ПК Скаут

Функциональные характеристики

Оглавление

1. Назначение ПК "Скаут"

ПК "Скаут" (далее Комплекс) представляет собой программный комплекс защиты от DDoS-атак для развертывания в виртуальной инфраструктуре. Комплекс рассчитан на решение задач по защите ресурсов и сервисов от DDoS-атак, используя следующие функциональные возможности:

- постоянный контроль трафика сети передачи данных и его глубокий анализ;
- обнаружение превышения объемов и количества трафика определенных сигнатур, направленного на хосты защищаемых ресурсов и сервисов;
- формирование детализированной статистики по выявленным векторам DDoS-атак;
- применение интеллектуальной фильтрации трафика с блокированием запрещенной составляющей и пропуском легитимной.

Комплекс включается на пути трафика к сервисам, которые он защищает. Он контролирует весь трафик к сервису, находит в нем атаки, отличает трафик реальных пользователей от трафика атаки и активирует меры противодействия для подавления атак. Комплекс способен противодействовать атакам на каналы связи, протоколы IP, TCP, UDP, DNS, веб-сервисы, сервисы IP-телефонии.

Комплекс способен защищать серверы популярных сетевых игр: Counter-Strike 1.6, Counter-Strike: Source, Counter-Strike: Global Offensive, Half-Life Deathmatch Classic, Half-Life Deathmatch Source, Half-Life 2 Deathmatch, Team Fortress Classic, Team Fortress 2, Day of Defeat, Day of Defeat: Source, Left4Dead, Left4Dead2, Garry's Mod..

Комплекс не требует приобретения специализированного оборудования и запускается на стандартных серверах с архитектурой x86/amd64 и платформе виртуализации Linux KVM.

2. Программные и аппаратные требования к системе

Виртуальная среда VMware ESXI 6 или QEMU Emulator в следующей конфигурации

- KVM QEMU 3.1, libvirt 5.0 или VMWare 6.7
- vCPU 3..6 x86/amd64 с поддержкой SSE4.2
- ОЗУ 32Гб
- HDD 500Гб
- Сетевой интерфейс (входной) virtio
- Сетевой интерфейс (выходной) virtio
- Сетевой интерфейс управления virtio
- Интерфейс serial - локальная консоль

либо

Физический сервер в следующей конфигурации

- ОС Debian 10, 11; DPDK 21.08+
- CPU 4..48 ядер x86/amd64 с поддержкой SSE4.2
- ОЗУ 32..256Гб
- HDD 500Гб
- Сетевой интерфейс (входной) DPDK

- Сетевой интерфейс (выходной) DPDK
- Сетевой интерфейс управления

Дополнительно может использоваться:

- Интернет - для получения лицензии и загрузки списков с внешних серверов
- Веб-браузер - для управления комплексом посредством веб-интерфейса
- Почтовый сервер - для отправки почтовых уведомлений
- Коллектор сообщений syslog - для приема сообщений CEF/LEEF
- Сервер времени - для автоматической синхронизации времени
- АПК «Периметр» - для построения эшелонированной защиты

Примечание. Для работы веб-интерфейса в браузере должна быть включена поддержка JavaScript и cookies.

3. Основные характеристики ПК "Скаут"

Комплекс характеризуется следующими функциональными возможностями:

- интеллектуальная фильтрация трафика с блокированием запрещенной составляющей и пропуском легитимной;
- автоматическое (при выявление соответствующего вектора атаки) или ручное включение предварительно настроенных контрмер для подавления DDoS-атак;
- сбор детализированной статистики по трафику при выявлении DDoS-атаки;
- сбор пакетов по заданному фильтру, декодирование пакетов, а также их выгрузка в формате pcap;
- разделение всего анализируемого трафика на группы защиты, имеющие индивидуальные настройки выявления DDoS-атак и фильтрации трафика;
- загрузка с внешних серверов списков источников вредоносного трафика и использование их для подавления DDoS-атак;
- взаимодействие с АПК "Периметр" для подавления атаки на мощностях провайдера, реализующее концепцию "подавление в облаке";
- отправка отчетов на e-mail при выявлении DDoS-атак;
- взаимодействие с внешними системами посредством API и протокола syslog.

4. Технические характеристики

Функции защиты от DDoS-атак:

- детектирование атак по профилю трафика;
- фильтрация по спискам: черные, белые, географические;
- фильтрация по правилам по параметрам протоколов IP, TCP, UDP;
- фильтрация по содержимому пакетов;
- фильтрация флуда фрагментированными пакетами;
- фильтрация неправильно сформированных пакетов;
- защита от хостов-зомби;
- ограничение по полосе пропускания для каждой отдельной сессии протоколов TCP/UDP или по правилам;
- контрмеры для защиты протокола TCP: подтверждение подлинности соединений, ограничение количества соединений, фильтрация простаивающих соединений;
- специализированные контрмеры для протоколов HTTP, TLS, DNS, SIP;
- защита серверов сетевых игр: Counter-Strike 1.6, Counter-Strike: Source, Counter-Strike: Global Offensive, Half-Life Deathmatch Classic, Half-Life Deathmatch Source, Half-Life 2 Deathmatch, Team Fortress Classic, Team Fortress 2, Day of Defeat, Day of Defeat: Source, Left4Dead, Left4Dead2, Garry's Mod.

Способ установки на сеть - в разрыв канала.

Режим работы - прозрачный L2 мост.

Управление - Web-интерфейс на русском языке, HTTPS API.

Уведомления - протокол syslog, форматы CEF/LEEF.

Отчеты - e-mail.

При использовании виртуальной машины:

- Пропускная способность*, bps - 1.5 Gbps
- Пропускная способность*, pps - 0.6 Mpps
- Вносимая задержка, менее - 100 мкс
- Сетевые интерфейсы управления - virtio
- Сетевые интерфейсы очистки - virtio

* пропускная способность зависит от распределения ядер VM и особенностей конфигурации и может отличаться в большую или меньшую сторону.

При использовании физического сервера:

- Пропускная способность, bps - до 100 Gbps
- Пропускная способность, pps - до 90 Mpps
- Вносимая задержка, менее - 100 мкс
- Сетевые интерфейсы управления - ethernet
- Сетевые интерфейсы очистки - dpdk-совместимые