Entienda cómo la característica automática de la actualización de firma del IPS de Cisco trabaja

Contenido

Introducción

Este documento proporciona a una descripción de la característica automática de la actualización del Cisco Intrusion Prevention System (IPS) y de su operación.

La característica automática de la actualización IPS fue introducida en la versión 6.1 IPS y provee de los administradores una forma sencilla de poner al día las firmas IPS en un intervalo regularmente programado.

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Las actualizaciones de firma requieren una suscripción y una llave de la licencia válidas de los Servicios de Cisco para IPS. Vaya a http://www.cisco.com/go/license y haga clic el **servicio de la suscripción de la firma IPS** para solicitar una llave de la licencia.
- Una cuenta de usuario de Cisco.com (CCO) que se asocia a una suscripción activa de los Servicios de Cisco para IPS.
- Privilegios de descargar el Software criptográfico. Vaya a: http://tools.cisco.com/legal/k9/controller/do/k9Check.x?eind=Y para controlar si usted tiene acceso.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software y hardware.

- Versiones 6.1 del IPS de Cisco y más adelante
- Características específicas para las versiones del IPS de Cisco 7.2(1), 7.3(1), y más adelante

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

Requisitos de la red

1. El comando y la interfaz de control del IPS requiere el acceso directo a Internet usando HTTPS (TCP 443) y HTTP (TCP 80).
2. El Network Address Translation (NAT) y el Listas de control de acceso (ACL) en los dispositivos de borde tales como Routers y Firewall necesitan ser configurados para permitir la Conectividad IPS a Internet.
3. Excluya el comando y la dirección IP de la interfaz de control de todos los filtros del contenido y talladoras del tráfico de la red.
4. La característica automática de la actualización utiliza los servidores proxy en 7.2(1) la versión certificada FIPS/CC. El resto de las versiones de software 6.x y 7.x no utilizan la actualización automática a través de un servidor proxy en este tiempo. 7.2(1) La versión incluye varios cambios al Secure Shell (SSH) del valor por defecto y a las configuraciones

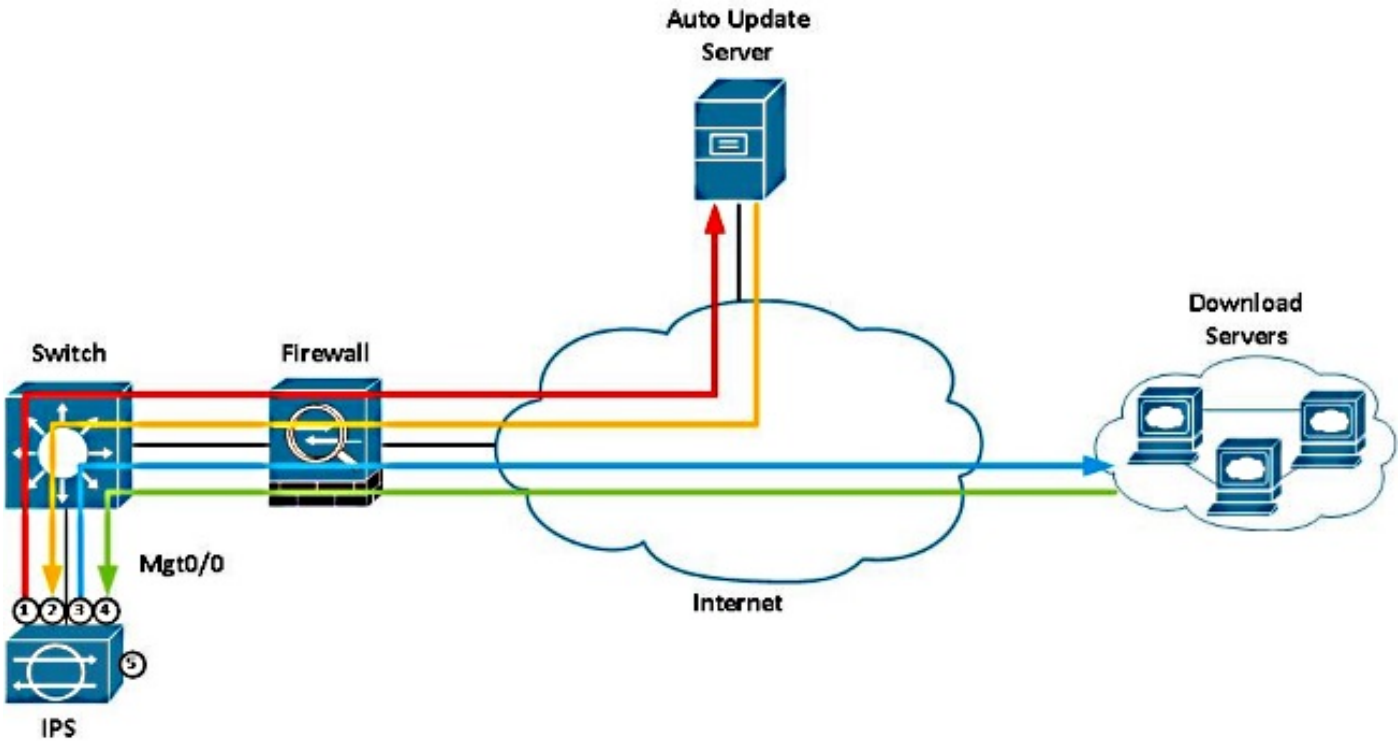
HTTPS. Refiera a los Release Note para el Cisco Intrusion Prevention System 7.2(1)E4 antes de que usted actualice a 7.2(1).

Advertencia: En la versión 7.0(8)E4 del IPS de Cisco, el valor predeterminado para la dirección IP del servidor de Cisco se cambia de 198.133.219.25 a 72.163.4.161 en la configuración auto de la actualización URL. Si su sensor se configura para las actualizaciones automáticas, usted puede ser que necesite poner al día las reglas de firewall para permitir que el sensor conecte con la nueva dirección IP. Para las versiones 7.2 del IPS de Cisco y más adelante, la dirección IP automática puesta en hard-code del servidor de actualización se substituye por un nombre de dominio completo (FQDN) y una búsqueda del Sistema de nombres de dominio (DNS) Nombrados. Refiera a la sección de configuración de este documento para la información adicional.

Desvíe las advertencias

Algunas actualizaciones de firma requieren las tablas de la expresión normal recompiled mientras tanto el IPS puede entrar el modo de desvío del software. Para los sensores en línea con el modo de desvío fijado al auto, se desvía el motor del análisis permitiendo que el tráfico atraviese los interfaces en línea y los pares en línea del VLA N sin el examen. Si fijan al modo de desvío a apagado, el sensor en línea para el pasar del tráfico mientras que la actualización es aplicada.

Proceso actualización del auto de la firma



1. El IPS autentica al servidor de actualización auto en 72.163.4.161 usando HTTPS (TCP 443).

2. El IPS envía a un cliente evidente al servidor de actualización auto, que incluye la identificación de la plataforma y un secreto compartido cifrado que el servidor utilice para

verificar la autenticidad del sensor del IPS de Cisco.

3. Una vez que está autenticado, el servidor de actualización responde con un servidor evidente que contenga una lista de opción de archivos de la transferencia directa asociada a la identificación de la plataforma. Los datos contenidos aquí incluyen relacionado con la información para poner al día la versión, la ubicación de la descarga, y los protocolos utilizados de la transferencia de archivos. De acuerdo con estos datos, la lógica auto de la actualización IPS determina si las opciones unas de los de la transferencia directa son válidas y después seleccionan el mejor paquete de actualización para la transferencia directa. Con objeto de la transferencia directa, el servidor provee del IPS un conjunto de las claves que se utilizarán para desencriptar el fichero de la actualización.

4. El IPS establece una nueva conexión al servidor de la transferencia directa identificado en el servidor evidente. La dirección IP del servidor de la transferencia directa varía, que es dependiente en la ubicación. El IPS utiliza el File Transfer Protocol definido en los datos URL de la transferencia directa del fichero aprendidos en el servidor evidente (actualmente las aplicaciones HTTP (TCP 80)).

5. El IPS utiliza las claves previamente descargadas para desencriptar el paquete de actualización y después aplica los archivos de firma al sensor.

Configurar

Configuración básica de la Auto-actualización de la firma

La característica automática de la actualización se puede configurar del administrador de dispositivos IPS (IDM) o del encargado IPS expreso (IME). Complete estos pasos:

1. De IDM/IME, elija la **Administración de la configuración > del sensor > la actualización del auto/Cisco.com.**