



Кейс гибкий контроль трафика в реальном времени





Постановка проблемы

В современном мире безопасность сетей становится критически важной задачей. Компании сталкиваются с необходимостью фильтровать сетевой трафик, чтобы предотвратить утечки данных, атаки или несанкционированный доступ. Традиционные файрволы могут быть громоздкими, ресурсоёмкими или недостаточно гибкими для специфических задач. Ваша команда должна разработать инновационное решение — файрвол на основе технологии eBPF, который обеспечит точечный контроль сетевого трафика.





Задача

Разработать прототип файрвола, использующего eBPF (extended Berkeley Packet Filter)



МАДРИГАЛ





Блокирует весь входящий и исходящий сетевой трафик, за исключением HTTP-трафика (протоколы HTTP и HTTPS)







02

Разрешает HTTP/HTTPS-трафик только на заданных портах (например, 80 для HTTP и 443 для HTTPS, либо порты, указанные пользователем)

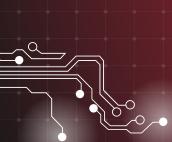


МАДРИГАЛ





Работает на уровне ядра операционной системы для обеспечения максимальной производительности









Поддерживает запуск на любой Linux-системе с поддержкой eBPF (например, Ubuntu 20.04+)









05

Реализован на любом языке программирования (например, C, Go, Python с использованием библиотек вроде ВСС или Cilium), где еВРF-программа взаимодействует с ядром



Цель

Создать минимально жизнеспособный продукт (MVP), который демонстрирует



Блокировку всего трафика, кроме HTTP/HTTPS на указанных портах within budget Простую настройку (например, через конф игурационный файл или CLI)

Логирование заблокированного и разрешённого трафика для анализа





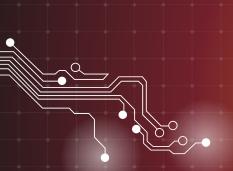
Условия

- Используйте открытые библиотеки и инструменты (ВСС, libbpf, Cilium и т.д.)
- Решение должно быть протестировано на виртуальной машине или контейнере (например, Docker)
- Докажите работоспособность с помощью простого теста (например, `curl` для проверки HTTP и
 `ping` для проверки блокировки)
- Добавить анализ полезной нагрузки пакета (payload) на уровне ядра
- Проверять, содержит ли пакет сигнатуру HTTP (например, строки GET, POST, HTTP/1.1) или HTTPS (шиф рованный траф ик через TLS handshake)
- Если это "простое TCP" без HTTP-формата, сбрасывать такие пакеты (например, с XDP_DROP)



По вопросам писать сюда







Контакты:

info@ madrigal.expert +7 863 285-50-80 мадригал.рус

Призовой фонд: 50 000 руб.

