IPS: защита сети от киберугроз

МегаФон

Станислав Погоржельский

Руководитель технологической поддержки

МегаФон

Проблематика

- Большинство считает, что достаточно МСЭ для защиты периметра

- Не обязательно иметь действующие контракты ТП для обновлений баз сигнатуры IPS|IDS

- Пренебрежение учёта сигнатур

Какие могут быть последствия взлома приложений?

- Простой бизнеса и прямые финансовые потери
- Утечка персональных данных и репутационные потери
- Кража денежных средств со счетов клиентов
- Компрометация учетных записей сотрудников
- Проникновение в локальную сеть организации
- Утечка конфиденциальных данных

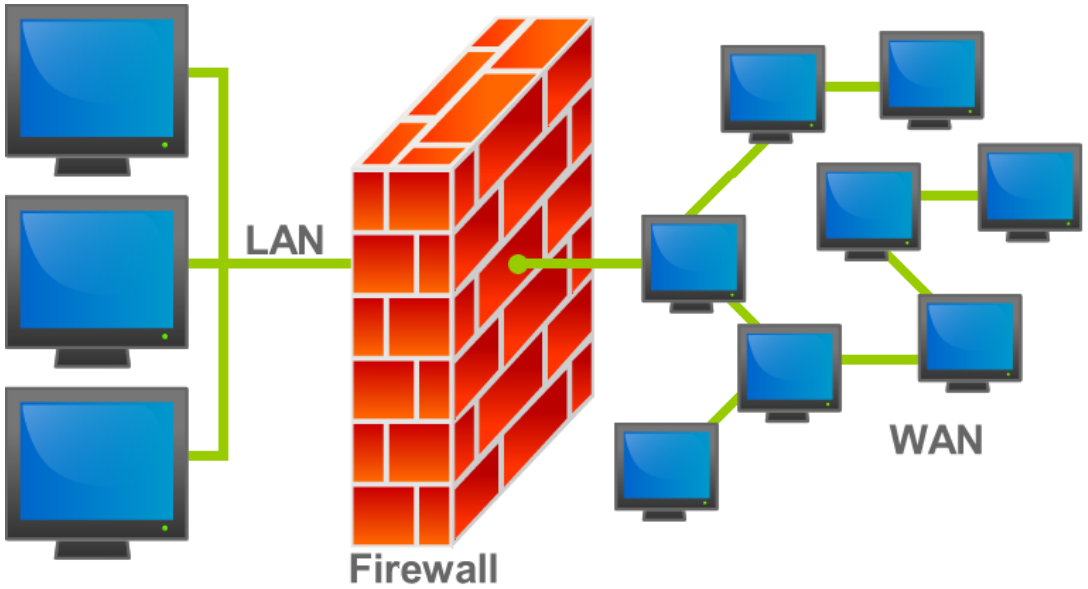
Основные риски, которые закрывает IPS IDS

- **Уязвимости и вредоносные атаки:** Без IPS в сети, она останется уязвимой для различных типов атак, таких как DDoS-атаки, сканирование уязвимостей, эксплойты и т. д
- **Непреднамеренные ошибки:** Несколько неосторожных действий пользователей или ошибок конфигурации сети могут стать причиной неожиданных проблем и нарушений безопасности
- **Повышенные риски при удаленном доступе:** Сотрудники, которые работают удаленно, могут подключаться к сети через различные устройства и сети, которые могут быть уязвимыми
- **Нарушения соответствия:** Без IPS, сеть может не соответствовать нормам безопасности, таким как HIPAA, PCI DSS и т. д. Это может привести к штрафам, репутационному ущербу и потере бизнеса
- **Увеличение времени простоя:** В случае, если сеть подверглась атаке, ее восстановление может занять значительное время и привести к простою бизнеса

Терминалогия

Межсетевые экраны

Межсетевой экран (МЭ, он же брандмауэр или фаервол) — программный или программно-аппаратный комплекс, предназначенный для фильтрации исходящего и входящего сетевого трафика.



Что делает МСЭ:

- Отделяет внутреннюю сеть от сети «Интернет»;
- Запрет на проникновения в сеть организации небезопасного трафика из недоверенных сетей;
- отслеживания состояния сессии;
- блокировки передачи трафика на основе протоколов, источников или приемников, портов отправки и назначения, а также иных параметров.

Система обнаружения вторжений

IDS (Intrusion Detection System, система обнаружения вторжений) — программная или аппаратно-программная система сетевой безопасности, предназначенная для выявления сетевых атак и аномалий.

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.**

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

Система предотвращения вторжений

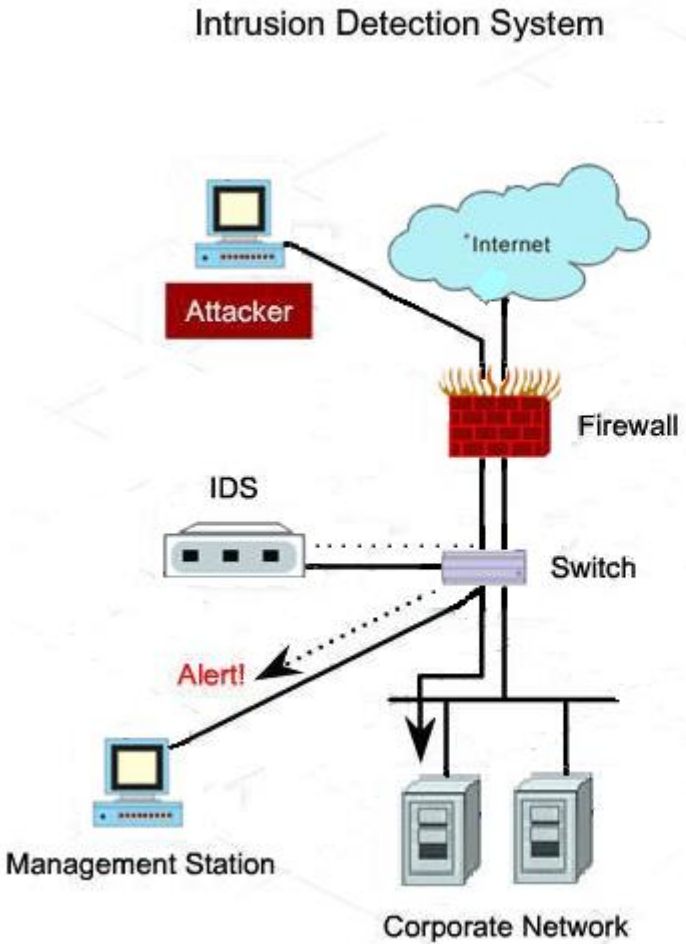
IPS (Intrusion Prevention System, система предотвращения вторжений) — программная или аппаратная система сетевой безопасности, предназначенная для обнаружения несанкционированных действий и атак, а также автоматизированного противодействия им.

IPS выполняет сопоставление трафика известным паттернам сетевых атак для выявления:

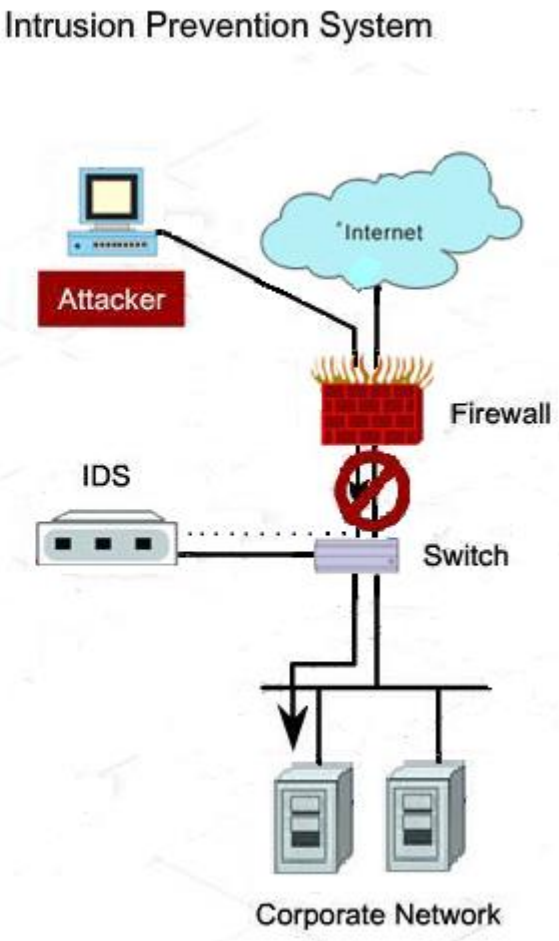
- **изменения тенденций сетевого трафика;**
- **попыток несанкционированного доступа;**
- **попыток обращения к небезопасным ресурсам из сети организации.**

Различия между ips и ids

Система обнаружения вторжений



Система предотвращений вторжений



Принцип действия защиты ips и ids

Сигнатурные.

IDS анализируют сигнатуры с имеющимися в постоянно обновляемой базе.
Если доступа к базе нет или она устарела, эффективность сигнатурного решения снижается. Сигнатурные IDS отслеживают состояние системы, а не события.

Основанные на аномалиях.

Решение использует технологии машинного обучения. Чтобы оно корректно работало на объекте, необходимо провести предварительное обучение. Срок обучения зависит от сложности ИТ-инфраструктуры компании.
Принцип работы следующий: система изучает работу сети на текущий период времени и сравнивает с аналогичным периодом в поиске аномалий трёх типов — статистических, аномалий протоколов и трафика. Такие системы защиты эффективны, но сложны.

Что такое Сигнатуры?

Что такое Сигнатуры?

Сетевая IDS сигнатура – набор данных, которые мы хотим найти в трафике.

Примеры и методы, которые позволяют их идентифицировать:

- **Попытки подключения с IP-адреса.** Могут быть легко обнаружены простой проверкой поля адреса в IP-заголовке.
- **Пакеты с недопустимыми комбинациями TCP-флажков.** Могут быть найдены сравнением набора флажков в TCP заголовке с известными допустимыми или недопустимыми комбинациями флажков.
- **Электронные сообщения, содержащие определенные вирусы.** IDS может сравнить имя поля объекта или вложения с известными именами, связанными с известными вирусами.
- Переполнение буфера в DNS при использовании недопустимого запроса. **Анализ DNS полей и проверка длины каждого из них** помогает идентифицировать попытку переполнения буфера.
- **DoS против POP3 сервера путем вызова одной и той же команды тысячи раз.** Сигнатура для этого типа нападения должна хранить информацию о том, сколько раз была вызвана команда и предупреждение, когда это число превысит некоторый порог.
- **Попытка запроса файла на FTP сервере без предварительной регистрации**. Сигнатура должна предупреждать в случае, когда произошла попытка вызова команды без подтверждения подлинности.

Что такое Zero day ?

Zero day - это уязвимость в программном обеспечении, которая еще не была обнаружена и исправлена разработчиками.

zero day - это угроза безопасности, которая может быть использована злоумышленниками для атаки на систему или сеть до того момента, пока не будет выпущено исправление от производителя программного обеспечения. IPS IDS могут обнаруживать и предотвращать атаки, использующие zero day уязвимости, на основе анализа трафика и сигнатур угроз.

Примеры и методы, которые позволяют идентифицировать уязвимости zero day:

- **Использование системы мониторинга уязвимостей:** позволяет отслеживать уязвимости, которые еще не были обнаружены и не имеют патчей для их исправления.
- **Анализ кода и бинарных файлов:** позволяет выявить уязвимости через анализ кода и бинарных файлов, которые могут быть использованы злоумышленниками для эксплойта.
- **Использование инструментов для поиска уязвимостей:** существуют специализированные инструменты, которые позволяют обнаруживать уязвимости, включая zero-day.
- **Проведение пентеста:** проведение пентеста на вашей сети и приложениях может помочь выявить уязвимости zero-day, которые могут быть использованы для атаки.

Примеры сигнатур

CVE-2022-26134 - "Atlassian Confluence"

Дата публикации: 06.06.2022

Новая сигнатура СОВ UserGate детектирует атаки, связанные с уязвимостью удаленного исполнения кода в продукте Atlassian Confluence (CVE-2022-26134).

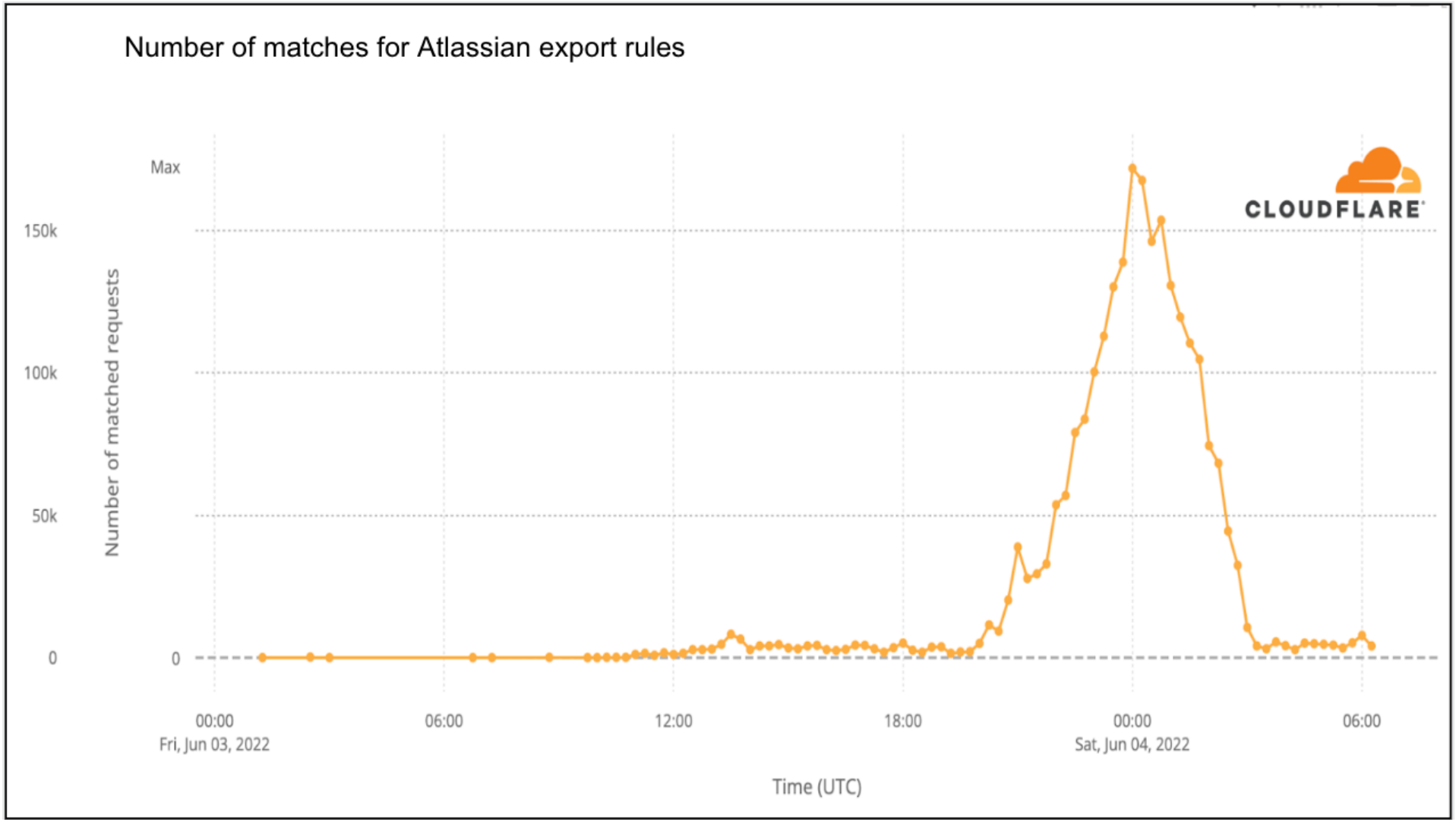
Центр мониторинга и реагирования UserGate добавил в «Систему Обнаружения Вторжений» (СОВ) UserGate новую сигнатуру, позволяющую детектировать атаки с использованием уязвимости CVE-2022-26134. Уязвимость позволяет потенциальным злоумышленникам одним запросом читать файлы на уязвимом сервере и исполнять произвольные команды.

Уязвимые продукты:

- Confluence Server версии <= 7.13.6 LTS и Data Center версии <= 7.18.0 "Latest".

https://www.usergate.com/ru/security-reports/CVE-2022-26134

Cloudflare observations of Confluence zero day (CVE-2022-26134)



Примеры сигнатур

CVE-2023-23415;BDU:2023-01227
Дата публикации: 29.03.2023

Центр Мониторинга и реагирования UserGate добавил в Систему обнаружения вторжений UserGate (IDPS) в версии NGFW 7.0 новую сигнатуру, позволяющую детектировать эксплуатацию уязвимости в реализации Internet Control Message Protocol (ICMP) от Microsoft в ОС Windows.

В подверженных версиях Windows, драйвер tcpip.sys имеет уязвимость в управлении памятью. Она возникает при обработке фрагментированных ICMP-пакетов с сообщением об ошибке, которые содержат вредоносные параметры IP-заголовка. Эта уязвимость позволяет удаленному злоумышленнику вызвать сбой системы Windows или может привести к удаленному выполнению вредоносного кода в случае, если на целевой машине запущено приложение, которое использует сырой сокет (raw socket).

Рейтинг согласно CVSSv3.1 — 9.8

https://www.usergate.com/ru/news/CVE-2023-23415

Где можно узнать про уязвимости

Банк данных угроз безопасности информации

https://bdu.fstec.ru/vul

Зарубежные сайты

https://vuldb.com/?

https://osv.dev/

1. Национальный институт стандартов и технологий (NIST) - организация, которая предоставляет информацию об уязвимостях и рекомендации по их устранению.
2. Центральный банк данных уязвимостей (CVE) - база данных, содержащая информацию об уязвимостях в программном обеспечении.
3. Компании-разработчики программного обеспечения - они могут предоставлять информацию об уязвимостях своего продукта и патчи для их устранения.
4. Компании-безопасности - они могут предоставлять информацию о новых уязвимостях и дашбордах уязвимостей.
5. Специализированные сайты и платформы, такие как Exploit Database, Metasploit и другие.

Технологии включают бизнес

Погоржельский Станислав
Руководитель технической поддержке по облачным и инфраструктурным решениям МегаФона

stanislav.pogorzhels@Megafon.ru

8 800 550 05 55
b2b.megafon.ru

МегаФон | ПроБизнес