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

Contenido

Introducción

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

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

Prerequisites

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 marcar 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 posterior
- Características específicas para las versiones del IPS de Cisco 7.2(1), 7.3(1), y posterior

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. Los servidores proxy automáticos de los soportes de característica de la actualización en 7.2(1) la versión certificada FIPS/CC. El resto de las versiones de software 6.x y 7.x no soportan la actualización automática a través de un servidor proxy ahora. 7.2(1) La versión incluye varios cambios al Secure Shell (SSH) predeterminado 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 posterior, 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 las 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 Auto Update Server en 72.163.4.161 usando HTTPS (TCP 443).

2. El IPS envía a un cliente evidente al Auto Update Server, que incluye la plataforma ID 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 descarga asociada a la plataforma ID. Los datos contenidos aquí incluyen relacionado con la información para poner al día la versión, la ubicación de la descarga, y los protocolos soportados 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 descarga son válidas y después selecciona el mejor paquete de la actualización para la descarga. Con objeto de la descarga, el servidor proporciona el IPS con un conjunto de las claves que se utilizarán para desencriptar el archivo de la actualización.

4. El IPS establece una nueva conexión al servidor de la descarga identificado en el servidor evidente. El dirección IP del servidor de la descarga varía, que es dependiente en la ubicación. El IPS utiliza el File Transfer Protocol definido en los datos URL de la descarga del archivo 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 del automóvil Update Button de la firma

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

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

2. Elija las **actualizaciones de la firma y del motor del habilitar de la** casilla de verificación del **cisco.com** en el panel derecho, y haga clic en el título azul de los **servidores establezca de Cisco.com** para caer abajo el cristal de la configuración.

3. Ingrese el nombre de usuario y contraseña CCO.

   Aquí está un ejemplo URL para las versiones del IPS de Cisco 7.0(8) y 7.1(6):

   https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl

   Aquí está un ejemplo URL para las versiones del IPS de Cisco 7.2(1), 7.3(1), y posterior:

   https://www.cisco.com//cgi-bin/front.x/ida/locator/locator.pl

   Note: No cambie el cisco.com URL. No debe necesitar ser cambiado de su configuración predeterminada. //es intencional y no un error tipográfico. En las versiones del IPS de Cisco 7.2(1), 7.3(1), y posterior, el sensor pregunta al servidor DNS que se define en la configuración de red del sensor para resolver www.cisco.com URL a un IP Address de Internet rutable.

4. Configure una hora de inicio y una frecuencia para programar la actualización de firma. Se recomienda para fijar la hora de inicio a un tiempo aleatorio que no esté en el top de la hora. En este ejemplo, la hora se fija a 23:15:00. La frecuencia se puede configurar para soportar cada hora o la actualización diaria intenta. El tecleo **se aplica** para aplicar los cambios de configuración.

Mejoras automáticas de la actualización de la firma

Muchas mejoras a la característica automática de la actualización se incluyen en las versiones del IPS de Cisco 7.2(1) y posterior. Las mejoras de la seguridad complementaria también se agregan a las versiones del IPS de Cisco 7.3(2) y posterior. Refiera a las opciones de configuración descritas en esta sección para la información adicional.

Ahora ponga al día la característica

La versión 7.2(1) del IPS de Cisco introdujo una nueva capacidad al IPS GUI y el CLI que permite que los administradores inicien una actualización automática de la firma inmediatamente, que desvía la necesidad de esperar el horario programado de ocurrir.

Para desviar el horario de la actualización y la actualización automáticos inmediatamente, navegue al IDM/IME y elija la **Administración de la configuración > del sensor > la actualización del auto/del cisco.com. Mientras** la actualización automática se configure y se aplique correctamente, usted puede hacer clic el **botón de** UpdateNow en la esquina superior derecha de la pantalla para accionar una tentativa de la actualización.

Usted puede también ingresar el comando del **autoupdatenow** en el sensor CLI para accionar una tentativa de la actualización. Aquí tiene un ejemplo:

```
SSP-60# autoupdatenow
Warning: Executing this command will perform an auto-upgrade on the sensor immediately.
Before executing this command, you must have a valid license to apply the Signature
AutoUpdates and auto-upgrade settings configured.After executing this command please
disable user-server/cisco-server inside 'auto-upgrade' settings, if you don't want
scheduled auto-updates
Continue? []: yes
Automatic Update for the sensor has been executed.Use 'show statistics host' command
to check the result of auto-update.Please disable user-server/cisco-server in
auto-upgrade settings, if you don't want scheduled auto-updates
```

Actualización automática vía el proxy de Internet

Para accionar una actualización automática vía el proxy de Internet, navegue al IDM/IME y elija la **configuración > el sensor puestos > red**. Ingrese el DNS y (opcionalmente) el IP Address del servidor proxy HTTP y vire hacia el lado de babor:

Valide los Certificados de la Raíz confiable

La versión 7.3(2) del IPS de Cisco introdujo la capacidad para que el IPS valide el encadenamiento de certificado raíz del servidor del updater cuando se descargan las actualizaciones. Con esta característica habilitada, el IPS valida si el certificado raíz en la Cadena de certificados es firmado por una Raíz confiable CA por ejemplo, los certificados raíz de TLS que se obtienen en el proceso de la actualización de firma del servidor de Cisco y se valida el servidor global de la correlación. Esta característica se inhabilita actualmente por abandono en la versión 7.3(2) del IPS de Cisco; sin embargo, puede ser que sea habilitada por abandono en una futura versión. Refiera al IPS *me leen* archivo para más información.

Vea el almacén local del certificado confiable

Para ver el objeto list actual de los Certificados instalados de la Raíz confiable en las versiones IPS 7.3(2) y posterior, navega a la **Administración de la configuración > del sensor > a los Certificados > a los Certificados de la Raíz confiable**:

Validación estricta del certificado de servidor de TLS del permiso

Complete estos pasos para habilitar la característica estricta de la validación del servidor de TLS:

1. Navegue a la **configuración > al sensor puestos > red**.
2. Amplíe el **HTTP, el FTP, Telnet, SSH, el CLI y el** menú desplegable de las **otras opciones**.
3. Marque el cuadro de **comprobación de validación estricto del servidor de TLS del permiso**.
4. El tecleo **se aplica** para aplicar la configuración al sensor.

Agregue/los certificados raíz de la actualización al almacén local del certificado confiable

Mientras que los Certificados expiran en los servidores del updater, Cisco se reserva la derecha de utilizar un encadenamiento de certificado raíz con excepción de GeoTrust y de Thawte. Si el certificado actualizado no existe en la imagen del software actual IPS, después el encadenamiento de certificado raíz actualizado se puede instalar manualmente en el almacén local del certificado confiable del sensor. Los Certificados DER-codificados se pueden colocar en un servidor de archivos y extraer por el sensor vía SCP o el HTTPS. El próximo ejemplo utiliza SCP para demostrar la instalación del certificado/el proceso actualización.

1. Del IDM/IME, navegue a la **configuración > a la Administración > a SSH del sensor > las claves sabidas del host RSA**.
2. El tecleo **agrega** y ingresa el IP Address del servidor del SCP.
3. El tecleo **extrae la clave de host** para hacer que el sensor automáticamente extraiga la clave pública del servidor.
4. El Haga Click en OK dos veces y entonces **se aplica** para aplicar la configuración al sensor. **Note**: Una advertencia aparece si el tamaño de clave presentado por el servidor de SCP es más pequeño de 2,048 bits.
5. El tecleo **sí** para agregar la clave a los host sabidos presenta o **ningún** para volver a la pantalla **sabida agregar de la clave del host RSA**.
6. Navegue a los **Certificados de la configuración > de la Administración > de la Raíz confiable del sensor**.
7. El tecleo **agrega/actualización** para agregar un nuevo archivo de certificado DER-codificado del servidor de SCP. Asegúrese de que el archivo de certificado esté preposicionado en el

servidor y disponible para la extracción remota vía SSH.

8. Seleccione el **SCP** como el protocolo y ingrese el URL, el nombre de usuario, y la contraseña.

9. Haga Click en OK para comenzar la transferencia y la instalación de archivo de certificado.

10. Tecleo **sí** para agregar el certificado al almacén local de la Raíz confiable IPS y después **AUTORIZACIÓN** para salir.

Verificación

Del IDM/IME, elija la **Administración de la configuración > del sensor > la actualización del auto/del cisco.com. Amplíe la sección de información del** AutoUpdate para revisar el estatus de la tentativa más reciente de la descarga. **Haga clic la** orden de Refreshin para restaurar los **datos de la información del** AutoUpdate.

Para verificar el estatus del proceso actualización automático vía el CLI, ingrese el **comando host de las estadísticas de la demostración**:

```
IPS# show statistics host
<Output truncated>
Auto Update Statistics
lastDirectoryReadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Read directory: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
= Success
lastDownloadAttempt = 16:55:03 GMT-06:00 Wed Jun 27 2012
= Download: http://CCOUser@72.163.7.55//swc/esd/06/273556262/guest/
IPS-sig-S654-req-E4.pkg
= Success
nextAttempt = 17:55:00 GMT-06:00 Wed Jun 27 2012
lastInstallAttempt = 16:55:46 GMT-06:00 Wed Jun 27 2012
= Success
<Output truncated>
```

Del IDM/IME, refiera al gadget de la autorización en el panel casero para ver el estatus de la licencia y la versión de firma actualmente instalada. La misma información se puede obtener vía el CLI con el **comando show version**.

```
SSP-60# show version
Application Partition:

Cisco Intrusion Prevention System, Version 7.3(2)E4

Host:
Realm Keys key1.0
Signature Definition:
Signature Update S805.0 2014-06-03
Threat Profile Version 7
OS Version: 2.6.29.1
Platform: ASA5585-SSP-IPS60
```

```
Serial Number: JAF1527CPNK
Licensed, expires: 21-Jun-2014 UTC
Sensor up-time is 39 days.
Using 46548M out of 48259M bytes of available memory (96% usage)
system is using 32.4M out of 160.0M bytes of available disk space (20% usage)
application-data is using 86.6M out of 377.5M bytes of available disk space (24% usage)
boot is using 63.4M out of 70.5M bytes of available disk space (95% usage)
application-log is using 494.0M out of 513.0M bytes of available disk space (96% usage)

MainApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
AnalysisEngine C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CollaborationApp C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500
Running
CLI C-2014_04_14_22_11_7_3_1_48 (Release) 2014-04-14T22:15:32-0500

Upgrade History:

* IPS-sig-S802-req-E4 16:07:23 UTC Thu May 29 2014
IPS-sig-S805-req-E4.pkg 16:18:51 UTC Mon Jun 09 2014

Recovery Partition Version 1.1 - 7.3(2)E4

Host Certificate Valid from: 15-Jul-2013 to 16-Jul-2015
```

Troubleshooting

Después de la configuración correcta de la actualización de firma auto, complete estos pasos para aislar y corregir los problemas comúnmente encontrados:

1. Para todos los dispositivos y los módulos IPS a excepción de AIM y del IDSM, asegúrese de que el comando y la interfaz de control esté conectado con la red local, asignada un IP Address válido/una máscara de subred/un gateway, y tenga alcance IP a Internet. Para los módulos de AIM y IDSM, utilizan al comando virtual y la interfaz de control según lo definido en la configuración. Para confirmar el estado operacional de la interfaz del CLI, ingrese este comando show:

   ```
   IPS# show interfaces
   <Output truncated>
   MAC statistics from interface Management0/0
   Interface function = Command-control interface
   Description = Media Type = TX
   Default Vlan = 0
   Link Status = Up <---
   <Output truncated>
   ```

2. Para validar si la cuenta de usuario CCO tiene privilegios necesarios de descargar los paquetes de la actualización de firma, abra a un buscador Web y inicie sesión al cisco.com con esta misma cuenta CCO. Una vez que está autenticado, descargue manualmente el último paquete de la firma IPS. La incapacidad para descargar manualmente el paquete es probablemente a causa a la falta de asociación de la cuenta de usuario a una suscripción válida de los Servicios de Cisco para IPS. Además, el acceso al software de la Seguridad en el CCO se restringe a los usuarios autorizados que han validado el acuerdo anual del

cifrado/de la exportación. Han conocido al error aprobar este acuerdo prevenir las descargas de la firma de IDM/IME/CSM. Para verificar si se haya validado este acuerdo, abra a un navegador y inicie sesión al cisco.com con la misma cuenta CCO. ¿Una vez que está autenticado, intente descargar manualmente el Cisco IOS? paquete de software con el conjunto de características del k9.

3. Marque si hay un proxy en el lugar para el tráfico encuadernado de Internet (todas las versiones excepto 7.2(1) y posterior). Si el tráfico del comando y del puerto de control pasa con este proxy, la característica auto de la actualización no trabaja. Configure de nuevo la red para no filtrar el comando y el tráfico del puerto de control con un proxy y pruebe otra vez.

4. Para los sensores que funcionan con las versiones 7.2 o el software 7.3, asegúrese de que configuren a uno o más servidores DNS. Se requiere esto de modo que el sensor pueda resolver el updater FQDN de www.cisco.com a un IP Address de Internet rutable.

5. Marque si hay algún filtrado de contenido o aplicaciones o dispositivos del modelado de tráfico en la trayectoria a Internet. Si el presente, configura una exclusión para permitir la dirección IP del comando y de la interfaz de control de acceder Internet sin la restricción.

6. Si el tráfico ICMP se permite hacia Internet, abra el CLI del sensor IPS e intente hacer ping a un IP Address público.

   Esta prueba se puede utilizar para verificar si la encaminamiento necesaria y las reglas NAT (si está utilizado) se configuran correctamente. Si la prueba ICMP tiene éxito con todo las actualizaciones autos continúan fallando, asegúrese de que los dispositivos de red tales como Routers y Firewall a lo largo de la trayectoria permitan el HTTPS y a las sesiones HTTP del IP del comando y de la interfaz de control IPS. Por ejemplo, si la dirección IP del comando y del control es 10.1.1.1, una entrada ACL simple en un Firewall ASA puede parecer este ejemplo:

```
IPS# show interfaces
<Output truncated>
MAC statistics from interface Management0/0
Interface function = Command-control interface
Description = Media Type = TX
Default Vlan = 0
Link Status = Up <---
<Output truncated>
```

7. El nombre de usuario CCO no debe contener ninguna caracteres especiales, por ejemplo, @. Refiera al Id. de bug Cisco CSCsq30139 para más información.

8. Cuando ocurren los errores del automóvil Update Button de la firma, utilice la tabla siguiente para hacer juego los códigos de error de HTTP asociados.

```
IPS# show statistics host
```

```
Auto Update Statistics
lastDirectoryReadAttempt = 19:31:09 CST Thu Nov 18 2010
= Read directory: https://72.163.4.161//cgi-bin/front.x/ida/locator/locator.pl
= Error: AutoUpdate exception: HTTP connection failed [1,110] <--
lastDownloadAttempt = 19:08:10 CST Thu Nov 18 2010
lastInstallAttempt = 19:08:44 CST Thu Nov 18 2010
nextAttempt = 19:35:00 CST Thu Nov 18 2010
```

Mensaje	Significado
Error: Excepción del AutoUpdate: [1,110] fallado conexión HTTP	Autenticación fallada. Marque el nombre de usuario y contraseña.
excepción del AutoUpdate del status=false: Reciba [3,212] fallado HTTP de respuesta	La petición al Auto Update Server medido el tiempo hacia fuera.
Error: respuesta de error HTTP: 400	Aseegurese la configuración Cisco-URL se omite. Si el ID DE CCO es mayor de 32 cara de largo, intente un diverso ID DE CCO. Esto puede ser una limitación en el servidor de descarga de Cisco.
Error: Excepción del AutoUpdate: [1,0] fallado conexión HTTP	La descarga prevenida problema de red o allí es un problema potencial con los servidore descarga.