Лекция

Защита вычислительных сетей от DDOS-атак

Лекция

Защита вычислительных сетей от DDOS-атак

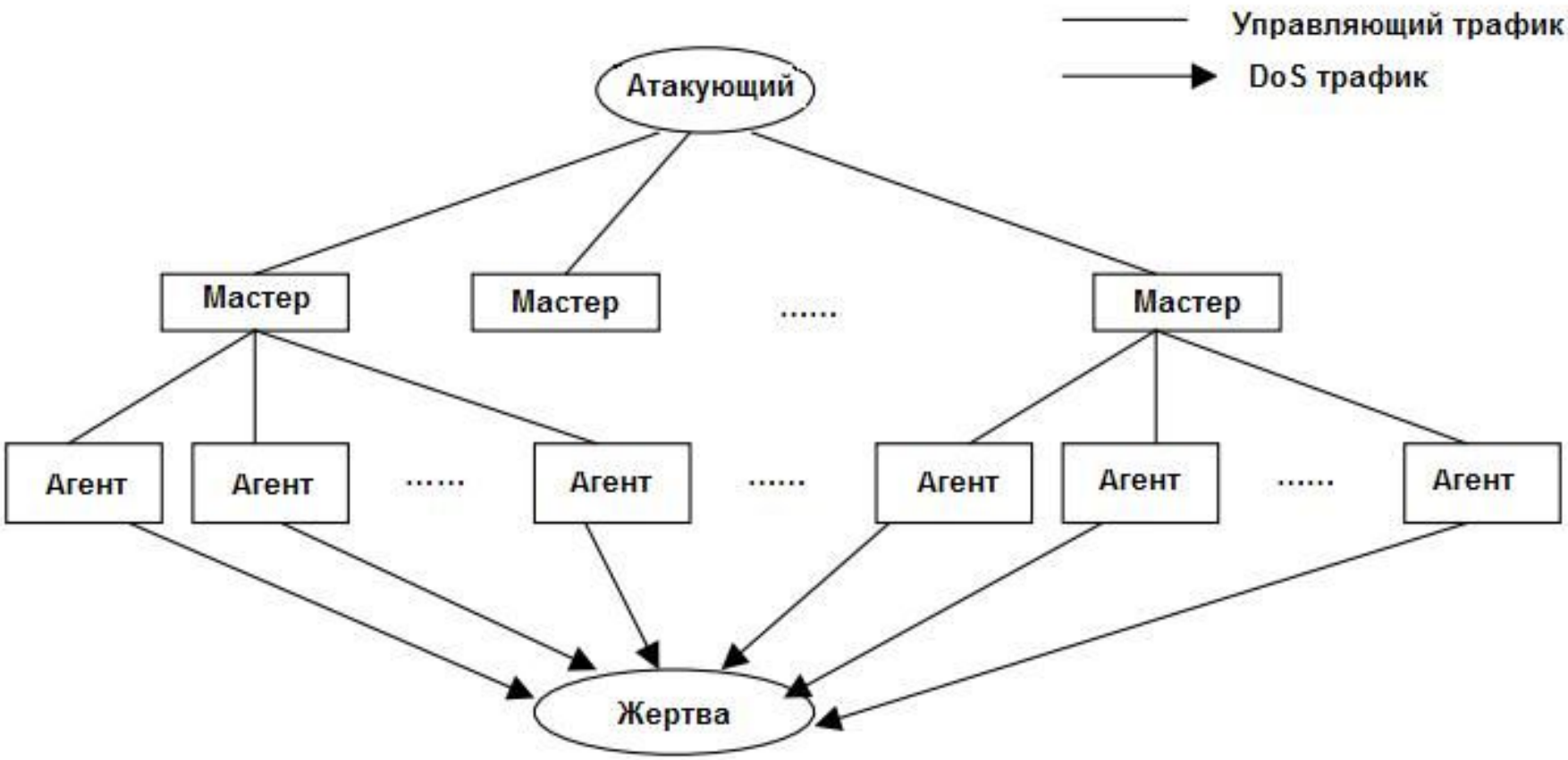
распределенный
отказ в обслуживании - это скоординированная атака
на нарушение доступности услуг (сервисов) системы
или сетевого ресурса

DDOS (Distributed Denial of Service) – распределенный отказ в обслуживании - это скоординированная атака на нарушение доступности услуг (сервисов) системы или сетевого ресурса

Базируется на реализации множества атак «отказ в обслуживании» (DOS) , проводимых множеством скомпрометированных узлов.

Spoofing – подмена IP адресов

Модель бот-сети



Классификация DDOS атак

1. Атаки на истощение ресурса сети:
Flood –атаки (UDP-flood, ICMP-flood, HTTP-flood, DNS-flood)
Атаки , использующие отражатели: (Smurf, Fraggle)

2. Атаки на истощение ресурса узла:
TCP SYN, Land, Ping Death, некорректные пакеты

Атака на истощение ресурсов сети заключается в посылке большого количества пакетов в атакуемую сеть. Они уменьшают ее пропускную способность сети для законных пользователей

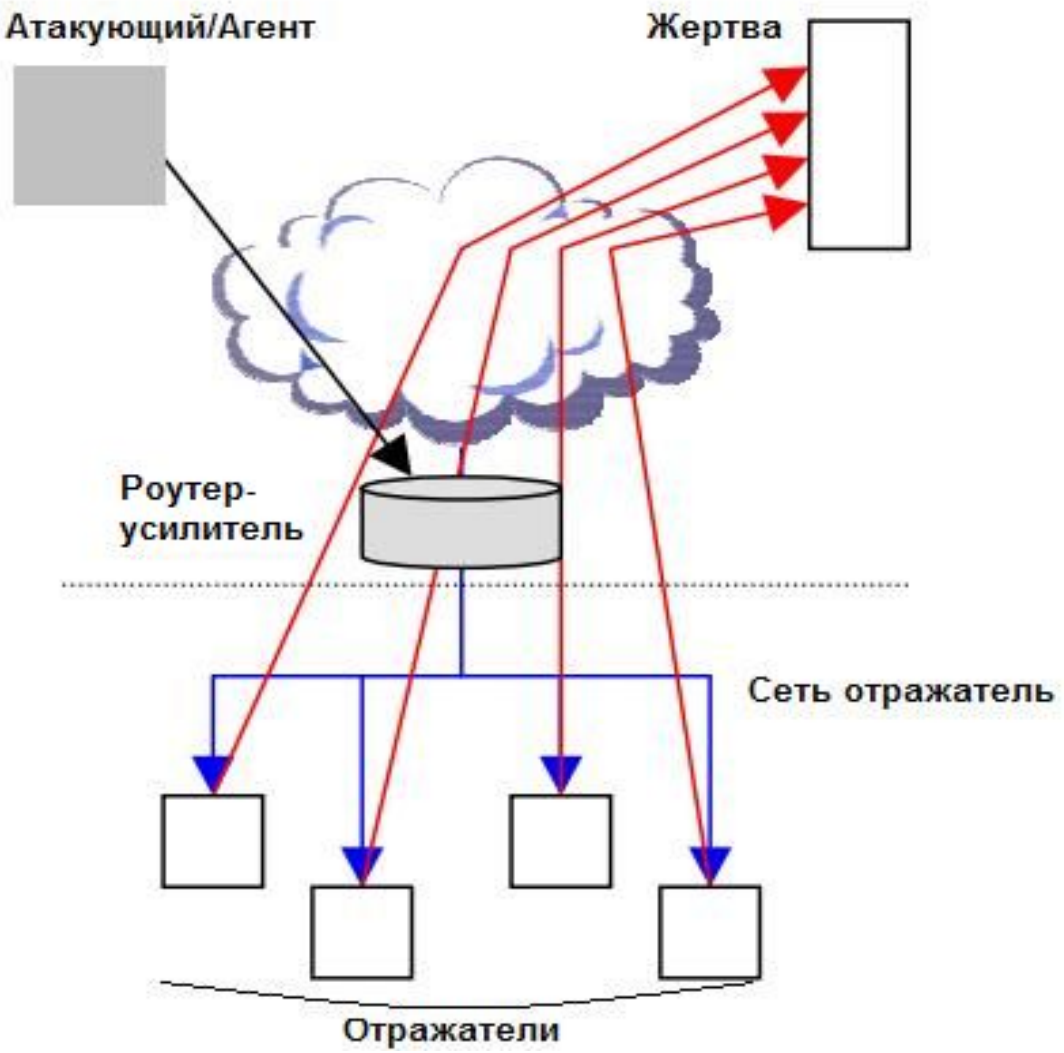
Атака на истощение ресурсов сети заключается в посылке большого количества пакетов в атакуемую сеть. Они уменьшают ее пропускную способность сети для законных пользователей

Атака на истощение ресурсов узла заключаются в посылке большого количества запросов этому узлу. Для каждого запроса выделяется определенный ресурс. Когда ресурс заканчивается, обслуживание поступающих запросов становится невозможным

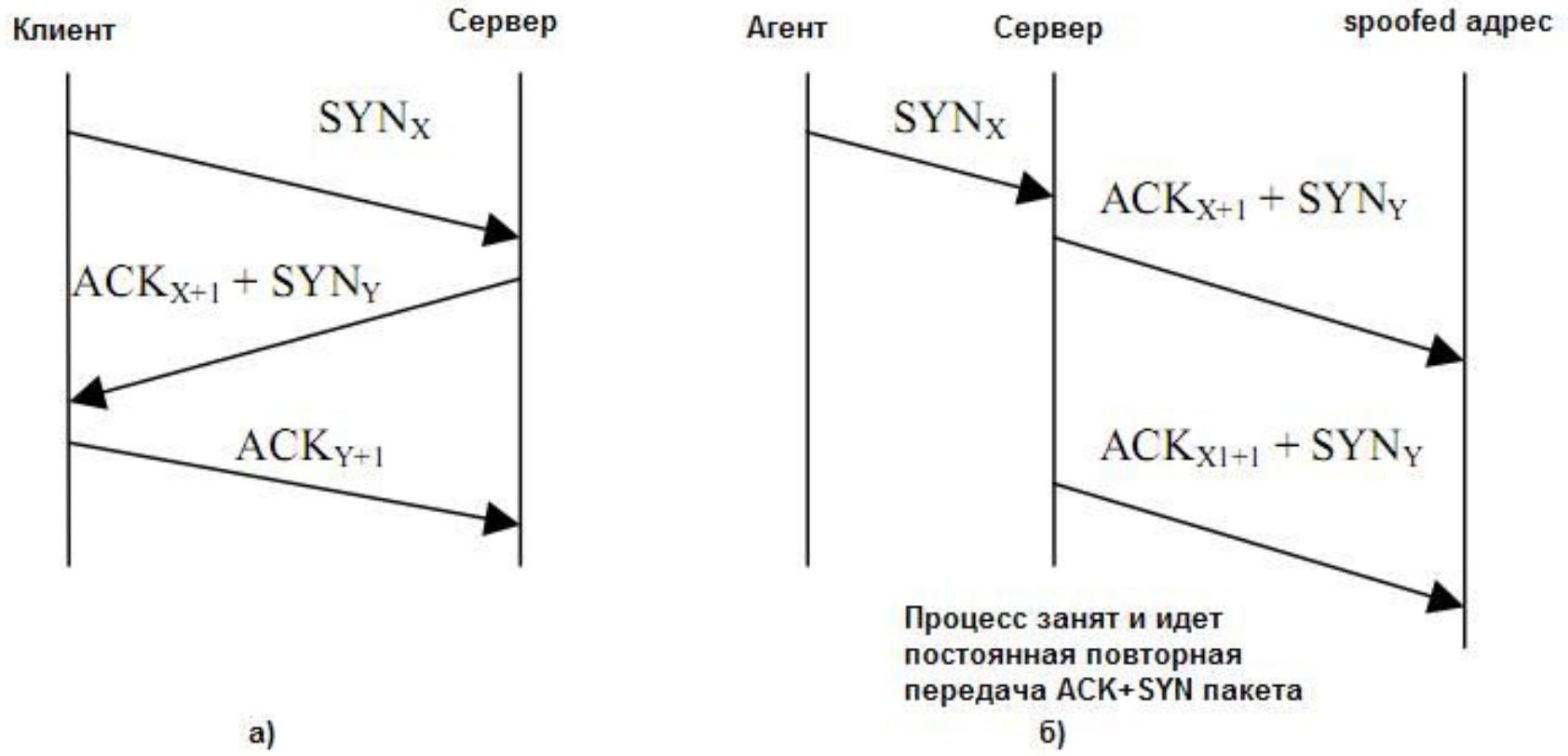
Flood (наводнение) атака – на жертву направляется огромное
количество пакетов, ставится задача исчерпания ресурсов
каналов связи

Flood (наводнение) атака – на жертву направляется огромное количество пакетов, ставится задача исчерпания ресурсов каналов связи

Атаки с использованием отражателей



Атака на истощение ресурсов узла

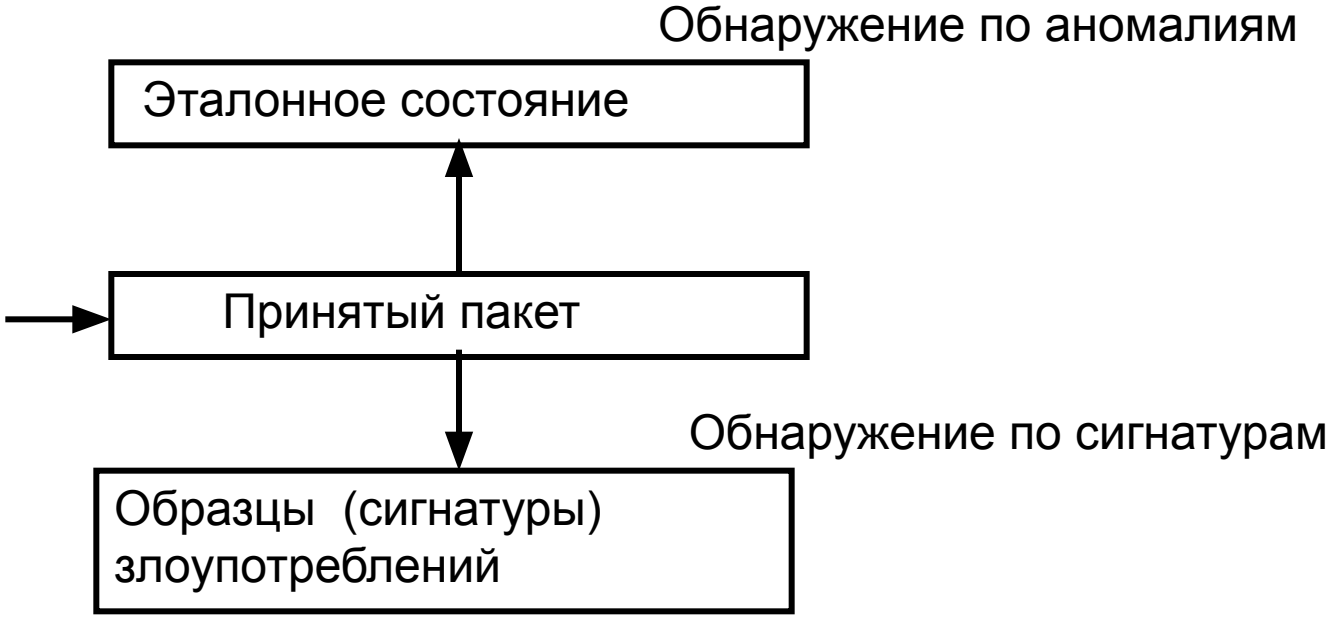


Защита от DDOS атак

Этапы защиты:
-предупреждение атаки;
-обнаружение факта атаки;
-определение источника атаки;
-противодействие атаке

Механизмы обнаружения DDOS-атак

Способы обнаружения:
-обнаружения злоупотреблений (обнаружение по сигнатурам);
- обнаружение по аномалиям



состояния защищаемого объекта с заранее определенными образцами (сигнатурами), которые описывают ту или иную атаку.

Обнаружение злоупотреблений –сравнение текущего состояния защищаемого объекта с заранее определенными образцами (сигнатурами), которые описывают ту или иную атаку.

Обнаружение атак по аномалиям заключается в сравнении текущего состояния системы с тем состоянием, когда нарушения состояния не было (с эталонным состоянием).

Преимущества сигнатурного метода:
-эффективное обнаружение атаки при малом количестве ложных срабатываний;
- простота использования не требующая высокой квалификации администратора ИБ.

Преимущества сигнатурного метода:
-эффективное обнаружение атаки при малом количестве ложных срабатываний;
- простота использования не требующая высокой квалификации администратора ИБ.

Недостатки:
-необходимо постоянно обновлять базу данных сигнатур;
-неспособен выявлять неизвестные атаки

Системы обнаружения атак по аномалиям

Метрики отклонения от модельного состояния:
-сравнение с порогом (нагрузка на сервис);
-спецификация пакетов;
-по вероятностным характеристикам

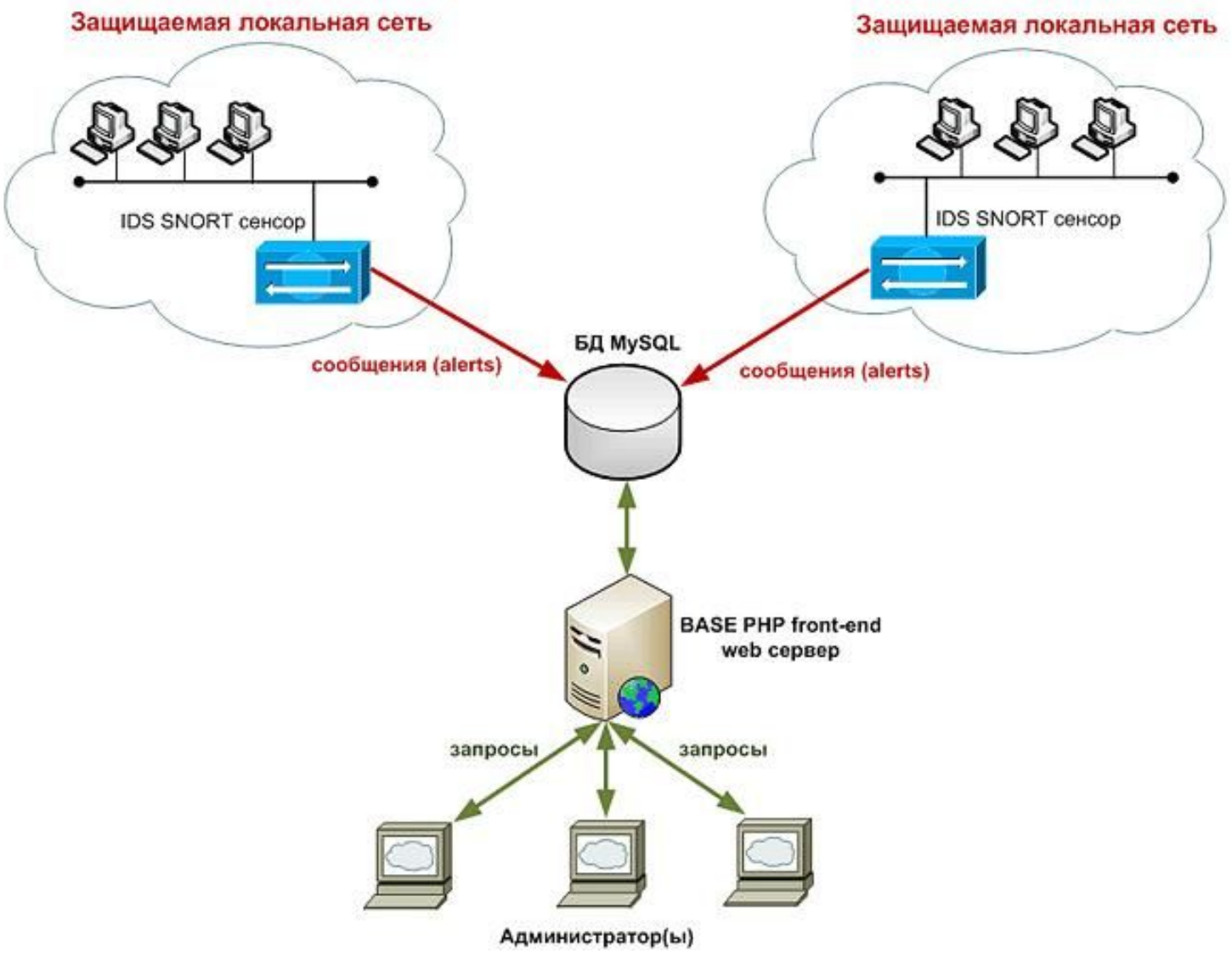
Примеры:
MIB variables;
MULTOPS;
Фильтрация по числу хопов;
D-ward

Системы обнаружения вторжений

IDS (Intrusion detect system)- программное или аппаратное средство для выявления фактов неавторизованного вторжения в компьютерную систему

Коммерческие: Tripwire, CISCO NetRanger;
Свободно распространяемые Snort, OSSEC, Untagle

IDS Snort


Защищаемая локальная сеть
Защищаемая локальная сеть
IDS SNORT сенсор
IDS SNORT сенсор
БД MySQL
сообщения (alerts)
сообщения (alerts)
BASE PHP front-end
web сервер
запросы
запросы
Администратор(ы)

Обеспечивающие компоненты Snort

операционная система FreeBSD или MS Windows;
Snort – сам сенсор с детекторами для обнаружения атак;
libpcap – сниффер для захвата пакетов;
СУБД MySQL – для хранения базы данных событий;
PHP – язык разработки для Web;
Apache – web-сервер;
Basic Analysis and Security Engine (BASE) – консоль управления и просмотра событий (alerts);
Oinkmaster – утилита для обновления сигнатур и некоторые другие.

Примеры настроек Snort

<action> <protocol> <first host> <first port> <direction> <second host> <second port> (<rule options>;)

alert icmp any any -> 192.168.1.1 any (msg: "Ping detected!";)

Правило ждёт ICMP-пакеты с любого узла, направленные на маршрутизатор (192.168.1.1), и при появлении таковых выводит сообщение "Ping detected!".

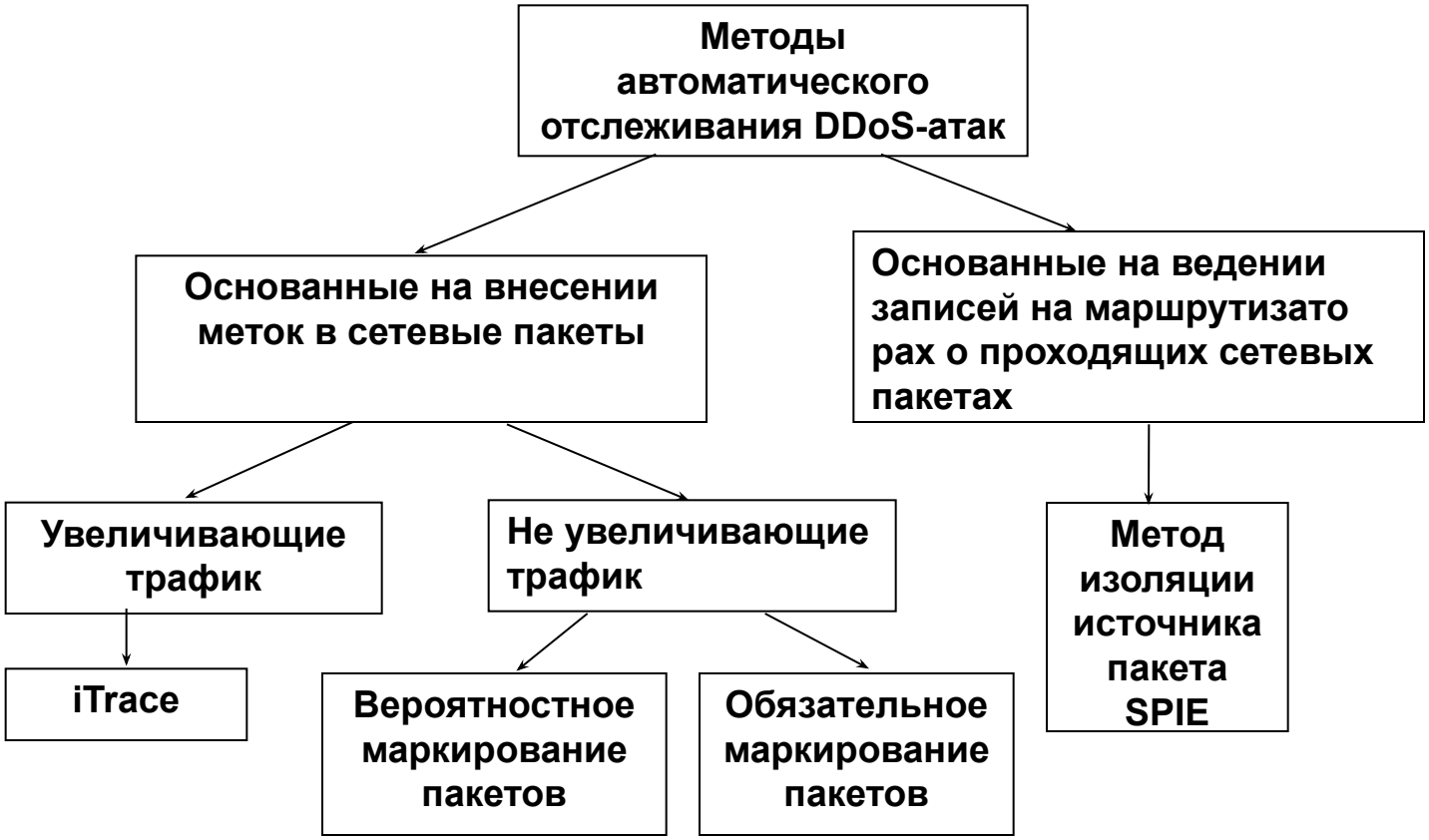
pass icmp any any -> any any (dsize:>65535; msg: "Ping of Death detected!";)

Агент посылет на жертву ICMP пакеты размером большие 65,535 байт, которые не могут быть корректным образом обработаны. Snort проверяет размер входящих ICMP пакетов с помощью параметра dsize и, в случае превышения пакетом установленного размера, отбрасывает их (pass):

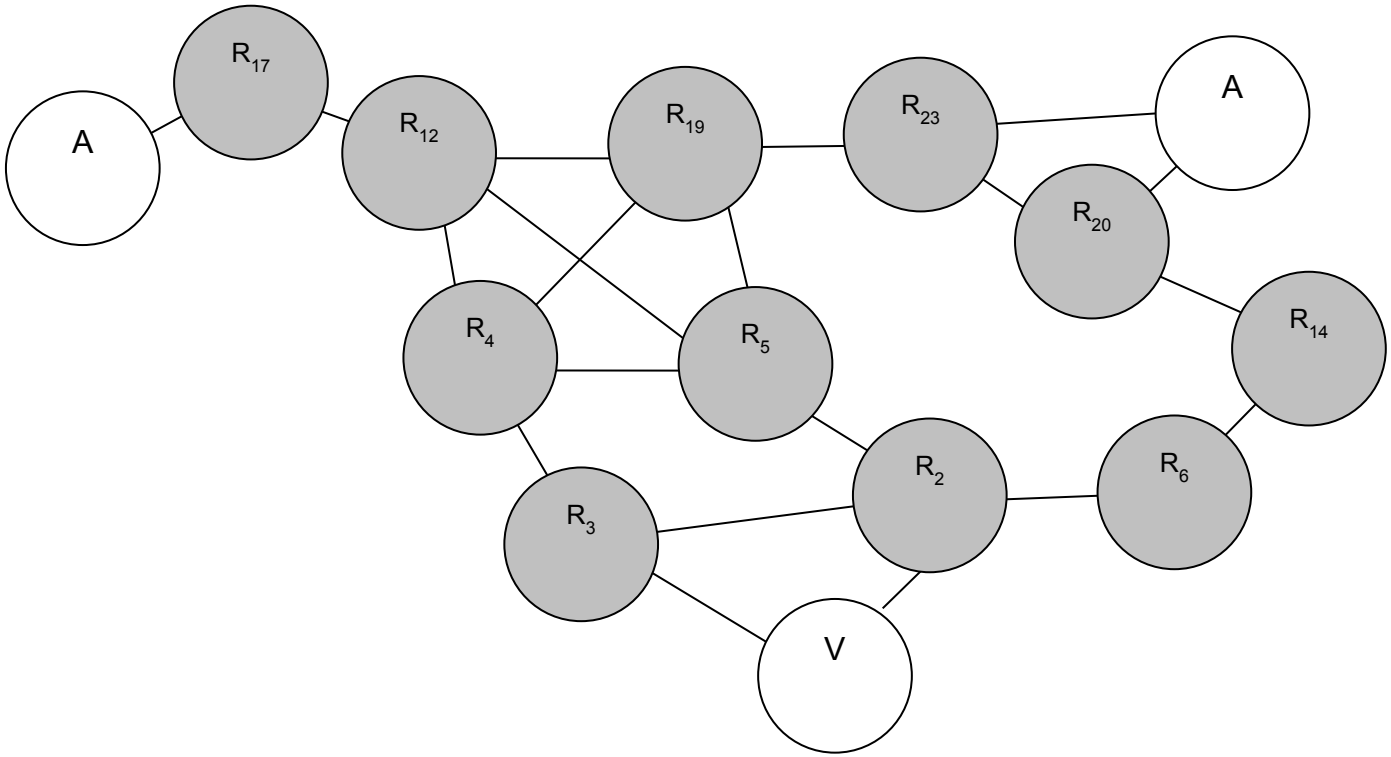
pass ip any any -> any any (sameip; msg: "Land attack detected!";)

Правило проверяет факт совпадения IP адресов, и отбрасывает пакет, если подобная атака имеет место быть:

Методы отслеживания DDOS-атак



Пример топологии сети




32 бита
Версия
IHL
Тип службы
Полная длина
Идентификатор
D F
M F
Смещение фрагмента
Время жизни
Протокол
Контрольная сумма заголовка
Адрес отправителя
Адрес получателя
Необязательная часть (0 или более слов)

Маркирование пакета

Метки, устанавливаемые в дополнительные поля пакета

IP-заголовок	**Начал. адрес**	**Конечн. Адрес**	**Путь**

Метки, устанавливаемые в «свободные» поля заголовка пакета

IP-заголовок

Хэш-код адр. маршр.	**Путь**