Настройте прозрачное перенаправление с WCCP для перенаправления собственного трафика FTP

Содержание

Введение

Этот документ описывает, как настроить Web Security Appliance (WSA) / маршрутизатор Cisco для поддержки прозрачного перенаправления HTTP, HTTPS и Собственного трафика FTP с протоколом WCCP.

Предварительные условия

Требования

Для этого документа отсутствуют особые требования.

Используемые компоненты

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

- Cisco Web Security Appliance, который выполняет Версию 6.0 AsyncOS или позже
- Собственный прокси FTP включен на WSA
- WCCPv2 совместимый маршрутизатор Cisco / Коммутатор или Межсетевой экран ASA

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

Когда Собственный трафик FTP перенаправлен прозрачно к WSA, WSA, как правило, получает трафик на стандартном порту 21 FTP. Следовательно, Собственный прокси FTP на WSA должен слушать на порту 21 (по умолчанию, собственный прокси FTP 8021). В GUI выберите **Security Services> FTP Proxy** для проверки.

Конфигурация WSA

1. Создайте идентичность для трафика FTP. В GUI выберите **Web Security Manager > Identities** и гарантируйте, что аутентификация была отключена для этого ID.
2. Создайте политику доступа. В GUI выберите **Web Security Manager > Access Policies,** который ссылается на идентичность в шаге 1.
3. При параметрах настройки прокси FTP модифицируйте FTP Пассивные порты, чтобы быть 11000-11006 , чтобы гарантировать, что все порты вписываются в одиночную группу сервисов.
4. Создайте эти Идентификаторы сервиса WCCP:

   _ Порты сервиса имен
   веб - кэширование 0 80 *(альтернативно, можно использовать 98 пользовательских вебов - кэширований при использовании множественного WSAs),* собственный компонент
   ftp 60 21,11000,11001,11002,11003,11004,11005,11006
   кэш https 70 443

Эти примеры перенаправляют три внутренних подсети, в то время как они обходят перенаправление WCCP для всех конфиденциально обращенных назначений, а также одиночного внутреннего хоста.

Типовая конфигурация ASA

```
wccp web-cache redirect-list web-cache group-list group_acl
wccp 60 redirect-list ftp-native group-list group_acl
wccp 70 redirect-list https-cache group-list group_acl

wccp interface inside web-cache redirect in
wccp interface inside 60 redirect in
wccp interface inside 70 redirect in

access-list group_acl extended permit ip host 10.1.1.160 any

access-list ftp-native extended deny ip any 10.0.0.0 255.0.0.0
access-list ftp-native extended deny ip any 172.16.0.0 255.240.0.0
access-list ftp-native extended deny ip any 192.168.0.0 255.255.0.0
access-list ftp-native extended deny ip host 192.168.42.120 any
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.42.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.99.0 255.255.255.0 any range 11000
11006
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any eq ftp
access-list ftp-native extended permit tcp 192.168.100.0 255.255.255.0 any range 11000
11006

access-list https-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list https-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list https-cache extended deny ip any 192.168.0.0 255.255.0.0
```

```
access-list https-cache extended deny ip host 192.168.42.120 any
access-list https-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq https
access-list https-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq https

access-list web-cache extended deny ip any 10.0.0.0 255.0.0.0
access-list web-cache extended deny ip any 172.16.0.0 255.240.0.0
access-list web-cache extended deny ip any 192.168.0.0 255.255.0.0
access-list web-cache extended deny ip host 192.168.42.120 any
access-list web-cache extended permit tcp 192.168.42.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.99.0 255.255.255.0 any eq www
access-list web-cache extended permit tcp 192.168.100.0 255.255.255.0 any eq www
```

Типовая конфигурация коммутатора (c3560)

Это должно работать на большинство маршрутизаторов также.

```
ip wccp web-cache redirect-list web-cache group-list group_acl
ip wccp 60 redirect-list ftp-native group-list group_acl
ip wccp 70 redirect-list https-cache group-list group_acl

interface Vlan99
ip address 192.168.99.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan100
ip address 192.168.100.1 255.255.255.0
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

interface Vlan420
ip address 192.168.42.1 255.255.255.0
ip helper-address 192.168.100.20
ip wccp web-cache redirect in
ip wccp 60 redirect in
ip wccp 70 redirect in

ip access-list extended ftp-native
deny   ip any 10.0.0.0 0.255.255.255
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq ftp
permit tcp 192.168.42.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.99.0 0.0.0.255 any eq ftp
permit tcp 192.168.99.0 0.0.0.255 any range 11000 11006
permit tcp 192.168.100.0 0.0.0.255 any eq ftp
permit tcp 192.168.100.0 0.0.0.255 any range 11000 11006

ip access-list extended https-cache
deny   ip any 10.0.0.0 0.255.255.255
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq 443
permit tcp 192.168.99.0 0.0.0.255 any eq 443
permit tcp 192.168.100.0 0.0.0.255 any eq 443

ip access-list extended web-cache
deny   ip any 10.0.0.0 0.255.255.255
```

```
deny   ip any 172.16.0.0 0.15.255.255
deny   ip any 192.168.0.0 0.0.255.255
deny   ip host 192.168.42.120 any
permit tcp 192.168.42.0 0.0.0.255 any eq www
permit tcp 192.168.99.0 0.0.0.255 any eq www
permit tcp 192.168.100.0 0.0.0.255 any eq www

ip access-list standard group_acl
permit 10.1.1.160
```

> **Примечание:** Из-за ограничения технологии WCCP, максимум восьми портов может быть назначен на идентификатор сервиса WCCP.

Проверка

В настоящее время для этой конфигурации нет процедуры проверки.

Устранение неполадок

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