

Guías de consulta para descargar los datos del centro de administración de la potencia de fuego a los dispositivos administrados

Contenido

[Introducción](#)

[Guías de consulta generales de la descarga](#)

[Descargar las actualizaciones de software](#)

[Descargar las actualizaciones de base de datos de la vulnerabilidad](#)

[Descargar las actualizaciones de la directiva del control de acceso y de la regla de la intrusión](#)

[Descargar las listas url](#)

Introducción

Mantener un despliegue de la potencia de fuego requiere que usted descargue periódicamente los datos del centro de administración de la potencia de fuego a los dispositivos que maneja. Este documento proporciona la información que usted puede utilizar para transferir con éxito las actualizaciones del centro de administración de la potencia de fuego a los dispositivos administrados.

Guías de consulta generales de la descarga

Para soportar el funcionamiento diario de su sistema de la potencia de fuego, Cisco recomienda el mantener de un ancho de banda de la red dedicado por lo menos del kbps 256 entre la interfaz externa y cada dispositivo administrado. Esté seguro que el ancho de banda asignado entre el centro de administración de la potencia de fuego y el Switch que utiliza para comunicar con sus dispositivos administrados es suficiente soportar por lo menos el kbps 256 para cada dispositivo. El ancho de banda adicional puede ser requerido al descargar las actualizaciones de software del centro de administración de la potencia de fuego a un dispositivo administrado, o al simultáneamente descargar las actualizaciones de las políticas múltiples o de los datos a un dispositivo administrado.

Precaución: Descargar las actualizaciones a los dispositivos administrados puede afectar al examen del tráfico, al flujo de tráfico, y al estado del link. En el caso de las actualizaciones de software, se inhabilita el correlador de los datos mientras que una actualización está en curso. Por lo tanto Cisco le recomienda las actualizaciones de la descarga en una ventana de mantenimiento o en un momento en que la carga en el dispositivo administrado que es actualizado es mínima y una interrupción tendrá el menos impacto en su despliegue.

El tiempo requerido para realizar cualquier tipo de descarga de los datos del centro de administración de la potencia de fuego a un dispositivo administrado depende del tamaño del paquete de los datos y del ancho de banda de la red dedicado entre los dos dispositivos. Las descargas de los datos a los dispositivos administrados fallarán si no pueden completar dentro de los períodos de agotamiento del tiempo de espera señalados que la potencia de fuego aplica en

las actividades de la descarga.

Nota: Los requerimientos de ancho de banda citados en este documento suponen los links sin pérdidas entre los dispositivos; si su red experimenta la Latencia alta o las altas velocidades de pérdida del paquete, el ancho de banda adicional será requerido para completar las descargas dentro de los descansos que la potencia de fuego requiere.

Si después de ajustar su entorno de red usando la información en este documento usted no puede descargar un paquete de actualización a un dispositivo administrado dentro del período de agotamiento del tiempo de espera, entre en contacto el TAC de Cisco.

Descargar las actualizaciones de software

Los tamaños del paquete de la actualización de software varían extensamente; vea las *notas del Sistema XX, versión de la potencia de fuego* para su versión para el proceso actualización completo así como los datos empaquetar el tamaño. La potencia de fuego aplica un descanso de 1 hora a las descargas del software. La tabla siguiente proporciona las fórmulas para aproximar la cantidad de tiempo que una descarga del software tomará dependiendo del tamaño del paquete y del Ancho de banda dedicado disponible entre los dispositivos.

Tamaño del paquete	Hora de descargar en el kbps 256	Hora de descargar en 512 kbps	Hora de descargar en el 2 mbps	Hora de descargar el 3 mbps
X MB	segundos 32X	segundos 16X	segundos 4X	segundos 3X

Precaución: Porque el proceso actualización puede afectar al examen del tráfico, al flujo de tráfico, y al estado del link, y porque se inhabilita el correlador de los datos mientras que una actualización está en curso, Cisco le recomienda realiza la actualización de software en una ventana de mantenimiento o en un momento en que la interrupción tendrá el menos impacto en su despliegue.

Descargar las actualizaciones de base de datos de la vulnerabilidad

Las actualizaciones de base de datos de la vulnerabilidad se extienden de tamaño a partir del 30 al 70 MB. Descargar una actualización VDB del centro de administración de la potencia de fuego a un dispositivo administrado falla si no completa en el plazo de 1 hora. El determinado ancho de banda de la red dedicado, doblando el ancho de banda disponible para la descarga parte en dos aproximadamente la cantidad de tiempo requerida para completar la descarga. Por ejemplo, la tabla abajo presenta los anchos de banda y la tiempo-a-descarga para un paquete VDB del 65 MB:

Tamaño del paquete	Hora de descargar en el kbps 256	Hora de descargar en 512 kbps	Hora de descargar en el 2 mbps	Hora de descargar el 4 mbps
65 MB	2130 segundos	1065 segundos	273 segundos	136 segundos

Las descargas de la actualización VDB ocurren asynchronously.

Precaución: Instalar una actualización VDB recomienza el proceso del Snort cuando usted despliega los cambios de configuración, interrumpiendo temporalmente el examen del tráfico. Si el tráfico cae durante esta interrupción o pasos sin el examen adicional depende del modelo del dispositivo administrado y cómo maneja el tráfico. Vea la *guía de configuración del centro de administración de la potencia de fuego* para más información.

Descargar las actualizaciones de la directiva del control de acceso y de la regla de la intrusión

El tamaño de una actualización de la directiva del control de acceso y de la regla de la intrusión varía dependiendo de varios factores, incluyendo el número de reglas en la actualización, las condiciones dentro de las reglas, el número de reutilizable se opone la referencia de las reglas, y el número de combinaciones directiva-variables del conjunto de la intrusión que las reglas se refieren. Mientras que ninguna fórmula fija puede predecir que tamaño del paquete para la directiva del control de acceso e intrusión gobierna las actualizaciones, la tabla siguiente proporciona los ejemplos que usted puede utilizar para estimar su propio tamaño del paquete. Para cada paquete de la muestra, la tabla proporciona el ancho de banda de la red dedicado mínimo requerido entre los dos dispositivos para completar la descarga dentro del descanso minucioso 5 que el sistema aplica.

Descripción de la directiva	Tamaño estimado del paquete	Ancho de banda mínimo
4 directivas de la intrusión y directivas 1K (las 4 intrusiones predeterminadas y 1000 reglas del control de acceso)	7.8 MB	223 kbps
4 directivas de la intrusión y directivas 5K (la intrusión predeterminada 4 + 5000 reglas del control de acceso)	8.2 MB	256 kbps
4 directivas de la intrusión y directivas 10K (las 4 intrusiones predeterminadas y 10000 reglas del control de acceso)	9 MB	256 kbps

La tabla representa solamente algunos escenarios de la actualización de la política de ejemplo. Los paquetes de actualización de la directiva que incluyen las directivas adicionales tales como archivo o políticas del sistema serán más grandes y requerirán el ancho de banda adicional descargar dentro del descanso que el sistema de la potencia de fuego aplica.

Precaución: Las actualizaciones de la regla del control de acceso que despliegan y de la intrusión pueden aumentar las demandas y el resultado del recurso en una pequeña cantidad de paquetes que caen sin el examen. Además, desplegar algunas configuraciones recomienza el proceso del Snort, que interrumpe el examen del tráfico. Si el tráfico cae durante esta interrupción o pasos sin el examen adicional depende del modelo del dispositivo administrado y cómo maneja el tráfico. Vea la *guía de configuración del centro de administración de la potencia de fuego* para más información.

Descargar las listas url

Debido a las limitaciones en la memoria, algunos modelos del dispositivo realizan la mayoría del Filtrado de URL con un más pequeño, menos granular, el conjunto de las categorías y las reputaciones. Por lo tanto las descargas de la lista url varían de tamaño dependiendo del modelo

del dispositivo; los tamaños aproximados se muestran en la tabla siguiente:

Tamaño del paquete	Descarga completa de la lista url	Actualización de la lista url
dispositivos de la Alto-memoria	450 MB	40 – 80 MB
dispositivos de la Bajo-memoria	20 MB	20 MB

los dispositivos de la Bajo-memoria incluyen la familia 7100 y los modelos siguientes ASA: ASA5506-X, ASA5506H-X, ASA5506W-X, ASA5508-X, ASA5512-X, ASA5515-X, ASA5516-X, y ASA5525-X. (Para NGIPSv, vea la *guía de instalación virtual del sistema de la potencia de fuego* para la información sobre afectar un aparato la cantidad de memoria correcta para realizar la categoría y el Filtrado de URL reputación-basado.)

Descargar una actualización de la lista url o de la lista url que se extiende de tamaño a partir de la 1 al 100 MB falla si no completa en el plazo de 10 minutos (600 segundos). Descargar una actualización de la lista url o de la lista url que se extiende de tamaño del 100 MB a 4 GB falla si no completa en el plazo de 1 hora (3600 segundos).

El determinado ancho de banda de la red dedicado, doblando el ancho de banda disponible para la descarga parte en dos aproximadamente la cantidad de tiempo requerida para completar la descarga, tal y como se muestra en de los ejemplos abajo:

Tamaño del paquete	Hora de descargar en el kbps 256	Hora de descargar en 512 kbps	Hora de descargar en el 2 mbps	Hora de descargar el 4 mbps
20 MB	640 segundos	320 segundos	80 segundos	42 segundos
450 MB	14745 segundos	7373 segundos	1887 segundos	944 segundos

Las descargas de las actualizaciones de la lista url ocurren asynchronously.