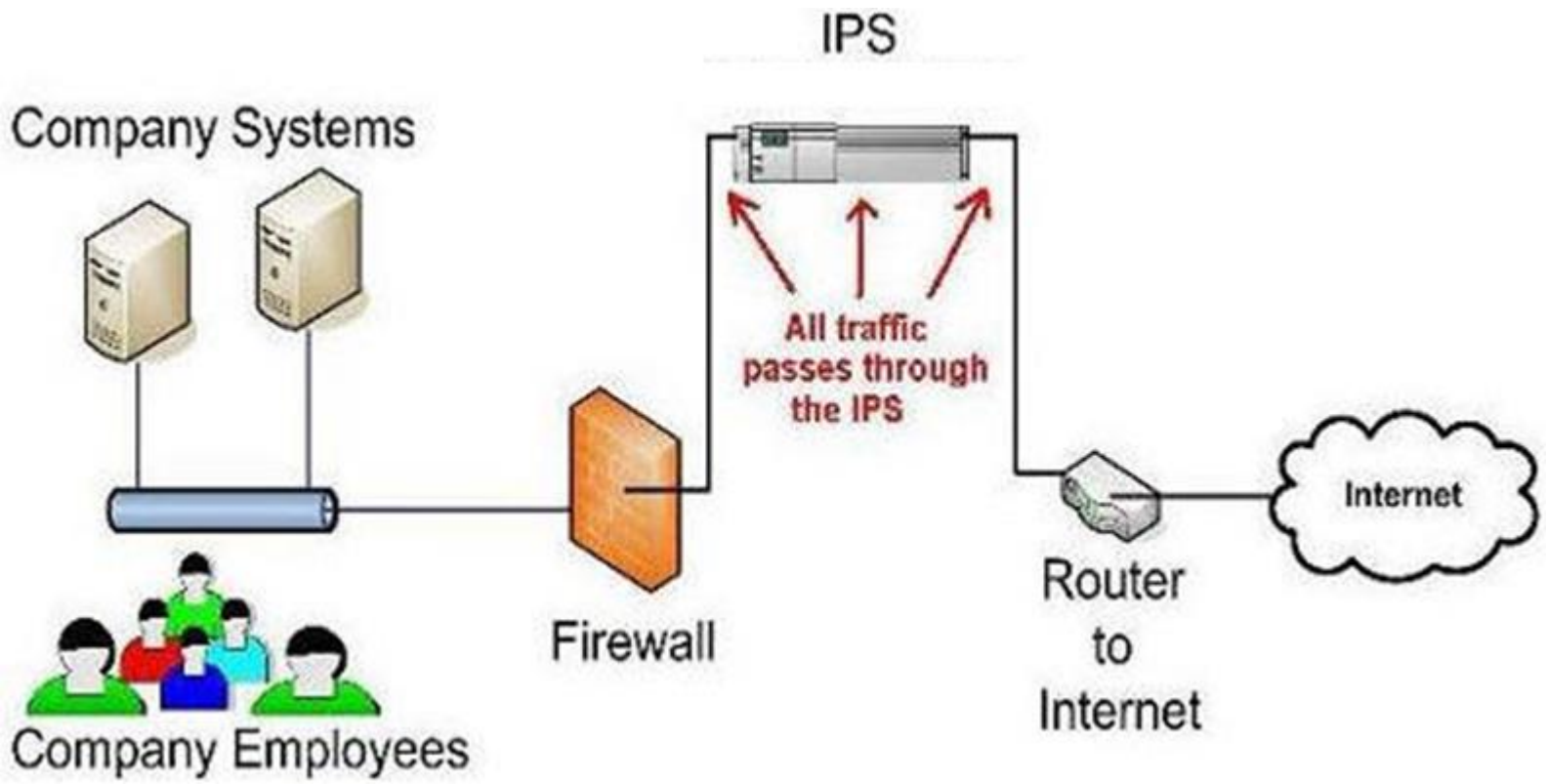
Сосновский Ю.В.
Таврический национальный ун-т им. В.И. Вернадского
Кафедра компьютерной инженерии и моделирования

Обзор развития IPS/IDS систем

IDS, IPS системы

- **Система обнаружения вторжений** (англ. *Intrusion Detection System*, ***IDS***) — программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть, либо несанкционированного управления ими (в основном через Интернет)
- **Система предотвращения вторжений** (англ. *Intrusion Prevention System*, ***IPS***) —система, обнаруживающая вторжения и автоматически защищающая от них
- **Система контроля угроз** (англ. *Unified Threat Management*, ***UTM***). Содержат FireWall, IDS/IPS, антивирус, прокси-сервер, контентный фильтр, антиспам

IPS


IPS
Company Systems
All traffic
passes through
the IPS
Internet
Router
to
Internet
Firewall
Company Employees

Методы IDS/IPS систем. RBID

- **RBID-системы** (англ. *Rule-Based Intrusion Detection*)
- Сигнатуры весьма разнообразны и могут определять конкретные параметры от номера порта в пакете до последовательности байт в серии пакетов
- После того, как сигнатура разработана, её использование обычно довольно эффективно предотвращает нежелательную сетевую активность
- **Временной лаг между созданием нового типа атаки и сигнатуры. Время на внедрение сигнатуры**

Методы IDS/IPS систем. SBID

- **Статистические системы (SBID)**
- Концепция SBID: система определяет «нормальную» сетевую активность и затем весь трафик, не подпадающий под определение «нормального», помечается как аномальный
- **Сравнительно высокий уровень ложных срабатываний**
- **Значительно более наукоемкая разработка**

SBID. Есть сведения о применении:

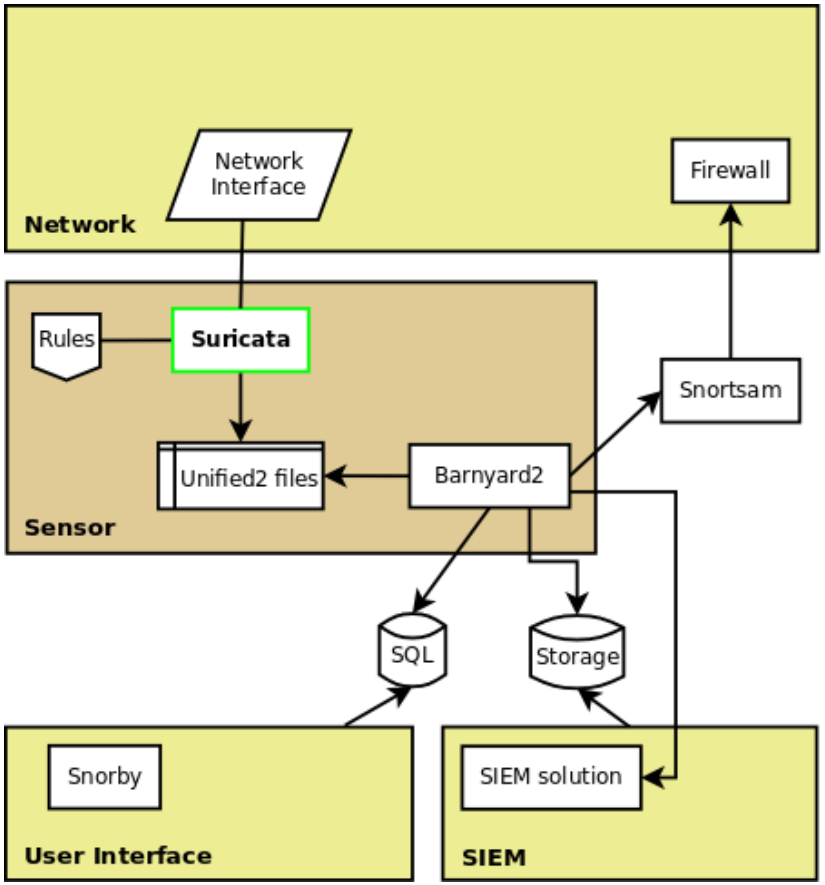
- циклического анализа [1]
- BDS-статистик [2]
- параметрических и непараметрических статистических критериев согласия [3]
- теории цифровых автоматов для анализа поведения объекта в рамках сети передачи данных [4]
- математического аппарата теории нечетких множеств для идентификации аномалий сетевого трафика [5]

1. Ажмухамедов И.М., Марьенков А.Н. Поиск и оценка аномалий сетевого трафика на основе циклического анализа Электронный научный журнал «Инженерный вестник Дона» 2012, №2 http://ivdon.ru/magazine/archive/n2y2012/742
2. МЕТОД ДЕТЕКТИРОВАНИЯ ВИРУСНЫХ АТАК НА ОСНОВЕ АНАЛИЗА СЕТЕВОГО ТРАФИКА А.А. Кузнецов, А.В. Северинов, С.Н. Симоненко, О.И. Качур Системи озброєння і військова техніка, 2011, № 1(25) с.211-214
3. Ловягин В.С. СТАТИСТИЧЕСКИЙ МОНИТОРИНГ ВИРУСНЫХ АТАК НА ОСНОВЕ ПАРАМЕТРИЧЕСКИХ КРИТЕРИЕВ Вісник СевНТУ: зб. наук. пр. Вип. 114/2011. Серія: Інформатика, електроніка, зв'язок. — Севастополь, 2011 с.31-35
4. ОБНАРУЖЕНИЕ КОМПЬЮТЕРНЫХ АТАК НА ОСНОВЕ АНАЛИЗА ПОВЕДЕНИЯ СЕТЕВЫХ ОБЪЕКТОВ ГамаюновД. Ю. Автореф. дисс. на соискание ученой степени к. ф.-м. наук, спец. 05.13.11 – математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетейМГУ, 2007
5. ОПРЕДЕЛЕНИЕ АНОМАЛИЙ ОБЪЕМА СЕТЕВОГО ТРАФИКА НА ОСНОВЕ АППАРАТА НЕЧЕТКИХ МНОЖЕСТВ АЖМУХАМЕДОВ И.М., МАРЬЕНКОВ А.Н. Вестник Астраханского государственного технического университета, 2011 № 1 с.48-51

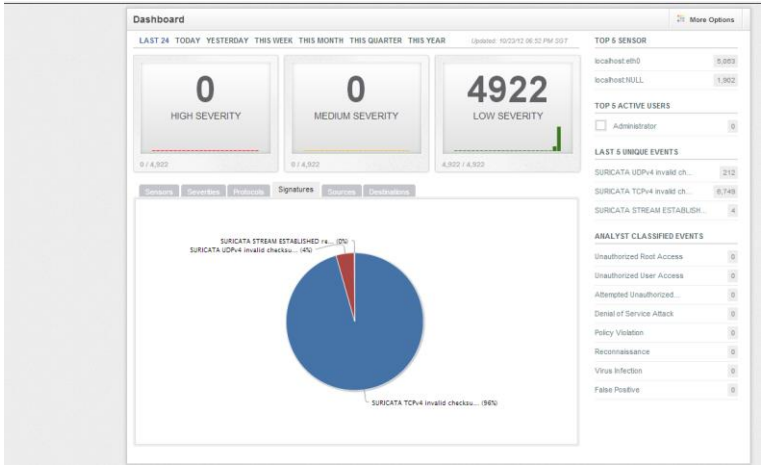
Suricata

- **RBID**-система
- Многопоточный режим (тестирование на системе 24 CPU и 128 ГБ)
- Аппаратная акселерация на стороне GPU за счет CUDA
- Блокировка производится средствами штатного пакетного фильтра ОС
- Автоматически определяет и сканирует протоколы IP, TCP, UDP, ICMP, HTTP, TLS, FTP, SMB, SMTP и SCTP
- Есть возможность подключать наборы правил, созданные другими проектами (Sourcefire VRT, OpenSource Emerging Threats и Emerging Threats Pro)
- Встроенные счетчики применяются для детектирования попыток подбора пароля
- Планируется появление механизма IP Reputation

Suricata



- SURICATA - 96% TCPv4 invalid checksum



Samhain

- **RBID-**система
- база данных сигнатур важных файлов, которая создается при первом запуске и в дальнейшем сравнивается с «живой» системой
- мониторинг и анализ записей в журналах
- контроль входа/выхода в систему
- мониторинг подключений к открытым сетевым портам
- контроль файлов с установленным SUID и скрытых процессов

StoneGate Intrusion Prevention System

STONESOFT
Network Security

- **RBID-**система с возможностью обновления до уровня UTM
- IPS, защита от DDoS и 0day атак, веб-фильтрация, шифрованный трафик
- может заблокировать вирус, spyware, работу приложений
- Для веб-фильтрации - обновляемая база в Интернет
- Процесс создания политик происходит в оффлайн-режиме, по окончании администратор их проверяет и загружает на удаленные узлы IPS
- Несколько устройств легко соединить в кластер и интегрировать с другими решениями StoneSoft
- Поставляется StoneGate IPS как в виде аппаратного комплекса, так и образа Vmware
- Доступна тестовая версия

IBM Security Network Intrusion Prevention System

- **Смешанная RBID/SBID** система. Алгоритмы поведенческого анализатора неизвестны
- анализа протоколов (PAM) — сочетает традиционный сигнатурный метод и **поведенческий анализатор**
- PAM различает 218 протоколов уровня приложений (атаки через VoIP, RPC, HTTP и т.д.) и форматы данных DOC, XLS, PDF, ANI, JPG
- Функции межсетевого экрана
- При необходимости администратор сам может создать и использовать сигнатуру
- **Очень много рекламных трюков, названий технологий с неизвестной эффективностью**

McAfee Network Security Platform 7

- **RBID**-система с автоматическим сбором данных об атаках
- собирает информацию с датчиков, установленных в Интернет и дает оценку репутации проходящим уникальным файлам, IP- и URL-адресам, протоколам
- умеет анализировать трафик между VM, а также VM и физическим хостом. Агентский модуль собирает информацию о трафике в VM и передает их в физическую среду для анализа
- Ядро системы различает более 1100 приложений, работающих на 7-ом уровне OSI, просматривая трафик при помощи механизма контент-анализа и предоставляя простые инструменты управления
- **Одна из лидирующих систем по оценкам специалистов**

Сведения об оценке эффективности IDS/IPS систем

- **Лаборатория «nsslabs»***, оцениваемые технические показатели при тестировании систем IPS/IDS:
  - число пакетов в секунду, обраб.системой
  - число байт в секунду (средний размер пакета)
  - *микс протокола*
  - количество уникальных хостов
  - скорость установления новых соединений
  - количество одновременных соединений
  - предупреждений в секунду
  - пропускная способности при передаче трафика TCP, HTTP и реалистичной смеси трафика различных протоколов прикладного уровня

ICDS 2011: The Fifth International Conference on Digital Society David J. Day Benjamin M. Burns A Performance Analysis of Snort and Suricata Network Intrusion Detection and Prevention Engines pp.187-192

Сведения об оценка эффективности IDS/IPS систем

- При тестировании аппаратного обеспечения BreakingPoint* компании Ixia оценивались **времена задержки передачи пакета** (*при аппаратной обработке 30 мкс, при программной – 150-250мкс*)
- **Основной оцениваемый показатель** – процент обнаруженных атак
- При тестах систем IPS/IDS различными компаниями данный показатель колеблется **от 70% до 10%** у Ixia*, в тоже время при тестировании продуктов семейства IPS/IDS лабораторией «nsslabs» в 2013 году средний процент обнаруженных атак **составляет 96,5%**

http://www.ixiacom.com/solutions/ips-test/

выводы:

1. Средства обнаружения, блокирования вторжений **трансформируются в системы объединенного контроля угроз**
2. IPS/IDS, UTM-систем работают **по сигнатурному принципу** анализа тр-ка
3. Развитие подобных систем идет по направлениям:

   а) **Повышение уровней анализа сетевого трафика** модели OSI (7-й)

   б) **Расширение базы сигнатур**, возможность импорта баз конкурирующих систем, создания собственных правил

   в) **Внедрение** в глобальной сети собственных **сканеров** (McAfee)

   г) **Объединение в одной системе множества известных функций** (антиспам, антивирус, защиту от вторжений (IDS/IPS) и контентную фильтрацию*)
4. **Путь развития систем IPS/IDS -> UTM выглядит экстенсивным**
5. Подавляющее большинство компаний-производителей систем IPS/IDS маркетологически описывает их возможности, **но не предоставляет информацию о тестировании** программного или аппаратного продуктов

* UTM-системы: Trend Micro Deep Security (ru.trendmicro.com), Kerio Control (kerio.ru), Sonicwall Network Security (sonicwall.com), FortiGate Network Security Platforms and Appliances (fortinet.com) или большинство специализированных дистрибутивов Linux

P.S. сертификация IPS/IDS систем

Россия:

- сертификация систем обнаружения и предотвращения вторжений ФСТЭК по классу СОВ4. Нормативный документ: МЕТОДИЧЕСКИЙ ДОКУМЕНТ ФСТЭК РОССИИ. Профиль: защиты систем обнаружения вторжений уровня сети четвертого класса защиты ИТ.СОВ.С4.ПЗ. Утвержден ФСТЭК России 3 февраля 2012 г.
- сертификация ФСБ России, перечень устройств и программных средств приведен в [http://clsz.fsb.ru/files/download/svedeniya_po_sertifikatam_01122013.doc]

Украина:

- ГСССЗИ Украины содержатся в ряде документов, в т.ч. НД ТЗИ 2.5-004-99 «Критерии оценки защищенности информации в компьютерных системах от несанкционированного доступа».

Западный мир:

- Network Intrusion Prevention System Protection Profile V1.1
- McAfee Network Security Platform Receives Key Certification from the US Department of Defense (DoD)
- In January 2012, Stonesoft 5.2.5 achieved the Common Criteria Certificate for both its maximum security Firewall/VPN and high availability failover component
- CSEC - The Swedish Certification Body for IT Security
- Common Criteria* is an international certification scheme setting standards for IT product security. Common Criteria is a widely recognized ISO standard that is ratified in 26 countries. **Stonesoft**

* Содержит обширный перечень профайлов безопасности информационных систем http://www.commoncriteriaportal.org/pps/archived/#DD