التأكد من وظائف الكشف عن تهديدات ASA وتكوينها

المحتويات

المقدمة

يصف هذا المستند المكونات الرئيسية الثالثة لوظائف الكشف عن التهديدات وتكوينها.

المتطلبات الأساسية

المتطلبات

ال توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

ال يقتصر هذا المستند على إصدارات برامج ومكونات مادية معينة.

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

يصف هذا المستند الوظائف والتكوين الأساسي لميزة اكتشاف التهديدات من جهاز الأمان القابل للتكيف (ASA) من Cisco. يوفر اكتشاف التهديدات لمسؤولي جدار الحماية الأدوات الضرورية لتحديد الهجمات وفهمها وتوقفها قبل وصولها إلى البنية الأساسية للشبكة الداخلية. وللقيام بذلك، تعتمد هذه الميزة على عدد من العوامل المشغلة والإحصاءات المختلفة، التي يرد وصفها بمزيد من التفصيل في هذه الأقسام.

يمكن إستخدام اكتشاف التهديدات على أي جدار حماية ASA الذي يشغل إصدار برنامج من 8.0(2) وأ إصدار أحدث. على الرغم من أن اكتشاف التهديدات ليس بديلا عن حلول بطاقات الوقاية/نظام منع الاختراقات (IPS) المخصص، إلا أنه يمكن إستخدامه في البيئات التي ال توفر فيها نظام منع الاختراقات (IPS) لتوفير طبقة إضافية من الحماية للوظائف الأساسية لنظام منع الاختراقات (ASA).

وظيفة اكتشاف التهديدات

تتضمن ميزة الكشف عن التهديدات ثلاثة مكونات رئيسية:

1. اكتشاف التهديد الأساسي
2. الكشف المتقدم عن التهديدات
3. الكشف عن التهديد خلال الفحص

ويرد وصف مفصل لكل عنصر من هذه المكونات في هذه الأقسام.

الكشف عن التهديدات الأساسية (معدلات مستوى النظام)

يتم تمكين الكشف عن التهديدات الأساسية بشكل افتراضي على جميع وحدات ASA التي تشغل الإصدار 8.0(2) والإصدارات الأحدث.

يراقب الكشف عن التهديدات الأساسية المعدلات التي يتم بها إسقاط الحزم لأسباب مختلفة من قبل هيئة المعايير الإئتمانية كل. وهذا يعني أن الإحصاءات التي يتم جمعها عن طريق الكشف الأساسي عن التهديدات ال تنطبق إلا على الجهاز بأكمله وهي عموما غير دقيقة بما يكفي لتوفير معلومات عن مصدر التهديد أو طبيعته. وبدال من ذلك، قامت شاشات ASA بإسقاط الحزم لهذه الأحداث:

- إسقاط قائمة التحكم في الوصول (ACL-drop) - يتم رفض الحزم بواسطة قوائم الوصول.

- PKTS سيئ (سيئ-packet-drop) - تنسيقات حزم غير صحيحة، والتي تتضمن رؤوس L3 و L4 التي لا تتوافق مع معايير RFC.
- حد المخالفة (conn-limit-drop) - الحزم التي تتجاوز حد اتصال مكون أو شامل.
- هجوم رفض الخدمة (DoS) - هجمات رفض الخدمة (DoS).
- جدار الحماية (ميزة الإسقاط الأمامي) - عمليات التحقق الأساسية لأمان جدار الحماية.
- هجوم ICMP (ICMP-drop) - حزم ICMP المشبوهة.
- الفحص (الفحص والإفالت) - الرفض حسب فحص التطبيق.
- الواجهة (interface-drop) - الحزم التي تم إسقاطها بواسطة عمليات التحقق من الواجهة.
- المسح الضوئي (تهديد بالمسح الضوئي) - هجمات المسح الضوئي للشبكة/المضيف.
- هجوم SYN (syn-attack) - هجمات الجلسة غير المكتملة، والتي تتضمن هجمات TCP SYN وجلسات عمل UDP أحادي الإتجاه التي ليس لها بيانات إرجاع.

تتوفر كل من هذه الأحداث على مجموعة معينة من المشغلات التي يتم إستخدامها لتحديد التهديد. يتم ربط معظم المشغلات بأسباب معينة لإسقاط ASP، على الرغم من أنه يتم أيضا مراعاة بعض syslog وإجراءات الفحص. تتم مراقبة بعض المشغلات بواسطة فئات تهديد متعددة. يتم توضيح بعض المشغلات الأكثر شيوعا في هذا الجدول، على الرغم من أنها ليست قائمة شاملة:

تهديد أساسي	سبب (أسباب) المشغل (المشغل) / سبب (أسباب) إسقاط ASP
ACL-Drop	ACL-Drop
Bad-Packet-drop	غير صالح-tcp-hdr-length عنوان ip غير صالح inspection-dns-pak-too-long inspection-dns-id غير مطابق
conn-limit-drop	الحد الطوارئ
dos-drop	sp-security-failed
إسقاط-fw	inspection-icmp-seq-num غير متطابق inspection-dns-pak-too-long inspection-dns-id غير مطابق sp-security-failed ACL-Drop
ICMP-drop	inspection-icmp-seq-num غير متطابق
فحص الإسقاط	عمليات إسقاط الإطارات التي يتم تشغيلها بواسطة محرك فحص

interface-drop	sp-security-failed رورملا عونمم
حسامملا ديدهت يئوضلا	tcp-3whs-failed tcp-not-syn sp-security-failed ACL-Drop inspection-icmp-seq-num قباطتم ريغ inspection-dns-pak-too-long inspection-dns-id قباطم ريغ
يعاعش موجه	%ASA-6-302014 syslog عم ببس لطعتلا ل "ةلهم SYN"

هذه ثودح تالدعم سايقب ةيساسألا تاديدهتلا نع فشكلا موقي ،ثدح لكل ةبسنلاب لدعملا ةرتف طسوتم ةينمزلا ةرتفلا هذه ىمست .ةنوكم ةينمز ةرتف لالخ تاضافخنإلا ARI لخاد ثدحت يتلا ثادحألا ددع زواجت اذإ .اموي 30 ىلإ ةيناث 600 نم حوارتت نأ نكميو (ARI) ASA ربتعي ،هنيوكت مت يذلا لدعملا دودح هذه ثادحألا تاديدهت ادية.

امل ةبسنلاب نيوكتلل نيلباق نيدح ىلع ةيساسألا تاديدهتلا نع فشكلا لمتشي ةطاسبب وه طسوتملا لدعملا .عافدنالا لدعمو لدعملا طسوتم امه ،اديدهت ثادحألا ربتعي ARI يذلا مت هنيوكت. ىلع ل ةينمزلا ةرتفلا لالخ ةيناثلا يف طوقسلا تالاح ددع طسوتم يف مكحتلا ةمئاق طاقسإ تايلمعل طسوتملا لدعملا دح نيوكت مت اذإ ،لاثملا ليبس ASA موقي ،ةيناث 600 ةدمل ARI عم 400 ل لوصولا مت يتلا مزحلا ددع طسوتم باسحب اذه نأ نيبت اذإ .ةيناث 600 رخآ يف (ACLs) لوصولا يف مكحتلا مئاوق ةطساوب اهطاقسإ ASA موقي ،ةيناثلا يف 400 نم ربكأ مقرلا ليجستب ديدهت.

وعلى نحو مماثل، فإن معدل الاندفاع لثامم ةياغلل هنكلو رظني ىلإ تارتف رغصأ نم تانايب ليبس ىلع .ARI نم رغصأ امئاد BRI نإ .عافدنالا لدعمل ينمزلا لصافلا ىمست ،تاطقللا لوصولاب مكحتلا ةمئاق تاضافخنالا ARI لدعم لازي ال ،قباسلا لاثملا ىلع ءانب ،لاثملا ACL) 600 ةيناث، وهو معدل الاندفاع نآلا يغلبي 800. عم هذه ةميقلا، موقي ASA باسحب ثيح ،ةيناث 20 يف لوصولا يف مكحتلا مئاوق ةطساوب تطقس يتلا مزحلا ددع طسوتم ،ةيناثلا يف طاقسإ ةيلمع 800 ةبوسحملا ةميقلا هذه تزواجت اذإ .BRI يه ةيناث 20 نوكت ،اهمادختسإ متي يتلا ةبولطملا تانوكملا يلامجإ ديدحت لجأ نمو .تاديدهتلا دحأ ليجست متي ASA باسحب ةميق 1/30 نم ARI. كلذل، يف لاثملااقباس مدختسملا، 1/30 نم 600 يناث موقي ،ناوث 10 هرادقم BRI نم ىندأ دح ىلع تاديدهتلا نع فشكلا يوتحي ،كلذ عمو .ةيناث 20 وه مهملا نمو .BRI ك ناوث 10 مدختسي لازي ال ASA نإف ،10 نم لقأ ARI نم 1/30 ددع ناك اذإ كلذل تناك يتلاو ،(1)8.2 ل ةقباسلا تارادصإلا يف افلتخم ناك كولسلا اذه نأ ةظحالم اضيأ هسفن وه يناث 10 BRI ىندألا دحلا .1/30 مقر نم الدب ،ARI نم 1/60 اهرادقم ةميق مدختست لكل ةيجمرب ةغيص.

عند اكتشاف تهديد أساسي، موقع ASA بإنشاء syslog ٪ASA-4-733100 ببساطة لتنبيه المسؤول إلى أنه تم تحديد تهديد محتمل. يمكن رؤية متوسط عدد الأحداث الحالية والإجمالية لكل فئة تهديد باستخدام الأمر show threat-rate detection. العدد الإجمالي للأحداث التراكمية هو مجموع عدد الأحداث التي تم رؤيتها في آخر 30 نموذج BRI.

يتم حساب معدل الاندفاع في syslog استنادا إلى عدد الحزم التي سقطت حتى الآن في BRI الحالي. يتم إجراء الحساب بشكل دوري في BRI. بمجرد حدوث خرق، يتم رفع syslog. هو محدود أن يتم إنشاء قطف واحد syslog في BRI. يتم حساب معدل الاندفاع في "show threat-detection rate" استنادا إلى عدد الحزم التي تم إسقاطها في BRI الأخيرة. المتصميم للفرق هو أن syslog حساس الوقت لذلك إذا حدث خرق في BRI الحالي، فإنه سيكون لها فرصة أن يتم التقاطها. "إظهار معدل الكشف عن التهديدات" هو أقل حساسية للوقت، لذلك يتم إستخدام الرقم من آخر BRI.

لا يتخذ الكشف عن التهديد الأساسي أي إجراءات من أجل إيقاف حركة المرور المنحرفة أو منع الهجمات المستقبلية. وبهذا المعنى، فإن الكشف عن التهديدات الأساسية هو معلومات محضة ويمكن إستخدامه كآلية للرصد أو الإبلاغ.

الكشف المتقدم عن التهديدات (إحصائيات مستوى الكائن و Top N)

على عكس الكشف الأساسي عن التهديدات، يمكن إستخدام "الكشف المتقدم عن التهديدات" لتعقب الإحصائيات الخاصة بالكائنات الأكثر دقة. يدعم ASA إحصائيات التعقب للمضيفين IPs والمنافذ والبروتوكولات وقوائم التحكم في الوصول (ACL) والخوادم المحمية بواسطة اعتراض TCP. يتم تمكين الكشف المتقدم عن التهديدات فقط بشكل افتراضي لإحصائيات قائمة التحكم في الوصول (ACL).

بالنسبة لكائنات المضيف والمنافذ والبروتوكول، يتتبع "اكتشاف التهديدات" عدد الحزم ووحدات البايت وعمليات الإسقاط التي تم إرسالها واستقبالها بواسطة هذا الكائن في غضون فترة زمنية محددة. بالنسبة لقوائم التحكم في الوصول (ACL)، يقوم موقع الكشف عن التهديدات بتتبع أفضل 10 وحدات ACE (السماح والرفض) التي تم الوصول إليها بشكل أكبر خلال فترة زمنية محددة.

وتتراوح الفترات الزمنية التي يتم تتبعها في جميع هذه الحالات بين 20 دقيقة وساعة واحدة و 8 ساعات و 24 ساعة. وعلى الرغم من أن الفترات الزمنية نفسها غير قابلة للتكوين، إلا أنه يمكن تعديل عدد الفترات التي يتم تعقبها لكل كائن باستخدام الكلمة الأساسية 'number-rate'. على سبيل المثال، إذا تم تعيين "عدد المعدل" على 2، ستري كافة الإحصائيات لمدة 20 دقيقة وساعة واحدة و 8 ساعات. إذا تم تعيين "عدد المعدل" على 1، سترى كافة الإحصائيات لمدة 20 دقيقة وساعة واحدة. ومهما يكن، فإن معدل ال 20 دقيقة يظهر دائما.

عند تمكين اعتراض TCP، يمكن أن يحتفظ "اكتشاف التهديدات" بتعقب الخوادم العشرة العليا التي تعتبر تحت الهجوم ومحمية بواسطة اعتراض TCP. تعد إحصائيات اعتراض TCP مماثلة لاكتشاف التهديد الأساسي بمعنى أن يمكن للمستخدم تكوين معدل-فاصل زمني ومقاييس معدل الاندفاع. لا توفر إحصائيات الكشف المتقدم عن التهديدات (BRI) والتدفق (ARI) المحدد المتوسط معدل الاعتراض TCP إلا في ASA 8.0(4) والإصدارات الأحدث.

يتم عرض إحصائيات اكتشاف التهديدات المتقدمة عبر إظهار إحصائيات اكتشاف التهديدات وإظهار الأوامر العليا لإحصائيات اكتشاف التهديدات. هذه أيضا هي الميزة المسؤولة عن تعبئة الرسوم البيانية "top" على لوحة معلومات جدار الحماية ل ASDM. Syslog الوحيدة

التي تم إنشاؤها بواسطة "الكشف المتقدم عن التهديدات" هي ٪ASA-4-733104 و٪ASA-4-733105، والتي يتم تشغيلها عند تجاوز متوسط معدلات الاندفاع (على التوالي) لإحصائيات اعتراض TCP.

على غرار الكشف عن التهديدات الأساسية، فإن الكشف المتقدم عن التهديدات هو عبارة عن معلومات محضة. لا يتم إتخاذ أي إجراءات لحظر حركة المرور استنادا إلى إحصائيات الكشف المتقدم عن التهديدات.

الكشف عن التهديد خلال الفحص

يتم إستخدام ميزة الكشف عن التهديدات بالمسح الضوئي لتعقب المهاجمين المشتبه فيهم الذين ينشئون إتصالات بمضيفين كثيرين جدا في شبكة فرعية، أو العديد من المنافذ على شبكة فرعية/مضيف. يتم تعطيل الكشف عن التهديدات عند المسح بشكل افتراضي.

يعتمد الفحص الدقيق واكتشاف التهديدات على مفهوم الكشف الأساسي عن التهديدات، والذي يحدد مسبقا فئة التهديد لهجوم الفحص. لذلك، يتم مشاركة إعدادات rate-interval، average rate (ARI)، و burst rate (BRI) بين الكشف عن التهديدات الأساسية والمسح الضوئي. أن إلى طقف "تاديدهتلا نع يساسألا فشكلا" ريشي امنيب هنأ وه 2 تازيمملا نيب قرفلا متوسط أو حد معدل الاندفاع قد تم تجاوزه، يحتفظ "الكشف عن تهديدات المسح الضوئي" بقاعدة بيانات لعناوين IP للمهاجم والهدف التي يمكن أن تساعد في توفير مزيد من السياق حول البيئات المضيفة المشاركة في المسح الضوئي. بالإضافة إلى ذلك، يتم إعتبار حركة المرور التي يتم استقبالها بالفعل من قبل المضيف/الشبكة الفرعية الهدف فقط من خلال مسح الكشف عن التهديدات. لا يزال من الممكن أن يؤدي الكشف عن التهديد الأساسي إلى تشغيل تهديد المسح الضوئي حتى إذا تم إسقاط حركة المرور بواسطة قائمة التحكم في الوصول (ACL).

يمكن أن يتفاعل مسح التهديد بشكل إختياري مع هجوم بتجنب IP للمهاجم. وهذا يجعل من الكشف عن تهديدات الفحص المجموعة الفرعية الوحيدة من ميزة اكتشاف التهديدات التي يمكن أن تؤثر بشكل فعال على الاتصالات من خلال ASA.

عند اكتشاف اكتشاف التهديدات للمسح الضوئي لهجوم، تم تسجيل دخول ٪ASA-4-733101 إلى عناوين IP الخاصة بالمهاجم و/أو الهدف. إذا تم تكوين الميزة لتجنب المهاجم، يتم تسجيل دخول ٪ASA-4-733102 عند قيام الكشف عن التهديدات بالمسح الضوئي بإنشاء تجنب. ٪ASA-4-733103 مسجل عند إزالة علامة التجنب. يمكن إستخدام الأمر show threat-detection scan-threat لعرض قاعدة بيانات تهديدات الفحص بالكامل.

القيود

- لا يتوفر اكتشاف التهديدات إلا في ASA 8.0(2) والإصدارات الأحدث. لا يساند هو على ال ASA 1000V منصة.
- يتم دعم الكشف عن التهديدات في طقف يف وضع سياق واحد.
- يتم اكتشاف تهديدات العبوة فقط. لا يتم إعتبار حركة المرور التي يتم إرسالها إلى ASA نفسها بواسطة اكتشاف التهديد.
- لا يتم حساب الاتصالات الواحدة باستخدام TCP التي يتم إعادة تعيينها بواسطة الخادم المستهدف كتهديد بموجه SYN أو المسح الضوئي.

التكوين

اكتشاف التهديد الأساسي

يتم تمكين الكشف عن التهديد الأساسي باستخدام الأمر الأساسي الخاص باكتشاف التهديد".

<#root>

ciscoasa(config)#

threat-detection basic-threat

يمكن عرض المعدلات الافتراضية باستخدام الأمر show run all threat-detection.

<#root>

ciscoasa(config)#

show run all threat-detection

```
threat-detection rate dos-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate dos-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate bad-packet-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate bad-packet-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate acl-drop rate-interval 600 average-rate 400 burst-rate 800
threat-detection rate acl-drop rate-interval 3600 average-rate 320 burst-rate 640
threat-detection rate conn-limit-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate conn-limit-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate icmp-drop rate-interval 600 average-rate 100 burst-rate 400
threat-detection rate icmp-drop rate-interval 3600 average-rate 80 burst-rate 320
threat-detection rate scanning-threat rate-interval 600 average-rate 5 burst-rate 10
threat-detection rate scanning-threat rate-interval 3600 average-rate 4 burst-rate 8
threat-detection rate syn-attack rate-interval 600 average-rate 100 burst-rate 200
threat-detection rate syn-attack rate-interval 3600 average-rate 80 burst-rate 160
threat-detection rate fw-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate fw-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate inspect-drop rate-interval 600 average-rate 400 burst-rate 1600
threat-detection rate inspect-drop rate-interval 3600 average-rate 320 burst-rate 1280
threat-detection rate interface-drop rate-interval 600 average-rate 2000 burst-rate 8000
threat-detection rate interface-drop rate-interval 3600 average-rate 1600 burst-rate 6400
```

ومن أجل ضبط هذه المعدلات باستخدام قيم مخصصة، قم بإعادة تكوين أمر معدل، اكتشاف التهديدات لفئة التهديد المناسبة.

<#root>

ciscoasa(config)#

threat-detection rate acl-drop rate-interval 1200 average-rate 250 burst-rate 550

يمكن أن يكون لكل فئة تهديد 3 معدلات مختلفة كحد أقصى محددة (مع معرفات المعدل 1، المعدل 2، والمعيار 3). تتم الإشارة إلى معرف المعدل الخاص الذي تم تجاوزه في syslog ٪ASA-4-733100.

في المثال السابق، يخلق اكتشاف التهديدات syslog 733100 فقط عندما يتجاوز دد حالات وأ ثانية 1200 لخلال الثانية/إسقاط عملية 250 (ACL) لوصول في التحكم قائمة انخفاض ثانية. 40 لخلال الثانية/إسقاط عملية 550

الكشف المتقدم عن التهديدات

أستخدم الأمر إحصائيات اكتشاف التهديدات لتمكين الكشف المتقدم عن التهديدات. إذا لم يتم توفير كلمة أساسية خاصة بميزة، فسيقوم الأمر بتمكين التعقب لجميع الإحصائيات.

<#root>

ciscoasa(config)#

threat-detection statistics ?

```
configure mode commands/options:
 access-list      Keyword to specify access-list statistics
 host            Keyword to specify IP statistics
 port            Keyword to specify port statistics
 protocol       Keyword to specify protocol statistics
 tcp-intercept   Trace tcp intercept statistics
 <cr>
```

لتكوين دد فواصل لمعدل التي يتم تتبعها لإحصائيات المضيف وأ المنفذ وأ لبروتوكول وأ قائمة التحكم في الوصول (ACL)، أستخدم الكلمة الأساسية number of rate.

<#root>

ciscoasa(config)#

threat-detection statistics host number-of-rate 2

تقوم الكلمة الأساسية دد المعدل بتكوين "اكتشاف التهديدات" لتعقب دد n الأقصر فقط من الفواصل.

لتمكين إحصائيات اعتراض TCP، أستخدم الأمر إحصائيات اكتشاف التهديد tcp-intercept.

<#root>

ciscoasa(config)#

```
threat-detection statistics tcp-intercept
```

لتكوين المعدلات المخصصة لإحصائيات اعتراض TCP، أستخدم الكلمات الأساسية rate-interval، وaverage-rate، وburst-rate.

```
<#root>

ciscoasa(config)#

threat-detection statistics tcp-intercept rate-interval 45 burst-rate 400 average-rate 100
```

الكشف عن التهديد خلال الفحص

لتمكين الكشف عن تهديدات الفحص، أستخدم الأمر الكشف عن التهديدات بالفحص الضوئي.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat
```

من أجل ضبط المعدلات لتهديد الفحص، أستخدم نفس الأمر لمعدل اكتشاف التهديد المستخدم من قبل الكشف الأساسي عن التهديد.

```
<#root>

ciscoasa(config)#

threat-detection rate scanning-threat rate-interval 1200 average-rate 250 burst-rate 550
```

للسماح بأن يتجنب ASA مهاجم مسح ضوئي IP، قم بإضافة الكلمة الأساسية shun إلى الأمر invalider-detection scan-threat.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun
```

وهذا يسمح بالكشف عن التهديدات بالمسح الضوئي لإنشاء تجنب لمدة ساعة واحدة للمهاجم. من أجل ضبط مدة الإيقاف، أستخدم الأمر Scan-Threat الخاص بالكشف عن التهديد

باملاسح الضوئي.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun duration 1000
```

في بعض الحالات، يمكنك منع ASA من تجنب عناوين IP معينة. للقيام بذلك، قم بإنشاء إستثناء باستخدام الأمر ماسح تهديد الكشف عن التهديد الضوئي باستثناء الأمر.

```
<#root>

ciscoasa(config)#

threat-detection scanning-threat shun except ip-address 10.1.1.1 255.255.255.255

ciscoasa(config)#

threat-detection scanning-threat shun except object-group no-shun
```

الأداء

الكشف عن التهديدات الأساسية له تأثير قليل جدا على أداء نظام ASA. تعتبر عمليات الكشف المتقدم عن التهديدات التي يتم فحصها أكثر استهلاكا للموارد لأنها مضطرون لمتابعة إحصائيات مختلفة في الذاكرة. يمكن قطع ال "الكشف عن تهديدات الفحص" لتمكين وظيفة قطع الاتصال التأثير بفعالية على حركة المرور التي كان سيتم السماح بها أو الذ لك.

مع تطور إصدارات برنامج ASA، تم تحسين إستخدام الذاكرة لاكتشاف التهديدات بشكل ملحوظ. ومع ذلك، يجب توخي الحذر لمراقبة إستخدام ذاكرة ASA قبل تمكين اكتشاف التهديد وبعد ذلك. في بعض الحالات، يكون من الأفضل قطع تمكين بعض الإحصاءات (على سبيل المثال، الإحصاءات المضيفة) وقوائم بين وقت لآخر باستكشاف مشكلة معينة وإصلاحها بنشاط.

للحصول على عرض أكثر تفصيلا لاستخدام ذاكرة اكتشاف التهديدات، قم بتشغيل الأمر show memory app-cache threat-detection [detail].

الإجراءات الموصى بها

توفر هذه الأقسام بعض التوصيات العامة بشأن الإجراءات التي يمكن إتخاذها عند وقوع أحداث مختلفة متعلقة بالكشف عن التهديدات.

عند تجاوز معدل إسقاط أساسي وإنشاء ASA-4-733100٪

حدد فئة التهديد المحددة المشار إليها في ٪ASA-4-733100 syslog وربط هذا بمخرجات show threat-detection rate . مع هذه المعلومات، تحقق من مخرجات show asp drop لتحديد أسباب إسقاط حركة المرور.

للحصول على عرض أكثر تفصيلا لحركة المرور التي يتم إسقاطها لسبب محدد، استخدم ASP إسقاط التقاط لعرض جميع الحزم التي يتم إسقاطها. على سبيل المثال، إذا تم تسجيل تهديدات إسقاط قائمة التحكم في الوصول، قم بالتقاط إسقاط ASP الخاص ب acl-drop :

<#root>

```
ciscoasa#
```

capture drop type asp-drop acl-drop

```
ciscoasa#
```

show capture drop

```
1 packet captured

   1: 18:03:00.205189 10.10.10.10.60670 > 192.168.1.100.53:  udp 34 Drop-reason:
 (acl-drop) Flow is denied by configured rule
```

يوضح هذا الالتقاط أن الحزمة التي تم إسقاطها هي حزمة UDP/53 من 10.10.10.10 إلى 192.168.1.100.

إذا أبلغ ٪ASA-4-733100 عن وجود تهديد بالمسح الضوئي، فقد يكون من المفيد أيضا تمكين تتبع الاحتفاظ بـ ASA لمسح مؤقتًا. وهذا يسمح للكشف عن تهديدات المسح الضوئي بالمصدر والجهة المشاركة في الهجوم.

من المهم تذكر أن "الكشف الأساسي عن التهديدات" يقوم في الغالب بمراقبة حركة مرور البيانات التي تم إسقاطها بالفعل من قبل مسار الأمان المعجل (ASP)، فإنه لا يلزم اتخاذ أي إجراء مباشر لاحتواء التهديد المحتمل. والاستثناء من هذا هو هجمات SYN وتهديدات المسح الضوئي، والتي تتضمن حركة مرور تمر عبر الـ ASA.

إذا كانت عمليات الإسقاط التي تم رؤيتها في التقاط إسقاط ASP مشروعة و/أو متوقعة لبيئة الشبكة، فعليك ضبط الفواصل الأساسية للمعدل إلى قيمة أكثر ملاءمة.

إذا أظهرت عمليات الإسقاط حركة مرور غير مشروعة، فيجب اتخاذ إجراءات لحظر حركة المرور أو تقييدها قبل وصولها إلى ASA. ويمكن أن يتضمن ذلك قوائم التحكم في الوصول (ACL) وجودة الخدمة (QoS) على أجهزة البث.

بالنسبة لهجمات SYN، يمكن حظر حركة المرور في قائمة التحكم في الوصول (ACL) على ASA. كما يمكن تكوين اعتراض TCP للحماية الخاصة (المخادع) المستهدف، ولكن قد يؤدي ذلك ببساطة إلى تهديد حد المخطور الذي تم تسجيله بدلا من ذلك.

بالنسبة لتهديدات الفحص، يمكن أيضا منع حركة المرور في قائمة التحكم في الوصول (ACL) على ASA. الكشف عن التهديد باستخدام shunيمكن تمكين الخيار للسماح ل ASA بحظر جميع الحزم من المهاجم لكشف استباقي لفترة زمنية محددة.

عند الكشف عن تهديد الفحص وتسجيل دخول ٪ASA-4-733101

٪ASA-4-733101 يجب أن يسرد إما المضيف/الشبكة الفرعية الهدف أو عنوان IP للمهاجم. تحقق من ناتج show threat-detection scanning-threat للحصول على القائمة الكاملة للأهداف والمهاجمين،.

يمكن أن تساعد عمليات التقاط الحزم على واجهات ASAs التي تواجه المهاجم و/أو الهدف (الأهداف) أيضا في توضيح طبيعة الهجوم.

إذا كان الفحص الذي تم اكتشافه غير متوقع، فيجب اتخاذ إجراءات لحظر حركة المرور أو تقييدها للحد من الوصول إليها قبل الوصول إلى ASA. ويمكن أن يتضمن ذلك قوائم التحكم في الوصول (ACL) وجودة الخدمة (QoS) على أجهزة البث. عندما تتم إضافة الخيار shunإلى تكوين الكشف عن التهديدات، يمكن أن يسمح ASA بإسقاط جميع الحزم من IP للمهاجم لكشف استباقي لفترة زمنية محددة. كحل أخير، يمكن أيضا حظر حركة المرور يدويا على ASA عبر سياسة قائمة التحكم في الوصول (ACL) أو اعتراض TCP.

إذا كان الفحص الذي تم الكشف عنه إيجابيا خاطئا، فقم بضبط الفواصل الزمنية لمعدل تهديد المسح الضوئي على قيمة أكثر ملاءمة لبيئة الشبكة.

عند تجنب المهاجم وتسجيل ٪ASA-4-733102

٪ASA-4-733102 يسرد عنوان IP للمهاجم الذي تم تجنبه. استخدم show threat-detection shun الأمر لعرض قائمة كاملة بالمهاجمين الذين تم تجنبهم بواسطة اكتشاف التهديد لكشف محدد.
استخدم show shun الأمر in order to لك من القائمة الكاملة القائمة الكاملة IPs أن يكون لكشف نشط أطلب ب ASA (هذا يتضمن من مصدر غير كشف التهديد).

وإذا كانت هذه الغفلة جزءا من هجوم مشروع، فلا حاجة إلى اتخاذ أي إجراء آخر. ومع ذلك، سيكون من المفيد منع حركة مرور المهاجم يدويا بعيدا نحو المنبع قدر الإمكان. ويمكن القيام بذلك عبر قوائم التحكم في الوصول (ACL) وجودة الخدمة (QoS). وهذا يضمن أن الأجهزة الوسيطة ال تحتاج إلى هدر الموارد على حركة المرور غير الشرعية.

إذا كان تهديد المسح الضوئي الذي تسبب في تجنب الخطأ إيجابيا لكشف خاطئ، فقم بإزالة العلة يدويا باستخدام clear threat-detection shun [IP_address] erasecat4000_flash:.

عند تسجيل ٪ASA-4-733104 و/أو ٪ASA-4-733105

٪ASA-4-733104 و٪ASA-4-733105 يسرد المضيف المستهدف بالهجوم المحمي حاليا بواسطة اعتراض TCP. لمزيد من التفاصيل حول معدلات الهجمات والخوادم المحمية، راجع مخرجات show threat-detection statistics top tcp-intercept .

```
<#root>

ciscoasa#
```

```
show threat-detection statistics top tcp-intercept


Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs
----------------------------------------------------------------------------------
1    192.168.1.2:5000 inside 1249 9503 2249245  Last: 10.0.0.3 (0 secs ago)
2    192.168.1.3:5000 inside 10 10 6080 10.0.0.200 (0 secs ago)
3    192.168.1.4:5000 inside 2 6 560 10.0.0.200 (59 secs ago)
4    192.168.1.5:5000 inside 1 5 560 10.0.0.200 (59 secs ago)
5    192.168.1.6:5000 inside 1 4 560 10.0.0.200 (59 secs ago)
6    192.168.1.7:5000 inside 0 3 560 10.0.0.200 (59 secs ago)
7    192.168.1.8:5000 inside 0 2 560 10.0.0.200 (59 secs ago)
8    192.168.1.9:5000 inside 0 1 560 10.0.0.200 (59 secs ago)
9    192.168.1.10:5000 inside 0 0 550 10.0.0.200 (2 mins ago)
10   192.168.1.11:5000 inside 0 0 550 10.0.0.200 (5 mins ago)
```

عندما يكتشف "الكشف المتقدم عن التهديدات" هجوما من هذا النوع، فإن ASA يقوم بالفعل بحماية الخادم المستهدف عبر اعتراض وروتوكول TCP. تحقق من حدود الاتصال التي تم تكوينها للتأكد من أنها توفر حماية كافية لطبيعة الهجوم ومعدله. كما أنه سيكون من المفيد منع حركة مرور المهاجم يدويا بعيدا عن المنبع قدر الإمكان. ويمكن القيام بذلك عبر قوائم التحكم في الوصول (ACL) وجودة الخدمة (QoS). وهذا يضمن أن الأجهزة الوسيطة ال تحتاج إلى رده الموارد على حركة المرور غير الشرعية.

إذا كان الهجوم الذي تم الكشف عنه إيجابيا خاطئا، فقم بتعديل معدلات هجوم اعتراض TCP إلى قيمة أكثر ملاءمة مع threat-detection statistics tcp-intercepterasecat4000_flash:.

كيفية إطلاق التهديد يدويا

لاختبار التهديدات المختلفة واستكشاف أخطائها وإصلاحها، يمكن أن يكون من المفيد تشغيل تهديدات متعددة يدويا. يحتوي هذا القسم على تلميحات حول كيفية تشغيل بعض أنواع التهديدات الشائعة.

التهديد الأساسي - إسقاط قائمة التحكم في الوصول (ACL) وجدار الحماية والمسح الضوئي

لتشغيل تهديد أساسي معين، ارجع إلى الجدول في قسم الوظائف السابق. أختر سببا لتشغيل محدد إلسقاط ASP وأرسل حركة مرور البيانات من خلال ASA التي سيتم إسقاطها بواسطة سبب إسقاط ASP المناسب.

على سبيل المثال، تعتبر جميع تهديدات إسقاط قائمة التحكم في الوصول وجدار الحماية والمسح الضوئي معدل الحزم التي تم إسقاطها بواسطة قائمة التحكم في الوصول (ACL). أكمل الخطوات التالية لتشغيل هذه التهديدات في نفس الوقت:

1. قم بإنشاء قائمة تحكم في الوصول (ACL) على الواجهة الخارجية ل ASA التي تقوم بإسقاط جميع حزم TCP التي يتم إرسالها إلى خادم ويب في داخل ASA (10.11.11.11):

   ```
   access-list outside_in extended line 1 deny tcp any host 10.11.11.11
   access-list outside_in extended permit ip any any
   access-group outside_in in interface outside
   ```

2. من مجاهم على الجزء الخارجي من ASA (10.10.10.10)، أستخدم nmap لتشغيل مسح TCP SYN الضوئي مقابل كل منفذ على المداخ الهدف:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

ملاحظة: موقع T5 بتكوين NMAP لتشغيل الفحص بأسرع ما يمكن. استنادا إلى موارد جهاز الكمبيوتر المهاجم، ال يزال هذا غير سريع بما يكفي لتشغيل بعض المعدالت الافتراضية. إذا كان هذا هو الحال، فما عليك سوى تقليل المعدالت التي تم تكوينها للتهديد الذي تريد رؤيته. عندما تقوم بضبط ARI و BRI إلى 0، يؤدي الكشف عن التهديد الأساسي إلى تشغيل التهديدات دائما بغض النظر عن المعدل.

3. الحظ أنه يتم اكتشاف التهديدات األساسية لقوائم التحكم في الوصول (ACL) وجدار الحماية والتهديدات المسح الضوئي:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 10; Current average rate is 9 per second,
 max configured rate is 5; Cumulative total count is 5538
%ASA-1-733100: [ ACL drop] drop rate-1 exceeded. Current burst rate is 19 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1472
%ASA-1-733100: [ Firewall] drop rate-1 exceeded. Current burst rate is 18 per second,
 max configured rate is 0; Current average rate is 2 per second,
 max configured rate is 0; Cumulative total count is 1483
```

ملاحظة: في هذا المثال، تم تعيين كل من قوائم التحكم في الوصول (ACL) وجدار الحماية ARI و BRI على 0، وبالتالي فإنها تتسبب دائما في حدوث تهديد. وهذا هو السبب في إدراج الحد األقصى للمعدالت التي تم تكوينها على أنه 0.

التهديد المتقدم - اعتراض TCP

1. قم بإنشاء قائمة تحكم في الوصول (ACL) على الواجهة الخارجية التي تسمح لجميع حزم TCP التي يتم إرسالها إلى مداخ هدف على داخل ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

2. إذا لم يكن المداخ الهدف موجودا بالفعل، أو قم بإعداد ضبط مراحل االتصال للمهاجم، فقم بتكوين إدخال ARP مزيف على ASA لتقييد حركة مرور الهجوم خارج الواجهة الداخلية:

```
arp inside 10.11.11.11 dead.dead.dead
```

3. قم بإنشاء سياسة اعتراض TCP بسيطة على ASA:

```
access-list tcp extended permit tcp any any
class-map tcp
  match access-list tcp
policy-map global_policy
  class tcp
    set connection conn-max 2
service-policy global_policy global
```

من مهاجم على الجزء الخارجي من ASA (10.10.10.10)، أستخدم nmap لتشغيل مسح TCP SYN الضوئي مقابل كل منفذ على الخادم الهدف:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

لاحظ أن الكشف عن التهديدات يتتبع الخادم المحمي بشكل مستمر:

```
<#root>

ciscoasa(config)#

show threat-detection statistics top tcp-intercept


Top 10 protected servers under attack (sorted by average rate)
Monitoring window size: 30 mins    Sampling interval: 30 secs

----------------------------------------------------------------------------
1    10.11.11.11:18589 outside 0 0 1 10.10.10.10 (36 secs ago)
2    10.11.11.11:47724 outside 0 0 1 10.10.10.10 (36 secs ago)
3    10.11.11.11:46126 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
4    10.11.11.11:3695 outside 0 0 1  Last: 10.10.10.10 (6 secs ago)
```

تهديد الفحص

1. قم بإنشاء قائمة تحكم في الوصول (ACL) على الواجهة الخارجية التي تسمح لجميع حزم TCP التي يتم إرسالها إلى خادم هدف على داخل ASA (10.11.11.11):

```
access-list outside_in extended line 1 permit tcp any host 10.11.11.11
access-group outside_in in interface outside
```

ملاحظة: من أجل مسح الكشف عن التهديدات لتعقب عناوين IP الخاصة بالهدف والمهاجم، يجب السماح بحركة المرور من خلال ASA.

---

2. إذا لم يكن الخادم الهدف موجودا بالفعل، أو قام بإعادة ضبط محاولات الاتصال للمهاجم، فقم بتكوين إدخال ARP ثابت على ASA لتقييد حركة مرور الهجوم خارج الواجهة الداخلية:

```
arp inside 10.11.11.11 dead.dead.dead
```

ملاحظة: ال يتم حساب الاتصالات التي يتم إعادة تعيينها بواسطة الخادم الهدف كجزء من التهديد.

3. من مهاجم على الجزء الخارجي من ASA (10.10.10.10)، أستخدم nmap لتشغيل مسح TCP SYN الضوئي مقابل كل منفذ على الخادم الهدف:

```
nmap -sS -T5 -p1-65535 -Pn 10.11.11.11
```

ملاحظة: يقوم T5 بتكوين NMAP لتشغيل الفحص بأسرع ما يمكن. استنادا إلى موارد جهاز الكمبيوتر المهاجم، ال يزال هذا غير سريع بما يكفي لتشغيل بعض المعدلات الافتراضية. إذا كان هذا هو الحال، فما عليك سوى تقليل المعدلات التي تم تكوينها للتهديد الذي تريد رؤيته. عندما تقوم بضبط ARI و BRI إلى 0، يؤدي الكشف عن التهديد الأساسي إلى تشغيل التهديد دائما بغض النظر عن المعدل.

4. لاحظ أنه يتم الكشف عن تهديد مسح ضوئي، ويتم تعقب IP الخاص بالمهاجم، ويتم تجنب المهاجم:

```
%ASA-1-733100: [ Scanning] drop rate-1 exceeded. Current burst rate is 17 per second,
max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 404
%ASA-4-733101: Host 10.10.10.10 is attacking. Current burst rate is 17 per second,
 max configured rate is 10; Current average rate is 0 per second,
 max configured rate is 5; Cumulative total count is 700
%ASA-4-733102: Threat-detection adds host 10.10.10.10 to shun list
```

معلومات ذات صلة

- دليل تكوين ASA
- مرجع أمر ASA
- رسائل Syslog سلسلة ASA لجدار الحماية الآمن من Cisco
- الدعم الفني والتنزيلات من Cisco

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).