

# Автоматический сбой обновления загрузки на центре управления огневой мощи

## Содержание

[Введение](#)

[Возможные причины для сбоя](#)

[Влияние](#)

[Проверка](#)

[Проверьте параметры настройки DNS](#)

[Проверьте соединение](#)

[Устранение неполадок](#)

[Дополнительная документация](#)

## Введение

Этот документ обсуждает, обосновывает, что могла бы отказать запланированная задача для обновления Центра управления Огневой мощи Cisco. Можно обновить Центр управления Огневой мощи Cisco вручную или автоматически. Для выполнения автоматического обновления ПО можно создать задачу списка на Центре управления для выполнения в будущее время.

## Возможные причины для сбоя

Когда одно из этих действий происходит в вашей сети, Центр управления Огневой мощи мог бы быть не в состоянии загружать файл обновления от Инфраструктуры Обновления Загрузки Cisco:

- Политика безопасности вашей компании блокирует трафик Системы доменных имен (DNS).
- Конфигурация за пределами вашего Центра управления влияет на загрузку. Например, правило межсетевого экрана могло бы позволить только один IP-адрес для `support.sourcefire.com`.

**Внимание.** : Cisco использует круговой DNS для распределения нагрузки, отказоустойчивости и времени работы без сбоев. Поэтому IP-адреса серверов DNS могли бы измениться.

## Влияние

При использовании этот метод...

Конфигурация системного параметра по умолчанию для автоматической загрузки

Загрузите файл обновления вручную и загрузите его к Центру управления

Вопрос для принятия решения

Действие не требуется

Действие не

Огневой мощи

Правила межсетевого экрана для фильтрации доступа к Cisco управляли  
Инфраструктурой Обновления Загрузки

требуется

Придерживайте  
решения

- Сбои частично смягчены тремя повторными попытками и следующим запланированным выполнением. Повторные сбои вероятны индикация относительно внешнего фактора, такого как межсетевые экраны или простой с Инфраструктурой.
- Поскольку круговой DNS находится на доменном имени, необходимо предпринять шаги, чтобы гарантировать, что нет никаких неустойчивых сбоев загрузки.

## Проверка

### Проверьте параметры настройки DNS

Гарантируйте, что ваш Центр управления Огневой мощи настроен для использования сервера DNS.

**Внимание.** : Cisco строго рекомендует поддерживать настройки по умолчанию.

- Information
- HTTPS Certificate
- Database
- **Network**
- Management Interface
- Process
- Time
- Remote Storage Device
- Change Reconciliation
- Console Configuration
- Cloud Services

### Network Settings

#### IPv4

Configuration

IPv4 Management IP  Netmask

Default Network Gateway

#### IPv6

Configuration

#### Shared Settings

Hostname

Domain

Primary DNS Server

Secondary DNS Server

Tertiary DNS Server

MTU

Remote Management Port

#### Configure Proxies to Access the Internet

**Direct connection**

Connected directly to the Internet.

**Manual proxy configuration**

HTTP Proxy

Port

Use Proxy Authentication

User Name

Password

Confirm Password

Можно настроить параметры настройки DNS в **Системе> Локальный> Конфигурация** под **Сегментом сети**. Под **Совместно используемым** разделом **Параметров настройки** можно задать до трех серверов DNS.

**Примечание:** При выборе **DHCP** в выпадающем списке **Конфигурации** вы не можете вручную задать **Совместно используемые Параметры настройки**.

## Проверьте соединение

Можно использовать различные команды, такие как `telnet`, `nslookup`, или `вырыть` для определения состояния сервера DNS и параметров настройки DNS на Центре управления Огневой мощи. Пример:

```
telnet support.sourcefire.com 443nslookup support.sourcefire.comdig support.sourcefire.com
```

**Примечание:** Эхо-запрос к `support.sourcefire.com` не работает. Следовательно это не должно использоваться в качестве теста подключения.

Чтобы к тестовому подключению к сайту поддержки от устройства (для загрузки обновлений, и так далее), можно войти устройство через SSH или доступ непосредственного консольного, и использовать эту команду:

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

Эта команда показывает согласование сертификата, а также предоставляет вам эквивалент сеанса Telnet к веб-серверу порта 80. Вот пример выходных данных команды:

```
admin@Firepower:~# sudo openssl s_client -connect support.sourcefire.com:443
```

На этом этапе не должно быть никакого приглашения. Однако, поскольку сеанс ждет ввода, можно тогда ввести команду:

```
GET /
```

Необходимо получить необработанный HTML, который является страницей входа сайта поддержки.

## Устранение неполадок

**Вариант 1:** Замените статический IP - адрес Доменным именем `support.sourcefire.com` на межсетевых экранах. Если необходимо использовать статический IP - адрес, удостоверьтесь, что это корректно. Вот подробные сведения сервера загрузки, используемого системой Огневой мощи:

- **Домен:** `support.sourcefire.com`
- **Порт:** `443/tcp` (двунаправленный)
- **IP-адрес:** `50.19.123.95`, `50.16.210.129`

Дополнительные IP-адреса, которые также используются `support.sourcefire.com` (в круговом методе):

```
54.221.210.248
54.221.211.1
54.221.212.60
54.221.212.170
54.221.212.241
54.221.213.96
54.221.213.209
54.221.214.25
54.221.214.81
```

**Вариант 2:** Можно загрузить обновления вручную web-браузером, и затем установить его вручную во время периода технического обслуживания.

**Параметр 3:** Добавьте запись для `support.sourcefire.com` на вашем сервере DNS.

## Дополнительная документация

- [Типы обновлений, которые могут быть установлены в системе огневой мощи](#)
- [Адреса нужного сервера для операций Усовершенствованной вредоносной защиты \(AMP\)](#)
- [Требуемые коммуникационные порты для работы системы огневой мощи](#)
- [Cisco Systems – техническая поддержка и документация](#)