كيف يمكن تكوين جهاز أمان الويب من Cisco وشبكة RSA DLP للتفاعل؟

المحتويات

سؤال:

كيف يمكن تكوين جهاز أمان الويب من Cisco وشبكة RSA DLP للتفاعل؟

نظرة عامة:

يقدم هذا المستند معلومات إضافية تتجاوز دليل المستخدم الخاص بنظام التشغيل Cisco WSA AsyncOS ودليل نشر شبكة RSA DLP 7.0.2 لمساعدة العملاء على تشغيل هذين المنتجين معا.

وصف المنتج:

يعد جهاز أمان الويب (WSA) من Cisco بمثابة جهاز قوي وآمن وفعال يحمي شبكات الشركات ضد البرامج الضارة وبرامج التجسس المستندة إلى الويب التي يمكن أن تعرض أمان الشركات للخطر وتعرض الملكية الفكرية. يوفر جهاز أمان الويب الفحص العميق لمحتوى التطبيق من خلال تقديم خدمة وكيل ويب لبروتوكولات الاتصال القياسية مثل HTTP و HTTPS و FTP.

تشتمل مجموعة RSA DLP على حل شامل لمنع فقدان البيانات يتيح للعملاء اكتشاف البيانات الحساسة وحمايتها في المؤسسة من خلال الاستفادة من السياسات الشائعة عبر البنية الأساسية لاكتشاف البيانات الحساسة وحمايتها في مركز البيانات والشبكة ونقاط النهاية. تتضمن مجموعة DLP المكونات التالية:

- **مركز بيانات RSA DLP**. يساعدك مركز بيانات DLP على تحديد موقع البيانات الحساسة بغض النظر عن مكان وجودها في مركز البيانات وفي أنظمة الملفات وقواعد البيانات وأنظمة البريد الإلكتروني وبيئات شبكة التخزين/وحدات التخزين المتصلة بالشبكة (SAN) الكبيرة.
- **شبكة RSA DLP**. تراقب شبكة DLP وتفرض إرسال المعلومات الحساسة على الشبكة، مثل البريد الإلكتروني وحركة مرور الويب.
- **نقطة نهاية RSA DLP**. تساعدك نقطة نهاية DLP على اكتشاف المعلومات الحساسة ومراقبتها والتحكم فيها في نقاط النهاية مثل أجهزة الكمبيوتر المحمولة والمكتبية.

تملك Cisco WSA القدرة على التفاعل مع شبكة RSA DLP.

تتضمن شبكة RSA DLP المكونات التالية:

- **وحدة التحكم في الشبكة**. الجهاز الرئيسي الذي يحتفظ بمعلومات حول سياسات نقل البيانات والمحتوى السرية. تقوم وحدة التحكم في الشبكة بإدارة الأجهزة المدارة وتحديثها باستخدام تعريف المحتوى الحساس والنهج بالإضافة إلى أي تغييرات في التكوين الخاص بها بعد التكوين الأولي.
- **الأجهزة المدارة**. تساعد هذه الأجهزة إرسال شبكة مراقبة DLP والإبلاغ عن الإرسال أو اعتراضه:
أجهزة الاستشعار. نظرا لتركيبها في حدود الشبكة، تقوم أجهزة الاستشعار بمراقبة حركة المرور التي تغادر

الشبكة أو تعبر حدود الشبكة بشكل غير فعال، وتقوم بتحليلها لضمان وجود محتوى حساس. المستشعر هو حل خارج النطاق، ولا يمكنه إلا مراقبة انتهاكات السياسة والإبلاغ عنها.**معترضات**. كما يتم تثبيتها في حدود الشبكة، تتيح لك عمليات الاعتراض تنفيذ عزل حركة مرور البريد الإلكتروني (SMTP) التي تحتوي على محتوى حساس و/أو رفضها. والمعترض هو وكيل شبكة خطي وبالتالي يمكن أن يمنع البيانات الحساسة من مغادرة المؤسسة.**خوادم ICAP**. أجهزة خادم الأغراض الخاصة التي تسمح لك بتنفيذ مراقبة حركة مرور HTTP أو HTTPS أو FTP التي تحتوي على محتوى حساس أو حظرها. يعمل خادم ICAP مع خادم وكيل (تم تكوينه كعميل ICAP) لمراقبة البيانات الحساسة أو حظرها من مغادرة المؤسسة
يعمل خادم ICAP لشبكة RSA DLP من Cisco.

القيود المعروفة

يدعم تكامل Cisco WSA الخارجي DLP مع شبكة RSA DLP الإجراءات التالية: السماح والحظر. لا يدعم بعد الإجراء "تعديل/إزالة المحتوى" (يسمى أيضا التنقيح).

متطلبات المنتج للتوافق

تم إختبار قابلية التشغيل البيني لشبكة Cisco WSA و RSA DLP والتحقق منها باستخدام نماذج المنتجات وإصدارات البرامج في الجدول التالي. وعلى الرغم من أن هذا الدمج قد يعمل بشكل وظيفي مع التباينات مع الطراز والبرنامج، فإن الجدول التالي يمثل التركيبات الوحيدة التي تم إختبارها والتحقق من صحتها ودعمها. يوصى بشدة باستخدام أحدث إصدار مدعوم من كلا المنتجات.

المنتج	إصدار البرامج
أجهزة أمان الويب (WSA) من Cisco	نظام التشغيل AsyncOS الإصدار 6.3 والإصدارات الأحدث
شبكة RSA DLP	7.0.2

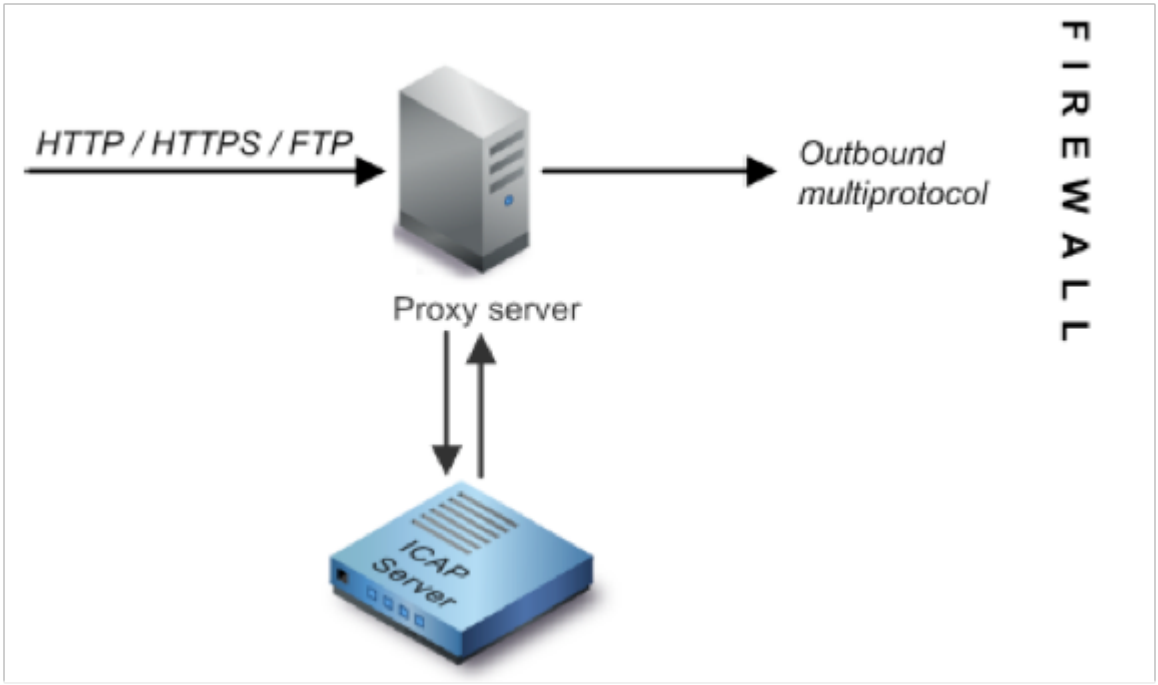
ميزة DLP الخارجية

باستخدام ميزة DLP الخارجية من Cisco WSA، يمكنك إعادة توجيه حركة مرور كل أو حركة مرور HTTP و HTTPS و FTP الصادرة المحددة من شبكة WSA إلى شبكة DLP. يتم نقل جميع حركات المرور باستخدام بروتوكول ملاءمة التحكم في الإنترنت (ICAP).

عمارة

يوضح دليل نشر شبكة RSA DLP البنية العامة التالية لشبكة RSA DLP المشتركة بين التشغيل مع خادم وكيل. لا تقتصر هذه البنية على WSA، ولكنها تنطبق على أي وكيل يعمل مع شبكة RSA DLP.

الشكل 1: بنية النشر لشبكة RSA DLP وأجهزة أمان الويب Cisco Web Security Appliance



تكوين جهاز أمان الويب من Cisco

1. تحديد نظام DLP خارجي على WSA الذي يعمل مع خادم ICAP لشبكة DLP. للحصول على تعليمات، يرجى الاطلاع على المقتطف المرفق من دليل مستخدم WSA "تعليمات دليل المستخدم التي تحدد أنظمة DLP الخارجية".

2. قم بإنشاء سياسة DLP خارجية واحدة أو أكثر تحدد حركة مرور البيانات التي يرسلها WSA إلى شبكة DLP لإجراء مسح للمحتوى باستخدام الخطوات التالية:

- تحت **GUI > إدارة أمان الويب>سياسات DLP الخارجية > إضافة سياسة**
- انقر فوق الارتباط الموجود ضمن عمود ***الوجهات*** لمجموعة السياسات التي تريد تكوينها
- تحت قسم "تحرير إعدادات الوجهة"، أختر ؟تحديد إعدادات مخصصة للمسح الضوئي للوجهات؟ من القائمة المنسدلة
- بعد ذلك، يمكننا تكوين النهج ل "مسح كافة عمليات التحميل ضوئيا" أو لمسح عمليات التحميل ضوئيا إلى مجالات/مواقع معينة محددة في فئات URL المخصصة

تكوين شبكة RSA DLP

يفترض هذا المستند أنه قد تم تثبيت وتكوين وحدة التحكم في شبكة RSA DLP وخادم ICAP و Enterprise Manager.

1. أستخدم RSA DLP Enterprise Manager لتكوين خادم ICAP للشبكة. للحصول على تعليمات تفصيلية حول إعداد خادم ICAP للشبكة DLP، ارجع إلى دليل نشر الشبكة RSA DLP. المعلمات الرئيسية التي يجب تحديدها في صفحة تكوين خادم ICAP هي: اسم المضيف أو عنوان IP الخاص بخادم ICAP.في قسم **الإعدادات العامة** من صفحة التكوين، أدخل المعلومات التالية: مقدار الوقت بالثواني الذي يعتبر الخادم قد انتهت مهلته في حقل **مهلة الخادم بالثواني**.حدد واحدا مما يلي كاستجابة **عند انتهاء مهلة الخادم**:**فشل الفتح**. حدد هذا الخيار إذا كنت تريد السماح بالإرسال بعد انتهاء مهلة الخادم.**فشل الإغلاق**. حدد هذا الخيار إذا كنت تريد حظر الإرسال بعد انتهاء مهلة الخادم.

2. أستخدم RSA DLP Enterprise Manager لإنشاء سياسة واحدة أو أكثر من السياسات الخاصة بالشبكة لمراجعة حركة مرور الشبكة التي تحتوي على محتوى حساس وحظرها. للحصول على إرشادات تفصيلية لإنشاء سياسات DLP، ارجع إلى دليل مستخدم شبكة RSA DLP أو تعليمات Enterprise Manager عبر الإنترنت. وتتمثل الخطوات الرئيسية المطلوب تنفيذها فيما يلي: من مكتبة قالب النهج تمكن على الأقل سياسة واحدة منطقية لبيئتك والمحتوى الذي ستقوم بمراقبته.ضمن هذا النهج، قم بإعداد قواعد انتهاك السياسة الخاصة بشبكة DLP التي تحدد الإجراءات التي سينفذها منتج الشبكة تلقائيا عند حدوث أحداث (انتهاكات النهج). قم بتعيين قاعدة كشف النهج لاكتشاف جميع البروتوكولات. تعيين إجراء السياسة على "التدقيق والحجب".

إختياريا، يمكننا إستخدام RSA Enterprise Manager لتخصيص إعلام الشبكة الذي يتم إرساله إلى المستخدم عند حدوث مخالفات للنهج. يتم إرسال هذا الإعلام بواسطة شبكة DLP كبديل لحركة المرور الأصلية.

إختبار الإعداد

1. قم بتكوين المستعرض لديك لتوجيه حركة المرور الصادرة من المستعرض لديك للانتقال مباشرة إلى وكيل WSA.

على سبيل المثال، إذا كنت تستخدم متصفح Mozilla FireFox، فقم بما يلي: في متصفح FireFox، حدد **أدوات > خيارات**. يظهر مربع الحوار خيارات.انقر على علامة التبويب **الشبكة**، ثم انقر على **إعدادات**. يظهر مربع الحوار "إعدادات الاتصال".حدد خانة الاختيار **تكوين الوكيل اليدوي**، ثم أدخل عنوان IP أو اسم المضيف لخادم وكيل WSA في حقل **وكيل HTTP** ورقم المنفذ 3128 (الافتراضي).طقطقت **ok**، بعد ذلك **ok** ثانية أن يحفظ العملية إعداد جديد.

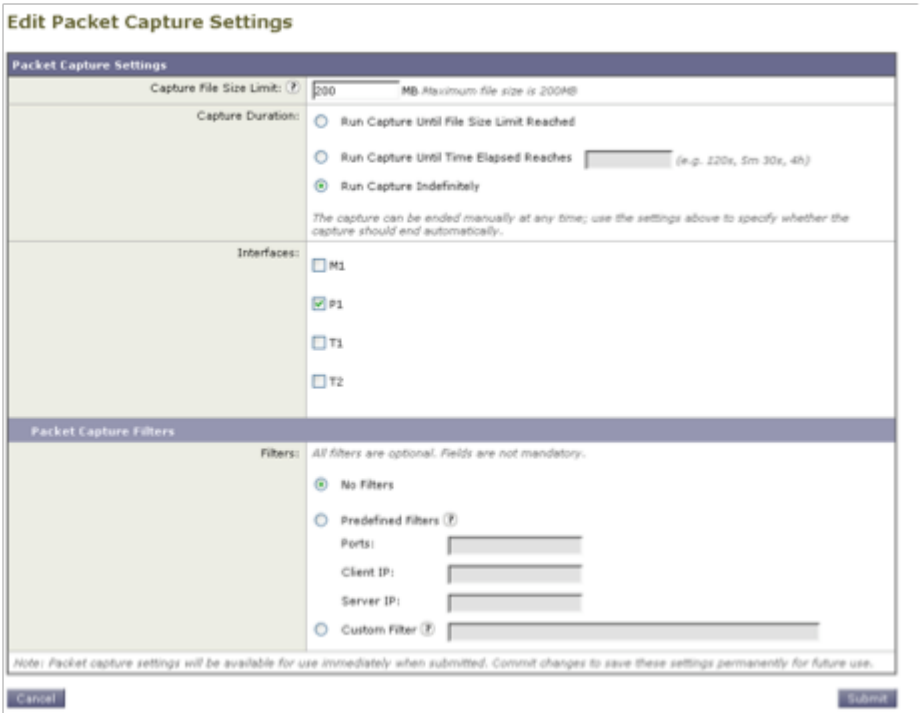
2. محاولة تحميل بعض المحتوى الذي تعلم أنه ينتهك نهج شبكة DLP الذي قمت بتمكينه مسبقا.
3. يجب أن ترى رسالة تجاهل ICAP للشبكة في المستعرض.
4. أستخدم "مدير المؤسسة" لعرض الحدث والحدث الناتجين اللذين تم إنشاؤهما نتيجة هذا الانتهاك للسياسة.

استكشاف الأخطاء وإصلاحها

1. عند تكوين خادم DLP خارجي على جهاز أمان الويب لشبكة RSA DLP، أستخدم القيم التالية:

عنوان الخادم: عنوان IP أو اسم مضيف خادم ICAP لشبكة RSA DLPالمنفذ: يستخدم منفذ TCP للوصول إلى خادم شبكة RSA DLP، عادة **1344**تنسيق عنوان URL للخدمة:
icap://*<hostname_or_ipaddress>*/srv_conalarm :مثال: icap://dlp.example.com/srv_conalarm
قم بتمكين ميزة التقاط حركة مرور البيانات ل WSA لالتقاط حركة مرور البيانات بين وكيل WSA وخادم ICAP للشبكة. يكون هذا مفيدا عند تشخيص مشاكل الاتصال. للقيام بذلك، قم بما يلي:

في واجهة المستخدم الرسومية WSA، انتقل إلى قائمة **الدعم والمساعدة** في أعلى يمين واجهة المستخدم. حدد **التقاط الحزمة** من القائمة، ثم انقر على زر **تحرير إعدادات**. تظهر نافذة تحرير إعدادات الالتقاط.



في قسم عوامل تصفية **التقاط** الحزم من الشاشة، أدخل عنوان IP الخاص بخادم ICAP للشبكة في حقل **خادم IP**.انقر فوق **إرسال** لحفظ التغييرات التي أجريتها.

3. أستخدم الحقل المخصص التالي في سجلات الوصول إلى WSA (تحت ***واجهة المستخدم الرسومية (GUI)>إدارة النظام > اشتراكات السجل>سجلات الوصول)للحصول على مزيد من المعلومات:***

٪xp: حكم الفحص الخاص بخادم DLP الخارجي (0 = عدم تطابق في خادم ICAP؛ 1 = تطابق النهج مقابل خادم ICAP و'- (شرطة)' = عدم بدء الفحص بواسطة خادم DLP الخارجي)

[تعليمات دليل المستخدم التي تحدد أنظمة DLP الخارجية.](#)

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).