# Cómo filtrar el código rojo en Cisco Cache y Content Engine

## Contenido



## Introducción

Este documento proporciona la información sobre la filtración del gusano Código rojo en el Cisco Cache y el Content Engine.

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

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

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

# Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

## Configuraciones

Al intentar conectarse con sitios inexistentes, muchas memorias caché transparentes se saturan. Este documento brinda una solución para filtrar el gusano Code Red, que puede afectar las soluciones Cisco de almacenamiento en memoria caché. El código rojo utiliza un desbordamiento de búfer en una secuencia de comandos default.ida en los Servidores de información de Internet (IIS). El código rojo utiliza esta petición del Hypertext Transfer Protocol (HTTP):

```
get http://random-ip-address/default.ida?long-string-of-data
```

La extensa secuencia de datos del ejemplo anterior es el desbordamiento del búfer y el código de instrucción para el gusano mismo. Puede filtrar esto por medio de una regla de bloques que use un url-regex para coincidir con el contenido. Para el hardware del Cisco Cache Engine que funciona con el software CE2.XX, y el hardware del Cisco Content Engine que funciona con el software 2.XX o 3.XX, configure como sigue:

```
rule enable
rule block url-regex ^http://.*/default\.ida$
rule block url-regex ^http://.*www\.worm\.com/default\.ida$
```

Publique el **comando show rule all** de visualizar la cantidad de aciertos que acumula contra esta regla de bloques. Para el hardware del Content Engine que funciona con el software 3.XX, usted puede ser más específico y no bloquear la petición, pero la reescritura a un servidor Web local de indicar que su sitio está infectado. Utilice una regla similar ésta:

```
rule enable
rule rewrite url-regsub ^http://.*/default\.ida$ http://local-webserver/codered.html
```

# Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

# Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.

# Información Relacionada

- Soporte de Producto de interconexión de redes de contenido
- Descargas de software de Cisco Cache Engine 3.0 (sólo para clientes registrados)
- Cisco Cache Engine 2.0 con descargas de software ( sólo clientes registrados)
- Soporte Técnico - Cisco Systems