СӘТБАЕВ УНИВЕРСИТЕТІ SATBAYEV UNIVERSITY

Дисциплина «Этичный хакинг и противодействие взлому»

Лекция 12

Системы обнаружения вторжений (IDS)

Преподаватель: **Батыргалиев Асхат Болатканович, PhD, ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»**

askhat.b.b@gmail.com

Содержание

1. Понятие IDS
2. Назначение IDS
3. Классификация IDS
4. Принцип работы IDS
5. Архитектура и технология IDS
6. Виды IDS по принципу действия
7. Места установки IDS
8. Open Source проекты и некоторые вендоры на рынке IDS

По завершению лекции Вы будете знать:

1. Понятие и назначение IDS
2. Классификацию и принцип работы IDS
3. Архитектуру и технологию IDS
4. Виды IDS по принципу действия
5. Места установки IDS
6. Open Source проекты и некоторые вендоры на рынке IDS

Понятие IDS

Intrusion Detection System (IDS) - система обнаружения вторжений - программный продукт или устройство, предназначенные для выявления несанкционированной и вредоносной активности в компьютерной сети или на отдельном хосте.

Задача IDS - обнаружить проникновение киберпреступников в инфраструктуру и сформировать оповещение безопасности (функций реагирования, например блокировки нежелательной активности, в таких системах нет), которое будет передано в SIEM-систему для дальнейшей обработки.

Системы обнаружения угроз отличаются от классических файрволов, поскольку последние опираются на набор статических правил и просто ограничивают трафик между устройствами или сегментами сети, не отправляя уведомлений. Развитием идеи IDS являются Intrusion Prevention System (IPS, системы предотвращения вторжений), способные не только фиксировать, но и блокировать угрозы.

Назначение IDS

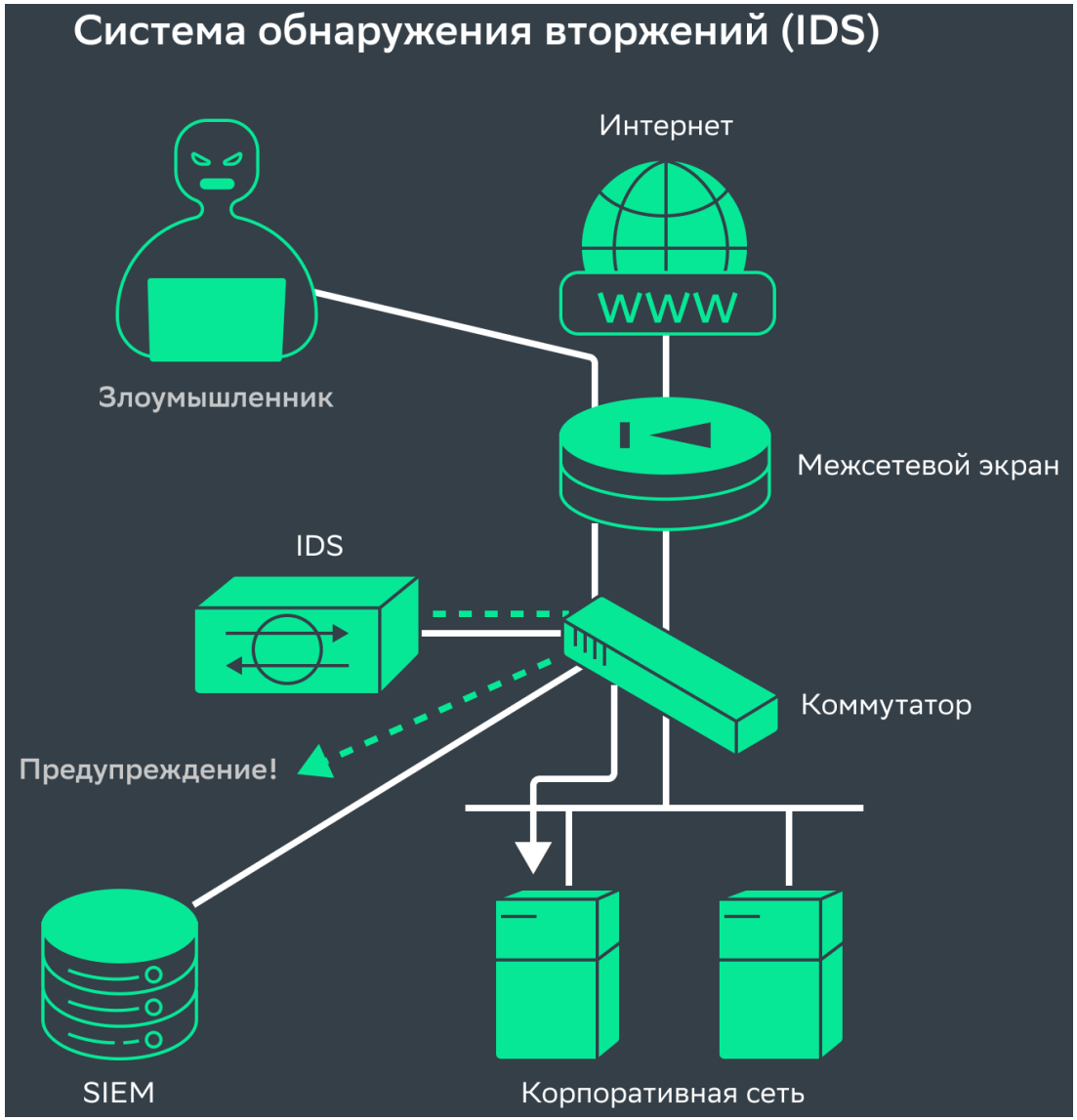
IDS отслеживает трафик, сравнивая его с собственной базой данных возможных сетевых атак и базовой сетевой активностью. Такой механизм работы позволяет обнаруживать:

- сетевые атаки;
- неавторизованный доступ к данным;
- действия вредоносных скриптов и программ;
- функционирование сканеров портов;
- нарушение политик безопасности;
- обращение к центрам управления бот-сетями и майнинг-пулам;
- аномальную активность.

Обнаружить нарушения политик безопасности можно за счет написания своих собственных паттернов детектирования. Это помогает отслеживать определенное поведение в сети.

Важно заметить, что IDS-система не отражает атаки, а только обнаруживает их и уведомляет администратора, помогая найти причину и устранить ее.

Назначение IDS



Принцип работы IDS

Принцип работы IDS заключается в определении угроз на основании анализа трафика, но дальнейшие действия остаются за администратором.

Системы обнаружения вторжения детектируют вредоносную активность одним из двух методов:

Обнаружение на основании сигнатур - метод, при котором IDS сравнивает проверяемые данные с известными образцами сигнатур атаки и создает оповещение безопасности в случае их совпадения. Так можно выявлять вторжения, которые основаны на ранее известных способах проникновения.

Обнаружение на основании аномалий. В этом случае IDS сравнивает активность в сети или на хосте с моделью корректного, доверенного поведения контролируемых элементов и фиксирует отклонения от нее. Этот метод позволяет выявлять новые угрозы.

Классификация IDS

Системы обнаружения вторжений принято классифицировать по сфере применения. Выделяют следующие типы IDS:

Network Intrusion Detection System (NIDS) - системы, анализирующие сетевой трафик с целью выявления вредоносной активности. В отличие от межсетевых экранов, NIDS выполняют мониторинг как входящего, так и внутреннего сетевого трафика.

Host Intrusion Detection System (HIDS) - инструменты, контролирующие работу отдельных устройств. Обычно HIDS фиксирует состояние всех файлов, размещенных на конечной точке, и информирует администратора об удалении или изменении системных объектов. Кроме того, этот вид IDS проверяет все пакеты данных, передаваемые на устройство или с него.

Protocol-based Intrusion Detection System (PIDS) - система проверки данных, передаваемых по протоколу HTTP/HTTPS. Обычно PIDS применяется для защиты веб-серверов и контролирует трафик, передаваемый между устройством пользователя и интернет-ресурсом.

Application Protocol-based Intrusion Detection System (APIDS) - система обнаружения вторжений, контролирующая пакеты, передаваемые по определенному протоколу прикладного уровня - например, заданному для обращения к базе данных SQL.

Hybrid Intrusion Detection System - гибридная система для комплексного обнаружения вредоносной активности, сочетающая свойства двух или более из вышеперечисленных типов, например NIDS и HIDS.

Архитектура и технология IDS

Сетевые системы обнаружения вторжения (NIDS)

Технология NIDS дает возможность установить систему в стратегически важных местах сети и анализировать входящий/исходящий трафик всех устройств сети. NIDS анализируют трафик на глубоком уровне, «заглядывая» в каждый пакет с канального уровня до уровня приложений.

NIDS отличается от межсетевого экрана, или файервола. Файервол фиксирует только атаки, поступающие снаружи сети, в то время как NIDS способна обнаружить и внутреннюю угрозу.

Сетевые системы обнаружения вторжений контролируют всю сеть, что позволяет не тратиться на дополнительные решения. Но есть недостаток: NIDS отслеживают весь сетевой трафик, потребляя большое количество ресурсов. Чем больше объем трафика, тем выше потребность в ресурсах CPU и RAM. Это приводит к заметным задержкам обмена данными и снижению скорости работы сети. Большой объем информации также может «ошеломить» NIDS, вынудив систему пропускать некоторые пакеты, что делает сеть уязвимой.

Архитектура и технология IDS

Хостовая система обнаружения вторжений (HIDS)

Альтернатива сетевым системам - хостовые. Такие системы устанавливаются на один хост внутри сети и защищают только его. HIDS также анализируют все входящие и исходящие пакеты, но только для одного устройства. Система HIDS работает по принципу создания снапшотов файлов: делает снимок текущей версии и сравнивает его с предыдущей, тем самым выявляя возможные угрозы. HIDS лучше устанавливать на критически важные машины в сети, которые редко меняют конфигурацию.

Другие разновидности IDS по месту установки

Кроме NIDS и HIDS, доступны также PIDS (Perimeter Intrusion Detection Systems), которые охраняют не всю сеть, а только границы и сигнализируют об их нарушении. Как забор с сигнализацией или «стена Трампа».

Еще одна разновидность - VMIDS (Virtual Machine-based Intrusion Detection Systems). Это разновидность систем обнаружения угрозы на основе технологий виртуализации. Такая IDS позволяет обойтись без развертывания системы обнаружения на отдельном устройстве. Достаточно развернуть защиту на виртуальной машине, которая будет отслеживать любую подозрительную активность.

Виды IDS по принципу действия

Все системы обнаружения атак IDS работают по одному принципу - поиск угрозы путем анализа трафика. Отличия кроются в самом процессе анализа. Существует три основных вида: сигнатурные, основанные на аномалиях и основанные на правилах.

Сигнатурные IDS

IDS этой разновидности работают по схожему с антивирусным программным обеспечением принципу. Они анализируют сигнатуры и сопоставляют их с базой, которая должна постоянно обновляться для обеспечения корректной работы. Соответственно, в этом заключается главный недостаток сигнатурных IDS: если по каким-то причинам база недоступна, сеть становится уязвимой. Также если атака новая и ее сигнатура неизвестна, есть риск того, что угроза не будет обнаружена.

Сигнатурные IDS способны отслеживать шаблоны или состояния. Шаблоны - это те сигнатуры, которые хранятся в постоянно обновляемой базе. Состояния - это любые действия внутри системы.

Начальное состояние системы - нормальная работа, отсутствие атаки. После успешной атаки система переходит в скомпрометированное состояние, то есть заражение прошло успешно. Каждое действие (например, установка соединения по протоколу, не соответствующему политике безопасности компании, активизация ПО и т.д.) способно изменить состояние. Поэтому сигнатурные IDS отслеживают не действия, а состояние системы.

Как можно понять из описания выше, NIDS чаще отслеживают шаблоны, а HIDS - в основном состояния.

Виды IDS по принципу действия

IDS, основанные на аномалиях

Данная разновидность IDS по принципу работы в чем-то схожа с отслеживанием состояний, только имеет больший охват.

IDS, основанные на аномалиях, используют машинное обучение. Для правильной работы таких систем обнаружения угроз необходим пробный период обучения. Администраторам рекомендуется в течение первых нескольких месяцев полностью отключить сигналы тревоги, чтобы система обучалась. После тестового периода она готова к работе.

Система анализирует работу сети в текущий момент, сравнивает с аналогичным периодом и выявляет аномалии. Аномалии делятся на три категории:

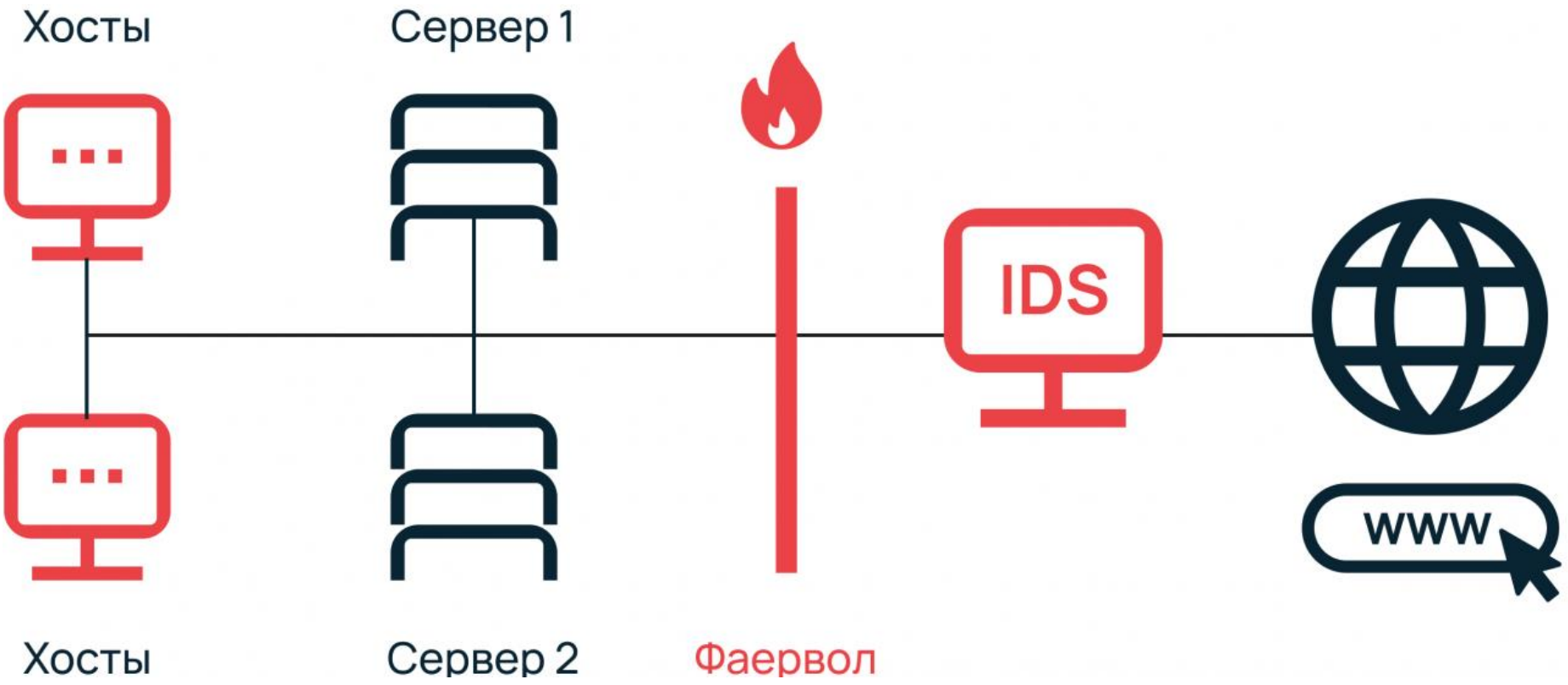
- статистические;
- аномалии протоколов;
- аномалии трафика.

Статистические аномалии выявляются, когда система IDS составляет профиль штатной активности (объем входящего/исходящего трафика, запускаемые приложения и т.д.) и сравнивает его с текущим профилем. Например, для компании характерен рост трафика по будним дням на 90%. Если трафик вдруг возрастет не на 90%, а на 900%, то система оповестит об угрозе.

Для выявления аномалий протоколов IDS-система анализирует коммуникационные протоколы, их связи с пользователями, приложениями и составляет профили. Например, веб-сервер должен работать на порте 80 для HTTP и 443 для HTTPS. Если для передачи информации по HTTP или HTTPS будет использоваться другой порт, IDS пришлет уведомление.

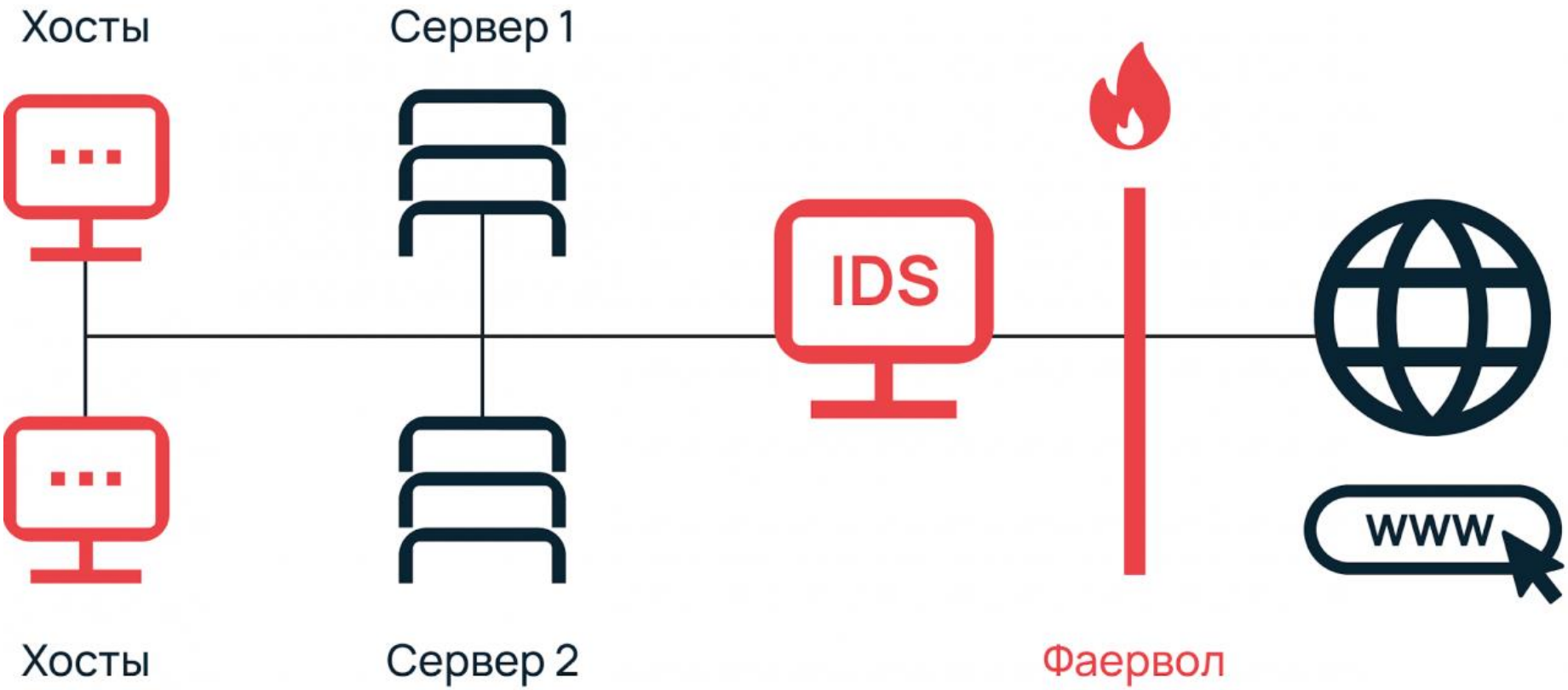
Также, IDS способны выявлять аномалии, любую небезопасную или даже угрожающую активность в сетевом трафике.

Места установки IDS



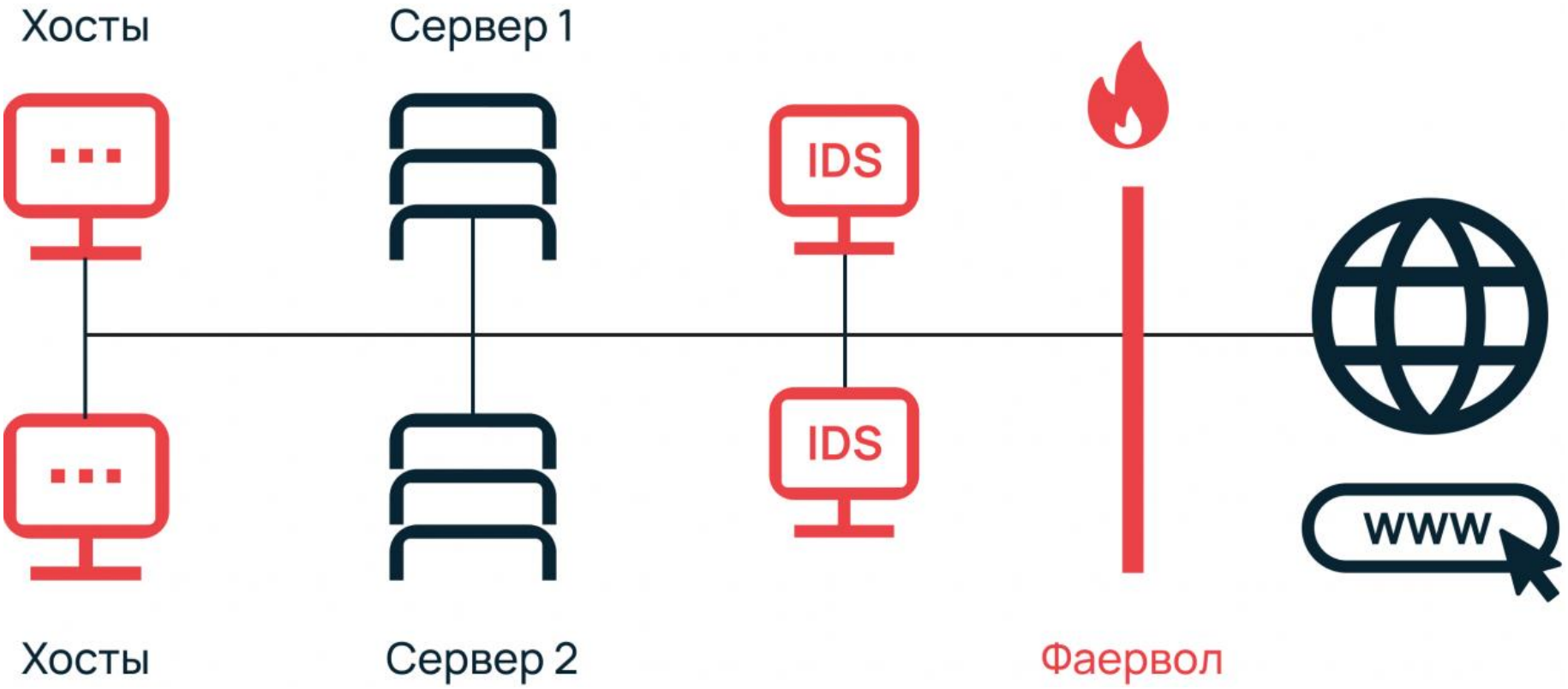
Система обнаружения вторжений может быть установлена перед файерволом с внутренней стороны сети. В таком случае IDS будет анализировать не весь трафик, а только тот, что не был заблокирован файерволом. Это логично: зачем анализировать данные, которые блокируются. К тому же это снижает нагрузку на систему.

Места установки IDS



IDS ставят также и на внешней границе сети, после файервола. В таком случае она фильтрует лишний шум глобальной сети, а также защищает от возможности картирования сети извне. При таком расположении система контролирует уровни сети с 4 по 7 и относится к сигнатурному типу. Такое развертывание сокращает число ложноположительных срабатываний.

Места установки IDS

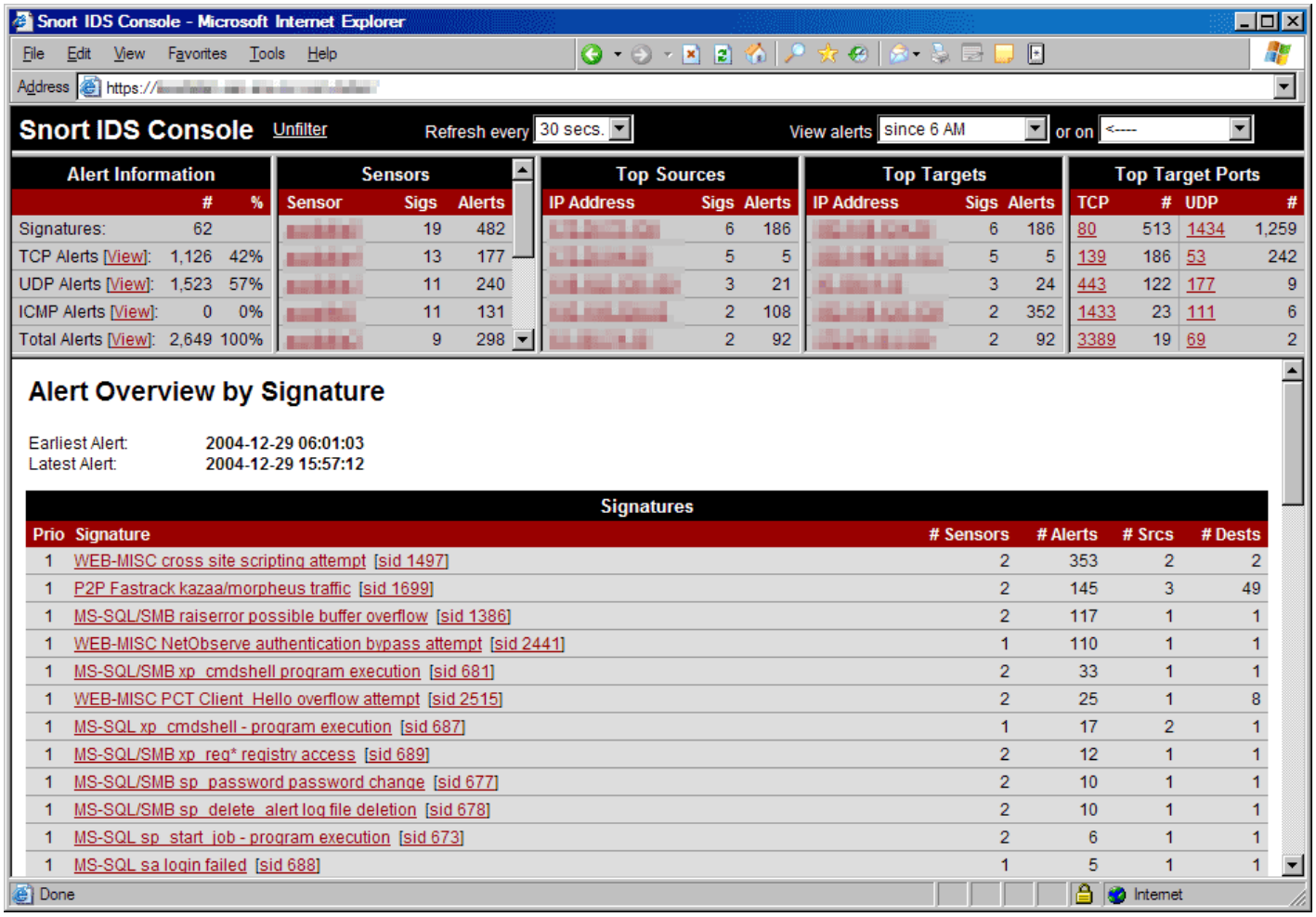


Установка нескольких копий системы обнаружения вторжений в критичных местах для защиты сети по приоритету важности. Также, допускается установка IDS внутри сети для обнаружения подозрительной активности.

Место установки необходимо выбирать в соответствии с требованиями к IDS, располагаемыми средствами и размерами сети.

Open Source проекты и некоторые вендоры на рынке IDS

Snort



Классическая NIDS - Snort. Система с открытым кодом, разрабатывалась как независимое ПО, в 2008 году ее приобрела компания Cisco, которая теперь является партнером и разработчиком. Snort лучше подходит маленьким и средним компаниям. Утилита включает в себя сниффер пакетов, поддерживает настройку правил и др.

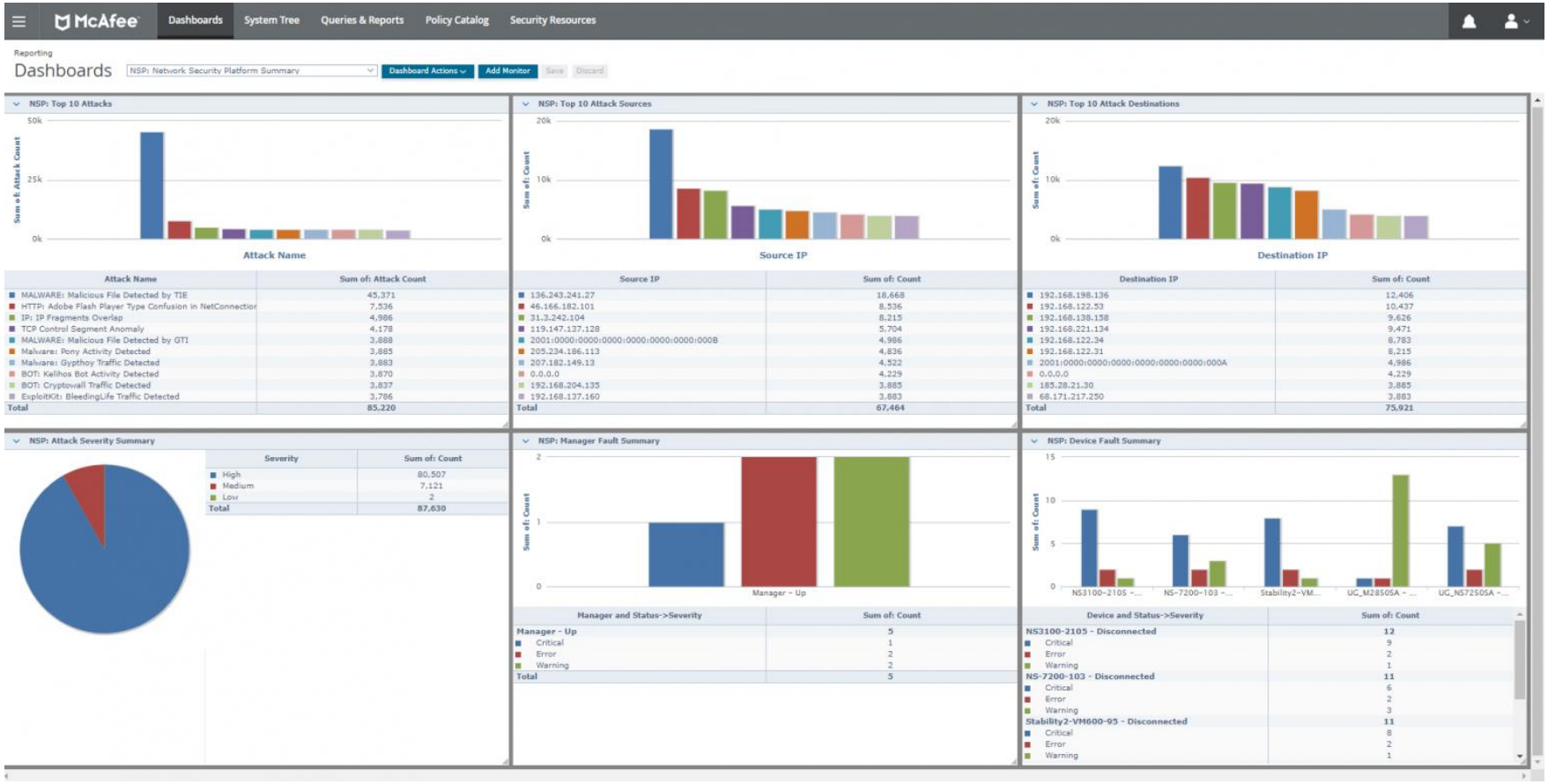
Open Source проекты и некоторые вендоры на рынке IDS

Suricata

Suricata - система с открытым исходным кодом, в ней нет большого количества legacy-кода. Система поддерживает те же модули, что и Snort. Она способна выявлять угрозы по сигнатурам и подходит для средних и больших компаний.

Open Source проекты и некоторые вендоры на рынке IDS

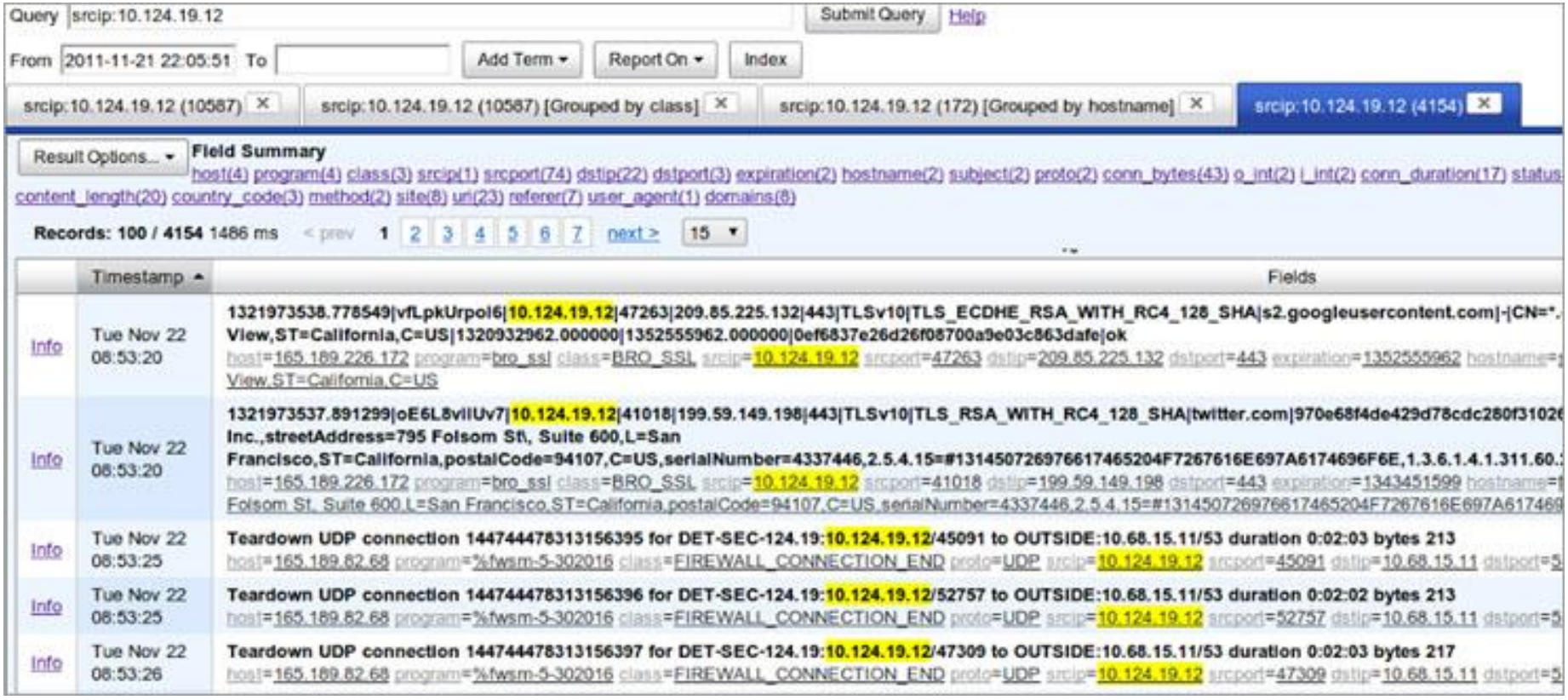
McAfee Network Security Platform



McAfee Network Security Platform позволяет блокироватьт большое количество угроз, доступ к вредоносным сайтам, предотвращает DDoS-атаки и т.д. В силу монументальности McAfee Network Security Platform может замедлять работу сети, поэтому тут требуется решить, что более значимо - интеграция с другими сервисами или максимальная безопасность.

Open Source проекты и некоторые вендоры на рынке IDS

Zeek (Bro)



Полностью бесплатная IDS с открытым исходным кодом. Поддерживает работу как в стандартном режиме обнаружения вторжений, так и в режиме обнаружения вредоносных сигнатур. Zeek может обнаруживать события и позволяет задавать собственные скрипты политик. Недостаток Zeek - сложность обращения с инструментом, так как разработка ведется с упором на функционал, а не графический интерфейс.