Содержание

Введение

Этот документ описывает, как настроить маршрутизатор, который действует как сервер Протокола управления динамическими узлами (DHCP) (DHCP) или клиент DHCP с функцией зонального межсетевого экрана (ZBF). Поскольку довольно распространено включить DHCP и ZBF одновременно, эти советы конфигурации помогают гарантировать, что эти функции взаимодействуют правильно.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с программным обеспечением Cisco IOS зональный межсетевой экран. См. Руководство по дизайну Zone-Based Policy межсетевого экрана и Руководство по приложениям для подробных данных.

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.

Информация о функциональной возможности

Когда ZBF включен на маршрутизаторе IOS, любом трафике к сам, зона (т.е. трафик, предназначенный к панели управления маршрутизатора), позволена по умолчанию в IOS 15.x серия кода.

При создании политики для какой-либо зоны (такой как 'внутри' или 'снаружи') к сам зона (out-self политика) или реверс (self-out политика), необходимо явно определить допустимый трафик в политике, подключенной к этим зонам. Используйте осматривание или действие прохода для определения допустимого трафика.

Анализ данных

DHCP использует широковещательные пакеты Протокола UDP для завершения процесса DHCP. Зональные конфигурации межсетевого экрана, которые задают осмотреть действие для этих широковещательных пакетов UDP, могли бы быть отброшены маршрутизатором, и процесс DHCP мог бы отказать. Вы могли бы также видеть это сообщение журнала:

См. проблему, описанную в идентификаторе ошибки Cisco, CSCso53376, "ZBF осматривают, не работает для широковещательного трафика".

Во избежание этой проблемы модифицируйте зональную конфигурацию межсетевого экрана так, чтобы действие прохода вместо осмотреть действия было применено к трафику DHCP.

> **Примечание:** Это требуется только, когда политике применяются к сам зона на маршрутизаторе.

Зональный межсетевой экран как клиент DHCP с действием прохода для трафика UDP

Настройка

Конфигурация данного примера использует набор действия прохода вместо осмотреть действия в policy-map для всего трафика UDP к или от маршрутизатора.

Проверка

Рассмотрите системные журналы, чтобы проверить, что маршрутизатор успешно получил адрес DHCP.

Когда и out-self и self-out политика настроены для передачи трафика UDP, маршрутизатор может получить IP-адрес из DHCP как показано в этом системном журнале:

Когда только out-self зональная политика настроена для передачи трафика UDP, маршрутизатор может также получить IP-адрес из DHCP, и этот системный журнал создан:

Когда только self-out зональная политика настроена для передачи трафика UDP, маршрутизатор может получить IP-адрес из DHCP, и этот системный журнал создан:

Зональный межсетевой экран с действием прохода для трафика DHCP

Настройка

Конфигурация данного примера показывает, как предотвратить весь трафик UDP от зоны в ваш маршрутизатор сам зона за исключением пакетов DHCP. Используйте access-list с определенными портами для разрешения просто трафика DHCP; в данном примере порт 67 UDP и порт 68 UDP заданы, чтобы совпасться. Class-map, который ссылается на access-list, применили действие прохода.

```
access-list extended 111
 10 permit udp any any eq 67

access-list extended 112
 10 permit udp any any eq 68

class-map type inspect match-any self-to-out
match access-group 111
class-map type inspect match-any out-to-self
match access-group 112

zone security outside
zone security inside

interface Ethernet0/1
zone-member security outside
interface Ethernet0/2
zone-member security inside

policy-map type inspect out-to-self
class type inspect out-to-self
pass
class class-default
drop
policy-map type inspect self-to-out
class type inspect self-to-out
pass
class class-default
drop

zone-pair security out-to-self source outside destination self
service-policy type inspect out-to-self
zone-pair security self-to-out source self destination outside
service-policy type inspect self-to-out
```

Проверка

Выходные данные анализа от **show policy-map type inspect zone-pair открывают сеанс** команду, чтобы подтвердить, что маршрутизатор разрешает трафик DHCP через зональный межсетевой экран. В выходных данных данного примера выделенные счетчики указывают, что пакеты передают через зональный межсетевой экран. Если эти счетчики являются нулем, существует проблема с конфигурацией, или пакеты не поступают в маршрутизатор для обработки.

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Сценарий для некорректных конфигураций

Этот пример сценария показывает то, что происходит, когда маршрутизатор неправильно настроен для определения осмотреть действия для трафика DHCP. В этом сценарии маршрутизатор настроен как клиент DHCP. Маршрутизатор отсылает сообщение DHCP DISCOVER, чтобы попытаться получить IP-адрес. Зональный межсетевой экран настроен для осмотра этого трафика DHCP. Это - пример конфигурации ZBF:

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
```

```
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Когда self-out политика настроена с осмотреть действием для трафика UDP, пакет обнаружения DHCP отброшен, и этот системный журнал создан:

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Когда и self-out и out-self политика настроены с осмотреть действием для трафика UDP, пакет обнаружения DHCP отброшен, и этот системный журнал создан:

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
```

```
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

То, когда out-self политика имеет осмотреть действие, включило, и self-out политике включили действие прохода для трафика UDP, пакет предложения DHCP отброшен после того, как пакет обнаружения DHCP передается, и этот системный журнал создан:

```
router#show policy-map type inspect zone-pair sessions

policy exists on zp out-to-self
Zone-pair: out-to-self
Service-policy inspect : out-to-self
Class-map: out-to-self (match-any)
Match: access-group 112
3 packets, 924 bytes
30 second rate 0 bps
Pass
6 packets, 1848 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes

policy exists on zp self-to-out
Zone-pair: self-to-out
Service-policy inspect : self-to-out
Class-map: self-to-out (match-any)
Match: access-group 111
6 packets, 3504 bytes
30 second rate 0 bps
Pass
6 packets, 3504 bytes

Class-map: class-default (match-any)
Match: any
Drop
0 packets, 0 bytes
```

Маршрутизатор как сервер DHCP

Если внутренний интерфейс маршрутизаторов действует как сервер DHCP и если клиенты, которые соединяются с внутренним интерфейсом, являются клиентами DHCP, этот трафик DHCP позволен по умолчанию, если нет никакого inside-self или само к внутренней части зональной политики.

Однако, если или той политики действительно существует, необходимо настроить действие прохода для трафика интереса (порт 67 UDP или порт 68 UDP) в зональной парной политике обслуживания.

Устранение неполадок

В настоящий момент какие-либо специальные данные по устранению неполадок для этих настроек отсутствуют.