# Фильтрация Code Red в Cisco Cache и Content Engines

## Содержание



## Введение

Этот документ предоставляет сведения о фильтрации Червя Code Red на Cisco Cache и Модулях контента.

## Предварительные условия

### Требования

Для этого документа отсутствуют особые требования.

### Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

### Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

# Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

## Конфигурации

Многие прозрачные кэши переполняются при попытке подключиться к несуществующим узлам. Данный документ содержит решение для фильтрации червя Code Red, который может повредить решениям для кэширования от Cisco. Червь Code Red использует переполнение буфера сценария default.ida информационного сервера Интернет (IIS). Code Red использует этот запрос Протокола HTTP:

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

. Это можно отфильтровать с помощью блочного правила, использующего URL-regex для сопоставления содержимого. Для аппаратных средств Cisco Cache Engine рабочий CE2. Программное обеспечение XX и аппаратные средства Модуля контента Cisco, работающие 2. XX или 3. Программное обеспечение XX, настройте следующим образом:

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

Выполните **команду show rule all** для отображения количества соответствий, которые накапливаются против этого правила блокировки. Для аппаратных средств Модуля контента, работающих 3. Программное обеспечение XX, можно быть более определенными и не заблокировать запрос, но переписать на локальный Web-сервер, чтобы указать, что заражен узел. Используйте правило, подобное этому:

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

# Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

# Устранение неполадок

Для этой конфигурации в настоящее время нет сведений об устранении проблем.

# Дополнительные сведения

- Поддержка продукта сетей передачи контента
- Cisco Cache Engine 3.0 загрузки программного обеспечения только для зарегистрированных пользователей)
- Загрузки программного обеспечения Cisco Cache Engine 2.0 (только для зарегистрированных клиентов)
- Техническая поддержка - Cisco Systems