جدول المحتويات: مستندات TAC عن خدمة FireSIGHT و AMP ونظام FirePOWER

المحتويات

وثائق TAC على FireSIGHT ونظام FirePOWER

تحديث البرامج والأمان وإعادة التصوير والترحيل والتثبيت

- أنواع ملفات التحديث التي قد يتم تثبيتها على نظام FireSIGHT
- تعرف على المصطلحات الجديدة لأنظمة FireSIGHT بعد الترحيل والترقية من x.4.10 إلى x.5
- تثبيت الوحدة الطرفية لخدمات FirePOWER على منصة ASA
- تركيب خدمات FirePOWER (SFR) على الوحدة النمطية للأجهزة ASA 5585-X
- نشر FireSIGHT Management Center على VMware ESXi
- إعادة تثبيت صورة مركز حماية Sourcefire وجهاز FirePOWER
- فشل التنزيل التلقائي في أحد مراكز إدارة FireSIGHT
- إرشادات لتنزيل البيانات من مركز إدارة Firepower إلى الأجهزة المدارة
- تكوين خدمات FirePOWER على جهاز ISR باستخدام خادم UCS-E نصلي

الترخيص والإعداد الأساسي الأولي

- مقارنة تراخيص الميزات الخاصة بأنظمة FireSIGHT
- الميزات والإمكانات المدعومة لنماذج الأجهزة المختلفة لنظام FireSIGHT
- خطوات التكوين الأولية لأنظمة FireSIGHT
- تسجيل جهاز باستخدام FireSIGHT Management Center
- تكوين موجه ظاهري على نظام FireSIGHT
- إدارة الوحدة النمطية SFR عبر نفق VPN بدون محول شبكة LAN
- الحصول على مفتاح الترخيص لجهاز FirePOWER ووحدة FirePOWER Service

الثغرات وتغطية القواعد والأحداث وتحليل الملفات

- تنزيل بيانات الحزمة (ملف PCAP) باستخدام واجهة مستخدم الويب
- إجراءات التقاط الحزم على أجهزة Sourcefire FirePOWER والأجهزة الظاهرية NGIPS
- خيارات لتقليل أحداث التطفل الإيجابية الزائفة
- قواعد الشخر المحلي المخصص على نظام FireSIGHT

اكتشاف الاقتحام والوقاية منه (IDS/IPS)، محرك الشبكة

- تحديد الحالة الافتراضية ل Sourcefire يوفر قاعدة في سياسة الاقتحام
- المقاييس المستخدمة لتحديد القواعد الافتراضية في سياسة أساسية
- تكوين متغير SNORT_BPF على مركز دفاع
- فحص حركة مرور بيانات تجميع الارتباطات بواسطة Sourcefire FirePOWER والأجهزة الظاهرية
- قم بتمكين المعالج المسبق للتطبيع المضمن وفهم الفحص المسبق للطرح واللاحق للطرح
- مجموعة من الملفات الأساسية من جهاز أمان FirePOWER
- تكوين قاعدة تمرير على نظام FireSIGHT
- إستبعاد رسائل EIGRP و OSPF و BGP من فحص إقتحام FirePOWER
- معالجة دورة تيار واحد كبيرة (تدفق الفيل) بواسطة خدمات FirePOWER

ذكاء الأمان وتحديد الموقع الجغرافي وتصفية عنوان URL

- تصفية URL على مثال تكوين نظام FireSIGHT
- تعذر تنزيل موجز معلومات الأمان أو تحديثه
- يتم حظر عنوان IP أو إدراجه في القائمة السوداء من قبل الاستخبارات الأمنية لنظام FireSIGHT
- أستكشاف أخطاء تصفية URL وإصلاحها على نظام FireSIGHT

التحكم في التطبيق، VDB، اكتشاف الشبكة

- قد يقوم FireSIGHT بالتعرف على المضيف بشكل غير صحيح، أو وضع علامة على الحدث كمعلق أو غير معروف

قاعدة التحكم في الوصول/جدار الحماية

- يبدو أن أحداث الاتصال تختفي من مركز إدارة FireSIGHT

واجهة المستخدم (GUI/CLI)، وصول المستخدم والمصادقة

- دمج نظام FireSIGHT مع ISE لمصادقة مستخدم RADIUS
- دمج نظام FireSIGHT مع ACS 5.x لمصادقة مستخدم RADIUS
- إعادة ضبط كلمة مرور مستخدم Admin على أنظمة FireSIGHT
- التحقق من كائن المصادقة على نظام FireSIGHT لمصادقة Microsoft AD عبر SSL/TLS
- تعريف سمات كائن LDAP لخدمة Active Directory لتكوين كائن المصادقة
- تكوين كائن مصادقة LDAP على نظام FireSIGHT
- التحقق من LDAP عبر (SSL/TLS (LDAPs وشهادة CA باستخدام LDP.exe

إستخدام وحدة المعالجة المركزية (CPU) والذاكرة وأداء الشبكة والنظام

- تعليمات تصنيف القواعد على نظام FireSIGHT
- مجموعة إحصائيات الأداء باستخدام خيار مراقبة الأداء لمدة ثانية واحدة
- تجميع البيانات من نظام FireSIGHT عندما تواجه الشبكة مشاكل في زمن الوصول
- أستكشاف أخطاء إسقاط الحزم وإصلاحها بسبب وجود وحدة الحد الأقصى للنقل (MTU) أعلى (الحزمة ذات الحجم الزائد)

إدارة النظام وصيانته

- إعادة تشغيل العمليات على نظام FireSIGHT وخدمة FirePOWER دون إعادة التشغيل
- إجراءات إنشاء الملف لاستكشاف أخطاء جهاز Sourcefire وإصلاحها
- أستكشاف أخطاء الشبكة الزمنية (NTP) وإصلاحها على أنظمة FireSIGHT
- أستكشاف أخطاء الاستخدام المفرط للأقراص على أجهزة Sourcefire وإصلاحها
- تكوين المكدس على أجهزة سلسلة Cisco Firepower 8000
- تكوين التجميع على أجهزة سلسلة FirePOWER 7000 و 8000 من Cisco

تشغيل الأجهزة

- تنبيهات الحماية من وحدة التزويد بالطاقة التابعة لنظام FireSIGHT
- أستكشاف مشكلة ما وإصلاحها فيما يخص ميزة إدارة إطفاء الأضواء (LOM) في مركز إدارة FireSIGHT أو جهاز FirePOWER
- يقوم نظام FireSIGHT بإرجاع رسالة "خطأ الإدخال/الإخراج"
- يتم تجميد جهاز أمان FirePOWER بعد محاولة تحميله في وضع مستخدم واحد
- أستكشاف المشكلات المتعلقة بالمراوح وحلها على نظام FireSIGHT
- إجراء إختبارات تشخيصية من لوحة LCD لجهاز FirePOWER
- إدراج وحدة نمطية للشبكة (NetMod) وازالتها على جهاز أمان FirePOWER من السلسلة 8000
- تحديد المشاكل المتعلقة ببطاقات محرك تدفق الشبكة في أجهزة سلسلة FirePOWER 7000 و Sourcefire 8000
- مشكلات شائعة حول مجموعة أدوات السكك الحديدية FirePOWER 8000 Series
- تعليمات تثبت مجموعة أدوات السكك الحديدية Firepower 7000 Series

- قد يؤدي نموذج FireSIGHT Management Center FS4000 إلى تشغيل تنبيه صحي "تعرض القرص للتدهور"
- إجراءات إعادة تكوين محرك الأقراص المزود بذاكرة مصنوعة من مكونات صلبة/محرك أقراص RAID للطرازين FireSIGHT Management Center FS2000 و FS4000

فك تشفير SSL

- إعادة تكوين جهاز Sourcefire SSL 1500/2000 إلى الإصدار 3.6 أو أعلى
- الحصول على كلمة مرور BIOS لجهاز SSL
- إجراءات التقاط الحزمة على جهاز SSL
- تكوين SNMP على جهاز SSL
- تكوين القواعد الأساسية على جهاز SSL
- تكوين سياسة فحص SSL على نظام FireSIGHT من Cisco

الدمج مع ISE و Estreamer و SIEM و User Agent (وكيل المستخدم) و API وموصل

- تسجيل الدخول إلى سطح مكتب بعيد باستخدام RDP يغير المستخدم المرتبط بعنوان IP
- أستكشاف المشكلات وإصلاحها بين نظام FireSIGHT وعميل SIEM (Streamer)
- تثبيت وكيل مستخدم Sourcefire وإلغاء تثبيته
- أستكشاف أخطاء الاتصال وإصلاحها مع وكيل مستخدم Sourcefire
- تكوين نظام FireSIGHT لإرسال تنبيهات إلى خادم syslog خارجي
- منح الحد الأدنى من الإذن لحساب مستخدم Active Directory المستخدم بواسطة عامل مستخدم Sourcefire
- يتم عرض حالة عامل المستخدم في الوقت الفعلي على أنها غير معروفة
- إنشاء بيانات أستكشاف أخطاء البرامج وإصلاحها من Sourcefire التي تعمل على النظام الأساسي BlueCoat X-Series
- فهم التحكم في الوصول المستند إلى TrustSec باستخدام FirePOWER و ISE
- لا يتم إعادة تشغيل خدمة قاعدة بيانات وكيل مستخدم FirePOWER من Cisco بعد توقف

وثائق TAC حول الحماية المتقدمة من البرامج الضارة

AMP لنقاط النهاية وموصل FireAMP

- مجموعة البيانات التشخيصية من موصل FireAMP يعمل على Windows
- مجموعة بيانات تشخيصية من موصل FireAMP يعمل على Mac OSX
- مجموعة من البيانات التشخيصية من موصل FireAMP يعمل على نظام التشغيل Linux
- صورة أو نسخ كمبيوتر به موصل FireAMP مثبت
- تكوين الاستثناءات وإدارتها في FireAMP
- إزالة ذاكرة التخزين المؤقت ل FireAMP وملفات المحفوظات على Windows
- محولات سطر الأوامر لمثبت موصل FireAMP
- تعطيل خدمة عميل FireAMP Connector وتمكينها
- قم بتشغيل خدمة عميل FireAMP Connector في الخلفية وإخفاء واجهة المستخدم
- ترقية موصل FireAMP على أنظمة تشغيل Windows
- فشلت خدمة موصل FireAMP في الإيقاف بسبب حماية الموصل
- أنواع الملفات التي يتم فحصها بواسطة موصل FireAMP
- دليل FireAMP لاستبعادات Windows
- الحصول على بيانات أستكشاف الأخطاء وإصلاحها على جهاز Android لمشاكل موصل FireAMP للجوال
- بدء عمليات الفحص المجدولة على FireAMP / AMP لنقاط النهاية
- تنفيذ إشارات نقطة النهاية لعمليات المسح على الحل الوسط (IOC) باستخدام AMP لنقاط النهاية أو FireAMP
- تثبيت الوحدة النمطية AMP وتكوينها من خلال أداة تمكين AnyConnect 4.x و AMP
- نشر الحماية المتقدمة (AMP) من Cisco لنقاط النهاية مع ثبات الهوية

- العمل مع الحماية المتقدمة من البرامج الضارة (AMP) الأحداث السلبية الخاطئة أو الإيجابية
- نظرة عامة على Cisco AMP لواجهة برمجة تطبيقات Endpoint

AMP للشبكة

- الخوادم المطلوبة لعمليات الحماية المتقدمة من البرامج الضارة
- أستكشاف أخطاء الاتصال والتسجيل وإصلاحها باستخدام AMP على مركز إدارة FireSIGHT
- معالجة إزالة الاتصالات بين مركز إدارة FireSIGHT ووحدة تحكم سحابة FireAMP

سحابة

- تركيب سحابة FireAMP الخاصة وتكوينها
- إنشاء ملف لقطة دعم على سحابة FireAMP الخاصة
- تحميل ملف إلى وحدة تحكم سحابة FireAMP لعرض تحليل الملف الأخير

شبكة تهديدات

- إنشاء لقطة دعم على جهاز شبكة تهديدات الحماية المتقدمة (AMP)

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).