Network Behaviour Analysis

Новый подход к защите корпоративных сетей

Мартин Шибл
Представитель в России

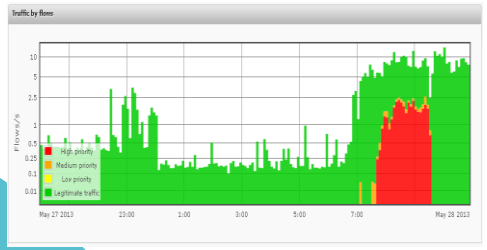
INVEA-TECH

- Чешский вендор инновационных сетевых продуктов
- Год основания- 2007
- Работа в следующих областях:
  - **Мониторинг потоков & Анализ поведения сети**
  - **Мониторинг производительности сети и приложений**
  - **Обнаружение и смягчение последствий DDoS**
- Достижения INVEA-TECH
  - Признание от Gartner с 2010
  - Deloitte CE Technology Fast 50
  - Технологическое партнерство: Cisco, Check Point, Extreme, Radware

Более 900 внедрений в мире

INVEATECH

Мониторинг сетевой безопасности



Network Visibility & Security

Perimeter security

End point security

63%
OF THE ORGANIZATIONS IN OUR RESEARCH ARE INFECTED WITH BOTS

CHECK POINT 2013 SECURITY REPORT

73%
OF ORGANIZATIONS HAD AT LEAST ONE BOT

CHECK POINT SECURITY REPORT 2014

LESS THAN 10% OF ANTIVIRUS ENGINES DETECTED UNKNOWN MALWARE

Gartner

Gartner last year stated that flow analysis should be done 80% of the time and that packet capture with probes should be done 20% of the time. Recommendations:

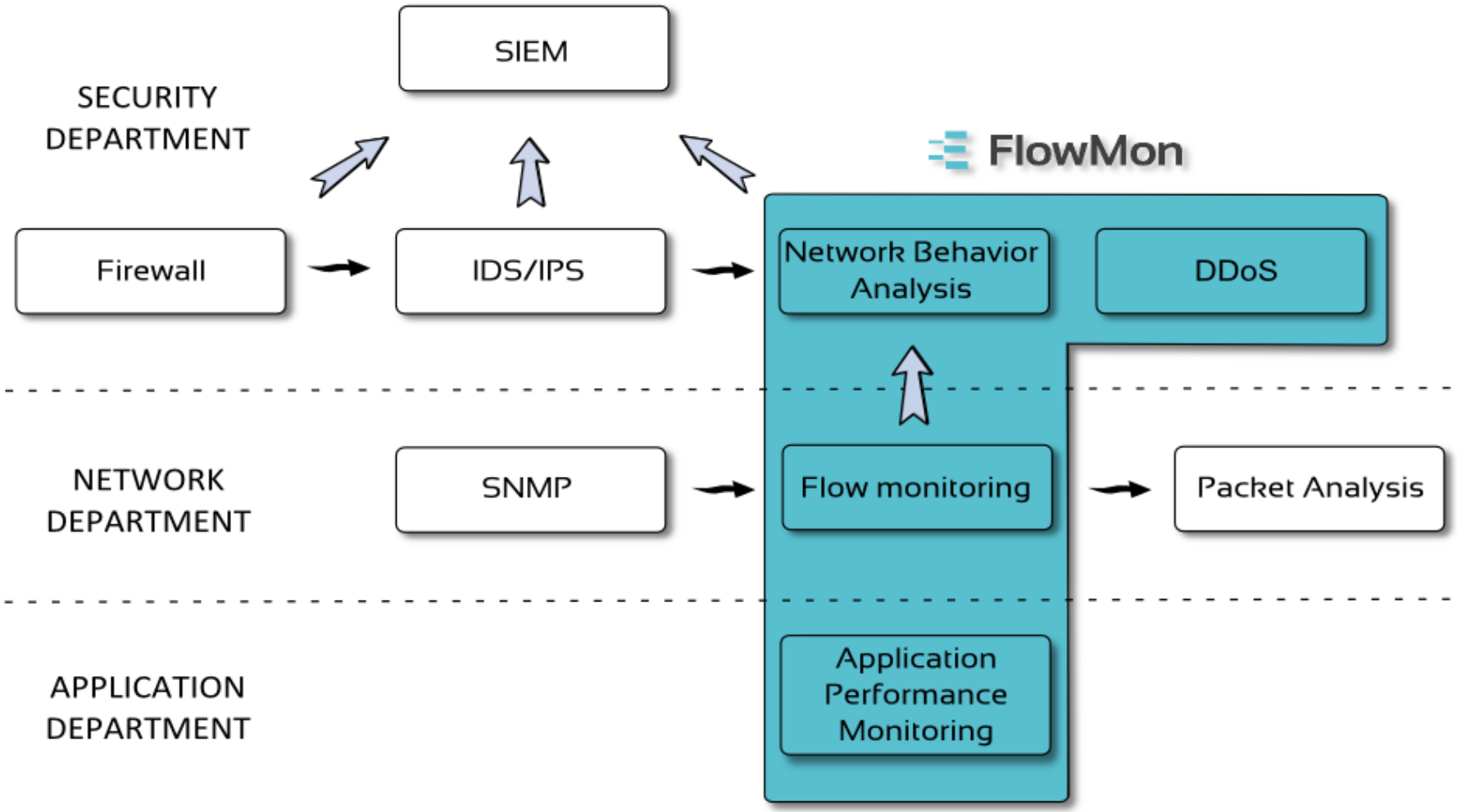
- Implement the use of advanced flow-based data sources to allow better measurement of the user experience.
- Implement flow-based monitoring technologies extensively, and leverage probes where detail is needed. Using a single platform for both makes management easier

Gartner

Security Recommendation

After you have successfully deployed firewalls and intrusion detection systems you should consider Network Behavior Analysis (NBA) to identify network events and behavior that are undetectable using other techniques.

Technology Overview



Мониторинг сетевых потоков и анализ поведения сетей разработаны с целью закрытия брешей, оставленных традиционными сигнатурными решениями, а также для повышения уровня прозрачности, видимости сети

IPS vs. NBA (IDS vs. ADS)

IPS (Система предотвращения вторжений)

- Детектирование атак основано на сигнатурном анализе пакетов
- Основана на анализе прикладного уровня - L7
- Защита от известных угроз, уже обнаруженных и описанных
- Зависит от образцов в базах данных вендора
- Работает на сетевом периметре, неэффективна для внутренних угроз
- Не может работать с зашифрованным трафиком
- Может блокировать подозрительный трафик

Signature detection ☒

Host or network level ☒

NBA (Анализ поведения сети)

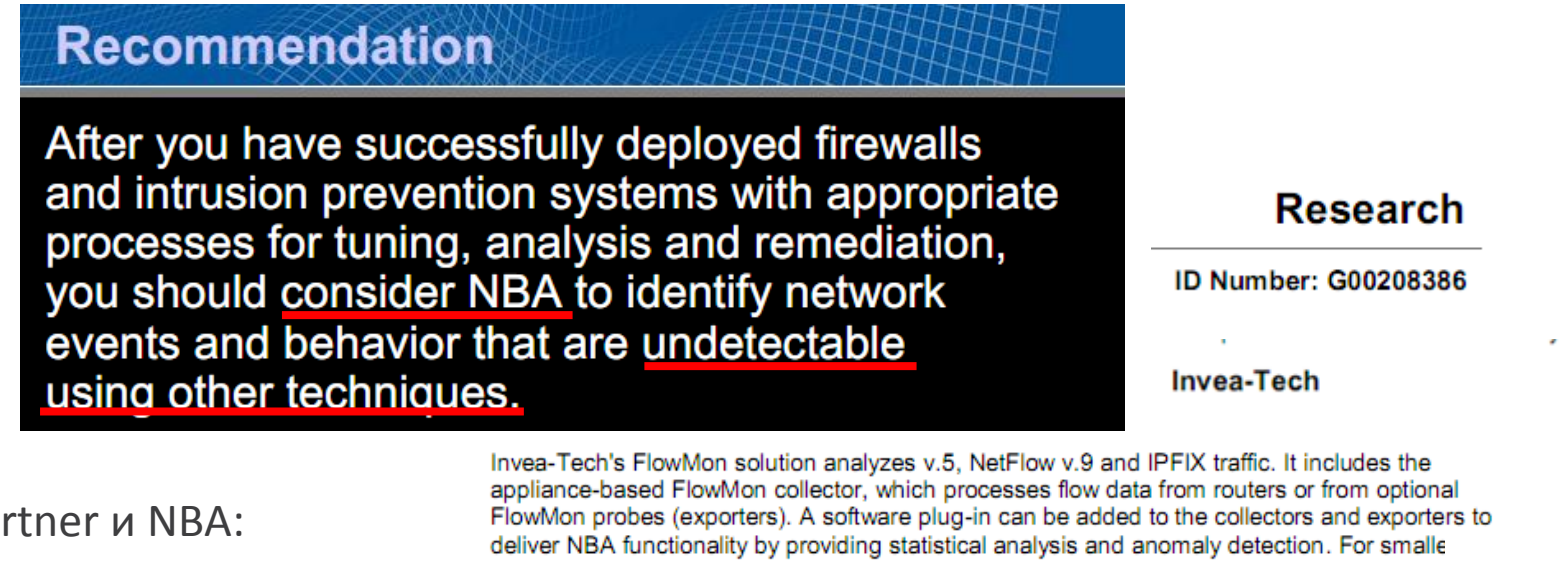
- Детектирование изменений поведения и подозрительного обмена данными
- Основан на статистическом анализе IP
- Детектирование APT-угроз (Advanced Persistent Threats), атак нулевого дня…
- Нет сигнатур
- Анализ **LAN**, WAN, периметра, детектирование внутренних угроз
- Эффективен для зашифрованного трафика
- Пассивен, только информация для действий в сети

Behavior detection ☑

Network level ☑

NBA – следующий шаг в обеспечении безопасности

- Анализ поведения сети , обнаружение аномалий (NBA, NBAD, ADS)

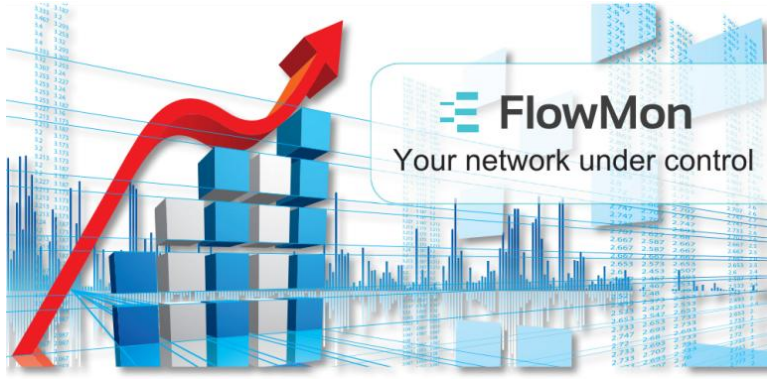


- Gartner и NBA:
  - «NBA предоставляет высший уровень прозрачности поведения вашей сети, выполняя то, что ожидалось от сигнатурных механизмов». Пол Е. Проктор, вице-президент компании Gartner
  - INVEA-TECH признана ведущим производителем средств мониторинга потоков и анализа поведения сети для любых потребителей

Анализ Поведения Сети - следующий шаг в обеспечении безопасности сетей

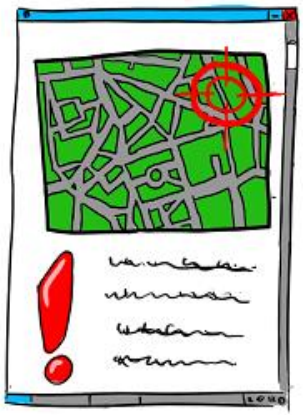
Решение FlowMon

- Инновационное решение для мониторинга сетей с использованием потоков IP
- На основе NetFlow v5/v9 и технологии IPFIX
- Содержит информацию о том, кто с кем общается, как долго, по какому протоколу, какой объем трафика передает и т.д.
- Лучшее соотношение цена/производительность в отрасли
- Решение для сетей всех размеров
- Исключительные преимущества для потребителя
- Ваша сеть под контролем!



...Отдел ИБ/Менеджмент...

- **Преимущества для отделов ИБ:**
  - обнаружение внутренних и внешних атак, изменений поведения в сети
  - контроль доступа пользователей к источникам данных
  - сравнение политик безопасности в реальной сети
  - отслеживание и доказательство инцидентов
  - предотвращение утечек информации из компании



- **Преимущества для менеджмента:**
  - сокращение административных и эксплуатационных расходов на сеть
  - статистические данные о сети (таблицы, круговые диаграммы)
  - более высокая эффективность работы сотрудников
    - проактивный подход: черные списки, белые списки, проактивный мониторинг
    - веб, IM, радио, видео, p2p-сети

Преимущества FlowMon

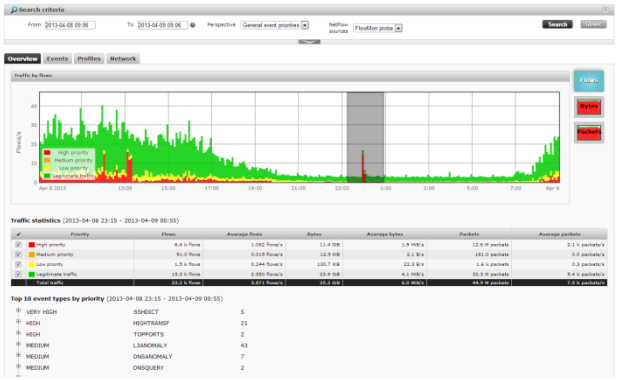
FlowMon: **Комплексное решение**

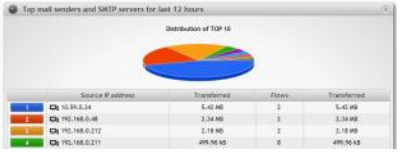
Flow Monitoring	Network Security Monitoring	On Demand Packet Capture	Network/ Application Performance	DDoS Protection
FlowMon Monitoring Center	FlowMon ADS	FlowMon Traffic Recorder	FlowMon APM	FlowMon DDoS Defender
2013		2014		2015

Мониторинг

- Сетевой трафик и мониторинг производительности следующего поколения (NetFlow/IPFIX)
  - Обеспечение видимости- “глаза” в сетевом трафике
  - Экономия времени и средств для сетевых администраторов
  - Быстрый поиск и устранение неисправностей
  - Существенное сокращение сетевого внедрения, эксплуатации и управленческих расходов

FlowMon Monitoring Center





Безопасность

- Отличительная особенность:
  поведения сети (Network Behavior Analysis)
- Сетевая безопасность, анализ поведения
  и детектирование аномалий следующего поколения
  - Обнаружение и предупреждение об аномальном поведении
  - Отчеты по аномалиям и постоянным угрозам повышенной сложности
  - Обнаружение вторжений и атак, невидимых стандартными сигнатурными инструментами

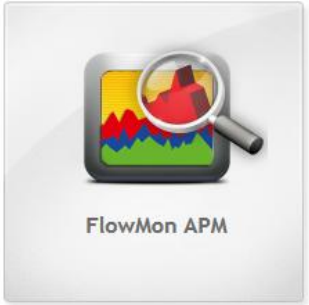
Which incidents does FlowMon ADS detect?

- Attacks (port scanning, dictionary attacks, Denial of Service, Telnet protocol)
- Anomalies in data traffic (DNS, multicast, non-standard communication)
- Anomalies in device behavior (change of the long-term behavior profile of a device)
- Unwanted applications (P2P networks, instant messaging, anonymization services)
- Internal security issues (viruses, spyware, botnets)
- Email traffic (outgoing spam)
- Operational problems (delays, excessive load, the reverse DNS records, broken updates)

User Perspective

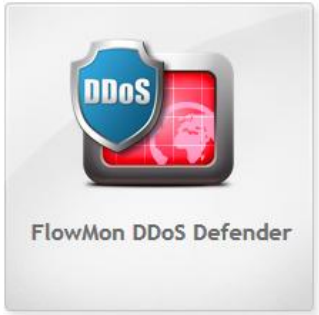
- Traffic Recorder
  - Перехват трафика по требованию (1G/10G/40G)
  - Контролирует весь сетевой трафик от уровня 2 до уровня 7 (хранит трафик в файле PCAP)
  - Основан на заданном фильтре (IP, MAC, VLan, …)
  - Распределенная архитектура без агента
  - Устранение проблем с помощью содержания пакета

- Application Performance Monitoring
  - Безагентский мониторинг всех приложении
  - Измерение времени отклика и общей производительности
  - Предназначен для HTTP/HTTPS, MSSQL приложений
  - Индекс APM- производительность приложений в виде цифрового значения
  - Проблемы выявляются до получения уведомлений от конечных пользователей
  - Определение источников ухудшения доступности



DDoS attacks

- FlowMon DDos Defender
  - Обнаружение и смягчение последствий волюметрических DDoS атак (flow-based)
  - Использование потока данных из любого источника (роутер, зонд, …)
  - Прогнозирование объема трафика с помощью динамических базовых показателей
  - Универсальные сценарии развертывания (простота в установке):



FlowMon DDoS Defender

Standalone

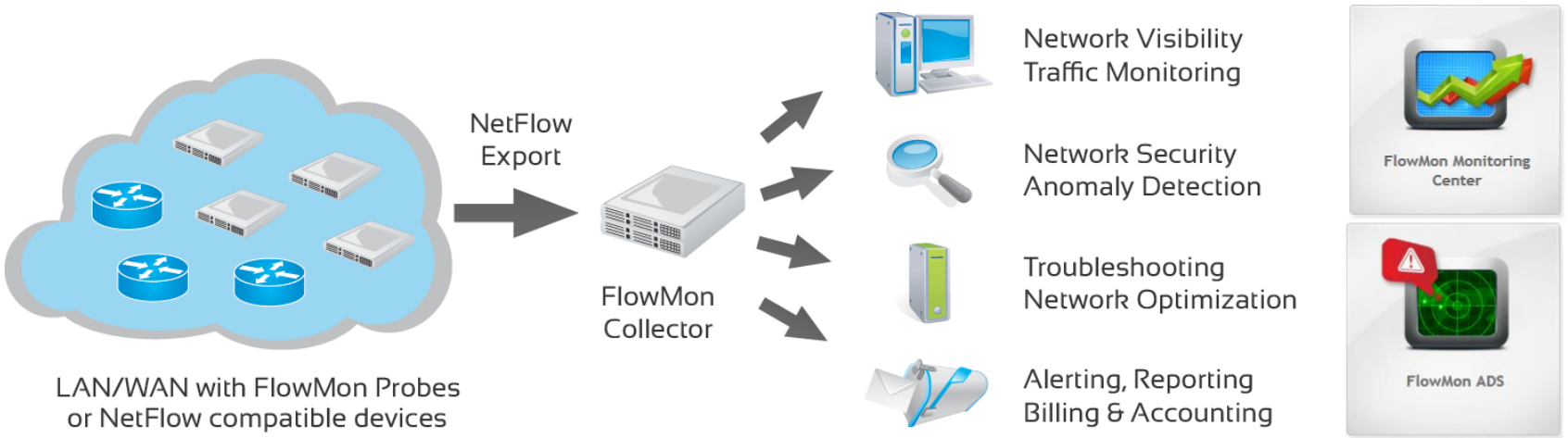
Out-of-band elimination of DDoS attack

(PBR, BGP)

Scrubbing Center

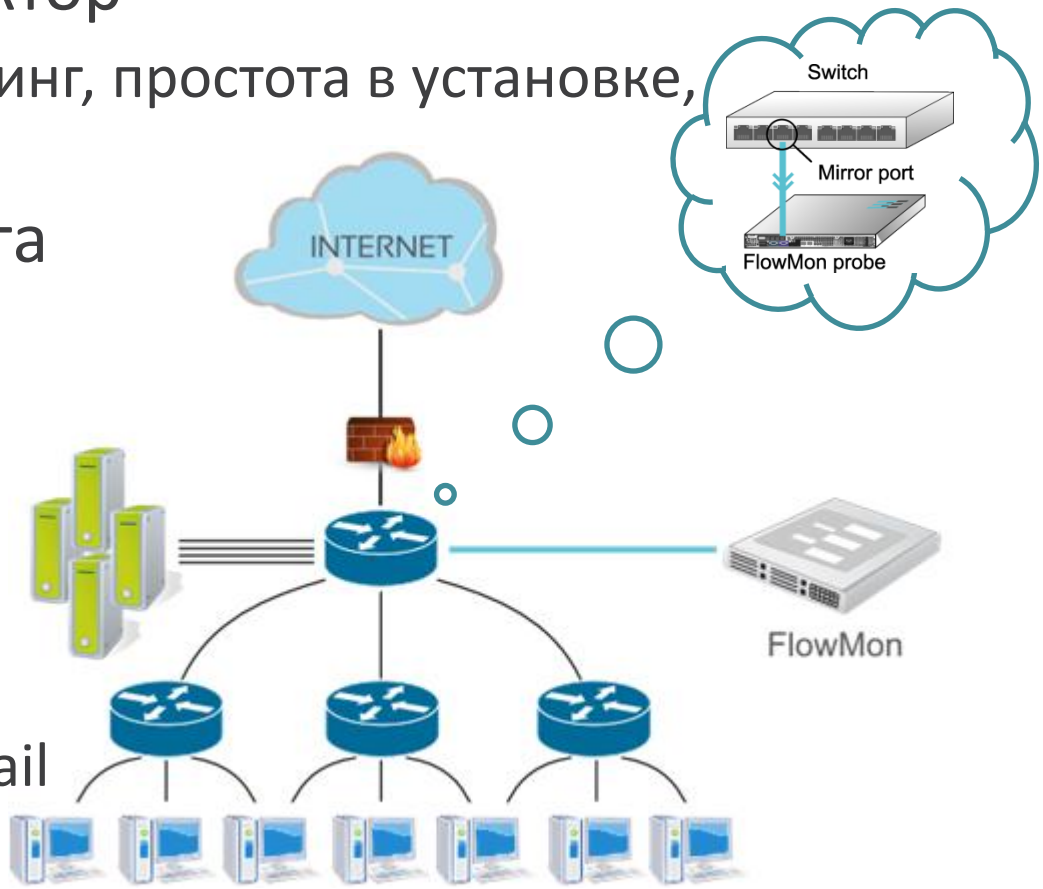
Компоненты FlowMon

- Датчики FlowMon (Зонды)
  - Пассивный источник данных NetFlow
- Коллекторы FlowMon
  - NetFlow данные, отчеты, анализ
- FlowMon плагины
  - Модули, расширяющие функциональность – ADS (автоматическое детектирование, анализ поведения)



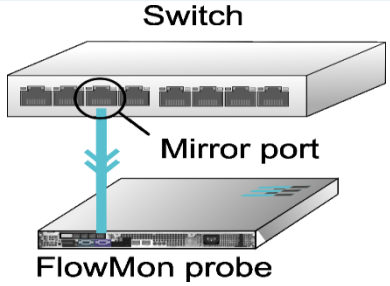
Развертывание на крупных предприятиях

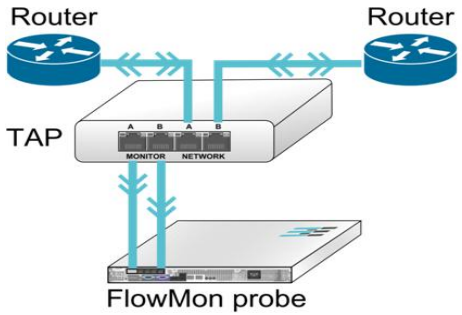
- Один зонд FlowMon для каждого участка, центральный коллектор
  - Пассивный мониторинг, простота в установке, безопасность
- Область мониторинга
  - Клиенты - серверы
  - Клиенты - WAN
  - Сервер - WAN
- Результаты
  - Веб-интерфейс
  - Оповещения по e-mail
  - SIEM (Syslog)

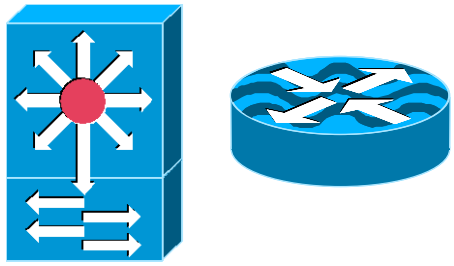


Схемы сбора потоков

	Probe on a SPAN port	Probe on a TAP	Flows from switch/router
Pros	• Точность • Производительность • Видимость L2/L3/L4/L7	• Same as „on a SPAN“ • Захват всех пакетов •Разделение RX и TX	• Сразу доступен • Не требуется дополнительного HW • Трафик на интерфейсах
Cons	• Ограничение по мощности • Нет номера интерфейса	• Дополнительное HW	• Обычно неточная видимость L3/L4 • Влияние на производительность
Facts	• Подходит для большинства клиентов • Ограниченное кол-во SPAN портов	• 2 порта мониторинга	• Всегда тестировать перед использованием
Use	• Enterprise networks	• ISP uplinks, DCs	• Branch offices (MPLS, …)







Технологическое лидерство INVEA

- Производительность & масштабируемость
  - Wire-speed NetFlow зонды, 40Г/100Г зонды
  - Масштабируемость коллектора до 250 000 потоков/с на устройстве

Расширенные возможности

- User identity awareness
- Multi-tenancy, RESTful API, BYOD, SaaS
- Видимость L7 (NBAR2), VoIP, HTTP, Country, …
- Мониторинг производительности сети и сетевых приложении
- Full packet capture (Запис трафика на L7)

Отзывы

«Решение FlowMon буквально открыло нам глаза на трафик в сети. Простой и детальный контроль предоставлен для системных администраторов и менеджеров. Рентабельность составила 150% за 12 месяцев.”

“FlowMon предупреждает нас о внутренних проблемах и ежедневных попытках внешних атак.”

“На основе отсканированных и оцененных данных нам удалось обнаружить компьютеры с опасным поведением в нашей системе.”

“Это позволяет нам обнаруживать и реагировать на неизвестные или конкретные угрозы. Устройство экономит время наших сетевых администраторов при выявлении и решении проблем в сети.”

“С автоматическим анализом поведения ,предоставленным FlowMon ,мы имеем сейчас полный обзор в режиме реального времени о нападениях и проблемах в нашей сети, и мы можем очень эффективно решать их.”

Отзывы

AEGON

“Теперь мы выполняем законодательные требования безопасности для мониторинга сетевого трафика.”

KBC

“FlowMon стал важной частью как внутренней безопасности сети,так и анти-DDOS стратегии. Он является “глазами” для нашей SIEM.”

Raiffeisen BANK

“Оптимизация структуры трафика и обнаружения ошибок помогли нам значительно снизить трафик в LAN и MPLS сетях , что позволяет экономить компании тысячи евро каждый месяц”

Allianz

“Мы ускорили и упростили управление нашей сетью. В каждый момент времени мы знаем, что происходит в нашей сети, и мы можем сразу откликнуться на конкретную ситуацию.”

Истории успеха

Международные **провайдеры, операторы и дата-центры** используют FlowMon для отслеживания трафика, отчетов, биллинга , соответствия или смягчения DDOS в сетях до 100 Гбит/с

Системные администраторы малых, средних и крупных предприятий используют FlowMon для эффективного управления своими сетями

Офицеры безопасности или команды CSIRT/CERT получили инструмент, который дополняет брандмауэры и антивирусы и позволяет обнаруживать современные проблемы безопасности

IT менеджеры измеряют SLA и выгоды от быстрого обнаружения проблемы в случае нападения или аномалии трафика. Это положительно влияет на качество и доступность предоставляемых услуг

Лёгкое начало

- Тестовая виртуальная версия FlowMon
- Доступность по запросу (топология сети)
- Лёгкая установка, не оказывает влияния на сеть, моментальные результаты
- Локальная и удалённая поддержка
- Совместимость с Netflow v5/v9, IPFIX (Cisco), NetStream (Huawei), jFlow (Juniper), sFlow (HP)
- Возможность бесплатного пилота

- Supported **VMware ESXi 4.1 and higher**
- Minimal storage requirements: **46GB**
- Recommended assigned memory: **16GB**
- Recommended assigned CPU cores: **4-8**
- Recommended IOPS value: **1000 IOPS**

FlowMon Interface Demo

Лицензирование зондов

Список моделей зондов FlowMon

Valid from 7th April 2015, rev. 4.0

Аппаратные устройства

P/N*	Модель	Производительность на порт	Мониторинг порт	RAID	Тип диска	CPU**	RAM	Удаленный контроль	Форм-фактор	Размеры (В x Ш x Г) см	Вес (кг)
IFP-1000-CU	FlowMon Probe 1000	1,48 млн. пак./с	1 x 10/100/1000 MbE	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-2000-CU	FlowMon Probe 2000	1,48 млн. пак./с	2 x 10/100/1000 MbE	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-4000-CU	FlowMon Probe 4000	1,48 млн. пак./с	4 x 10/100/1000 MbE	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-4000-SFP	FlowMon Probe 4000 SFP	1,48 млн. пак./с	4 x 1Gb Ethernet	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-6000-SFP	FlowMon Probe 6000 SFP	1,48 млн. пак./с	6 x 1Gb Ethernet	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-10000-SFP+	FlowMon Probe 10000 SFP+	1,5 млн. пак./с	1 x 10Gb Ethernet	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-20000-SFP+	FlowMon Probe 20000 SFP+	1,5 млн. пак./с	2 x 10Gb Ethernet	-	1 x SATA	8	8 GB	Express	1U	4,2 x 43,4 x 39,4	8,05
IFP-40000-SFP+	FlowMon Probe 40000 SFP+	5 млн. пак./с	4 x 10Gb Ethernet	RAID1	2 x SATA	32	32 GB	Enterprise	1U	4,3 x 43,4 x 64,2	19,9
IFP-10000PRO-SFP+	FlowMon Probe 10000 Pro SFP+	14,8 млн. пак./с	1 x 10Gb Ethernet	RAID1	2 x SATA	32	32 GB	Enterprise	1U	4,3 x 43,4 x 64,2	19,9
IFP-20000PRO-SFP+	FlowMon Probe 20000 Pro SFP+	14,8 млн. пак./с	2 x 10Gb Ethernet	RAID1	2 x SATA	32	32 GB	Enterprise	1U	4,3 x 43,4 x 64,2	19,9
IFP-40000PRO-SFP+	FlowMon Probe 40000 Pro SFP+	14,8 млн. пак./с	4 x 10Gb Ethernet	RAID1	2 x SATA	32	32 GB	Enterprise	1U	4,3 x 43,4 x 64,2	19,9
IFP-80000PRO-QSFP+	FlowMon Probe 80000 Pro QSFP+	20 млн. пак./с 5 млн. пак./с	2 x 40Gb Ethernet 8 x 10Gb Ethernet	RAID1	2 x SATA	32	32 GB	Enterprise	1U	4,3 x 43,4 x 73,2	19,8
IFP-100000PRO-CFP4	FlowMon Probe 100000 Pro CFP4	148,8 млн. пак./с	1 x 100Gb Ethernet	RAID1	2 x SATA	TBA	TBA	Enterprise	2U	8,7 x 43,4 x 75,6	31,5

* CU – медный интерфейс мониторинга. Другие интерфейсы предназначены для использования трансивера в соответствии с контролируемой сетью.

** Число ядер процессора с поддержкой Hyper Threading..

Версия **Express удаленного контроля** включает в себя доступ к командной строке и веб интерфейс для удаленного наблюдения за состоянием устройства. Версия **Enterprise** удаленного контроля включает, в том числе, выделенный сетевой интерфейс и виртуальную консоль.

Зонд FlowMon **IFP-80000-PRO-QSFP+** не поддерживает корпоративное расширение L7 Invea-Tech (HTTP i, статистику VoIP и другую информацию на уровне L7) и полный захват пакетов с помощью FlowMon Traffic Recorder в 2 x 40Гб или 8 x 10Гб Ethernet режимах работы. Поддержка этих функций доступна в 1 x 40Гб или 4 x 10Гб Ethernet режимах работы.

Все модели аппаратных зондов FlowMon имеют встроенный коллектор объемом 500 Гб.

Виртуальные устройства

P/N	Model	Производительность на порт	Интерфейсы мониторинга	VMware ESXi	Рекомендуемая конфигурация
IFP-1000-VA	FlowMon Probe 1000 VA	до 0,3 млн. пак./с	1 x 1Gb Ethernet	4.1 and higher	2 CPU cores, 4 GB RAM, min. 11 GB HDD
IFP-2000-VA	FlowMon Probe 2000 VA	до 0,3 млн. пак./с	2 x 1Gb Ethernet	4.1 and higher	2 CPU cores, 4 GB RAM, min. 11 GB HDD
IFP-4000-VA	FlowMon Probe 4000 VA	до 0,3 млн. пак./с	4 x 1Gb Ethernet	4.1 and higher	2 CPU cores, 4 GB RAM, min. 11 GB HDD
IFP-6000-VA	FlowMon Probe 6000 VA	до 0,3 млн. пак./с	6 x 1Gb Ethernet	4.1 and higher	2 CPU cores, 4 GB RAM, min. 11 GB HDD
IFP-10000-VA	FlowMon Probe 10000 VA	до 0,7 млн. пак./с	1 x 10Gb Ethernet	4.1 and higher	4 CPU cores, 8 GB RAM, min. 11 GB HDD
IFP-20000-VA	FlowMon Probe 20000 VA	до 0,7 млн. пак./с	2 x 10Gb Ethernet	4.1 and higher	4 CPU cores, 8 GB RAM, min. 11 GB HDD

Производительность виртуальных зондов FlowMon зависит от выделенных ресурсов, общей нагрузки на систему и среды развертывания.

INVEA-TECH a.s. U Vodarny 2965/2, Brno 616 00, Web: E-mail: Phone: +420 511 205 250

Лицензирование коллекторов

Список моделей коллекторов FlowMon

Valid from 7th April 2015, rev. 4.0

Аппаратные устройства

P/N	Модель	Производительность (потоков/с)*	Объем диска	RAID	Тип диска	CPU**	RAM	Удаленный контроль	Форм фактор	Размеры (В x Ш x Г), см	Вес (кг)
IFC-R5-1000	FlowMon Collector R5-1000	75 000	1 TB	SW RAID5	3 x SATA Hot Swap	12	12 GB	Express	1U	4,3 x 43,4 x 62,5	19,3
IFC-R5-2000	FlowMon Collector R5-2000	100 000	2 TB	SW RAID5	3 x SATA Hot Swap	12	12 GB	Express	1U	4,3 x 43,4 x 62,5	19,3
IFC-R5-3000PRO	FlowMon Collector R5-3000 Pro	150 000	3 TB	HW RAID5	4 x SATA Hot Swap	24	32 GB	Enterprise	1U	4,3 x 43,4 x 62,5	19,9
IFC-R5-6000PRO	FlowMon Collector R5-6000 Pro	150 000	6 TB	HW RAID5	4 x SATA Hot Swap	24	32 GB	Enterprise	1U	4,3 x 43,4 x 62,5	19,9
IFC-R6-12000PRO	FlowMon Collector R6-12000 Pro	200 000	12 TB	HW RAID6	8 x SATA Hot Swap	24	64 GB	Enterprise	2U	8,7 x 43,4 x 64,6	28,2
IFC-R6-24000PRO	FlowMon Collector R6-24000 Pro	200 000	24 TB	HW RAID6	8 x SATA Hot Swap	24	64 GB	Enterprise	2U	8,7 x 43,4 x 64,6	28,2

* Максимальная производительность (в потоках/с) может меняться в зависимости от настроек устройства и установленных плагинов.

** Число ядер процессора с поддержкой Hyper Threading.

Версия **Express удаленного контроля** включает в себя доступ к командной строке и веб интерфейс для удаленного наблюдения за состоянием устройства. Версия **Enterprise** удаленного контроля включает, в том числе, выделенный сетевой интерфейс и виртуальную консоль.

Виртуальные устройства

P/N	Модель	Производительность (потоков/с)*	Объем диска	VMware ESXi	Минимальная конфигурация
IFC-500-VA	FlowMon Collector 500 Virtual Appliance	up to 75 000	0.5 TB	4.1 и выше	2 CPU cores, 4 GB RAM, 500 IOPS
IFC-1000-VA	FlowMon Collector 1000 Virtual Appliance	up to 75 000	1 TB	4.1 и выше	2 CPU cores, 4 GB RAM, 500 IOPS
IFC-2000-VA	FlowMon Collector 2000 Virtual Appliance	up to 75 000	2 TB	4.1 и выше	2 CPU cores, 4 GB RAM, 500 IOPS
IFC-3000-VA	FlowMon Collector 3000 Virtual Appliance	up to 150 000	3 TB	4.1 и выше	4 CPU cores, 8 GB RAM, 1000 IOPS
IFC-6000-VA	FlowMon Collector 6000 Virtual Appliance	up to 150 000	6 TB	4.1 и выше	4 CPU cores, 8 GB RAM, 1000 IOPS
IFC-12000-VA	FlowMon Collector 12000 Virtual Appliance	up to 200 000	12 TB	4.1 и выше	8 CPU cores, 16 GB RAM, 2000 IOPS
IFC-24000-VA	FlowMon Collector 24000 Virtual Appliance	up to 200 000	24 TB	4.1 и выше	8 CPU cores, 16 GB RAM, 2000 IOPS

* Максимальная производительность (в потоках/с) может меняться в зависимости от настроек устройства и установленных плагинов. Максимальная производительность может быть достигнута за счет выделения достаточного количества аппаратных ресурсов в соответствии с описанием аппаратного коллектора включая достаточную производительность диска.

Коллекторы FlowMon в форме виртуальных устройств включают порта мониторинга, которые позволяют напрямую отслеживать сетевой трафик и генерировать статистику NetFlow/IPFIX

Модели 1U/2U/Virtual Appliance:

vmware

Hyper-V

INVEA-TECH a.s.

U Vodarny 2965/2, Brno 616 00, Czech Republic

Web: www.invea.com

E-mail: info@invea.com

Phone: +420 511 205 250

ADS for SMBs/Enterprises

	Lite	Standard	Business	Corporate
Размер сети до	250 ПК	1 000 ПК	5 000 ПК	10 000 ПК
Производитель-ность, потоков/с	1x100	1x1000	2x2000	3x3000
Поддержка SIEM (Syslog, SNMP)	NO	NO	YES	YES
Набор функций	ограниченный	стандартный	полный	полный
Модули для сбора & обработки данных о потоках	1	1	2	3

- Подробная информация о версии Enterprise и цены по запросу

ADS for ISPs/DCs/operators

	ISP 1	ISP 4	ISP 10	ISP 40
Для полосы пропускания	1Гбит/с	4Гбит/с	10Гбит/с	40Гбит/с
Производитель-ность, потоков/с, после взятия проб	1 x 5000	2 x 5000	1 x 10000	2 x 10000
Поддержка SIEM (Syslog, SNMP)	Да	Да	Да	Да
Набор функций	полный	полный	полный	полный
Модули для сбора & обработки данных о потоках	1	2	1	2

- Подробная информация о версии ISP100 и цены по запросу

Спасибо за внимание!

High-Speed Networking Technology Partner

Мартин Шибл
sibl@invea.com
+7 916 847 3345

INVEA-TECH a.s.
U Vodárny 2965/2
616 00 Brno, Czech Republic
www.invea.com