Solución de problemas de filtrado de URL en un sistema FireSIGHT

Contenido

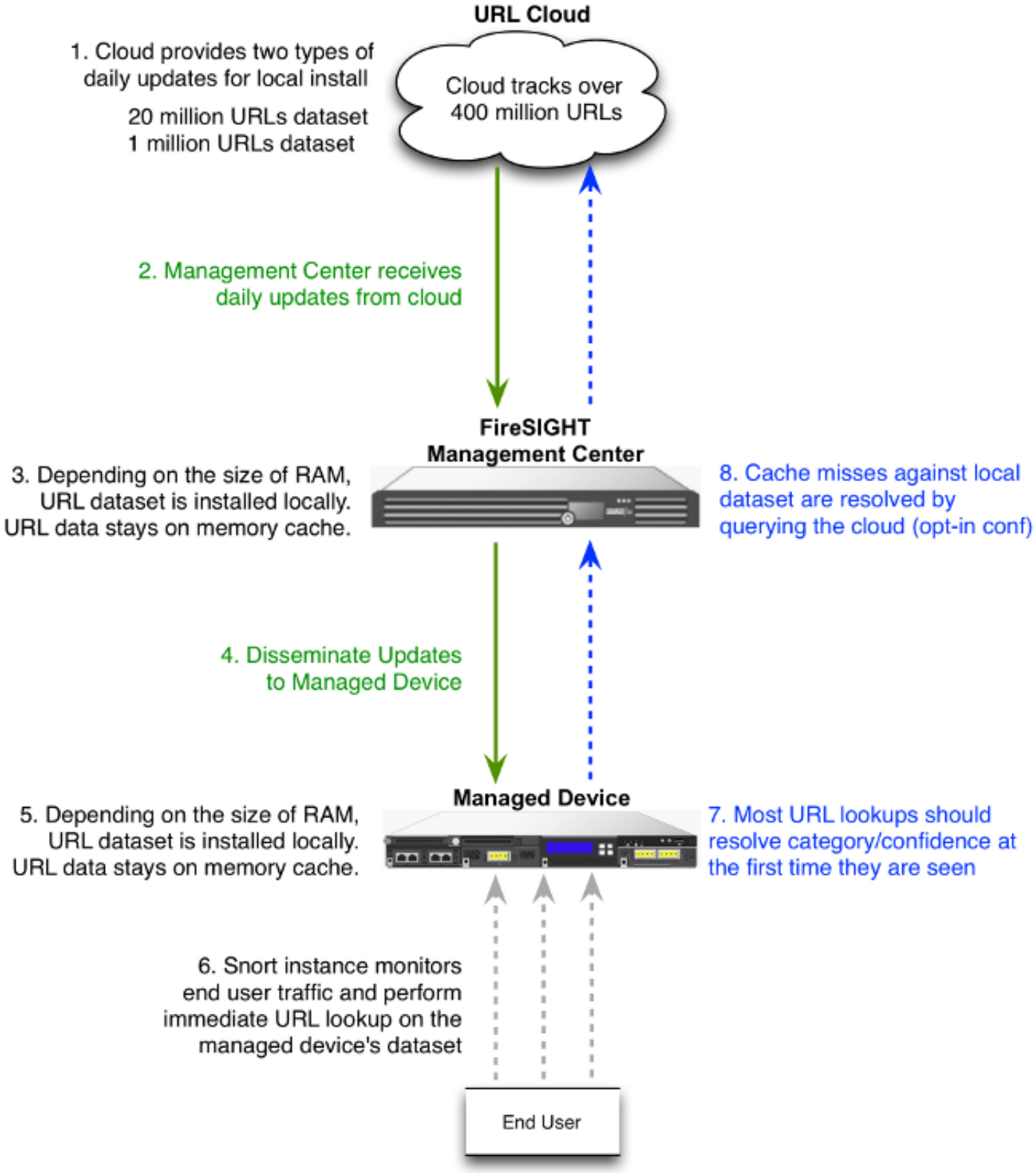
Introducción

Este documento describe problemas comunes con el filtrado de URL. La función de filtrado de URL de FireSIGHT Management Center clasifica el tráfico de los hosts supervisados y permite escribir una condición en una regla de control de acceso basada en la reputación.

Proceso de búsqueda de filtrado de URL

Para acelerar el proceso de búsqueda de URL, el filtrado de URL proporciona un conjunto de datos que se instala localmente en un sistema Firepower. Dependiendo de la cantidad de memoria (RAM) disponible en un dispositivo, existen dos tipos de conjuntos de datos:

Tipo de conjunto de datos	Requisitos de memoria	
	En la versión 5.3	En la versión 5.4 o superior
20 millones de conjuntos de datos URL	>2 GB	>3,4 GB
1 millón de conjuntos de datos URL	<= 2 GB	<= 3,4 GB



Problemas de conectividad a la nube

Paso 1: Compruebe las licencias

¿Está instalada la licencia?

Puede agregar condiciones de URL basadas en la categoría y la reputación a las reglas de control de acceso sin una licencia de filtrado de URL; sin embargo, no puede aplicar la política de control de acceso hasta que agregue primero una licencia de filtrado de URL a FireSIGHT

Management Center y, a continuación, la habilite en los dispositivos de destino de la política.

¿Ha caducado la licencia?

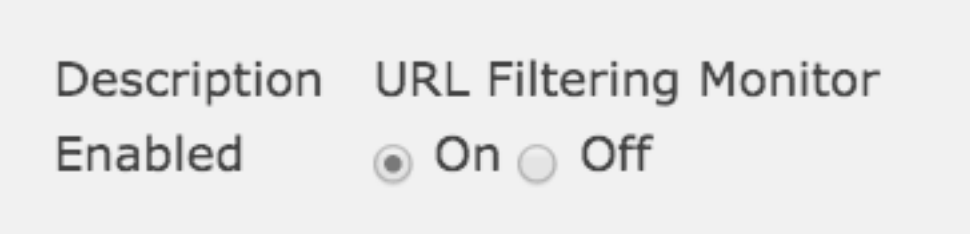
Si vence una licencia de filtrado de URL, las reglas de control de acceso con condiciones de URL basadas en categoría y reputación dejan de filtrar URL y FireSIGHT Management Center deja de ponerse en contacto con el servicio en la nube.

> **Consejo:** Lea Ejemplo de configuración de filtrado de URL en un sistema FireSIGHT para aprender a habilitar la función de filtrado de URL en un sistema FireSIGHT y aplicar la licencia de filtrado de URL en un dispositivo administrado.

Paso 2: Comprobar alertas de estado

El módulo Monitor de filtrado de URL realiza un seguimiento de las comunicaciones entre FireSIGHT Management Center y la nube de Cisco, donde el sistema obtiene sus datos de filtrado de URL (categoría y reputación) para las URL más visitadas. El módulo Monitor de filtrado de URL también realiza un seguimiento de las comunicaciones entre un FireSIGHT Management Center y cualquier dispositivo administrado en el que haya activado el filtrado de URL.

Para habilitar el módulo Monitor de filtrado de URL, vaya a la página **Configuración de la política de salud**, elija **Monitor de filtrado de URL**. Haga clic en el botón de opción **On** para la opción **Enabled** para habilitar el uso del módulo para las pruebas de estado. Debe aplicar la directiva de mantenimiento a FireSIGHT Management Center si desea que la configuración surta efecto.



- **Alerta crítica**: Si FireSIGHT Management Center no puede comunicarse correctamente con la nube o recuperar una actualización de la misma, la clasificación de estado de ese módulo cambia a *Crítico*.
- **Alerta de advertencia**: Si FireSIGHT Management Center se comunica correctamente con la nube, el estado del módulo cambia a *Advertencia* si Management Center no puede enviar nuevos datos de filtrado de URL a sus dispositivos administrados.

Paso 3: Comprobar configuración de DNS

FireSIGHT Management Center se comunica con estos servidores durante la búsqueda en la nube:

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

Una vez que se haya asegurado de que ambos servidores están permitidos en el firewall, ejecute estos comandos en FireSIGHT Management Center y verifique si Management Center puede resolver los nombres:

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

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

Paso 4: Verifique la conectividad a los puertos requeridos

Los sistemas FireSIGHT utilizan los puertos 443/HTTPS y 80/HTTP para comunicarse con el servicio en la nube.

Una vez que confirme que Management Center puede realizar una nslookup exitosa, verifique la conectividad con el puerto 80 y el puerto 443 con telnet. La base de datos de URL se descarga con database.brightcloud.com en el puerto 443, mientras que las consultas de URL desconocidas se realizan en service.brightcloud.com en el puerto 80.

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

Este resultado es un ejemplo de una conexión exitosa de telnet a database.brightcloud.com.

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

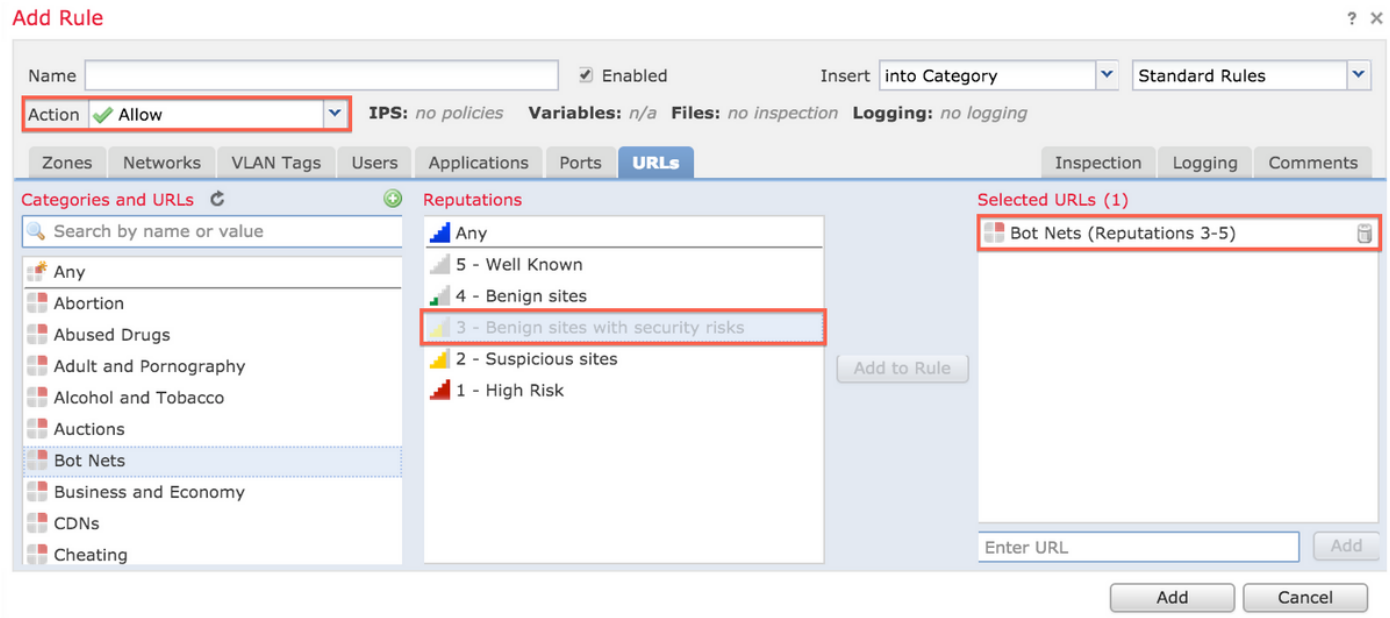
Problemas de control de acceso y clasificación errónea

Problema 1: URL con nivel de reputación no seleccionado permitido/bloqueado

Si observa que una URL está permitida o bloqueada, pero no seleccionó el nivel de reputación de esa URL en su Regla de control de acceso, lea esta sección para entender cómo funciona una regla de filtrado de URL.

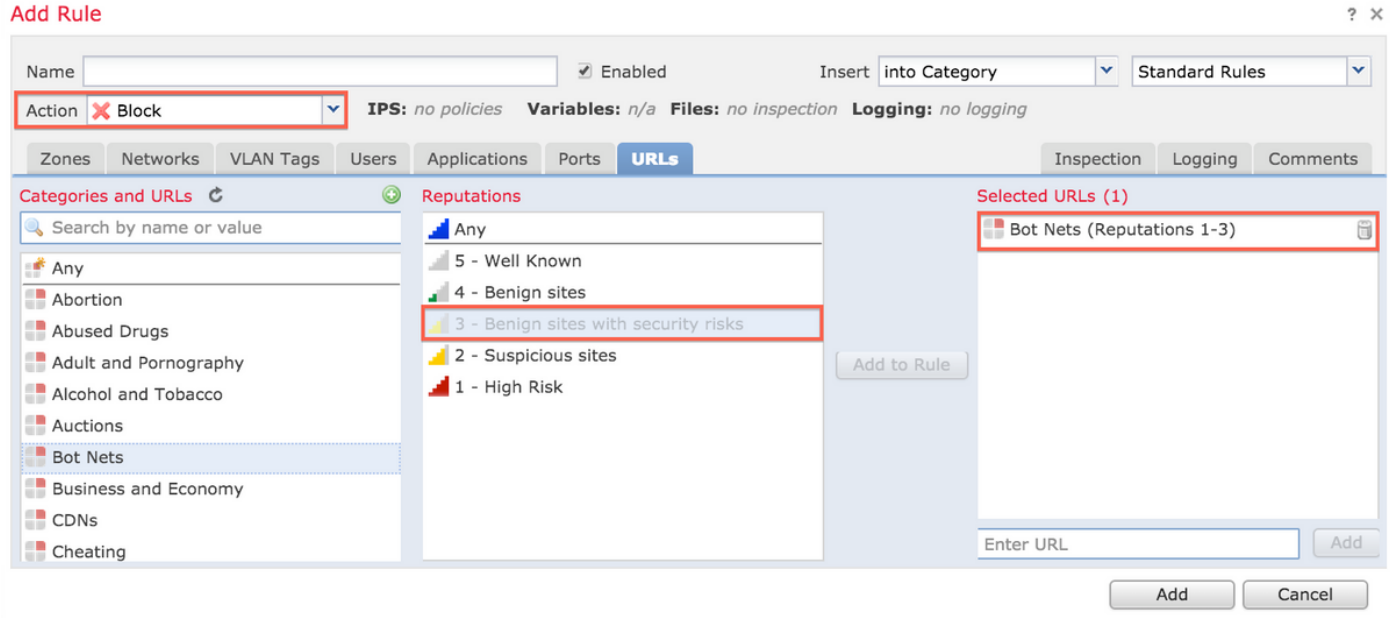
La acción de regla es Permitir

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



La acción de regla es Bloquear

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



Matriz de selección de URL

Nivel de reputación seleccionado	Acción de regla seleccionada				
	Riesgo alto	**Sitio sospechoso**	**Sitio benigno con riesgo de seguridad**	**Sitio benigno**	**Bien conoci**
1 - Riesgo alto	Bloquear, Permitir	Permiso	Permiso	Permiso	Permis
2 - Sitios sospechosos	Bloqueo	Bloquear, Permitir	Permiso	Permiso	Permis
3 - Sitios benignos con riesgo	Bloqueo	Bloqueo	Bloquear, Permitir	Permiso	Permis

de seguridad					
4 - Sitios benignos	Bloqueo	Bloqueo	Bloqueo	Bloquear, Permitir	Permis
5 - Bien conocido	Bloqueo	Bloqueo	Bloqueo	Bloqueo	Bloque Permit

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

El sistema FireSIGHT no admite la especificación de un comodín en una condición de URL. Esta condición podría no alertar en cisco.com.

```
*cisco*.com
```

Además, una URL incompleta puede coincidir con otro tráfico, lo que provoca un resultado no deseado. Al especificar direcciones URL individuales en condiciones de URL, debe tener en cuenta cuidadosamente otro tráfico que pueda verse afectado. Por ejemplo, considere un escenario donde desee bloquear explícitamente cisco.com. Sin embargo, la coincidencia de subcadenas significa que el bloqueo de cisco.com también bloquea sanfrancisco.com, lo que podría no ser su intención.

Cuando introduzca una URL, introduzca el nombre de dominio y omita la información del subdominio. Por ejemplo, escriba cisco.com en lugar de www.cisco.com. Cuando utilice cisco.com en una regla Allow, los usuarios podrán navegar a cualquiera de estas URL:

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

Problema 3: La categoría de URL y la reputación no se han rellenado

Si una URL no está en una base de datos local y es la primera vez que se ve en el tráfico, es posible que no se rellene una categoría o reputación. Esto significa que la primera vez que se ve una URL desconocida, no coincide con la regla AC. En ocasiones, las búsquedas de URL de las URL visitadas con más frecuencia pueden no resolverse la primera vez que se ve una URL. Este problema se corrige en las versiones 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 FireSIGHT
- Soporte Técnico y Documentación - Cisco Systems