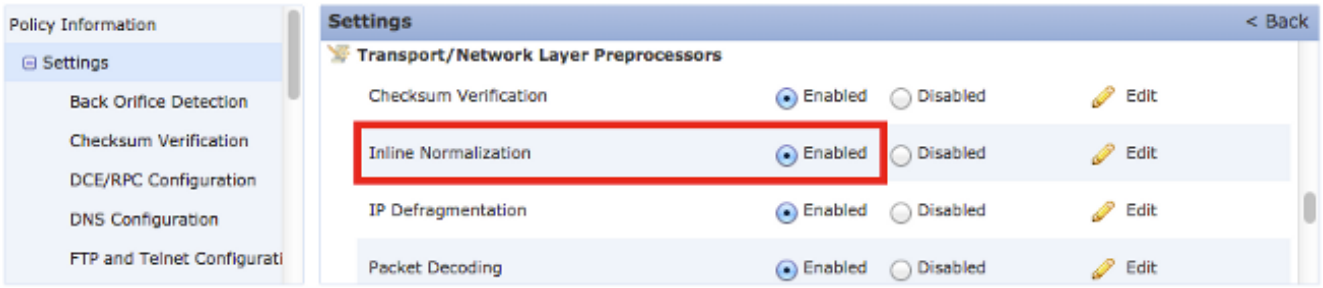
4. حدد *نهج تحليل الشبكة* الذي ترغب في تطبيقه على الجهاز الذي تتم إدارته.

5. انقر فوق أيقونة *القلم الرصاص* لبدء التحرير، وتظهر صفحة *تحرير النهج*.

6. انقر فوق **الإعدادات** الموجودة على الجانب الأيسر من الشاشة، وتظهر الصفحة *إعدادات*.

7. حدد موقع خيار **التطبيع المضمن** في منطقة *معالج الشبكة المسبق/طبقة النقل*.

8. حدد زر **تمكين** الخيار لتمكين هذه الميزة:



يجب إضافة NAP مع عملية التطبيع المضمنة إلى سياسة التحكم بالوصول حتى يتم إجراء عملية التطبيع داخل السطر. يمكن إضافة NAP من خلال علامة التبويب *خيارات متقدمة* لسياسة التحكم بالوصول:

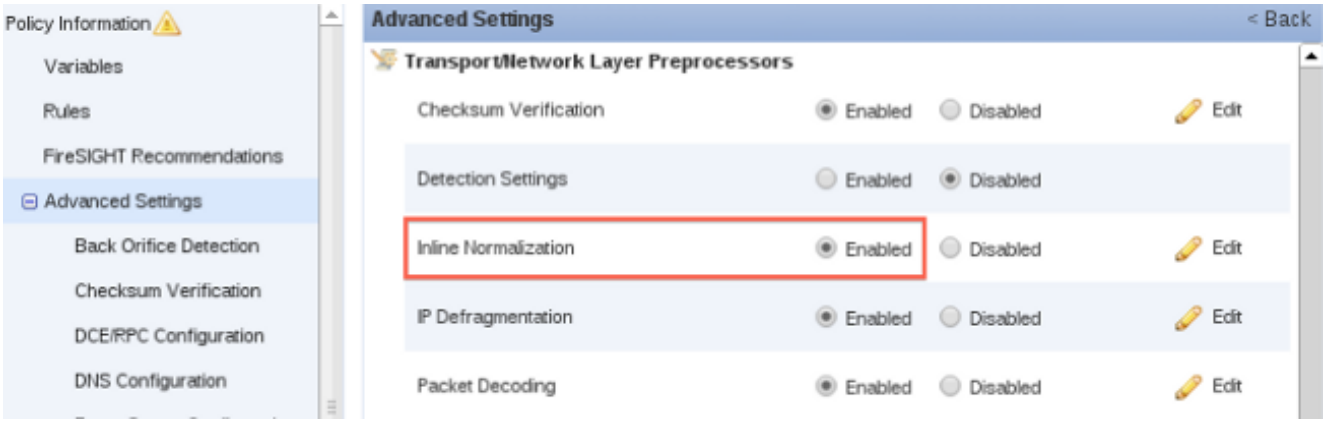
ويجب بعد ذلك تطبيق نهج التحكم في الوصول على جهاز التفتيش.

> **ملاحظة**: بالنسبة للإصدار 5.4 أو إصدار أحدث، يمكنك تمكين التطبيع الداخلي لحركة مرور معينة وتعطيلها لحركة مرور أخرى. إذا كنت ترغب في تمكينها لحركة مرور معينة، فقم بإضافة *قاعدة تحليل شبكة* وتعيين معايير حركة المرور وسياستها على تلك التي تم تمكين تسوية مضمنة لها. إذا كنت تريد تمكينها بشكل عام، فعليك تعيين نهج *تحليل الشبكة الافتراضي* على النهج الذي تم تمكين التسوية داخل السطر به.

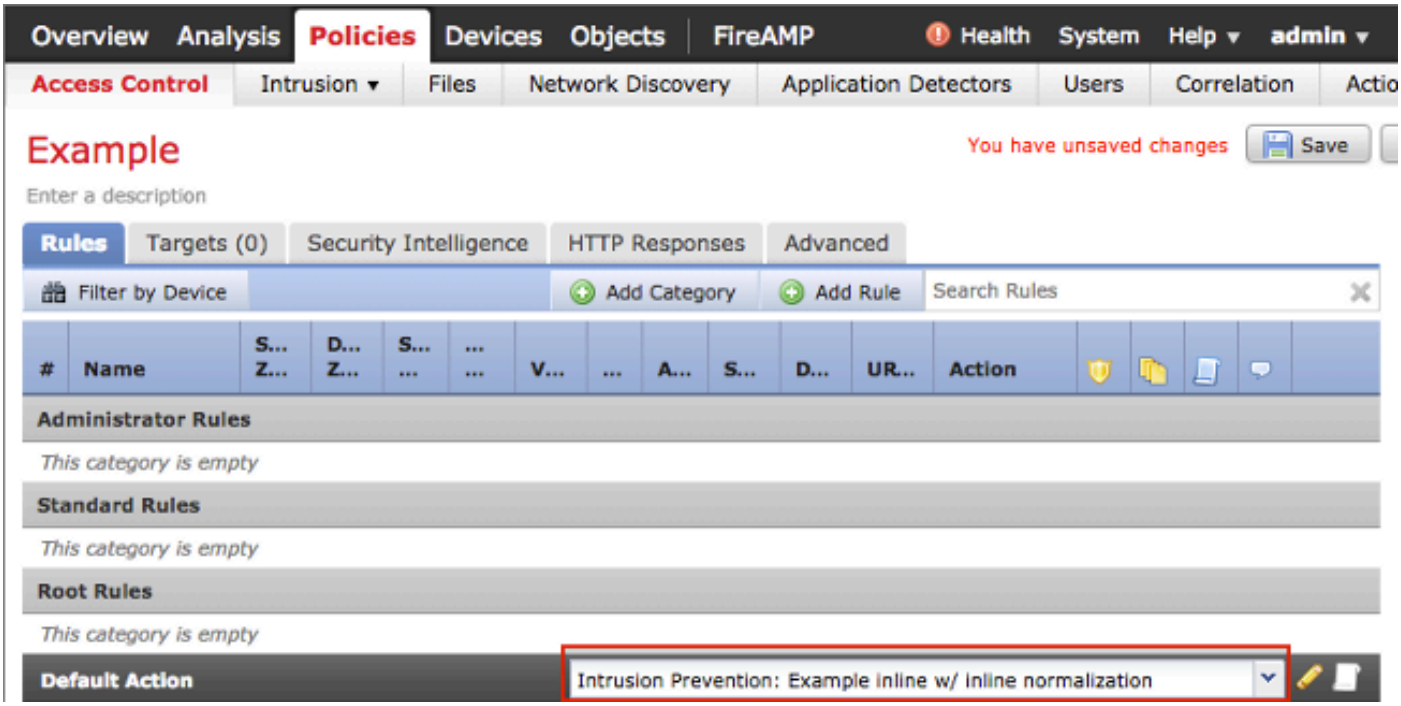
تمكين التطبيع المضمن في الإصدارات 5.3 والإصدارات الأقدم

أكمل هذه الخطوات لتمكين التطبيع الداخلي في سياسة الاقتحام:

1. قم بتسجيل الدخول إلى واجهة مستخدم الويب الخاصة بمركز إدارة FireSIGHT.
2. انتقل إلى **السياسات > الاقتحام > سياسات الاقتحام**.
3. حدد *سياسة اقتحام* تريد تطبيقها على الجهاز المدار.
4. انقر فوق أيقونة *القلم الرصاص* لبدء التحرير، وتظهر صفحة *تحرير النهج*.
5. انقر على **إعدادات متقدمة**، **وتظهر** صفحة ***الإعدادات المتقدمة***.
6. حدد موقع خيار **التطبيع المضمن** في منطقة معالج *النقل/طبقة الشبكة المسبق*.
7. حدد زر **تمكين** الخيار لتمكين هذه الميزة:



بمجرد تكوين سياسة الاقتحام للتطبيع داخل السطر، يجب إضافتها كإجراء افتراضي في سياسة التحكم بالوصول:



ويجب بعد ذلك تطبيق نهج التحكم في الوصول على جهاز التفتيش.

يمكنك تكوين معالج التسوية المسبق المضمن من أجل تطبيع حركة مرور IPv4 و IPv6 في أي مجموعة. يحدث Internet Control Message Protocol الإصدار 4 (ICMPv4) و ICMPv6 و TCP تطبيع كل بروتوكول تلقائيا عند تمكين تطبيع ذلك البروتوكول.

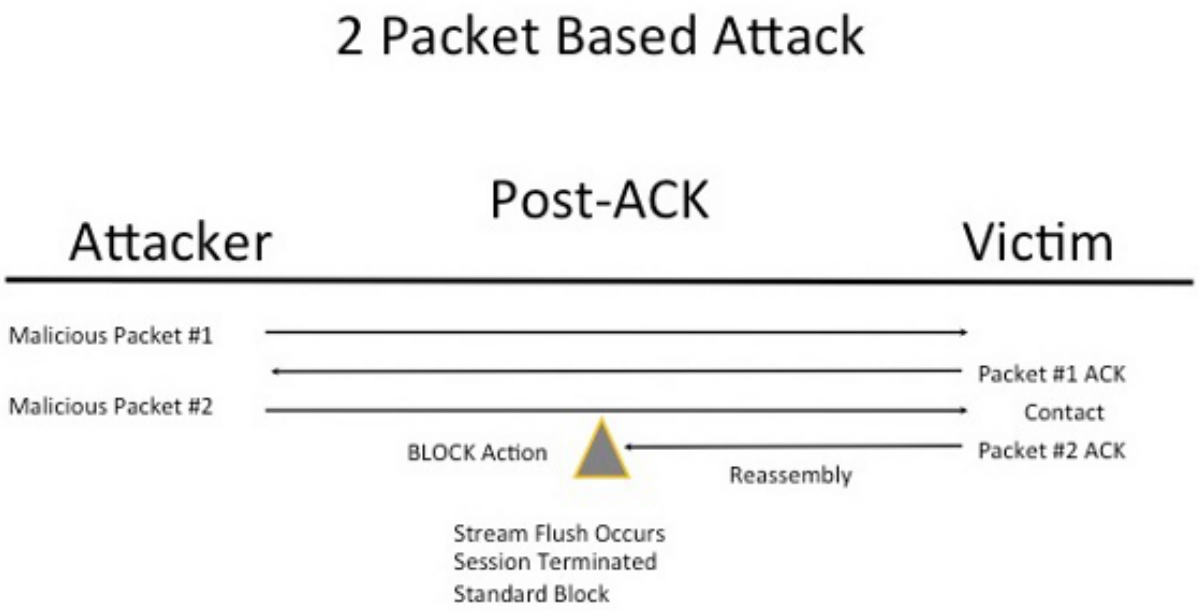
تمكين الفحص بعد طرح المنتجات والفحص قبل طرح المنتجات

بعد تمكين المعالج الأولي للتطبيع الداخلي، يمكنك تحرير الإعدادات لتمكين خيار *تطبيع حمولة TCP*. هذا خيار في السطر تطبيع سابق المعالج بين إثنان أسلوب مختلف من التفتيش:

- الإقرار بالبريد (بعد ACK)
- إقرار مسبق (قبل ACK)

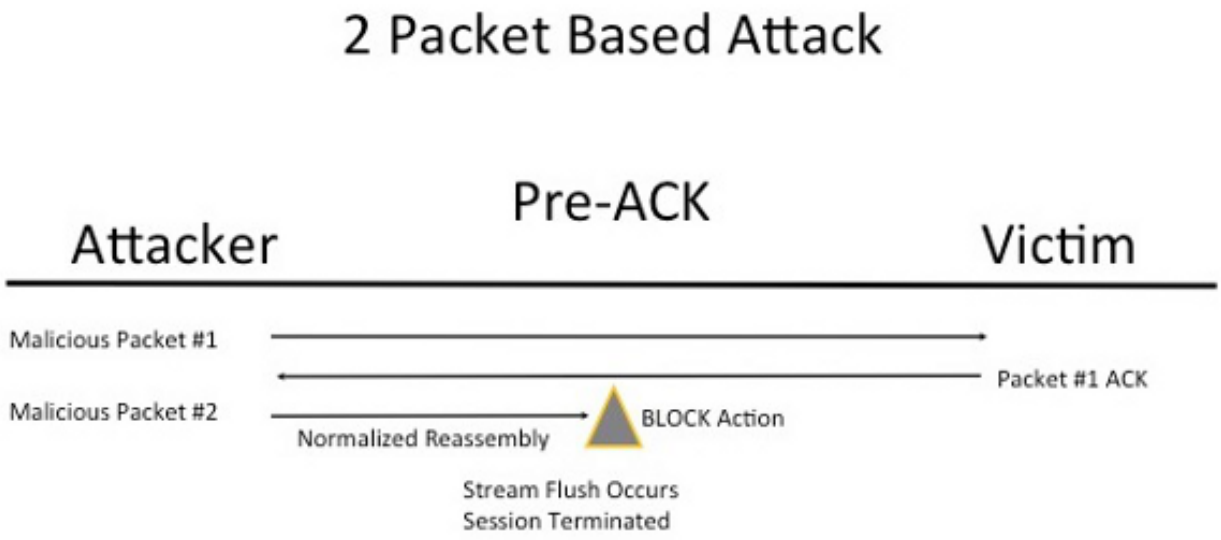
فهم فحص ما بعد التصرف (تطبيع TCP/تطبيع حمولة TCP معطلة)

أثناء الفحص التالي للحزمة، يتم إعادة تجميع تدفق الحزمة، والتفريغ (وضع اليد في الجزء المتبقي من عملية التفتيش)، والكشف في حالة التطفل بعد تلقي إخطار (ACK) من الضحية للحزمة التي تكمل الهجوم بواسطة نظام منع التسلل (IPS). قبل حدوث تدفق التدفق، وصلت الحزمة المسيئة بالفعل إلى الضحية. لذلك، يحدث التنبيه/الإسقاط بعد أن تصل الحزمة المسيئة إلى الضحية. يحدث هذا الإجراء عندما يصل ACK من الضحية للحزمة المسيئة إلى IPS.



فهم الفحص المسبق للحمولة (تهيئة TCP/تطبيع حمولة TCP الممكنة)

تقوم هذه الميزة بتطبيع حركة المرور مباشرة بعد فك تشفير الحزمة وقبل معالجة أي وظيفة snort أخرى لتقليل جهود التهرب من بروتوكول TCP. وهذا يضمن أن الحزم التي تصل إلى التبديل داخل الشاشة هي نفسها تلك التي يتم تمريرها إلى الضحية. يقوم الشيخ بإسقاط حركة المرور على الحزمة التي تكمل الهجوم قبل أن يصل الهجوم إلى ضحيته.



عندما تقوم بتمكين *تطبيع TCP*، يتم إسقاط حركة المرور التي تطابق هذه الشروط أيضا:

- نسخ معاد إرسالها من الحزم التي تم إسقاطها مسبقا
- حركة المرور التي تحاول متابعة جلسة عمل تم إسقاطها مسبقا
- حركة المرور التي تطابق أي من قواعد معالج مسبق لتدفق TCP هذه:

  129:1129:3129:4129:6129:8129:11129:14 حتى 129:19

  ملاحظة: لتمكين التنبيهات الخاصة بقواعد تدفق TCP التي يتم إسقاطها بواسطة معالج التسوية المسبق، يجب تمكين ميزة *تشوهات الفحص* الذي *يشير إلى حالة* في تكوين تدفق TCP.

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).