Problemas del Troubleshooting con el Filtrado de URL en un sistema de FireSIGHT

Contenido

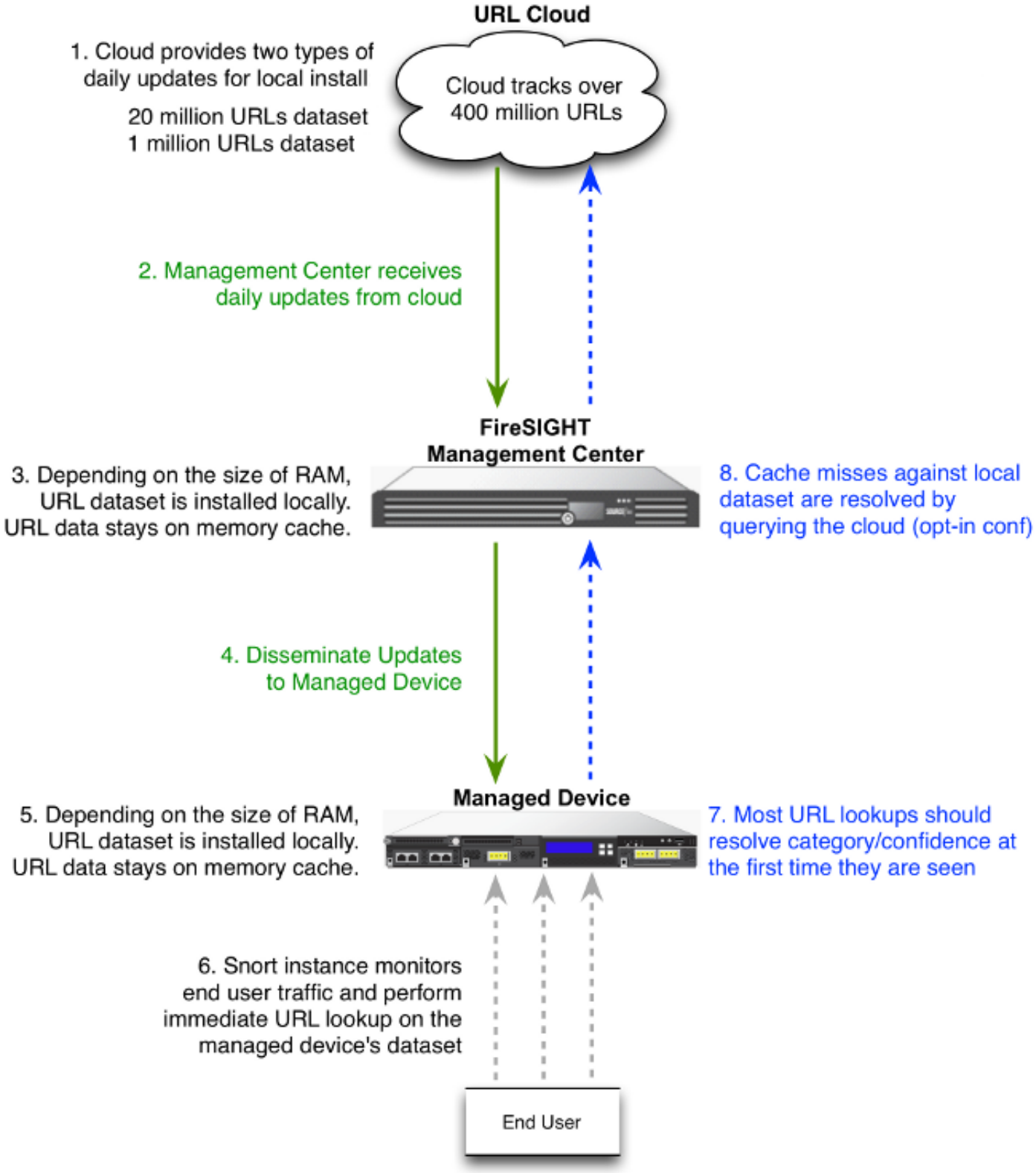
Introducción

Este documento describe los problemas frecuentes con el Filtrado de URL. La característica del Filtrado de URL en el centro de administración de FireSIGHT categoriza el tráfico de los host monitoreados y permite que usted escriba una condición en una regla del control de acceso basada en la reputación.

Proceso de búsqueda del Filtrado de URL

Para acelerar el proceso de búsqueda URL, el Filtrado de URL proporciona un grupo de datos que esté instalado en un sistema de la potencia de fuego localmente. El dependiente sobre la cantidad de memoria (RAM) disponible en un dispositivo, allí es dos tipos de grupos de datos:

Tipo de grupo de datos	Requisito de memoria	
	En la versión 5.3	En la versión 5.4 o posterior
20 millones de grupos de datos URL	>2GB	>3.4 GB
1 millón de grupos de datos URL	<= 2GB	<= 3.4 GB



Problemas de conectividad de la nube

Paso 1: Marque las licencias

¿La licencia está instalada?

Usted puede agregar la categoría y las condiciones reputación-basadas URL a las reglas del control de acceso sin un Filtrado de URL autorizan, no obstante usted no puede aplicar la directiva del control de acceso hasta que usted primero agregue una licencia del Filtrado de URL

al centro de administración de FireSIGHT, después lo habilita en los dispositivos apuntados por la directiva.

¿Se expira la licencia?

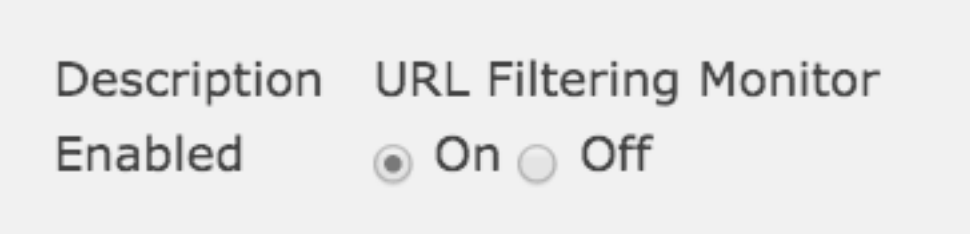
Si expira una licencia del Filtrado de URL, el control de acceso gobierna con la categoría y las condiciones reputación-basadas URL paran el filtrar de los URL, y el centro de administración de FireSIGHT entra en contacto no más el servicio de la nube.

> Consejo: Lea el Filtrado de URL en un ejemplo de la configuración del sistema de FireSIGHT para aprender cómo habilitar la característica del Filtrado de URL en un sistema de FireSIGHT y aplicar la licencia del Filtrado de URL en un dispositivo administrado.

Paso 2: Alertas de la salud del control

El módulo del monitor del Filtrado de URL sigue las comunicaciones entre el centro de administración de FireSIGHT y la nube de Cisco, donde el sistema obtiene sus datos del Filtrado de URL (categoría y reputación) para los URL comúnmente visitados. El módulo del monitor del Filtrado de URL también sigue las comunicaciones entre un centro de administración de FireSIGHT y cualquier dispositivo administrado donde usted ha habilitado el Filtrado de URL.

Para habilitar el módulo del monitor del Filtrado de URL, vaya a la página de la **configuración de la política de la salud**, eligen el **monitor del Filtrado de URL**. Haga clic **encendido el** botón de radio para la opción **habilitada** para habilitar el uso del módulo para la prueba del estado de salud. Usted debe aplicar la política sanitaria al centro de administración de FireSIGHT si usted quisiera que sus configuraciones tomaran el efecto.



- **Alerta crítica**: Si el centro de administración de FireSIGHT no puede comunicar con éxito con o extraer una actualización de la nube, la clasificación del estatus para los cambios de ese módulo a *crítico*.
- **Alerta amonestadora**: Si el centro de administración de FireSIGHT comunica con éxito con la nube, el estado del módulo cambia a *advertir* si el centro de administración no puede avanzar los nuevos datos del Filtrado de URL a sus dispositivos administrados.

Paso 3: Configuraciones del control DNS

Un centro de administración de FireSIGHT comunica con estos servidores durante las operaciones de búsqueda de la nube:

```
database.brightcloud.com
service.brightcloud.com
```

Una vez que usted se aseegura que ambos servidores están permitidos en el Firewall, funcione con estos comandos en el centro de administración de FireSIGHT y verifiquelos si el centro de

administración puede resolver los nombres:

```
admin@FireSIGHT:~$ sudo nslookup database.brightcloud.com admin@FireSIGHT:~$ sudo nslookup
service.brightcloud.com
```

Paso 4: Conectividad del control a los puertos requeridos

El uso de los sistemas de FireSIGHT vira 443/HTTPS y 80/HTTP hacia el lado de babor para comunicar con el servicio de la nube.

Una vez que usted confirma que el centro de administración puede realizar un `nslookup` acertado, verifique la Conectividad al puerto 80 y al puerto 443 con el `telnet`. La base de datos URL se descarga con `database.brightcloud.com` en el puerto 443, mientras que las interrogaciones desconocidas URL se hacen en `service.brightcloud.com` en el puerto 80.

```
telnet database.brightcloud.com 443
telnet service.brightcloud.com 80
```

Esta salida es un ejemplo de una `conexión Telnet` acertada a `database.brightcloud.com`.

```
Connected to database.brightcloud.com.
Escape character is '^]'.
```

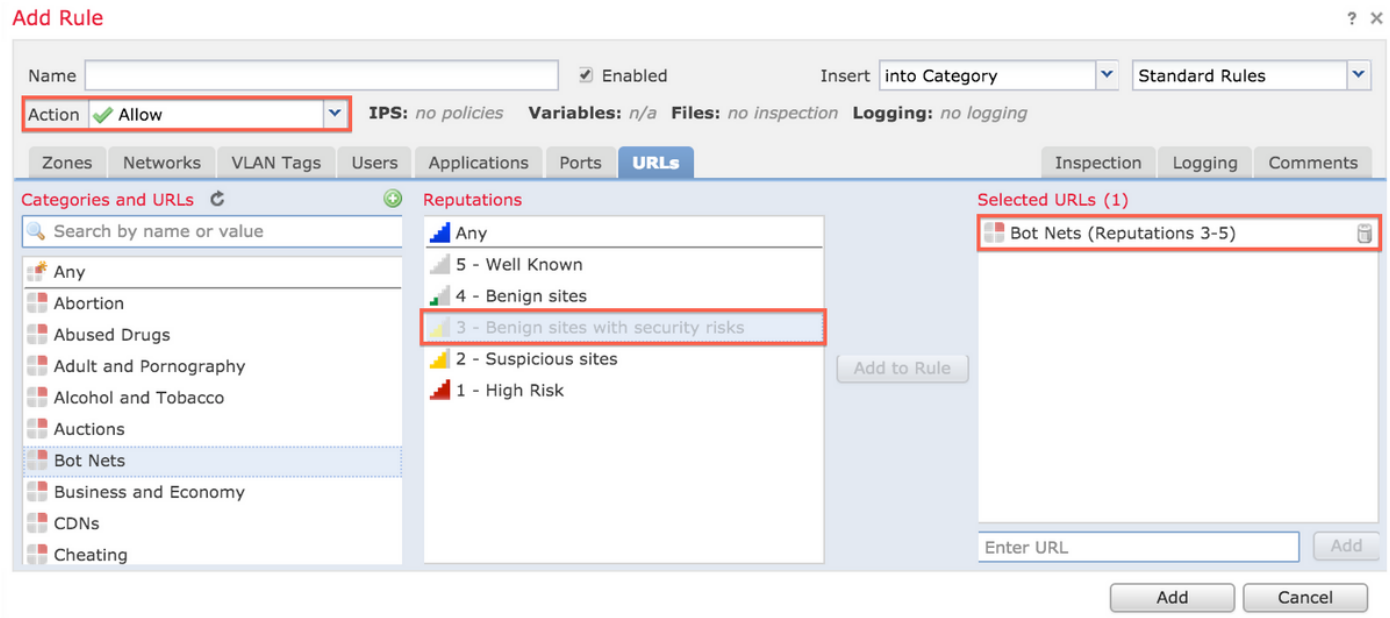
Control de acceso y problemas de Miscategorization

Problema 1: El URL con el nivel no seleccionado de la reputación se permite/se bloquea

Si usted nota se permite o se bloquea un URL, pero usted no seleccionó la reputación llana de ese URL en su regla del control de acceso, lee esta sección para entender cómo una regla de Filtrado de URL trabaja.

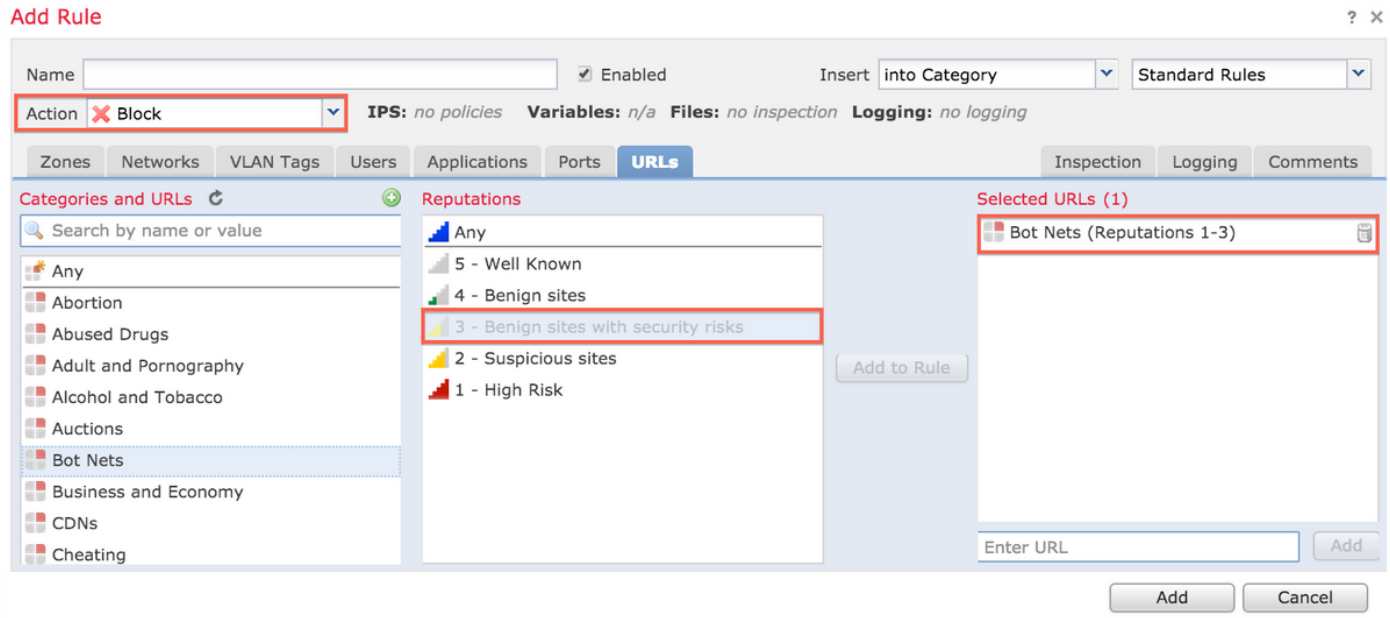
La acción de la regla es permite

Cuando usted crea una regla **para permitir el** tráfico basado en un nivel de la reputación, la selección de un nivel de la reputación también selecciona todos los niveles de la reputación menos seguros que el nivel que usted seleccionó originalmente. Por ejemplo, si usted configura una regla para permitir los *sitios benignos con los riesgos de seguridad* (nivel 3), también permite automáticamente los *sitios benignos* (nivel 4) y *bien conocido* (los sitios del nivel 5).



La acción de la regla es bloque

Cuando usted crea una regla **para bloquear el** tráfico basado en un nivel de la reputación, la selección de un nivel de la reputación también selecciona todos los niveles de la reputación más severos que el nivel que usted seleccionó originalmente. Por ejemplo, si usted configura una regla para bloquear los *sitios benignos con los riesgos de seguridad* (nivel 3), también bloquea automáticamente los *sitios sospechosos* (nivel 2) y *alto riesgo* (sitios del nivel 1).



Matriz de la selección URL

Nivel seleccionado de la reputación	Acción seleccionada de la regla				
	Alto riesgo	**Sitio sospechoso**	**Sitio benigno con el riesgo de seguridad**	**Sitio benigno**	**Bien conoci**
1 - Alto riesgo	El bloque, permite	Permita	Permita	Permita	Permit
2 - Sitios sospechosos	Bloque	El bloque, permite	Permita	Permita	Permit
3 - Sitios benignos con el	Bloque	Bloque	El bloque, permite	Permita	Permit

riesgo de seguridad					
4 - Sitios benignos	Bloque	Bloque	Bloque	El bloque, permite	Permit
5 - Bien conocido	Bloque	Bloque	Bloque	Bloque	El bloc permit

Problema 2: El comodín no trabaja en la regla del control de acceso

El sistema de FireSIGHT no soporta la especificación de un comodín en una condición URL. Esta condición pudo no poder alertar en `cisco.com`.

```
*cisco*.com
```

Además, un URL incompleto pudo hacer juego contra el otro tráfico que causa un resultado indeseado. Cuando usted especifica los URL individuales en las condiciones URL, usted debe considerar cuidadosamente el otro tráfico que pudo ser afectado. Por ejemplo, considere un escenario donde usted quiere bloquear explícitamente `cisco.com`. Sin embargo, el corresponder con de la subcadena significa que eso el bloqueo de `cisco.com` también bloquea `sanfrancisco.com`, que no pudieron ser su intento.

Cuando usted ingresa un URL, ingrese el Domain Name y omita la información del subdomain. Por ejemplo, teclee `cisco.com` bastante que `www.cisco.com`. Cuando usted utiliza `cisco.com` en una regla de la **permit**, los usuarios podrían hojear a ninguno de estos URL:

```
http://cisco.com
http://cisco.com/newcisco
http://www.cisco.com
```

Problema 3: La categoría y la reputación URL no se pueblan

Si un URL no está en una base de datos local y es la primera vez que el URL está visto en el tráfico, una categoría o una reputación no pudo ser poblada. Esto significa que la primera vez que se ve un URL desconocido, no hace juego la regla AC. Las operaciones de búsqueda URL para los URL comúnmente visitados no pudieron resolver a veces en la primera vez que se ve un URL. Este problema se repara en la versión 5.3.0.3, 5.3.1.2, y 5.4.0.2, 5.4.1.1.

Información Relacionada

- Configuración del Filtrado de URL en un sistema de FireSIGHT
- Soporte Técnico y Documentación - Cisco Systems