ASA 8. 2: поток пакетов через межсетевой экран ASA

Содержание

Введение

Этот документ описывает поток пакетов через устройство адаптивной защиты Cisco (ASA) межсетевой экран. Это показывает процедуру Cisco ASA для обработки внутренних пакетов. Также анализируются различные ситуации, в которых пакет может быть отброшен и ситуации, в которых он передается дальше.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с ASA серии 5500 Cisco.

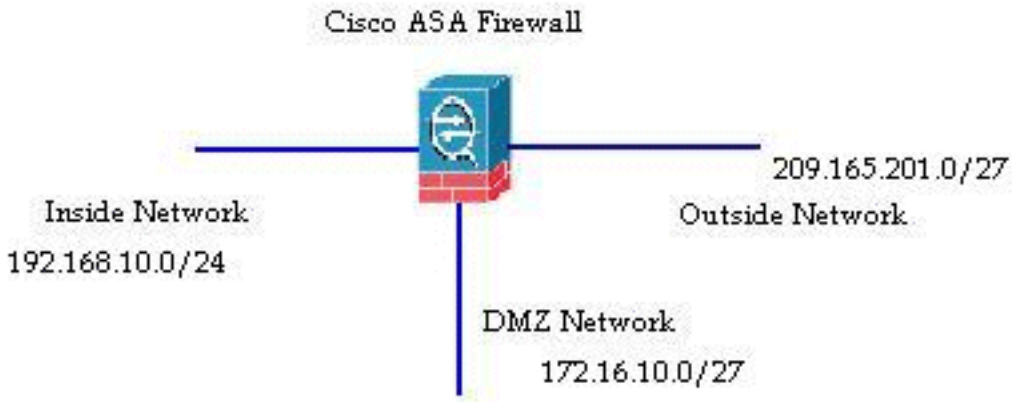
Используемые компоненты

Сведения в этом документе основываются на ASA серии 5500 Cisco ASA, которые работают под управлением ПО версии 8.2.

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.

Общие сведения

Интерфейс, который получает пакет, называют **входным интерфейсом** и интерфейсом, через который выходит пакет, назван **исходящим интерфейсом**. Когда вы обращаетесь к потоку пакетов через любое устройство, задача легко упрощена при рассмотрении его с точки зрения этих двух интерфейсов. Вот пример сценария:



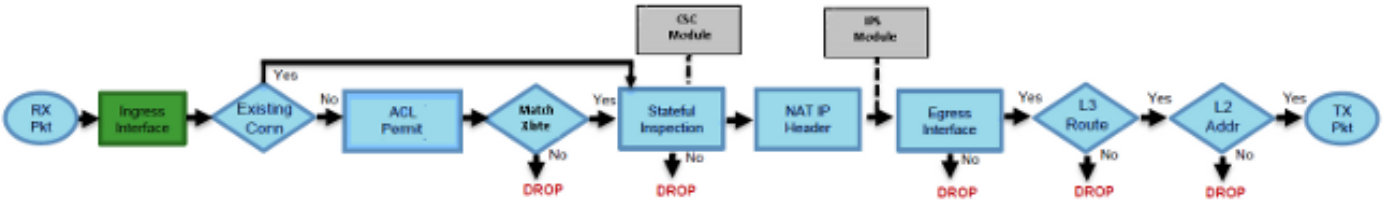
Когда внутренний пользователь (192.168.10.5) попытки обратиться к Web-серверу в сети (DMZ) демилитаризованной зоны (172.16.10.5), поток пакетов похож на это:

- Исходный адрес- 192.168.10.5
- Исходный порт- 22966
- Адрес назначения (DA) - 172.16.10.5
- Номер порта- 8080
- Входной интерфейс - Внутри
- Исходящий интерфейс - DMZ
- Используемый протокол - TCP (Протокол управления передачей)

После определения подробных данных потока пакетов, как описано здесь легко изолировать проблему к этому определенному соединению.

Пакетный алгоритм процесса Cisco ASA

Вот схема того, как Cisco ASA обрабатывает пакет, который это получает:



Вот отдельные шаги подробно:

1. Пакет достигнут во входном интерфейсе.
2. Как только пакет достигает внутреннего буфера интерфейса, счетчик входных

сигналов интерфейса инкрементно увеличен одним.
3. Cisco ASA сначала посмотрел на свои подробные данные таблицы внутреннего подключения, чтобы проверить, является ли это текущим соединением. Если поток пакетов совпадает с текущим соединением, то проверка Списка контроля доступа (ACL) обойдена, и пакет продвинут.Если поток пакетов не совпадает с текущим соединением, то состояние TCP проверено. Если это - SYN - пакет или UDP (Протокол датаграммы пользователя) пакет, то счетчик соединения инкрементно увеличен одним, и пакет передан для проверки ACL. Если это не SYN - пакет, пакет отброшен, и событие зарегистрировано.
4. Пакет обработан согласно интерфейсным ACL. Это проверено в последовательном порядке записей ACL и если это совпадает с какой-либо из записей ACL, это продвигается. В противном случае пакет отброшен, и информация зарегистрирована. Когда пакет совпадает с записью ACL, количество соответствия ACL инкрементно увеличено тем.
5. Пакет проверен для правил трансляции. Если пакет проходит через эту проверку, то соединение создано для этого потока, и пакет продвигается. В противном случае пакет отброшен, и информация зарегистрирована.
6. Пакет подвергнут Инспекционной Проверке. Этот контроль проверяет, соответствует ли этот определенный поток пакетов протоколу. Cisco ASA имеет встроенный инспекционный механизм, который осматривает каждое соединение согласно его предустановленному набору функциональности уровня приложения. Если это прошло осмотр, это продвинуто. В противном случае пакет отброшен, и информация зарегистрирована.Если Безопасность содержания (CSC) модуль будет включена, проверки дополнительных мер безопасности будут внедрены.
7. Информация о IP - заголовке преобразована согласно правилу Трансляции сетевых адресов / преобразования адресов портов (NAT/PAT), и контрольные суммы обновлены соответственно. Когда модуль AIP включен, пакет передан к Усовершенствованному Модулю Сервисов безопасности Контроля и Предотвращения (SSM AIP) для отнесенных проверок безопасности IPS.
8. Пакет передан к исходящему интерфейсу на основе правил трансляции. Если никакой исходящий интерфейс не задан в правиле трансляции, то интерфейс назначения решен на основе глобального поиска маршрута.
9. На исходящем интерфейсе выполнен поиск интерфейсного маршрута. Помните, исходящий интерфейс определен правилом трансляции, которое берет приоритет.
10. Как только маршрут Уровня 3 был найден, и следующий переход определен, разрешение Уровня 2 выполнено. Перезапись Уровня 2 заголовка MAC происходит на данном этапе.
11. Пакет передан на проводе и инкременте счетчиков интерфейса на исходящем интерфейсе.

Пояснение NAT

См. эти документы для получения дополнительной информации о заказе операции NAT:

- Версия программного обеспечения 8.2 Cisco ASA и ранее
- Версия программного обеспечения 8.3 Cisco ASA и позже

Команды "show"

Вот некоторые полезные команды, которые помогают отслеживать подробные данные потока пакетов на других этапах в процессе:

```
show interface
show conn
show access-list
show xlate
show service-policy inspect
show run static
show run nat
show run global
show nat
show route
show arp
```

Сообщения системного журнала предоставляют полезные сведения о пакетной обработке. Вот некоторые сообщения системного журнала в качестве примера для вашей ссылки:

- Сообщение системного журнала, когда нет никакого соединения:`%ASA-6-106015: Deny TCP (no connection) from IP_address/port to IP_address/port flags tcp_flags on interface interface_name`
- Сообщение системного журнала, когда пакет запрещен ACL:`%ASA-4-106023: Deny protocol src [interface_name:source_address/source_port] dst interface_name:dest_address/dest_port by access_group acl_ID`
- Сообщение системного журнала, когда нет никакого найденного правила трансляции:`%ASA-3-305005: No translation group found for protocol src interface_name: source_address/source_port dst interface_name:dest_address/dest_port`
- Сообщение системного журнала, когда пакет запрещен Проверкой безопасности:`%ASA-4-405104: H225 message received from outside_address/outside_port to inside_address/inside_port before SETUP`
- Сообщение системного журнала, когда нет никаких сведений о маршруте:`%ASA-6-110003: Routing failed to locate next-hop for protocol from src interface:src IP/src port to dest interface:dest IP/dest port`

Для полного списка всех сообщений системного журнала, генерируемых Cisco ASA наряду с кратким объяснением, обратитесь к Сообщениям системного журнала Серии Cisco ASA.

Дополнительные сведения

- Страница технической поддержки Cisco ASA
- Справочник по командам серии 5500 Cisco ASA, 8.2
- Руководство по настройке Cisco ASA 5500, 8.3
- Cisco Systems – техническая поддержка и документация