Administrador de dispositivo 5.1 del sistema de prevención de intrusiones - Firma del ajuste

Contenido

Introducción

El Sistema de prevención de intrusiones (IPS) 5.1 contiene sobre 1000 firmas predeterminadas del accesorio. Usted no puede retitular o borrar las firmas de la lista de firmas incorporadas, sino que usted puede retirar las firmas para quitarlas del motor de detección. Usted puede activar más adelante las firmas jubiladas. Sin embargo, este proceso requiere los motores de detección reconstruir su configuración, que toma tiempo y podría retrasar el proceso del tráfico. Usted puede ajustar las firmas incorporadas cuando usted ajusta varios parámetros de la firma. Las firmas incorporadas se han modificado que se llaman las *firmas ajustadas*.

Este documento ilustra los pasos para utilizar para ajustar la firma usando el administrador de dispositivo IPS (IDM). El IDM es un basado en web, la aplicación Java que le permite para configurar y para manejar su sensor. El servidor Web para el IDM reside en el sensor. Usted puede accederlo a través de los buscadores Web del Internet Explorer, de Netscape, o del Mozilla.

Nota: Usted puede crear las firmas, que se llaman las *firmas de encargo*. Los ID de la firma de encargo comienzan en 60000. Usted puede configurarlos para varias cosas, tales como corresponder con de las cadenas en las conexiones UDP, seguimiento de las inundaciones de la red, y exploraciones. Cada firma se crea usando un motor de firma diseñado específicamente para el tipo de tráfico se monitorea que.

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información en este documento se basa en el administrador de dispositivo 5.x del Cisco Intrusion Prevention System.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

Para configurar un sensor para monitorear el tráfico de la red para una firma determinada, usted debe habilitar la firma. Por abandono, se habilitan las firmas más críticas cuando usted instala la actualización de firma. Cuando se detecta un ataque que hace juego una firma habilitada, el sensor genera una alerta, que se salva en el almacén del evento del sensor. Las alertas, así como otros eventos, se pueden extraer del almacén del evento por los clientes basados en web. Por abandono, el sensor registra todas las alertas informativas o más arriba.

Algunas firmas tienen firmas secundarias. Es decir, la firma se divide en las subcategorías. Cuando usted configura una firma secundaria, los cambios realizados a los parámetros de una firma secundaria se aplican solamente a esa firma secundaria. Por ejemplo, si usted edita la firma secundaria 1 de la firma 3050 y cambia la gravedad, el cambio de la gravedad se aplica solamente a la firma secundaria 1 y no a 3050 2, 3050 3, y 3050 4.

Firmas del ajuste

A + el icono indica que más opciones están disponibles para este parámetro. Haga clic **+** icono para ampliar la sección y para ver los parámetros restantes.

Un icono verde indica que el parámetro utiliza actualmente el valor predeterminado. Haga clic el icono verde para cambiarlo al rojo, que activa el campo del parámetro así que usted puede editar el valor.

Procedimiento Paso a Paso

Complete estos pasos para ajustar las firmas:

1. Inicie sesión al IDM usando una cuenta con los privilegios del administrador o del operador.
2. Elija la **configuración > la definición de la firma > la configuración de la firma**.El cristal de la configuración de la firma aparece.
3. Para localizar una firma, elija una opción de clasificación del **selecto por la** lista.Por ejemplo, si usted busca para una firma de la inundación UDP, elija el **protocolo L2/L3/L4** y entonces las **inundaciones UDP**.El cristal de la configuración de la firma restaura y visualiza solamente

esas firmas que hagan juego sus criterios de clasificación.

4. Para ajustar una firma existente, seleccione la firma y complete estos pasos:El tecleo **edita** para abrir el cuadro de diálogo de la firma del editar.Revise los Valores de parámetro y cambie el valor de cualquier parámetro que usted quiera ajustar.**Nota:** Para elegir más de una acción del evento, mantenga la clave del **Ctrl**.Bajo estatus, elija **sí** habilitar la firma.**Nota:** La firma se debe habilitar para que el sensor detecte activamente el ataque especificado por la firma.Bajo estatus, especifique si se retira esta firma. Haga clic **no** para activar la firma. Esto coloca la firma en el motor.**Nota:** Una firma se debe activar para que el sensor detecte activamente el ataque especificado por la firma.**Nota:** Haga clic la **cancelación** para deshacer sus cambios y cerrar el cuadro de diálogo de la firma del editar.Haga clic en OK.La firma editada ahora aparece en la lista con el conjunto del tipo a ajustado.**Nota:** Si usted quiere deshacer sus cambios, haga clic la **restauración**.
5. El tecleo **se aplica** para aplicar sus cambios y para salvar la configuración revisada.

Información Relacionada

- Cisco Intrusion Prevention System
- Soporte Técnico y Documentación - Cisco Systems