Router y (SDM) y Cisco IOS CLI del Administrador de dispositivos de seguridad en el ejemplo de configuración del Cisco IOS Intrusion Prevention System (IPS)

Contenido

Introducción
prerrequisitos
Requisitos
Componentes Utilizados
Convenciones
Configurar
Cisco IOS IPS del permiso con un valor predeterminado de fábrica SDF
Añada las firmas al final del fichero adicionales después de habilitar el valor por defecto SDF
Seleccione las firmas y trabaje con las categorías de la firma
Ponga al día las firmas para los archivos predeterminados SDF
Información Relacionada

Introducción

En el (SDM) 2.2 de Router de Cisco y Administrador de dispositivo de seguridad, la configuración IPS del ® del Cisco IOS es integrada dentro de la aplicación del SDM. Le requieren no más iniciar una ventana separada para configurar el Cisco IOS IPS.

En el SDM 2.2 de Cisco, un nuevo asistente de configuración IPS le dirige a través del Cisco IOS necesario IPS del permiso de los pasos en el router. Además, usted puede todavía utilizar las opciones de configuración avanzada de habilitar, de inhabilitar, y de ajustar el Cisco IOS IPS con el SDM 2.2 de Cisco.

Cisco recomienda que usted funciona con el Cisco IOS IPS con los archivos de definición pretuned de la firma (SDFs): attack-drop.sdf, 128MB.sdf, y 256MB.sdf. Estos archivos se crean para el Routers con diversas cantidades de memoria. Los archivos se lían con el SDM de Cisco, que recomienda SDFs cuando usted primero habilita el Cisco IOS IPS en un router. Estos archivos se pueden también descargar de http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers solamente).

El proceso para habilitar el SDFs predeterminado se detalla en el Cisco IOS IPS del permiso con un valor predeterminado de fábrica SDF. Cuando el SDFs predeterminado no es suficiente o usted quiere agregar las nuevas firmas, usted puede utilizar el procedimiento descrito adentro añade las firmas al final del fichero adicionales después de habilitar el valor por defecto SDF.

prerrequisitos

Requisitos

La versión 1.4.2 o posterior del Entorno de tiempo de ejecución Java (JRE) se requiere para utilizar el SDM 2.2 de Cisco. Un archivo de firma Cisco-recomendado y ajustado (basado en el DRAM) se lía con el SDM de Cisco (cargado en la memoria de memoria Flash del router con el SDM de Cisco).

Componentes Utilizados

La información en este documento se basa en el (SDM) 2.2 de Router de Cisco y Administrador de dispositivo de seguridad.

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 Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

Cisco IOS IPS del permiso con un valor predeterminado de fábrica SDF

Procedimiento CLI

Complete este procedimiento para utilizar el CLI para configurar a un Cisco 1800 Series Router con el Cisco IOS IPS para cargar 128MB.sdf en memoria Flash del router.

1. Configure al router para habilitar la notificación de evento del intercambio del evento del dispositivo de seguridad (SDEE).`yourname#`**`conf t`**
2. Ingrese los comandos configuration (uno por la línea), y después presione Cntl+Z para terminar.`yourname(config)#`**`ip ips notify sdee`**
3. Cree un nombre de la regla IPS que se utilice para asociarse a las interfaces.`yourname(config)#`**`ip ips name myips`**
4. Configure un comando location IPS de especificar de qué archivo leerá el sistema IPS del Cisco IOS las firmas.Este ejemplo utiliza el archivo en el flash: 128MB.sdf. La porción de la ubicación URL de este comando puede ser cualquier URL válido que utilice el flash, el disco, o los protocolos vía el FTP, el HTTP, el HTTPS, el RTP, SCP, y el TFTP para señalar a los archivos.`yourname(config)#`**`ip ips sdf location flash:128MB.sdf`** **Nota:** Usted debe habilitar el **comando terminal monitor** si usted configura al router vía una sesión telnet o usted no ve los mensajes SDEE cuando el motor de firma está construyendo.
5. Habilite el IPS en la interfaz donde usted quiere permitir al Cisco IOS IPS para analizar el tráfico. En este caso, habilitamos en las ambas direcciones en el FastEthernet 0 de la

interfaz.
```
yourname(config)#interface fastEthernet 0
yourname(config-if)#ip ips myips in
*Oct 26 00:32:30.297: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl
*Oct 26 00:32:30.921: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from flash:128MB.sdf
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_READY: OTHER - 0 ms - packets for this engines will be scanned
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new
signature definitions for this engine
*Oct 26 00:32:30.921: %IPS-6-ENGINE_BUILDING:
STRING.ICMP - 1 signatures - 3 of 15 engines
*Oct 26 00:32:30.941: %IPS-6-ENGINE_READY:
STRING.ICMP - 20 ms - packets for this engine will be scanned
*Oct 26 00:32:30.945: %IPS-6-
ENGINE_BUILDING: STRING.UDP - 17 signatures - 4 of15 engines
*Oct 26 00:32:31.393: %IPS-6-
ENGINE_READY: STRING.UDP - 448 ms - packets for this engine will be scanned
*Oct 26
00:32:31.393: %IPS-6-ENGINE_BUILDING: STRING.TCP - 58 signatures - 5 of 15 engines
*Oct 26
00:32:33.641: %IPS-6-ENGINE_READY: STRING.TCP - 2248 ms - packets for this engine will be
scanned
*Oct 26 00:32:33.641: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15
engines
*Oct 26 00:32:33.657: %IPS-6-ENGINE_READY: SERVICE.FTP - 16 ms - packets for this
engine will be scanned
*Oct 26 00:32:33.657: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2
signatures - 7 of 15 engines
*Oct 26 00:32:33.685: %IPS-6-ENGINE_READY: SERVICE.SMTP - 28
ms - packets for this engine will be scanned
*Oct 26 00:32:33.689: %IPS-6-ENGINE_BUILDING:
SERVICE.RPC - 29 signatures - 8 f 15 engines
*Oct 26 00:32:33.781: %IPS-6-ENGINE_READY:
SERVICE.RPC - 92 ms - packets for this engine will be scanned
*Oct 26 00:32:33.781: %IPS-6-
ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines
*Oct 26 00:32:33.801: %IPS-
6-ENGINE_READY: SERVICE.DNS - 20 ms - packets for this engine will be scanned
*Oct 26
00:32:33.801: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures - 10 of 15 engines
*Oct
26 00:32:44.505: %IPS-6-ENGINE_READY: SERVICE.HTTP - 10704 ms - packets for this engine
will be scanned
*Oct 26 00:32:44.509: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures -
11 of 15 engines
*Oct 26 00:32:44.513: %IPS-6-ENGINE_READY: ATOMIC.TCP - 4 ms - packets for
this engine will be scanned
*Oct 26 00:32:44.513: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9
signatures - 12 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.UDP - 4 ms
- packets for this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING:
ATOMIC.ICMP - 0 signatures - 13 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-
ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15
engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.IPOPTIONS - 0 ms - packets for
this engine will be scanned
*Oct 26 00:32:44.517: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5
signatures - 15 of 15 engines
*Oct 26 00:32:44.517: %IPS-6-ENGINE_READY: ATOMIC.L3.IP - 0
ms - packets for this engine will be scanned
yourname(config-if)#ip ips myips out
yourname(config-if)#ip virtual-reassembly
```
La primera vez que una regla IPS se aplica a una interfaz, el comienzo IPS del Cisco IOS construyó las firmas del archivo especificado por el comando de las ubicaciones SDF. Los mensajes SDEE se registran a la consola y se envían al servidor de Syslog si están configurados. Los mensajes SDEE con el <number> de los motores del <number> indican el proceso de construcción del motor de firma. Finalmente, cuando los dos números son lo mismo, se construyen todos los motores.**Nota:** El nuevo ensamble virtual IP es una característica de la interfaz que (cuando está girado) automáticamente vuelve a montar los paquetes fragmentados que entran en al router a través de esa interfaz. Cisco recomienda que usted habilita al virtual-ensamblaje del IP en todas las interfaces donde el tráfico entra en al router. En el ejemplo antedicho, además de girar al “virtual-ensamblaje del IP” en el FastEthernet 0 de la interfaz, lo configuramos en el VLAN1 de la interfaz interior también.
```
yourname(config)#int vlan 1
yourname(config-if)#ip virtual-reassembly
```

Procedimiento del SDM 2.2

Complete este procedimiento para utilizar el SDM 2.2 de Cisco para configurar a un Cisco 1800 Series Router con el Cisco IOS IPS.

1. En la aplicación del SDM, haga clic la **configuración**, y después haga clic la **prevención de intrusiones**.

2. Haga clic la lengueta **IPS del crear**, y después haga clic al **Asisitente de la regla IPS del lanzamiento**.El SDM de Cisco requiere la notificación de evento IPS vía SDEE para configurar la característica IPS del Cisco IOS. Por abandono, la notificación SDEE no se habilita. El SDM de Cisco le indica a que habilite la notificación de evento IPS vía SDEE tal y como se muestra en de esta imagen:
3. Haga clic en OK.La recepción a la ventana del Asistente de las directivas IPS del cuadro de diálogo del Asisitente de las directivas IPS aparece.
4. Haga clic en Next (Siguiente).La ventana selecta de las interfaces aparece.
5. Elija las interfaces para las cuales usted quiere habilitar el IPS, y haga clic o el **entrante** o **Casilla de selección saliente** para indicar la dirección de esa interfaz.**Nota:** Cisco recomienda que usted habilita entrante y a las direcciones salientes cuando usted habilita el IPS en una interfaz.
6. Haga clic en Next (Siguiente).La ventana de las ubicaciones SDF aparece.
7. El tecleo **agrega** para configurar una ubicación SDF.El agregar un cuadro de diálogo de la ubicación de la firma aparece.
8. Haga clic el **especificar SDF en el** botón de radio **de destello**, y elija 256MB.sdf del **nombre del archivo en la** lista desplegable **de destello**.
9. Haga clic el checkbox del **salvar automáticamente**, y haga clic la **AUTORIZACIÓN**.**Nota:** La opción del salvar automáticamente salva automáticamente el archivo de firma cuando hay un cambio de la firma.La ventana de las ubicaciones SDF visualiza la nueva ubicación SDF.**Nota:** Usted puede agregar las ubicaciones adicionales de la firma para señalar un respaldo.
10. Haga clic la casilla de verificación **incorporada de las firmas del uso (como respaldo)**.**Nota:** Cisco recomienda que usted no utiliza la opción incorporada de la firma a menos que usted haya especificado una o más ubicaciones.
11. Tecleo **después** para continuar.La ventana de resumen aparece.
12. Haga clic en Finish (Finalizar).El cuadro del cuadro de diálogo de estado de la salida de los comandos visualiza el estatus mientras que el motor IPS compila todas las firmas.
13. Una vez que el proceso es completo, haga clic la **AUTORIZACIÓN**.El cuadro del cuadro de diálogo de estado de la compilación de la firma visualiza la información de la compilación de la firma.Esta información muestra se han compilado qué motores y el número de firmas en ese motor. Para los motores que visualizan *saltado* en la Columna de estado, no hay firma cargada para ese motor.
14. Tecleo **cercano** para cerrar el cuadro del cuadro de diálogo de estado de la compilación de la firma.
15. Para verificar qué firmas se cargan actualmente en el router, haga clic la **configuración**, y después haga clic la **prevención de intrusiones**.
16. Haga clic la lengueta **IPS del editar**, y después haga clic las **firmas**.La lista de firma IPS aparece en la ventana de las firmas.

Añada las firmas al final del fichero adicionales después de habilitar el valor por defecto SDF

Procedimiento CLI

No hay comando CLI disponible crear las firmas o leer la información de firma del archivo distribuido IOS-Sxxx.zip. Cisco recomienda que usted utiliza el SDM o el centro de administración para los sensores IPS para manejar las firmas en los sistemas IPS del Cisco IOS.

Para los clientes que tienen un archivo de firma listo y quieren ya combinar este archivo con el SDF que se ejecuta en un sistema IPS del Cisco IOS, usted puede utilizar este comando:

```
yourname#show running-config | include ip ips sdf ip ips sdf location flash:128MB.sdf yourname#
```

El archivo de firma definido por el comando location de la firma es donde el router carga los archivos de firmas cuando recarga o cuando se configura de nuevo el IOS IPS del router. Para que el proceso de combinación sea acertado, el archivo definido por el comando location del archivo de firma debe también ser actualizado.

1. Utilice el **comando show** para marcar las ubicaciones actualmente configuradas de la firma.La salida muestra las ubicaciones configuradas de la firma. Este comando muestra de donde se cargan las firmas corrientes actuales.`yourname#show ip ips signatures Builtin signatures are configured` Las firmas eran último cargado de flash:128MB.sdfVersión S128.0 de Cisco SDFVersión V0.0 de la tendencia SDF
2. Utilice el comando **IPS-sdf del <url> de la copia**, junto con la información del paso anterior, para combinar los archivos de firma.`yourname#copy tftp://10.10.10.5/mysignatures.xml ips-sdf Loading mysignatures.xml from 10.10.10.5 (via Vlan1): ! [OK - 1612 bytes] *Oct 26 02:43:34.904: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from opacl No entry found for lport 55577, fport 4714 No entry found for lport 51850, fport 4715 *Oct 26 02:43:34.920: %IPS-6-SDF_LOAD_SUCCESS: SDF loaded successfully from tftp://10.10.10.5/mysignatures.xml *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: OTHER - 4 signatures - 1 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: OTHER - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: MULTI-STRING - 0 signatures - 2 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: MULTI-STRING - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.ICMP - 1 signatures - 3 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.ICMP - there are no new signature definitions for this engine *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILDING: STRING.UDP - 17 signatures - 4 of 15 engines *Oct 26 02:43:34.920: %IPS-6-ENGINE_BUILD_SKIPPED: STRING.UDP - there are no new signature definitions for this engine *Oct 26 02:43:34.924: %IPS-6-ENGINE_BUILDING: STRING.TCP - 59 signatures - 5 of 15 engines *Oct 26 02:43:36.816: %IPS-7-UNSUPPORTED_PARAM: STRING.TCP 9434:0 CapturePacket=False - This parameter is not supported *Oct 26 02:43:37.264: %IPS-6-ENGINE_READY: STRING.TCP - 2340 ms - packets for this engine will be scanned *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.FTP - 3 signatures - 6 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.FTP - there are no new signature definitions for this engine *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.SMTP - 2 signatures - 7 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.SMTP - there are no new signature definitions for this engine *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILDING: SERVICE.RPC - 29 signatures - 8 of 15 engines *Oct 26 02:43:37.288: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.RPC - there are no new signature definitions for this engine *Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILDING: SERVICE.DNS - 31 signatures - 9 of 15 engines *Oct 26 02:43:37.292: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.DNS - there are no new signature definitions for this engine *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILDING: SERVICE.HTTP - 132 signatures - 10 of 15 engines *Oct 26 02:43:37.296: %IPS-6-ENGINE_BUILD_SKIPPED: SERVICE.HTTP - there are no new signature definitions for this engine *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.TCP - 11 signatures - 11 of 15 engines *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.TCP - there are no new signature definitions for this engine *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILDING: ATOMIC.UDP - 9 signatures - 12 of 15 engines *Oct 26 02:43:37.316: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.UDP - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.ICMP - 0 signatures - 13 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.ICMP - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.IPOPTIONS - 1 signatures - 14 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.IPOPTIONS - there are no new signature definitions for this engine *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILDING: ATOMIC.L3.IP - 5 signatures - 15 of 15 engines *Oct 26 02:43:37.320: %IPS-6-ENGINE_BUILD_SKIPPED: ATOMIC.L3.IP - there are no new signature definitions for this engine yourname#` Después de que usted publique el **comando copy**, el router carga el archivo de

firma en la memoria y después construye los motores de firma. En la salida del mensaje de la consola SDEE, el estatus del edificio para cada motor de firma se visualiza.%IPS-6-ENGINE_BUILD_SKIPPED indica que no hay nuevas firmas para este motor.%IPS-6-ENGINE_READY indica que hay nuevas firmas y el motor está listo. Como antes, el "15 mensaje de 15 motores" indica que se han construido todos los motores.IPS-7-UNSUPPORTED_PARAM indica que cierto parámetro no es soportado por el Cisco IOS IPS. Por ejemplo, CapturePacket y ResetAfterIdle.**Nota:** Estos mensajes están para la información solamente y no tendrán ninguna influencia en la capacidad o el funcionamiento de la firma IPS del Cisco IOS. Estos mensajes de registración pueden ser apagados fijando el nivel de registro más alto que el debugging (nivel 7).

3. Ponga al día el SDF definido por el comando location de la firma, tales que cuando las recargas de router, él tendrán el conjunto de firmas combinado con las firmas actualizadas. Este ejemplo muestra la diferencia del tamaño del archivo después de que la firma combinada se guarde al archivo Flash 128MB.sdf.`yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 504630 Aug 30 2005 22:58:34 +00:00 128MB.sdf yourname#`**`copy ips-sdf flash:128MB.sdf`** `yourname#`**`show flash:`** `-#- --length-- -----date/time------ path 4 522656 Oct 26 2005 02:51:32 +00:00 128MB.sdf` **Advertencia:** El nuevo 128MB.sdf ahora contiene las firmas cliente-combinadas. El contenido es diferente predeterminado de Cisco del archivo 128MB.sdf. Cisco recomienda que usted cambia este archivo a un nombre diferente para evitar la confusión. Si se cambia el nombre, el comando location de la firma necesita ser cambiado también.

Procedimiento del SDM 2.2

Después de que se haya habilitado el Cisco IOS IPS, las nuevas firmas se pueden agregar en el router que funciona con un conjunto de firmas con la función de la importación del SDM de Cisco. Complete estos pasos para importar las nuevas firmas:

1. Elija el SDFs predeterminado o el archivo de la actualización IOS-Sxxx.zip para importar las firmas adicionales.
2. Haga clic la **configuración**, y después haga clic la **prevención de intrusiones**.
3. Haga clic la lengueta **IPS del editar**, y después haga clic la **importación**.
4. Elija del **PC de la** lista desplegable de la importación.
5. Seleccione el archivo del cual usted quiere importar las firmas.Este ejemplo utiliza la última actualización descargada del cisco.com y guardada en PC local el disco duro.
6. Tecleo **abierto**.**Advertencia:** Debido a la restricción de memoria, solamente un número limitado de nuevas firmas se puede agregar encima de las firmas que se han desplegado ya. Si se seleccionan demasiadas firmas, el router no pudo poder cargar todas las nuevas firmas debido a la falta de memoria.Una vez que la carga del archivo de firma completa, el cuadro de diálogo de la importación IPS aparece.
7. Navegue con la vista de árbol izquierda, y haga clic la casilla de verificación de la **importación** al lado de las firmas que usted quiere importar.
8. Haga clic el botón de radio de la **fusión**, y después haga clic la **AUTORIZACIÓN**.**Nota:** La opción del reemplace substituye el conjunto de firmas actual en el router por las firmas que usted selecciona para importar.Una vez que usted hace clic la AUTORIZACIÓN, la aplicación del SDM de Cisco entrega las firmas al router.**Nota:** CPU elevada la utilización ocurre durante la compilación y el cargamento de las firmas. Después de que el Cisco IOS IPS se habilite en la interfaz, el archivo de firma comienza a cargar. El router tarda cerca de cinco minutos para cargar el SDF. Usted puede intentar utilizar el **comando show process cpu** para ver la utilización de la CPU del Cisco IOS Software CLI. Sin embargo, no intente

utilizar los comandos adicionales o cargar el otro SDFs mientras que el router está cargando el SDF. Esto puede hacer el proceso de la compilación de la firma durar para completar (puesto que la utilización de la CPU está cercana a la utilización 100-percent a la hora de cargar el SDF). Usted puede ser que necesite hojear a través de la lista de firmas y habilitar las firmas si no están en el estado *habilitado*.El número total de la firma ha aumentado a 519. Este número incluye todas las firmas disponibles en el archivo IOS-S193.zip que pertenecen a la subcategoría de la capacidad de compartir archivos.

Para más temas más complejos sobre cómo utilizar el SDM de Cisco para manejar la característica IPS del Cisco IOS, refiera a la documentación del SDM de Cisco en este URL:

Seleccione las firmas y trabaje con las categorías de la firma

Para determinar cómo seleccionar con eficacia las firmas correctas para una red, usted debe conocer algunas cosas sobre la red que usted está protegiendo. La información actualizada de la categoría de la firma en el SDM 2.2 de Cisco y posterior fomenta a los clientes de la ayuda para seleccionar el conjunto correcto de las firmas para proteger la red.

La categoría es una manera de agrupar las firmas. Ayuda a estrechar abajo la selección de la firma a un subconjunto de firmas que sean relevantes el uno al otro. Una firma podría pertenecer a solamente una categoría o podría pertenecer a las categorías múltiples.

Éstas son las cinco categorías a nivel superior:

- OS — clasificación Operación-sistema-basada de la firma
- Ataque — clasificación Ataque-basada de la firma
- Servicio — Clasificación basada en el servicio de la firma
- Protocolo de la capa 2-4 — clasificación Protocolo-nivel-basada de la firma
- Versiones — clasificación Versión-basada de la firma

Cada uno de estas categorías se divide más a fondo en las subcategorías.

Como un ejemplo, considere una red doméstica con una conexión de banda ancha a Internet y un túnel VPN a la red corporativa. El router de banda ancha tiene Firewall Cisco IOS habilitado en la conexión abierta (NON-VPN) a Internet para evitar que cualquier conexión sea originada de Internet y que conectada con la red doméstica. Se permite todo el tráfico que origina de la red doméstica a Internet. Asuma que el usuario utiliza un PC basado en Windows y utiliza las aplicaciones como el HTTP (exploración de la Web) y el email.

Poder configurar el Firewall para solamente las aplicaciones que las necesidades de usuario están permitidas atravesar al router. Esto controlará el flujo de tráfico indeseado y potencialmente malo que puede separarse en la red. Considere que el usuario casero no necesita ni utiliza un servicio específico. Si ese servicio se permite atravesar el Firewall, hay un agujero potencial que un ataque puede utilizar para fluir en la red. Las mejores prácticas permiten solamente los servicios que son necesarios. Ahora, es más fácil seleccionar qué firmas a habilitar. Usted necesita habilitar las firmas solamente para los servicios que usted permite atravesar el Firewall. En este ejemplo, los servicios incluyen el email y el HTTP. El SDM de Cisco simplifica esta configuración.

Para utilizar la categoría para seleccionar las firmas requeridas, elija el **servicio > el HTTP**, y habilite todas las firmas. Este proceso de selección también trabaja en el diálogo de la importación de la firma, donde usted puede seleccionar todas las firmas HTTP e importarlas en su router.

Las categorías adicionales que necesitan ser seleccionadas incluyen el DNS, NETBIOS/SMB, el HTTPS, y el S TP.

Firmas de la actualización para los archivos predeterminados SDF

El SDFs por-construido tres (attack-drop.dsf, 128MB.sdf, y 256MB.sdf) se fija actualmente en el cisco.com en http://www.cisco.com/pcgi-bin/tablebuild.pl/ios-sigup (registeredcustomers solamente). Las versiones más recientes de estos archivos serán fijadas tan pronto como estén disponibles. Para poner al día al Routers que funciona con el Cisco IOS IPS con estos valor por defecto SDFs, va al sitio web y descarga las últimas versiones de estos archivos.

Procedimiento CLI

1. Copie los archivos descargados a la ubicación del donde configuran al router para cargar estos archivos. Para descubrir dónde configuran al router actualmente, utilice los ejecutar-**config de la demostración | en el** comando del **sdf IPS del IP**.`Router#show running-config | in ip ips sdf ip ips sdf location flash://256MB.sdf autosave` En este ejemplo, el router utiliza 256MB.sdf en el flash. El archivo es actualizado cuando usted copia el nuevo 256MB.sdf descargado a memoria Flash del router.
2. Recargue el subsistema IPS del Cisco IOS para funcionar con los nuevos archivos.Hay dos maneras de recargar el Cisco IOS IPS: recargue al router o configure de nuevo el Cisco IOS IPS para accionar el subsistema IOS IPS para recargar las firmas. Para configurar de nuevo el Cisco IOS IPS, quite todas las reglas IPS de las interfaces configuradas, y después reaplique las reglas IPS de nuevo a las interfaces. Esto accionará el sistema IPS del Cisco IOS para recargar.

Procedimiento del SDM 2.2

Complete estos pasos para poner al día el SDFs predeterminado en el router:

1. Haga clic la **configuración**, y después haga clic la **prevención de intrusiones**.
2. Haga clic la lengueta **IPS del editar**, y después haga clic las **configuraciones globales**.El top del UI muestra las configuraciones globales. La en el centro de la parte inferior del UI muestra las ubicaciones actualmente configuradas SDF. En este caso, el archivo 256MB.sdf de memoria flash se configura.
3. Elija la **administración de archivos del** menú de archivos.El cuadro de diálogo de la administración de archivos aparece.
4. **Archivo de la carga del** tecleo del **PC**.El cuadro de diálogo del archivo de la salvaguardia aparece.
5. Elija el SDF que necesita ser puesto al día, y haga clic **abierto**.El mensaje de advertencia del SDM aparece.
6. Tecleo **sí** para substituir el archivo existente.Un cuadro de diálogo visualiza el progreso del proceso de la carga.
7. El proceso de la carga es una vez completo, las **firmas de la recarga del** tecleo situadas en la barra de herramientas de la ubicación SDF. Esta acción recarga el Cisco IOS IPS.**Nota:** El paquete IOS-Sxxx.zip contiene todas las firmas que el Cisco IOS IPS soporte. Las actualizaciones a este paquete de la firma se fijan en el cisco.com tan pronto como estén disponibles. Para poner al día las firmas contenidas en este paquete, vea Step2.

Información Relacionada

- Cisco Intrusion Prevention System
- Field Notice de seguridad del producto (CiscoSecure Intrusion Detection incluyendo)
- Soporte Técnico - Cisco Systems