

# Содержание

[Введение](#)

[Предварительные условия](#)

[Требования](#)

[Используемые компоненты](#)

[Настройка](#)

[Обзор конфигурации](#)

[Пример конфигурации](#)

[Проверка](#)

[Устранение неполадок](#)

[Дополнительные сведения](#)

## Введение

Этот документ описывает, как настроить протокол WCCP для устройства адаптивной защиты Cisco (ASA) через Cisco Web Security Appliance (WSA).

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco WSA
- Cisco ASA
- WCCP
- Развертывания режима прозрачного прокси

### Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Cisco версия 7 WSA. x
- Cisco ASA версии 8.x

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.

# Настройка

Используйте этот раздел для настройки WCCP для ASA.

## Обзор конфигурации

Это команды, которые введены в WSA для настройки WCCP для ASA:

```
hostname(config)# wccp {web-cache | service_number} [redirect-list access_list]
[group-list access_list] [password password]
```

```
hostname(config)# wccp interface interface_name {web-cache | service_number}
redirect in
```

Это описания записи для этой команды:

- **служебное число:** Это - динамический для сервиса идентификатор, что означает, что определение сервиса диктует кэш. Динамический для сервиса номер может колебаться от 0 до 255. Максимальный допустимый номер 256, который включает сервис веба - кэширования, который задан с ключевым словом веба - кэширования.

- **список перенаправления:** Это - дополнительная запись. Это используется со списком доступа, который управляет трафиком, который перенаправлен к этой группе сервисов. Аргумент access-list является строкой не больше, чем 64 символов (название или номер), который задает список доступа.

**Примечание:** Версии программного обеспечения ASA 8.1 и ранее не принимают порт TCP в списке перенаправления; только сетевые адреса могут использоваться.

- **group-list:** Это - дополнительная запись списка доступа, которая определяет веб-кэши, которым позволяют участвовать в группе сервисов. Аргумент access-list является строкой не больше, чем 64 символов (название или номер), который задает список доступа.

- **password:** Это - дополнительная запись, которая задает аутентификацию алгоритма представления сообщения в краткой форме 5 (MD5) для сообщений, которые получены от группы сервисов. От сообщений, которые не приняты аутентификацией, сбрасывают.

**Примечание:** Стандартный сервис является вебom - кэшированием (Идентификатор сервиса 0), который только перехватывает Порт TCP 80 (HTTP) трафик. Для любых других специализированных сервисов Cisco рекомендует использовать Идентификатор сервиса между 90 и 97.

## Пример конфигурации

Выполните эти шаги для настройки WCCP для ASA через WSA:

1. Введите эту команду для использования веба - кэширования группы сервиса по умолчанию:

```
wccp web-cache
```

```
wccp interface inside web-cache redirect in
```

2. Введите эту команду для использования динамического для сервиса идентификатора группы для перенаправления трафика HTTP и Трафика HTTPS:

```
wccp 90 redirect-list wccp-hosts group-list wccp-routers
```

3. Введите эту команду для использования безопасности WCCP:

```
wccp 90 redirect-list wccp-hosts group-list wccp-routers password securewccp
```

4. Список доступа может быть настроен так, чтобы он запретил трафик, который передается ASA как IP - адрес назначения и перенаправляет его к WSA. Это особенно полезно, когда ASA настроен для перенаправления трафика ко множественному WSAs. Например, WSAs можно было бы назначить эти IP-адреса:

IP-адрес WSA1 = 10.0.0.1 IP-адрес WSA2 = 10.0.0.2

Введите эти команды для настройки списка доступа для запрета трафика:

```
access-list wccp-hosts extended deny tcp any host 10.0.0.1  
access-list wccp-hosts extended deny tcp any host 10.0.0.2
```

5. Введите эту команду, чтобы позволить трафику HTTP быть перенаправленным:

```
access-list wccp-hosts extended permit tcp any any eq www
```

6. Введите эту команду, чтобы позволить Трафику HTTPS быть перенаправленным:

```
access-list wccp-hosts extended permit tcp any any eq https
```

7. Введите эти команды для определения WSAs, которым позволяют участвовать в связи WCCP:

```
access-list wccp-routers standard permit host 10.0.0.1  
access-list wccp-routers standard permit host 10.0.0.2
```

8. Если команда списка перенаправления не принята, то расширенный список доступа мог бы быть необходим. Введите эти команды для настройки расширенного списка доступа:

```
access-list wccp-routers extended permit ip host 10.0.0.1 any  
access-list wccp-routers extended permit ip host 10.0.0.2 any
```

9. Введите эту команду для применения конфигурации:

```
wccp interface inside 90 redirect in
```

## Проверка

Для отображения глобальных статистических данных, которые отнесены к WCCP, вводят команду **wccp показа** в привилегированный режим EXEC:

```
show wccp {web-cache | service-number}[detail | view]  
show run | inc wccp
```

**Примечание:** Тип трафика (HTTP, HTTPS, FTP), который перенаправлен, определен конфигурацией WCCP WSA. ASA может только фильтровать перенаправленный трафик с использованием списка перенаправления.

## Устранение неполадок

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

## Дополнительные сведения

- [Настройка служб Web Cache при помощи WCCP](#)
- [Cisco Systems – техническая поддержка и документация](#)