

ОСНОВНЫЕ ВОЗМОЖНОСТИ СИСТЕМЫ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ HP TIPPINGPOINT

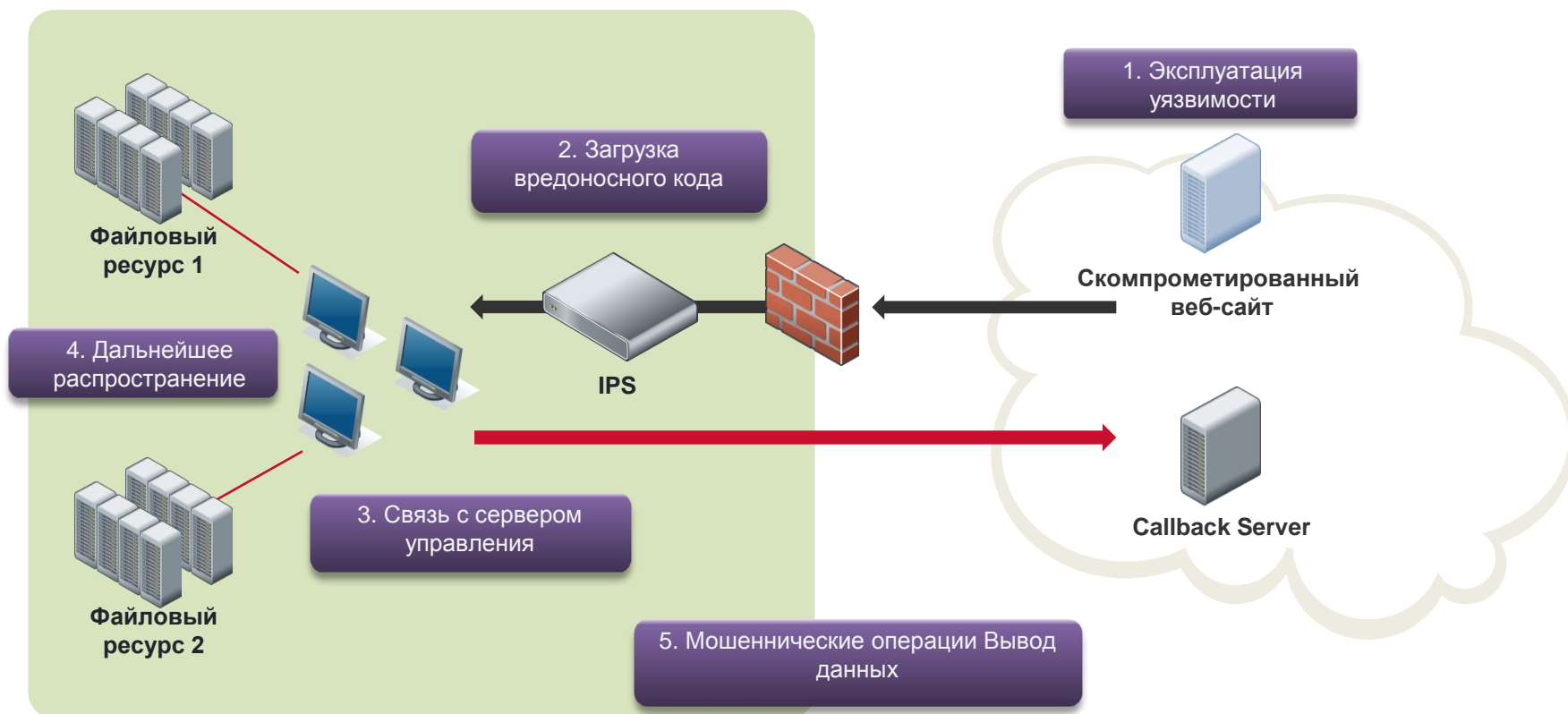
Наумов Илья

Старший специалист отдела технических решений

ЗАО «ДиалогНаука»

Актуальные угрозы ИБ

Детектирование эксплойтов очень важно!
Все последующие этапы могут быть скрыты



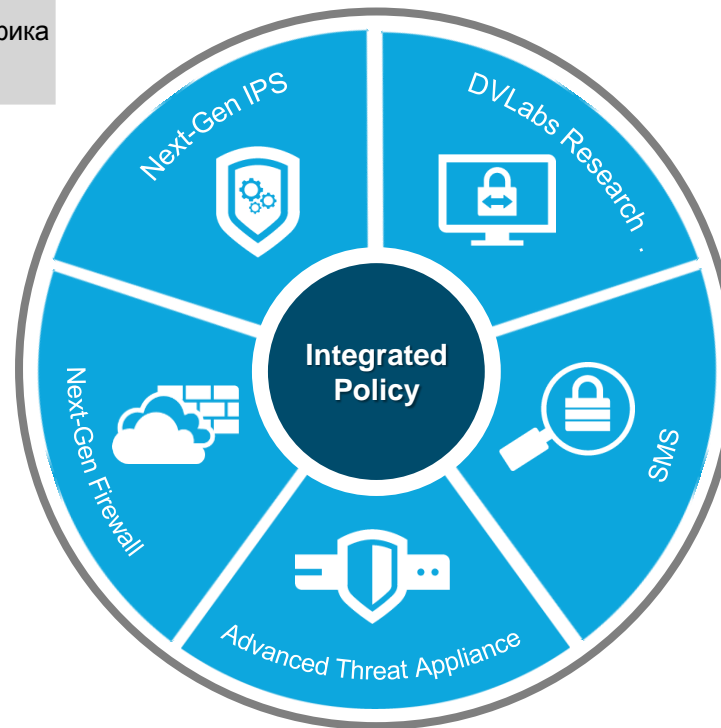
Линейка HR TippingPoint

IPS нового поколения

- Глубокий анализ сетевого трафика на известные уязвимости

Digital Vaccine Labs

- Ведущая лаборатория по анализу угроз
- Анализ актуальных угроз в день из обнаружения



Система управления безопасностью

- Централизованное управление FW и IPS
- Единая консоль для управления и оборудованием и политиками

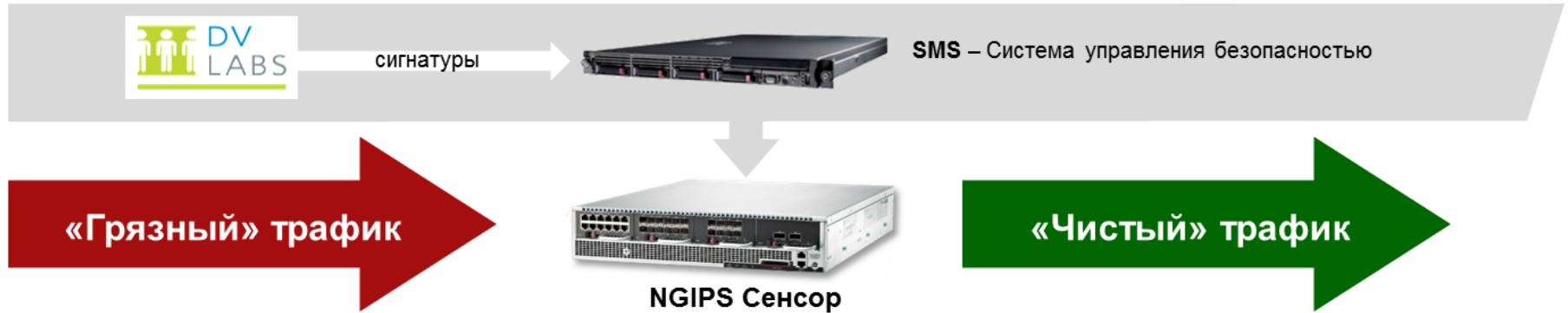
Межсетевой экран нового поколения

- Корпоративный межсетевой экран и IPS нового поколения
- Подробный контроль приложений

Advanced Threat Appliance (ATA)

- Поддерживает проверку более 80 протоколов
- Защищает от потенциальных атак «нулевого дня» и «горизонтального» распространения

HP TippinPoint IPS



Платформа IPS

Разработана для будущих требований и сервисов

Полезность

- Линейная надежность
- Линейная производительность
- Точность фильтров

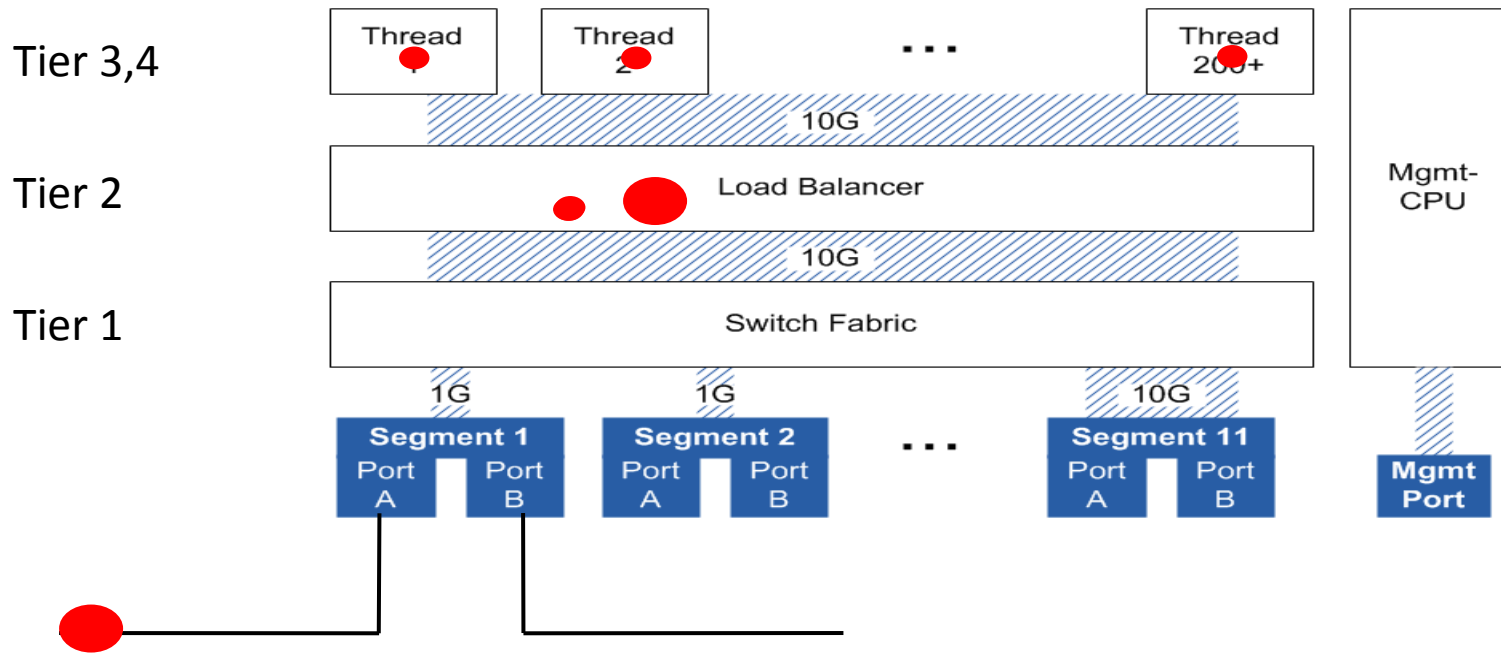
Безопасность

- Лидирующая исследовательская группа
- Быстрая реакция на угрозы
- Широчайший охват

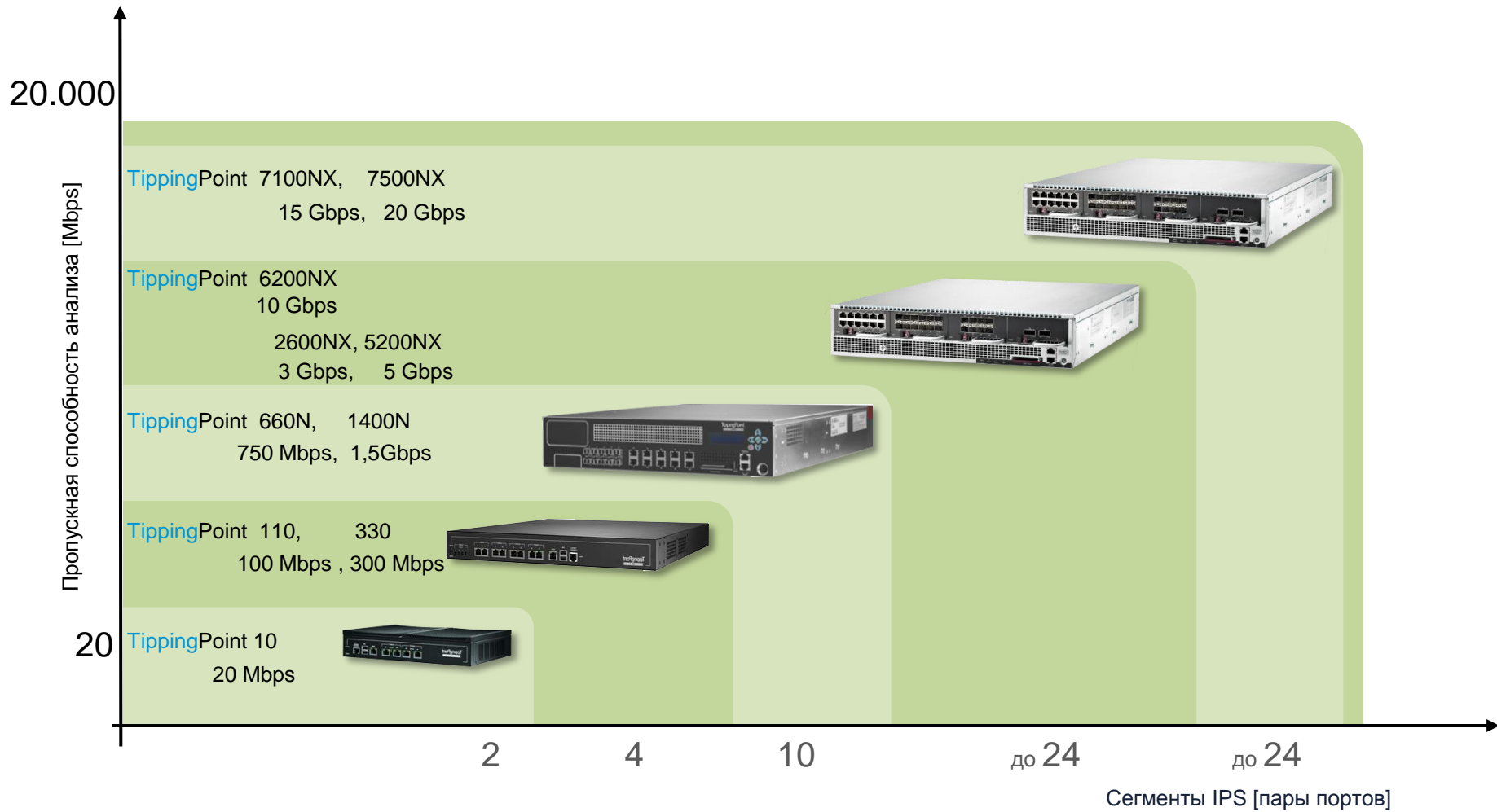
Стоимость

- Легкая в развертывании
- Автоматизированное блокирование угроз
- Легкая в управлении



























TSE ядро предотвращения угроз





Модельный ряд




Модельный ряд

NGIPS Appliance	Inspection Thrgp. [Mbps]	Inline IPS Segments	Ports	Network Thrgp. [Mbps]	Connections per Second	Concurrent Sessions
10	20	2		20	3.600	1.000.000
110	100	4		100	9.700	1.000.000
330	300	4		300	18.500	1.000.000
660 N	750	10	 	750	115.000	6.500.000
1400 N	1.500	10	 	1.500	115.000	6.500.000
2600 NX	3.000	≤24	  	40.000	300.000	30.000.000
5200 NX	5.000	≤24	   	40.000	300.000	30.000.000
6200 NX	10.000	≤24	   	40.000	450.000	60.000.000
7100 NX	15.000	≤24	   	100.000	450.000	60.000.000
7500 NX	20.000	≤24	   	100.000	450.000	60.000.000

 1Gbps Ethernet Copper

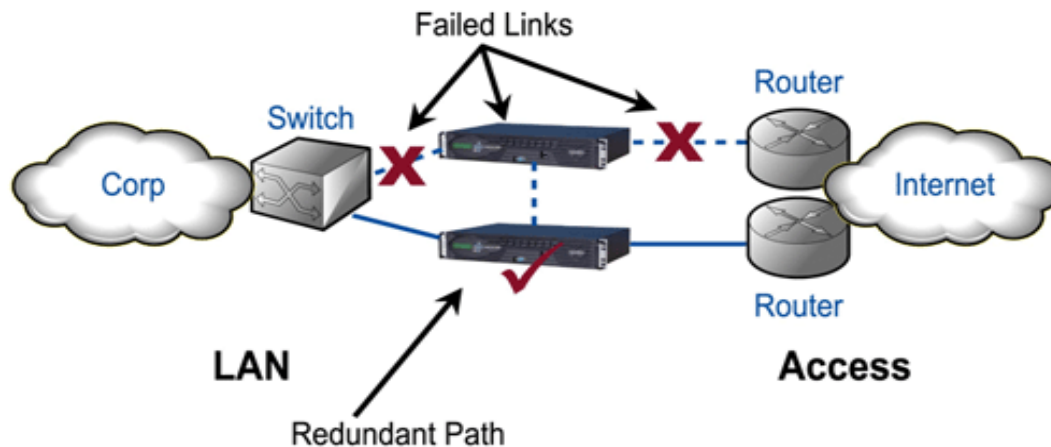
 10Gbps Ethernet Fiber

 40Gbps Ethernet Fiber

 1Gbps Ethernet Fiber

Методы обеспечения отказоустойчивости

- Разделение Control-Plane и Data-Plane
- Дублирование блоков питания (только серии N и NX)
- ZPNA (zero-power high ability)
- Intrinsic HA (L2 failback)
- Transparent HA
- Архитектурные методы



Система управления безопасностью (SMS)

HP Security Management System H3 Appliance



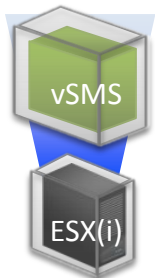
HP DL360
1U
2x600Gb диски (RAID1)

HP Security Management System H3 XL Appliance

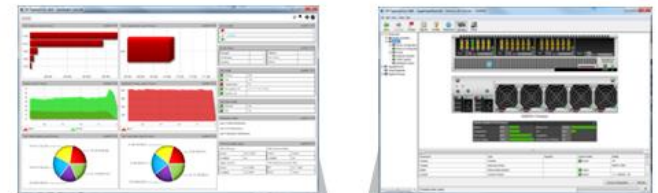


HP DL380
2U
6x600Gb диски (RAID 1+0)

vSMS



VMware ESX/ESXi v4.0 или новее
Требует vCenter
Требования:
300GB на диске
2 virtual CPU
6GB available memory
2 virtual network adapters



Одновременный доступ



Готовый программно-аппаратный комплекс

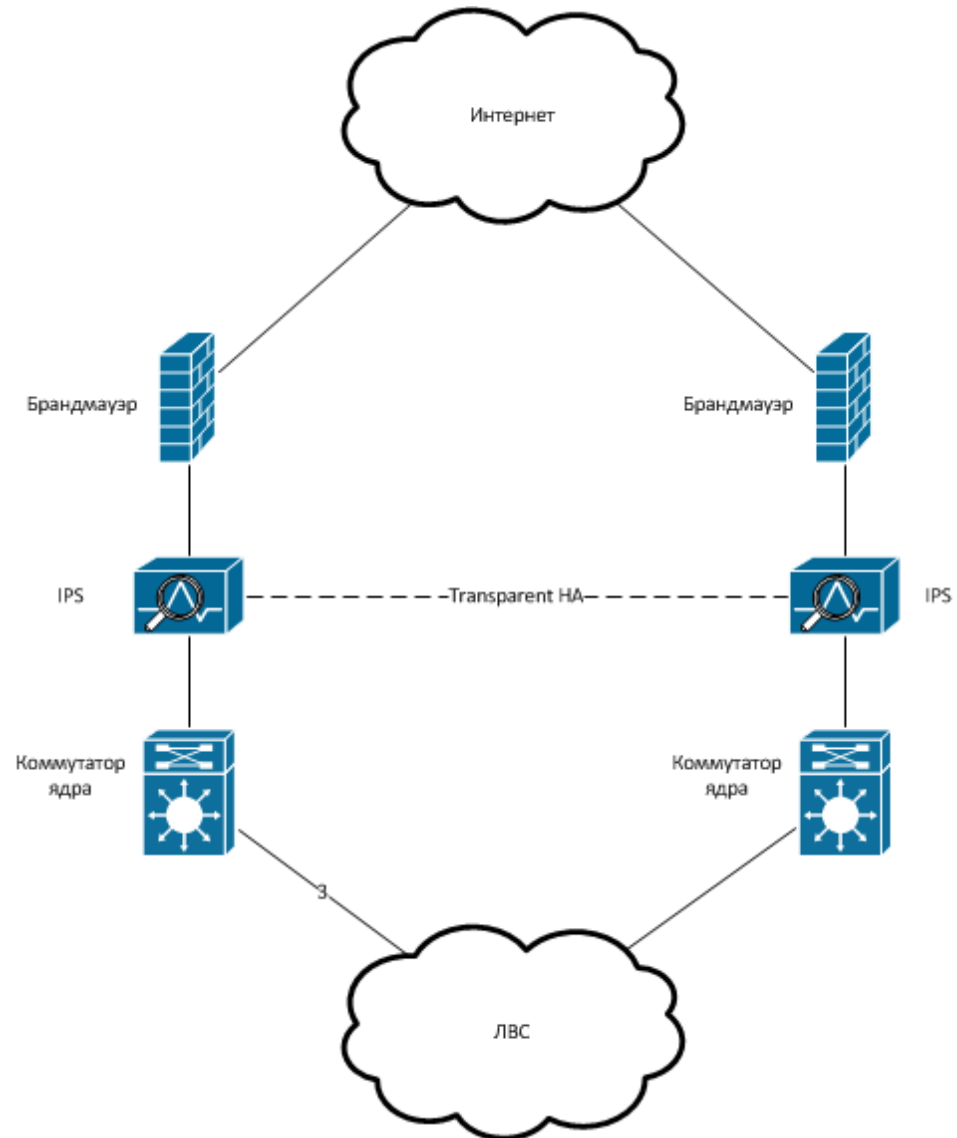


Управление многими устройствами



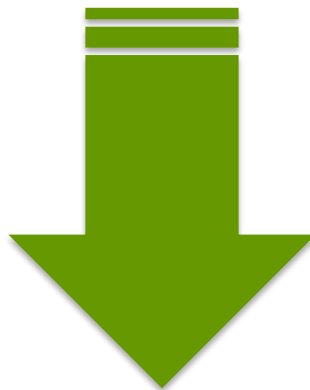
Варианты реализации

- Зеркалирование трафика
- Установка «в разрыв»
- Установка «на палке»
- Комбинированный подход
- Обеспечение отказоустойчивости на двух каналах



Управление сегментами и политиками

- Несколько аппаратных сегментов разных устройств могут объединяться в виртуальные сегменты
- Виртуальные сегменты можно выделять на уровне VLAN id и/или подсети
- Для каждого сегмента можно устанавливать свою уникальную политику безопасности



- Для любой сети\сервиса в организации можно задать уникальную политику в рамках всей системы централизованного управления.

Политика безопасности

Доступность

- Protocol Anomalies
- Denial-Of-Service
- (Distributed) Denial-Of-Service
- ...

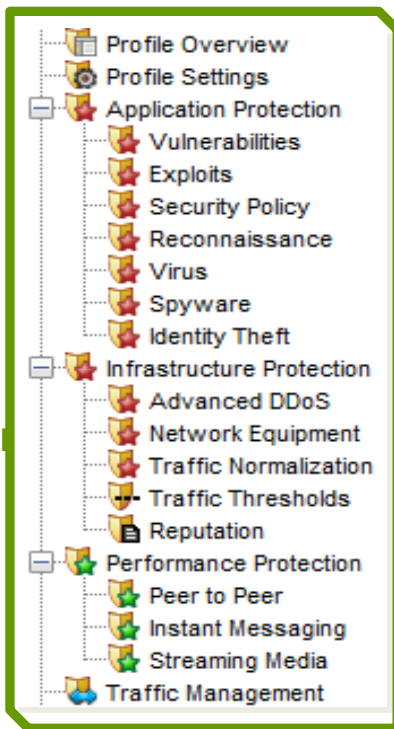
Управление полосой пропускания

- App. Rate Limiter

Корпоративная политика

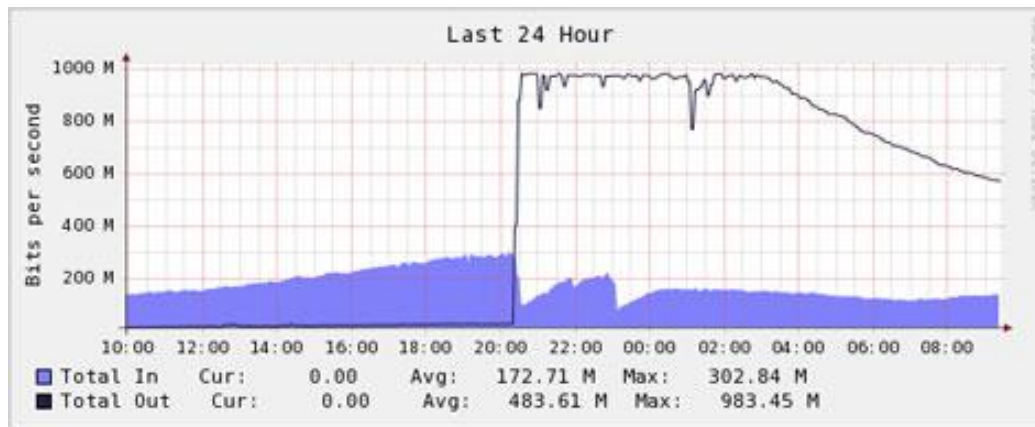
- Security Policy
- Access Validation
- Tunneling
- Rogue Applications
- Peer-to-Peer
- Streaming Media
- ...

Профиль безопасности HP TippingPoint



Кибер-атаки

- Reconnaissance
- Trojan
- Backdoor
- Virus
- Worm
- Spyware
- Phishing
- Buffer Overflow
- Heap Heap Overflow
- SQL-Injection
- Cross-Site-Scripting
- Cross Site Rquest Forgery
- Malicious Documents
- ...



Методы обеспечения защиты от DoS\DDoS

- SYN Proxy
- Quarantine
- RepDV
- IPS Filters
- DV-Toolkit
- Интеграция с другим оборудованием\представителями услуг связи

Интеграция с другими продуктами безопасности

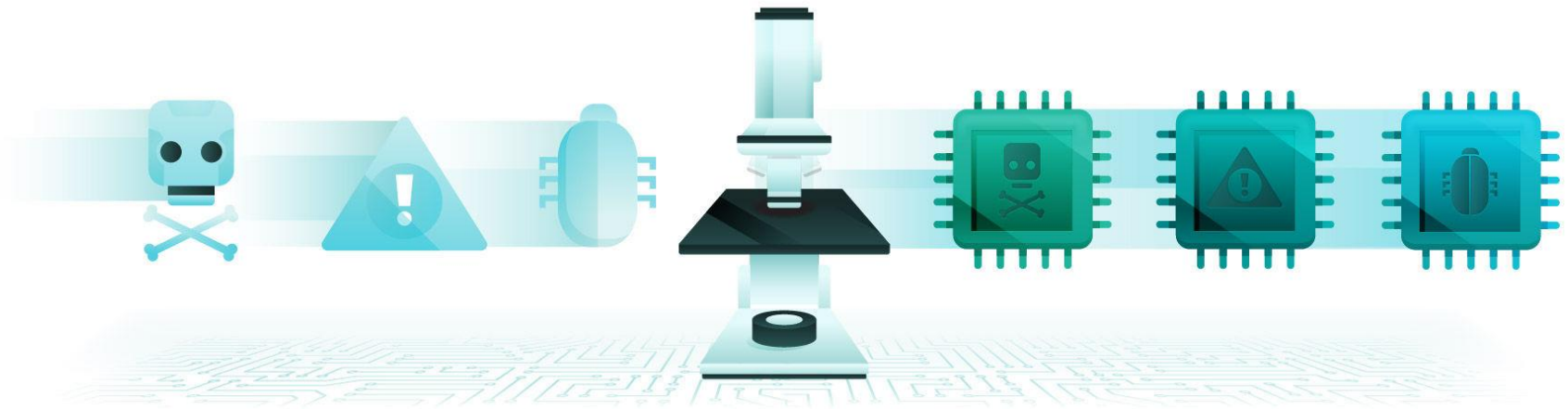
Протоколы:

- Syslog
- Email\SNMP-trap
- SNMP
- Web-API

Назначения:

- Корреляция событий ИБ (SIEM, например HP ArcSight)
- Мониторинг оборудования (в реальном времени и на уровне событий)
- Взаимодействие с другими системами в режиме управления (ведущий и ведомый)
- Все, что Вы еще сможете придумать

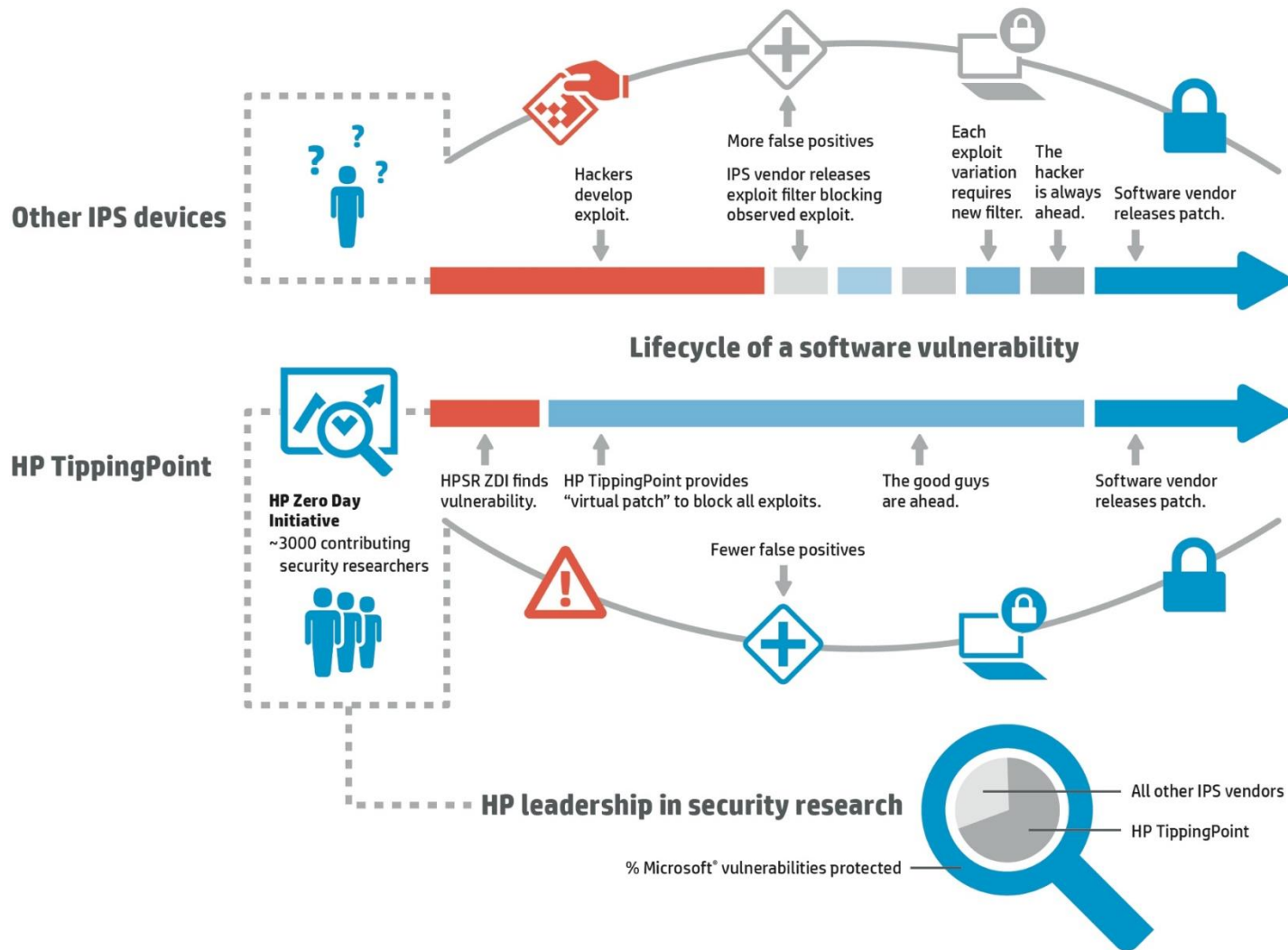
Лаборатория DV Labs



TIPPINGPOINT DIGITAL VACCINE LABS

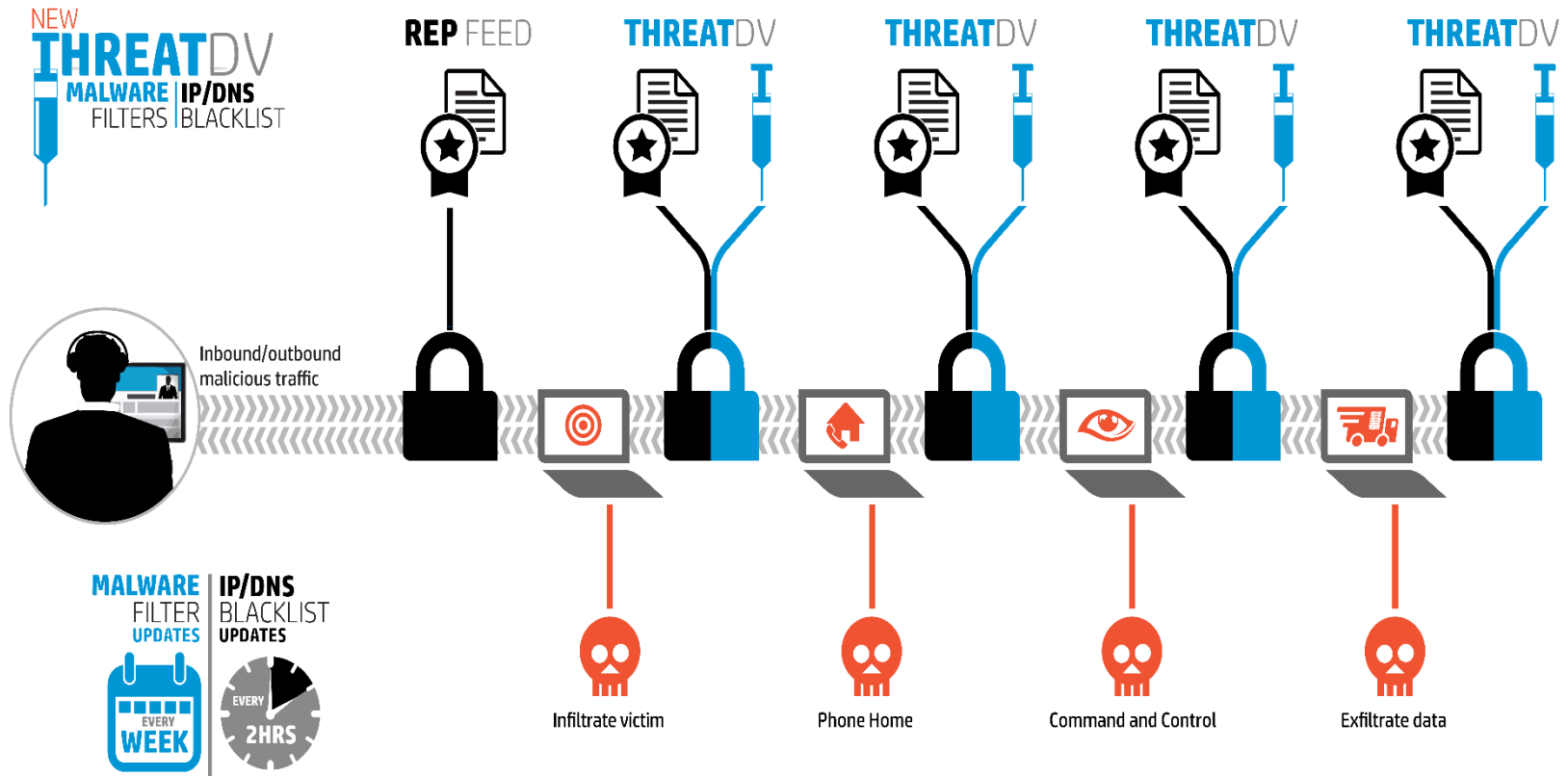
- Разработка фильтров (DV)
- Обеспечение регулярного обновления всех типов сигнатур
- Взаимодействие с исследователями и производителями

ZDI Инициатива «нулевого дня»

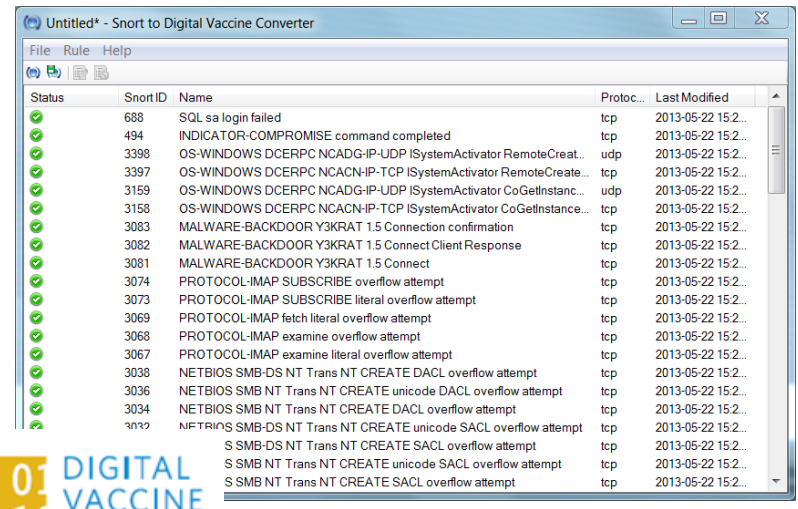
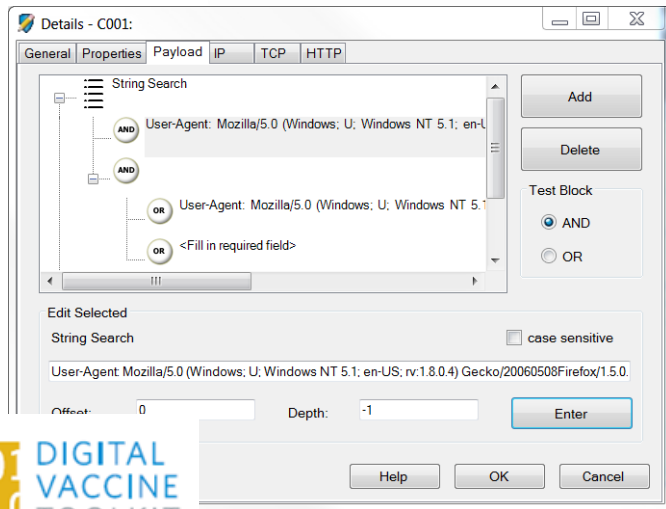


Что мы имеем на выходе?

- Сигнатуры уязвимостей (Digital Vaccine)
- Сигнатуры ВПО (Malware Vaccine)
- Репутационные базы (RepDV Digital Vaccine)
- Анти-DoS/DDoS фильтры и профили
- Сигнатуры приложений (Application Visibility)



- Создание фильтров самостоятельно на основе анализа трафика (DV Toolkit)
- Импорт правил в формате SNORT (DV Converter)



- Сертификат №3232 от 12.09.14г (НДВ-4, СОВ-4, 1Г, ИСПДн-1)
- Требования к системам обнаружения вторжений» (ФСТЭК России 2011)
- Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России 2012)

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ



ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ № 3232

Выдан 12 сентября 2014 г.
Действителен до 12 сентября 2017 г.

Настоящий сертификат удостоверяет, что **программно-аппаратный комплекс HP TippingPoint серий N и NX с операционной системой TOS версия 3 и системой управления SMS версия 3**, разработанный компанией Hewlett-Packard Company и производимый ЗАО «МВП «СВЕМЕЛ», является программно-техническим средством защиты информации, не содержащей сведений, составляющих государственную тайну, реализующим функции системы обнаружения вторжений уровня сети и соответствует требованиям документов «Требования к системам обнаружения вторжений» (ФСТЭК России, 2011) и «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» (ФСТЭК России, 2012) при выполнении указаний по эксплуатации, приведенных в формуляре 39543412.5014.010ФО.

- Защищает не от вирусов, а именно от взломов
- Высокая скорость реакции на новые угрозы с выходом сигнатур
- Высокая точность – наименьшее количество ложных срабатываний
- Высокая доступность за счет архитектуры
- Гибкий инструмент для большого кол-ва разных вариантов даже в пределах одного устройства
- Простота установки и простота настройки. Обучение админа по данной технологии – максимум 3 дня.

Наумов Илья

117105, г. Москва, ул. Нагатинская, д. 1, стр.1

Телефон: +7 (495) 980-67-76

Факс: +7 (495) 980-67-75

<http://www.DialogNauka.ru>

e-mail: ilya.naumov@DialogNauka.ru

