Contenidos: Documentos del TAC sobre FirePOWER Service, FireSIGHT System y AMP

Contenido

Documentos del TAC sobre FireSIGHT y Firepower System

Actualización, recreación de imágenes, migración e instalación de software y seguridad

- Tipos de archivos de actualización que se pueden instalar en un sistema FireSIGHT
- Conozca las nuevas terminologías de los sistemas FireSIGHT tras una migración y actualización de 4.10.x a 5.x
- Instalación y configuración de un módulo de servicios Firepower en una plataforma ASA
- Instalación de los servicios FirePOWER (SFR) en el módulo de hardware ASA 5585-X
- Implementación de FireSIGHT Management Center en VMware ESXi
- Recreación de imágenes de un centro de defensa de Sourcefire y un appliance FirePOWER
- Falla de actualización de descarga automática en un FireSIGHT Management Center
- Pautas para descargar datos desde Firepower Management Center a dispositivos administrados
- Configuración de Firepower Services en un dispositivo ISR con un blade UCS-E

Licencia y configuración básica inicial

- Comparación de licencias de funciones en sistemas FireSIGHT
- Funciones y capacidades compatibles de los diversos modelos de hardware del sistema FireSIGHT
- Pasos iniciales de configuración de los sistemas FireSIGHT
- Registrar un dispositivo con FireSIGHT Management Center
- Configuración de un router virtual en un sistema FireSIGHT
- Gestión del módulo SFR sobre túnel VPN sin switch LAN
- Obtención de la clave de licencia para un dispositivo Firepower y un módulo de servicio Firepower

Análisis de archivos, eventos y cobertura de reglas y vulnerabilidades

- Descargar datos de paquetes (archivo PCAP) mediante la interfaz de usuario web
- Procedimientos de captura de paquetes en appliances FirePOWER de Sourcefire y appliances virtuales NGIPS
- Opciones para reducir los eventos de intrusión de falsos positivos
- Reglas de Snort locales personalizadas en un sistema FireSIGHT

Detección y prevención de intrusiones (IDS/IPS), motor Snort

- Determinación del estado predeterminado de una regla proporcionada por Sourcefire en una directiva de intrusiones
- Métricas Utilizadas para Determinar las Reglas Predeterminadas en una Política Base
- Configuración de la variable SNORT_BPF en un centro de defensa

- Inspección del tráfico agregado de enlaces mediante FirePOWER y appliances virtuales de Sourcefire
- Habilitar el preprocesador de normalización en línea y comprender la inspección previa y posterior al ACK
- Recopilación de archivos de núcleo de un appliance FirePOWER
- Configuración de una regla de aprobación en un sistema FireSIGHT
- Exclusión de mensajes EIGRP, OSPF y BGP de la inspección de intrusiones de Firepower
- Procesamiento de sesiones a gran escala de un solo flujo (Elephant Flow) mediante Firepower Services

Inteligencia de seguridad, geolocalización y filtrado de URL

- Ejemplo de Configuración de Filtrado de URL en un Sistema FireSIGHT
- No se puede descargar o actualizar la fuente de inteligencia de seguridad
- La inteligencia de seguridad de un sistema FireSIGHT bloquea o lista negra la dirección IP
- Solución de problemas de filtrado de URL en un sistema FireSIGHT

Control de aplicaciones, VDB, detección de redes

- FireSIGHT puede identificar un host de forma incorrecta o marcar un evento como pendiente o desconocido

Firewall/regla de control de acceso

- Los eventos de conexión parecen desaparecer de FireSIGHT Management Center

Interfaz de usuario (GUI/CLI), acceso de usuario y autenticación

- Integración del sistema FireSIGHT con ISE para la autenticación de usuarios RADIUS
- Integración del sistema FireSIGHT con ACS 5.x para la autenticación de usuarios RADIUS
- Restablecer la contraseña del usuario administrador en sistemas FireSIGHT
- Verificación del objeto de autenticación en el sistema FireSIGHT para la autenticación de Microsoft AD sobre SSL/TLS
- Identificar atributos de objeto LDAP de Active Directory para la configuración del objeto de autenticación
- Configuración del objeto de autenticación LDAP en el sistema FireSIGHT
- Verificación de LDAP sobre SSL/TLS (LDAPS) y certificado de CA mediante Ldp.exe

Uso de la CPU y la memoria, rendimiento de la red y del sistema

- Instrucciones de generación de perfiles de reglas en FireSIGHT System
- Recopilación de estadísticas de rendimiento mediante la opción "Monitor de rendimiento de 1 segundo"
- Recopilación de datos de un sistema FireSIGHT cuando una red experimenta problemas de latencia
- Solución de problemas de descarte de paquetes debido a una MTU superior (paquete excesivo)

Administración y mantenimiento del sistema

- Reinicie los procesos en un sistema FireSIGHT y un servicio FirePOWER sin reiniciar
- Procedimientos de generación de archivos para solucionar problemas del dispositivo Sourcefire
- Resolución de problemas con el protocolo de tiempo de la red (NTP) en sistemas FireSIGHT
- Resolución de problemas de uso excesivo de disco en dispositivos Sourcefire
- Configuración de la pila en los dispositivos Cisco Firepower serie 8000

- Configuración de la agrupación en clústeres en dispositivos Cisco FirePOWER series 7000 y 8000

Funcionamiento del hardware

- Alertas de estado de la unidad de fuente de alimentación del sistema FireSIGHT
- Resolución de problemas con la gestión a distancia (LOM) en un FireSIGHT Management Center o un appliance FirePOWER
- El sistema FireSIGHT devuelve el mensaje "Error de entrada/salida"
- Un appliance FirePOWER se congela tras intentar arrancarlo en modo de usuario único
- Resolución de problemas con los ventiladores de un sistema FireSIGHT
- Realizar pruebas de diagnóstico desde el panel LCD de un appliance FirePOWER
- Inserción y extracción de un módulo de red (NetMod) en un appliance FirePOWER serie 8000
- Identificación de problemas con las tarjetas de motor de flujo de red en los appliances FirePOWER de Sourcefire series 7000 y 8000
- Preocupaciones habituales sobre el kit de raíles para appliances FirePOWER serie 8000
- Instrucciones de instalación del kit de raíles para dispositivos Firepower serie 7000
- Un modelo FireSIGHT Management Center FS4000 puede activar una alerta de estado de "degradación de disco"
- Procedimientos de reconfiguración de SSD/RAID para los modelos FS2000 y FS4000 de FireSIGHT Management Center

Descifrado SSL

- Recreación de imágenes de un appliance Sourcefire SSL 1500/2000 a la versión 3.6 o superior
- Obtener una contraseña de BIOS para un dispositivo SSL
- Procedimientos de captura de paquetes en un dispositivo SSL
- Configuración de SNMP en un dispositivo SSL
- Configuración del conjunto de reglas básico en un dispositivo SSL
- Configuración de una política de inspección SSL en el sistema Cisco FireSIGHT

Integración con ISE, Streamer, SIEM, agente de usuario, API y conector

- Iniciar sesión en un escritorio remoto mediante RDP cambia el usuario asociado a una dirección IP
- Solución de problemas entre el sistema FireSIGHT y eStreamer Client (SIEM)
- Instalación y desinstalación del agente de usuario de Sourcefire
- Solucionar problemas de conectividad con el agente de usuario de Sourcefire
- Configuración de un sistema FireSIGHT para enviar alertas a un servidor Syslog externo
- Conceder el permiso mínimo a una cuenta de usuario de Active Directory utilizada por el agente de usuario de Sourcefire
- El estado en tiempo real del agente de usuario se muestra como desconocido
- Generar datos de solución de problemas para el software Sourcefire que se ejecuta en la plataforma BlueCoat serie X
- Control de acceso basado en TrustSec con Firepower e ISE
- El servicio de base de datos del agente de usuario de Cisco Firepower no se reinicia tras una detención

Documentos del TAC sobre protección frente a malware avanzado

AMP para terminales, conector FireAMP

- Recopilación de datos de diagnóstico de un conector de FireAMP que se ejecuta en Windows
- Recopilación de datos de diagnóstico de un conector FireAMP que se ejecuta en Mac OSX
- Recopilación de datos de diagnóstico de un conector FireAMP que se ejecuta en Linux
- Crear una imagen o clonar un ordenador con el conector FireAMP instalado
- Configuración y administración de exclusiones en FireAMP
- Eliminación de la caché de FireAMP y los archivos de historial en Windows
- Switches de línea de comandos para el instalador del conector FireAMP
- Desactivar y activar el servicio de cliente del conector de FireAMP
- Ejecutar el servicio de cliente del conector de FireAMP en segundo plano y ocultar la interfaz de usuario
- Actualización de un conector FireAMP en sistemas operativos Windows
- El servicio del conector FireAMP no se detiene debido a la protección del conector
- Tipos de archivos analizados por el conector de FireAMP
- Guía de FireAMP para exclusiones en Windows
- Obtenga datos de solución de problemas en un dispositivo Android para problemas del conector móvil FireAMP
- Iniciar análisis programados en FireAMP/AMP para terminales
- Realización de análisis de indicadores de compromiso (IOC) de terminales con AMP para terminales o FireAMP
- Instalación y configuración del módulo AMP mediante AnyConnect 4.x y el habilitador AMP
- Implementación de Cisco AMP para terminales con persistencia de identidad
- Trabaje con los eventos de falsos positivos o falsos negativos de la protección frente a malware avanzado (AMP)
- Descripción general de la API de Cisco AMP para terminales

AMP para red

- Servidores necesarios para las operaciones de protección frente a malware avanzado (AMP)
- Solución de problemas de conectividad y registro con AMP en FireSIGHT Management Center
- Proceso para eliminar conexiones entre un FireSIGHT Management Center y una consola en la nube de FireAMP

Nube

- Instalación y configuración de la nube privada de FireAMP
- Generar un archivo de instantáneas de soporte en una nube privada de FireAMP
- Cargar un archivo en la consola de nube de FireAMP para ver los análisis de archivos recientes

Threat Grid

- Generar una instantánea de soporte en un appliance AMP Threat Grid