Prácticas recomendadas de Secure Firewall Content Update Scheduling

Problema

Las organizaciones que gestionan dispositivos de defensa frente a amenazas de firewall (FTD) con Firewall Management Center (FMC) necesitan orientación sobre las prácticas recomendadas para aplicar actualizaciones de contenido y seguridad. Específicamente, existe incertidumbre acerca de la frecuencia con la que deben aplicarse los diferentes tipos de actualizaciones, si las actualizaciones se pueden programar en lugar de aplicar inmediatamente y cuáles son los impactos operativos de estas actualizaciones. La pregunta surge porque Cisco publica actualizaciones de contenido con frecuencia, a veces semanalmente, y los administradores necesitan saber si estas actualizaciones deben aplicarse inmediatamente después del lanzamiento o si pueden programarse según las ventanas de mantenimiento de la organización y las políticas de gestión de cambios.

Entorno

- Cisco Secure Firewall Firepower, todas las versiones
- Firepower Management Center, todas las versiones

Resolución

Esta tabla muestra el propósito de cada tipo de actualización en Firepower.

Tipo de actualización	Propósito	Notas
SRU/LSP	Actualizaciones de reglas de intrusión (Snort 2 y Snort 3, respectivamente)	Mantiene reglas de detección/prevención de intrusiones

GeoDB	Datos de geolocalización para direcciones IP	Se utiliza para el filtrado de tráfico basado en geolocalización
VDB	Información sobre vulnerabilidades e impresiones dactilares de hosts	Se utiliza para la evaluación de vulnerabilidades y el análisis de riesgos

Las actualizaciones de contenido de Cisco Secure Firewall se clasifican en tres tipos distintos, cada uno con diferentes frecuencias de versión y prácticas de programación recomendadas. En esta tabla se describen las recomendaciones de programación de prácticas recomendadas para cada tipo de actualización:

Tipo de actualización	Frecuencia de lanzamiento	Programación sugerida	Programación predeterminada de FMC	Ruta De Navegación (Para Modificar)
SRU/LSP	Frecuente	Diario	Diario	System > Content Updates > Rule Updates
GeoDB	~Semanalmente	Semanalmente	Semanalmente	System > Content Updates > Geolocation Updates
VDB	~Mensual	Semanalmente	Semanalmente	Sistema > Herramientas: Programación > Descarga semanal de software

Para conseguir una condición y una configuración de seguridad óptimas, se recomienda aplicar cualquiera de estas actualizaciones en cuanto Cisco las publique. Algunos de estos archivos de actualización pueden ser bastante grandes y es necesario considerar las asignaciones de ancho de banda. Se recomienda instalar las actualizaciones de mayor tamaño fuera de las horas de tráfico máximo, si se utiliza la misma red.

Actualizaciones de SRU/LSP (Intrusion Rules)

Las actualizaciones de reglas de Snort (SRU) y los paquetes de seguridad ligeros (LSP) contienen reglas de detección y prevención de intrusiones. Estas actualizaciones deben aplicarse con la mayor frecuencia posible desde el punto de vista operativo para mantener la protección frente a las amenazas emergentes.

Para modificar la programación SRU/LSP: Vaya a System > Content Updates > Rule Updates en la interfaz de FMC para ajustar la configuración de la hora, la fecha y la frecuencia.

Las actualizaciones de SRU/LSP admiten una implementación automatizada y se pueden programar para que se implementen automáticamente después de la descarga y la instalación.

Actualizaciones de GeoDB (base de datos de geolocalización)

Las actualizaciones de la base de datos de geolocalización proporcionan datos de ubicación geográfica actuales para las direcciones IP y, por lo general, se publican semanalmente.

Para modificar la programación de GeoDB: Vaya a System > Content Updates > Geolocation Updates en la interfaz de FMC para ajustar los parámetros de programación.

Las actualizaciones de GeoDB se pueden programar para su descarga e instalación, pero la implementación en los dispositivos administrados requiere una pulsación manual y no se pueden automatizar completamente como las actualizaciones de SRU/LSP.

Actualizaciones de VDB (base de datos de vulnerabilidades)

Las actualizaciones de la base de datos de vulnerabilidades se publican aproximadamente mensualmente y se gestionan como actualizaciones de software en lugar de como actualizaciones de contenido.

Para modificar la programación de VDB: Vaya a Sistema > Herramientas: Programación y modificación de la tarea Descarga semanal de software para ajustar la frecuencia y el tiempo de descarga.

Las actualizaciones de VDB se incluyen en las actualizaciones de software y no se pueden implementar de forma independiente. Se incluyen cuando se realizan implementaciones manuales que compilan todos los cambios pendientes.

Consideraciones de implementación

Al implementar actualizaciones, FMC compila todos los cambios de configuración pendientes y puede incluir varios tipos de actualizaciones de contenido en una única operación de implementación. Algunas actualizaciones pueden provocar breves reinicios del servicio Snort durante la implementación, lo que debe tenerse en cuenta al programar actualizaciones durante las horas de producción.

Las organizaciones deben alinear los programas de actualización con sus políticas de gestión de cambios y considerar la programación de actualizaciones durante los períodos de mantenimiento si las breves interrupciones de servicio son una preocupación para su entorno operativo.

Causa

Se trataba de una solicitud de orientación operativa y de configuración en lugar de un mal funcionamiento técnico. La necesidad de clarificación surgió de la incertidumbre sobre las prácticas de programación de actualizaciones, las capacidades de automatización y el impacto operativo de los diferentes tipos de actualizaciones de contenido en los entornos de Cisco Secure Firewall.

Contenido relacionado

- Guía de administración de Cisco Secure Firewall Management Center, 7.6: Actualizaciones
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).