НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР
ФОРС

# Межсетевые экраны. Способы организации защиты (Firewall)

# Содержание

- **Межсетевые экраны. Способы организации защиты (Firewall)**
- **Межсетевой экран (Firewall)**
- **Классификация межсетевых экранов**
- **Фильтрующие маршрутизаторы**
- **Шлюзы сеансового уровня (Сервер аутентификации) AAA**
- **Шлюзы уровня приложений (firepower) Фильтры уровня приложений**
- **Защита сети от несанкционированного доступа из Интернет**
- **Защита корпоративной сети на основе межсетевого экрана**

# Содержание

- Классификация межсетевых экранов
- Cisco ASA и PIX Firewall. Характеристики
- Алгоритм ASA (Adaptive Security Algorithm)
- Технология аутентификации - Cut-through proxy
- Инспектирование протоколов и приложений
- Виртуальный firewall (Security Context)
- Поддержка отказоустойчивости (Failover)
- Прозрачный firewall (Transparent firewall)
- Управление через Web интерфейс

# Межсетевой экран (Firewall)

Межсетевой экран — это система межсетевой защиты, позволяющая разделить каждую сеть на две и более части и реализовать набор правил, определяющих условия прохождения пакетов с данными через границу из одной части общей сети в другую.

# Классификация межсетевых экранов

- экранирующий шлюз (прикладной шлюз), синоним Шлюзы уровня приложений.

- экранирующий транспорт (шлюз сеансового уровня),- синоним здесь Шлюзы сеансового уровня.

- экранирующий маршрутизатор (пакетный фильтр); - синоним здесь описан как Фильтрующие маршрутизаторы. (фильтрует заголовки)

# Фильтрующие маршрутизаторы

- Фильтрация IP-пакетов на основе группы полей заголовка пакета:
  - IP-адрес отправителя;
  - IP-адрес получателя;
  - порт отправителя;
  - порт получателя;
  - Флаги (пакет приходящий с таким-то флагом не пропускать, все входящие соединения с флагом setup мы отбрасываем).

# Фильтрующие маршрутизаторы

Преимущества:

+ невысокая стоимость;
+ гибкость в определении правил фильтрации;
+ небольшая задержка при прохождении пакетов.

Недостатки:

− внутренняя сеть маршрутизируется из сети Интернет;
− правила фильтрации пакетов трудны в описании и требуют очень хороших знаний технологий TCP и UDP;
− при нарушении работоспособности межсетевого экрана с фильтрацией пакетов все компьютеры за ним становятся полностью незащищенными либо недоступными;
− отсутствует аутентификация на пользовательском уровне.

# Шлюзы сеансового уровня (Сервер аутентификации) AAA

# Шлюзы уровня приложении (firepower)
## Файервалл уровня приложений

Преимущества:

+ невидимость структуры защищаемой сети из глобальной сети Интернет;
+ надежная аутентификация и регистрация;
+ приемлемое соотношение цены и эффективности;
+ простые правила фильтрации;
+ возможность организации большого числа проверок;

Недостатки:

− относительно низкая производительность по сравнению с фильтрующими маршрутизаторами;
− более высокая стоимость по сравнению с фильтрующими маршрутизаторами.

# Недостатки применения межсетевых экранов

- большое количество остающихся уязвимых мест;
- неудовлетворительная защита от атак сотрудников компании;
- ограничение в доступе к нужным сервисам;
- концентрация средств обеспечения безопасности в одном месте. Это позволяет легко осуществлять администрирование работы межсетевого экрана;
- ограничение пропускной способности.

# Защита сети от несанкционированного доступа из Интернет

- аппаратно-программный или программный межсетевой экран;
- маршрутизатор со встроенным пакетным фильтром;
- специализированный маршрутизатор, реализующий механизм защиты на основе списков доступа;
- операционная система семейства UNIX или, реже, MS Windows, усиленная специальными утилитами, реализующими пакетную фильтрацию.

- семантическая фильтрация потоков данных;
- фильтрация на основе сетевых адресов отправителя и получателя;
- фильтрация запросов на транспортном уровне на установление виртуальных соединений;
- фильтрация запросов на прикладном уровне к прикладным сервисам;
- локальная сигнализация попыток нарушения правил фильтрации;
- запрет доступа неизвестного субъекта или субъекта, подлинность которого при аутентификации не подтвердилась;

# Классификация межсетевых экранов

- по исполнению:
  - аппаратно-программный,
  - программный;
- по функционированию на уровнях модели OSI:
  - шлюз экспертного уровня,
  - экранирующий шлюз (прикладной шлюз),
  - экранирующий транспорт (шлюз сеансового уровня),
  - экранирующий маршрутизатор (пакетный фильтр);
- по используемой технологии:
  - контроль состояния протокола,
  - на основе модулей-посредников (proxy);
- по схеме подключения:
  - схема единой защиты сети,
  - схема с защищаемым закрытым и не защищаемым открытым сегментами сети,
  - схема с раздельной защитой закрытого и открытого сегментов сети.

# Межсетевые экраны

Cisco ASA и PIX Firewall


ZyXEL ZyWALL 5


D-LINK **DFL**-1600 Medium Business/Workgroup **Firewall** с ZoneDefense

# Cisco ASA и PIX Firewall. Характеристики

- Собственная операционная система (Proprietary operating system)
- Использование алгоритма ASA (Adaptive Security Algorithm)
- Поддержка user-based аутентификации (Cut-through proxy)
- Инспектирование протоколов и приложений (Application-Aware Inspection)
- Виртуальный фаервол (Security Context)
- Поддержка избыточности (Failover)
- Прозрачный фаервол (Transparent firewall)
- Управление устройством через Web интерфейс (ASDM)

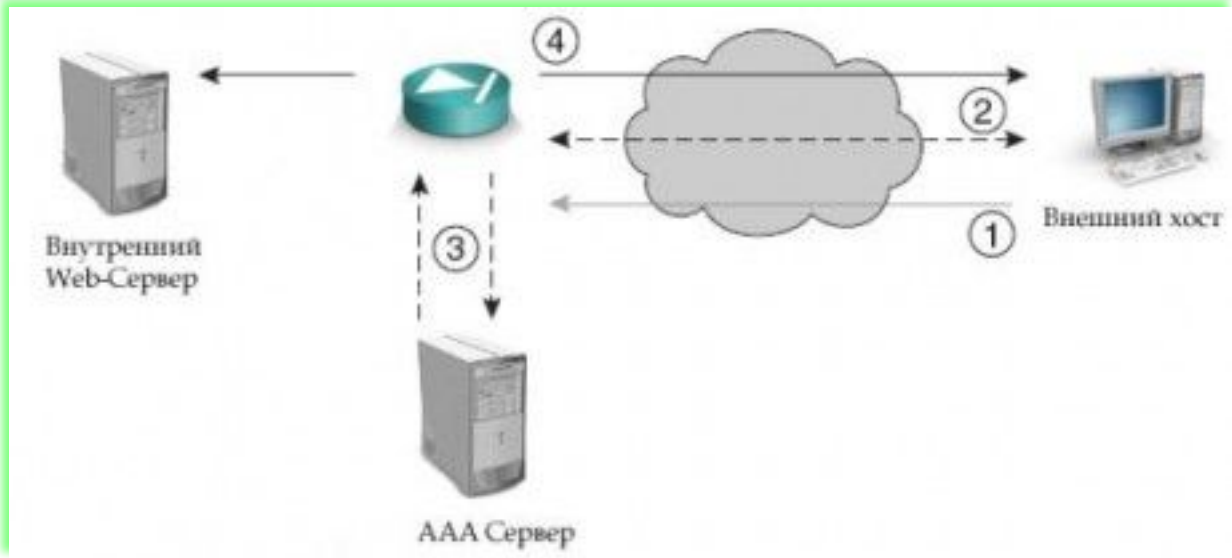
# Алгоритм ASA (Adaptive Security Algorithm)


1. Внутренний хост инициирует соединение на внешний ресурс.
2. Cisco ASA ( PIX Firewall ) делает запись следующей информации в таблицу состояния (state table):
   1. Адрес источника и порт
   2. Адрес назначения и порт
   3. Дополнительные TCP/UDP флаги
   4. Произвольно сгенерированный TCP sequence number
   5. Данная запись называется объектом сессии (session object)
3. Объект сессии (session object) сравнивается с политикой безопасности. Если соединение не разрешено, объект сессии (session object) удаляется и соединение сбрасывается.
4. Если соединение одобрено политикой безопасности, адрес источника

# Пример объекта сессии

| State Table | Session Object | |
|---|---|---|
| Адрес источника | 192.168.0.10 | 10.0.0.1 |
| Адрес назначения | 172.16.0.10 | 172.16.0.10 |
| Порт источника | 1027 | 1027 |
| Порт назначения | 80 | 80 |
| Initial TCP sequence | 49769 | 49091 |
| Ack | | |
| Flag | Syn | Syn |

# Технология аутентификации - Cut-through proxy



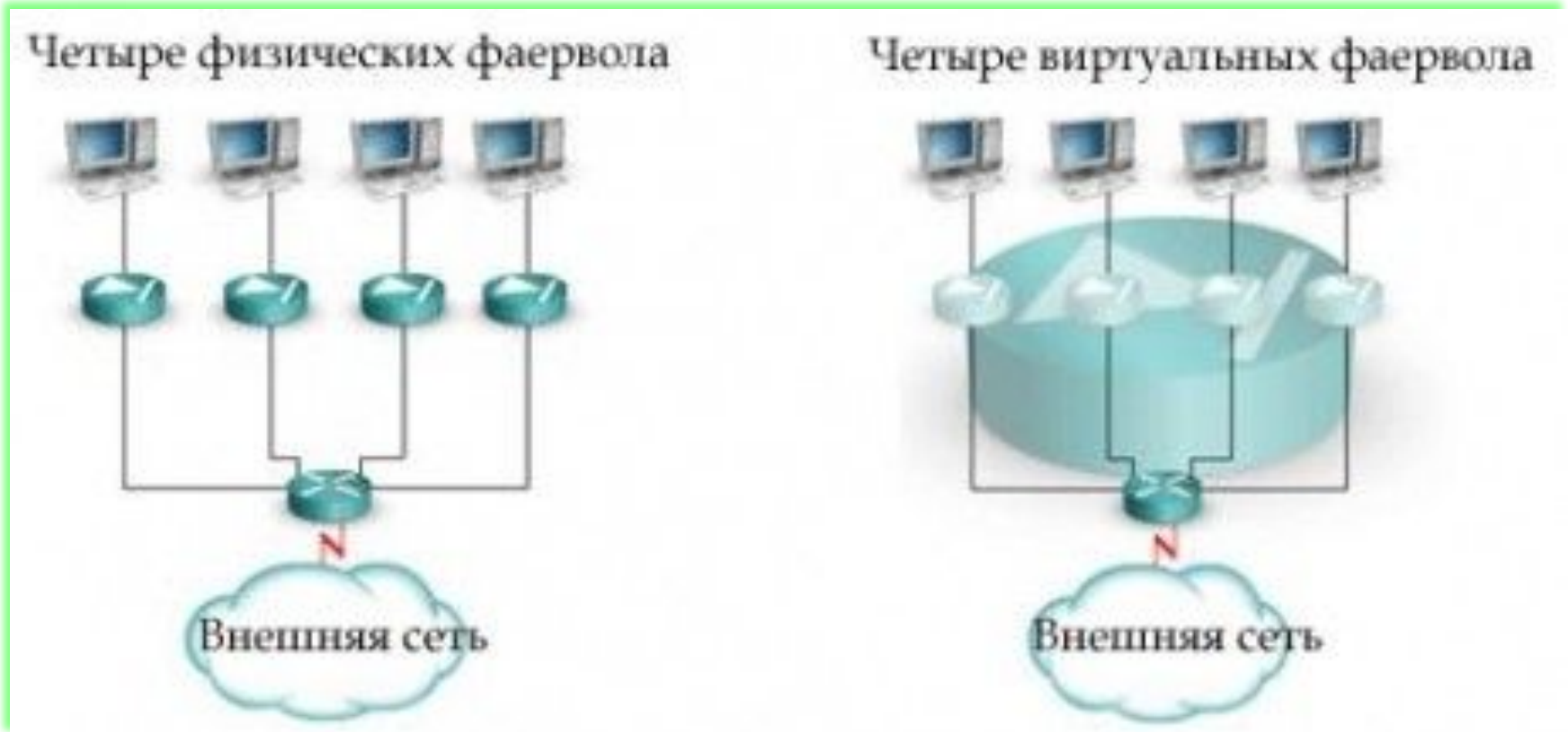

- 1 - Пользователем инициируется FTP, HTTP(S) либо Telnet соединение на внутренний веб-сервер
  2 - Cisco ASA ( PIX Firewall ) в ответ на это предлагает аутентификацию и пользователь вводит данные учетной записи.
  3 - Cisco ASA ( PIX Firewall ) используя протокол TACACS+ либо RADIUS, связывается с сервером AAA, где пользователь успешно аутентифицируется.
  4 - Открывается соединение с веб-сервером на сетевом уровне, информация о сессии записывается в таблицу соединений (connection table) и в дальнейшем трафик соединения инспектируется алгоритмом ASA.

# Инспектирование протоколов и приложений


Требования в межсетевому экрану:

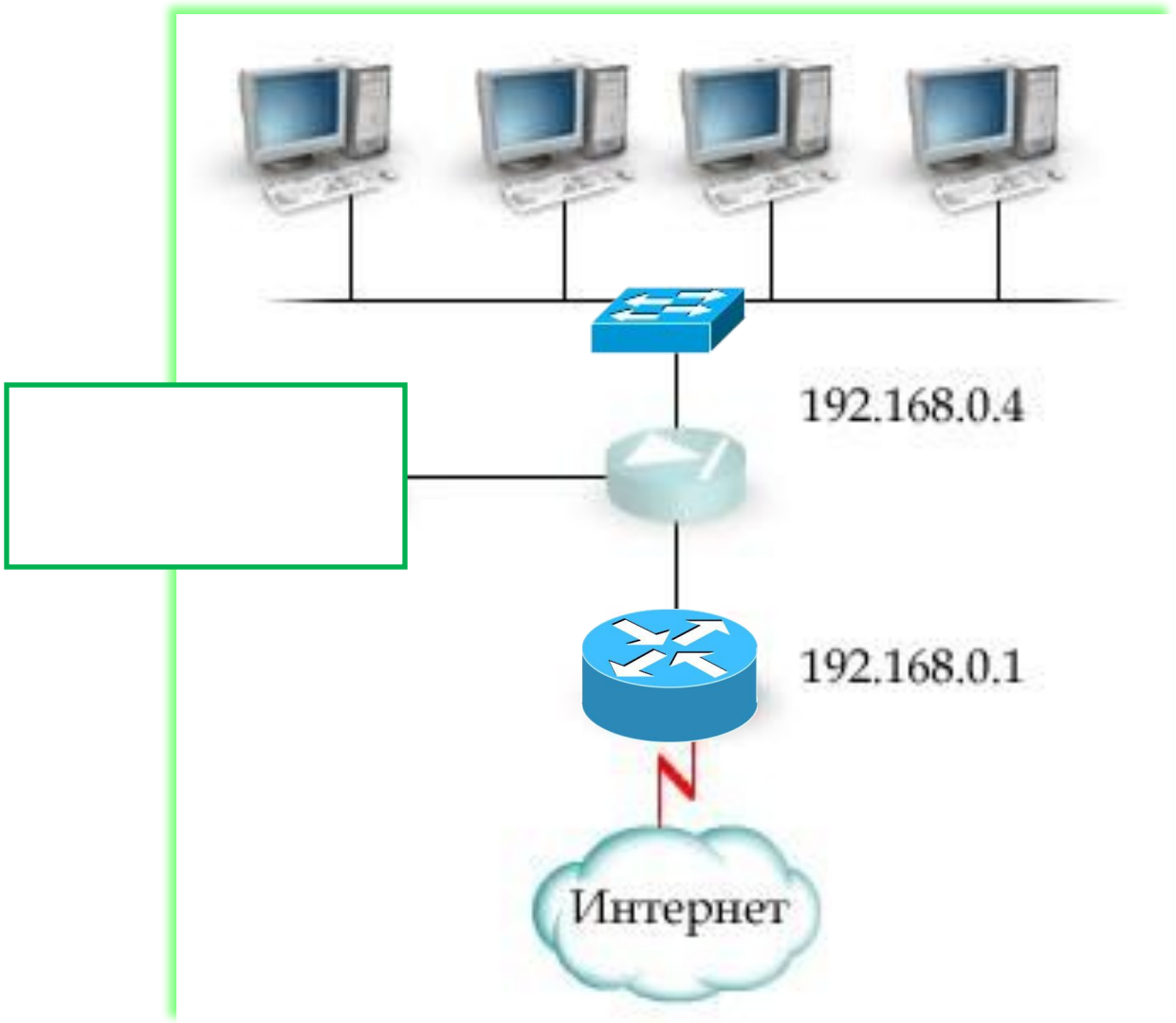
- Безопасно открывать и закрывать динамически выделяемые порты или IP адреса на фаерволе для разрешенных клиет-серверных соединений.
- Использовать сетевую трансляцию адреса (NAT) внутри IP пакета
- Использовать трансляцию портов (PAT) внутри пакета
- Инспектировать пакеты на предмет неправильного (злонамеренного) использования приложений.

# Виртуальный firewall (Security Context)



# Поддержка отказоустойчивости (Failover)

# Прозрачный firewall (Transparent firewall)



# Управление через Web интерфейс

НАУЧНО-
ИССЛЕДОВАТЕЛЬСКИЙ
ЦЕНТР
ФОРС

# Вопросы?