Высокопроизводительная безопасность

Павел Родионов
Cisco CSE Security

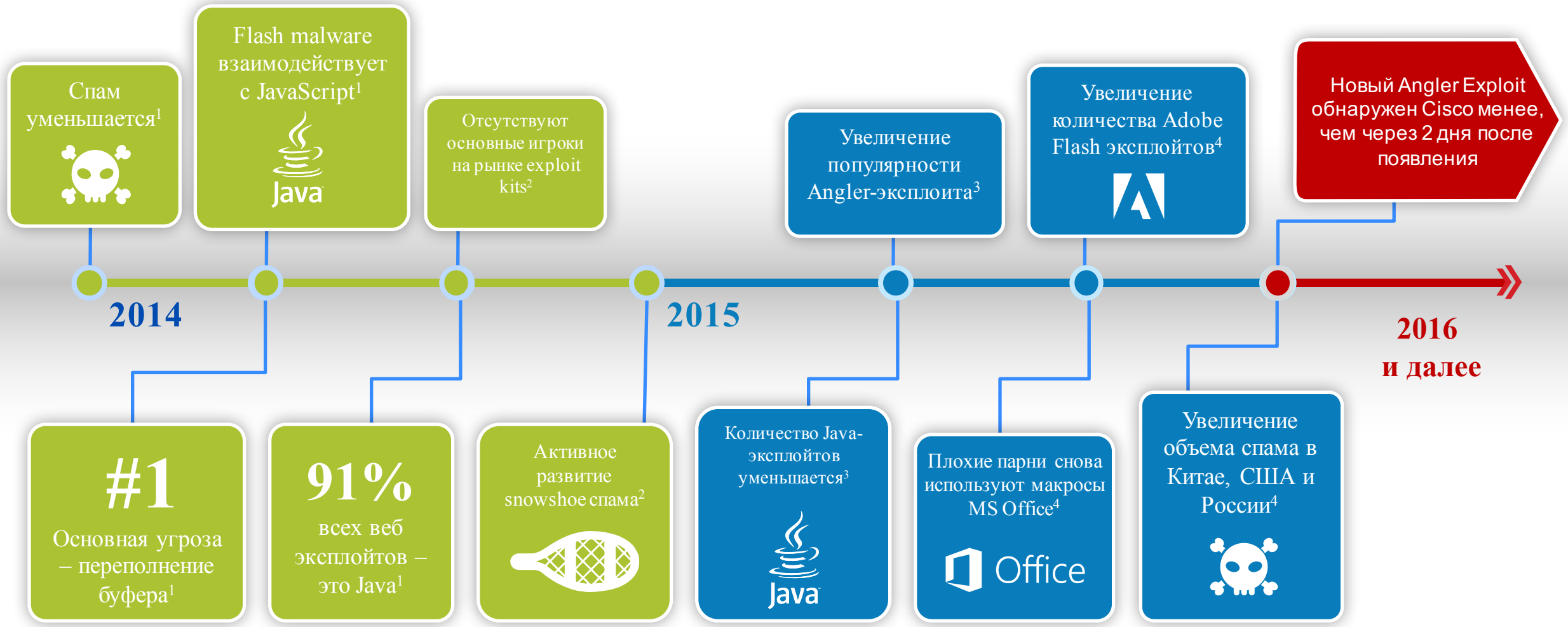
18 мая 2016

Cisco Forum

Программа

- Ландшафт угроз
- ASA FirePower – первый межсетевой экран, ориентированный на угрозы
- Что умеет делать FirePower?
- Развитие NGFW
- Firepower 4100/9300. Новый подход к высокопроизводительной безопасности

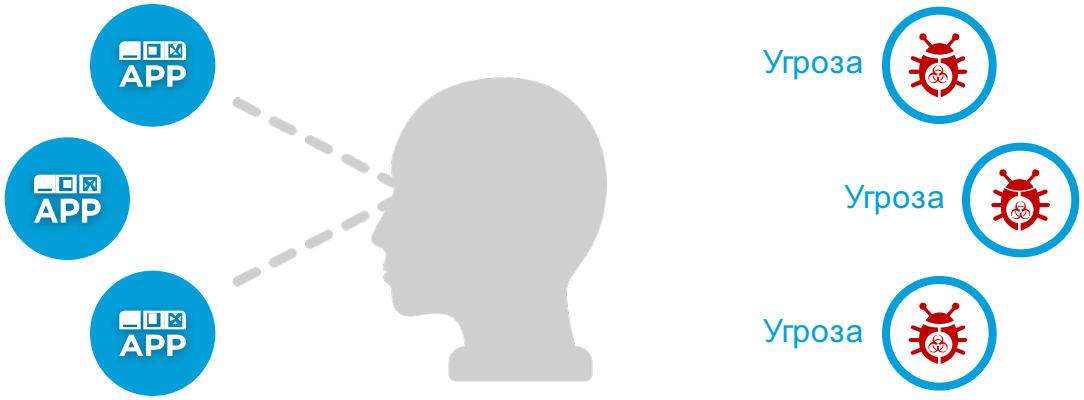
Ландшафт угроз меняется с увеличивающейся скоростью



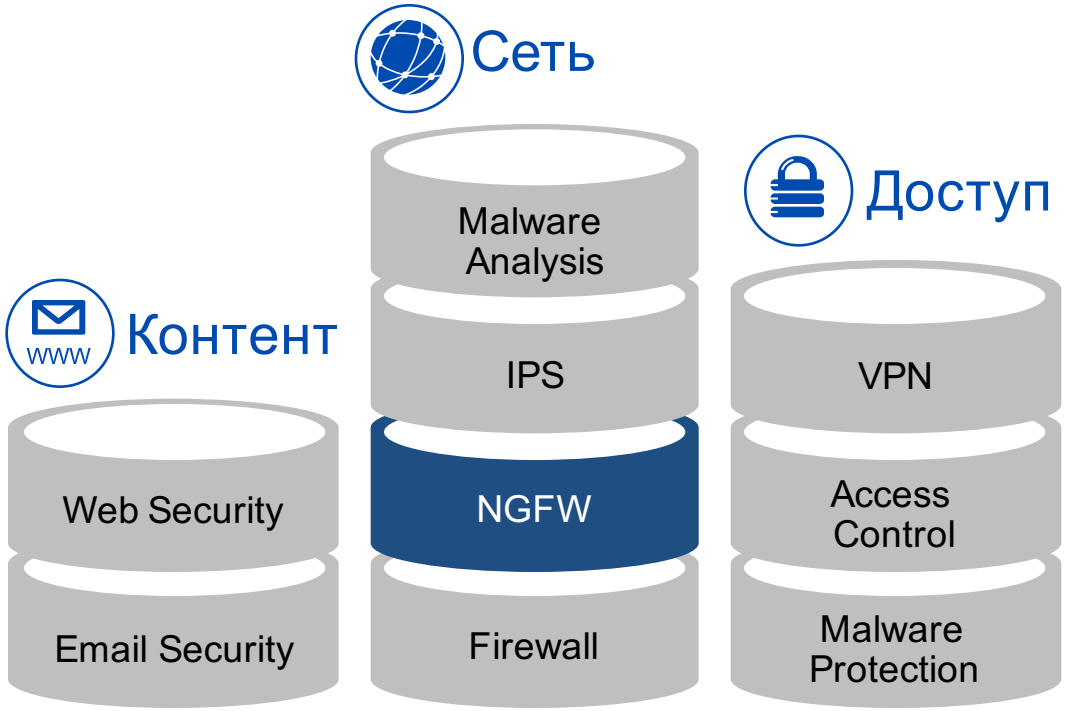
Source:
[1]Cisco Annual Security Report2014
[2]Cisco Midyear Security Report 2014
[3]Cisco Annual Security Report2015
[4]Cisco Midyear Security Report 2015

Комплексная защита от угроз в течение всего жизненного цикла атаки

Типичный NGFW узко ориентирован и сложно управляем

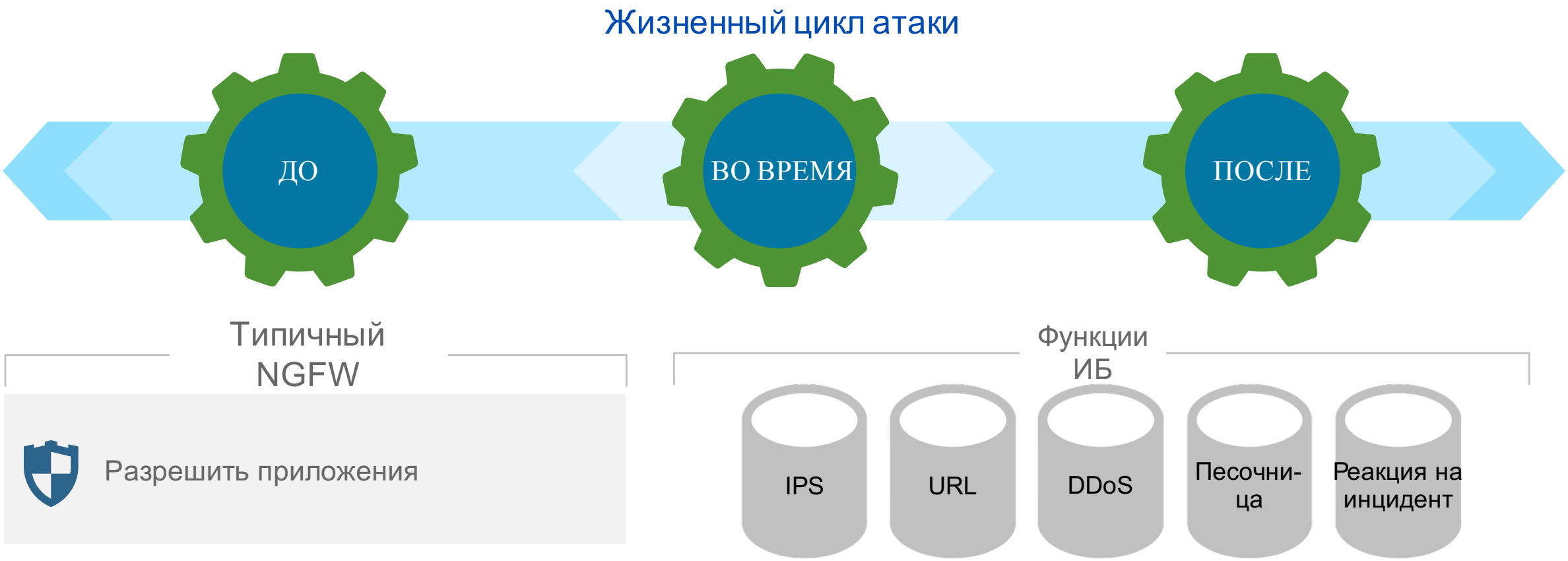


Фокус на приложениях, не угрозах

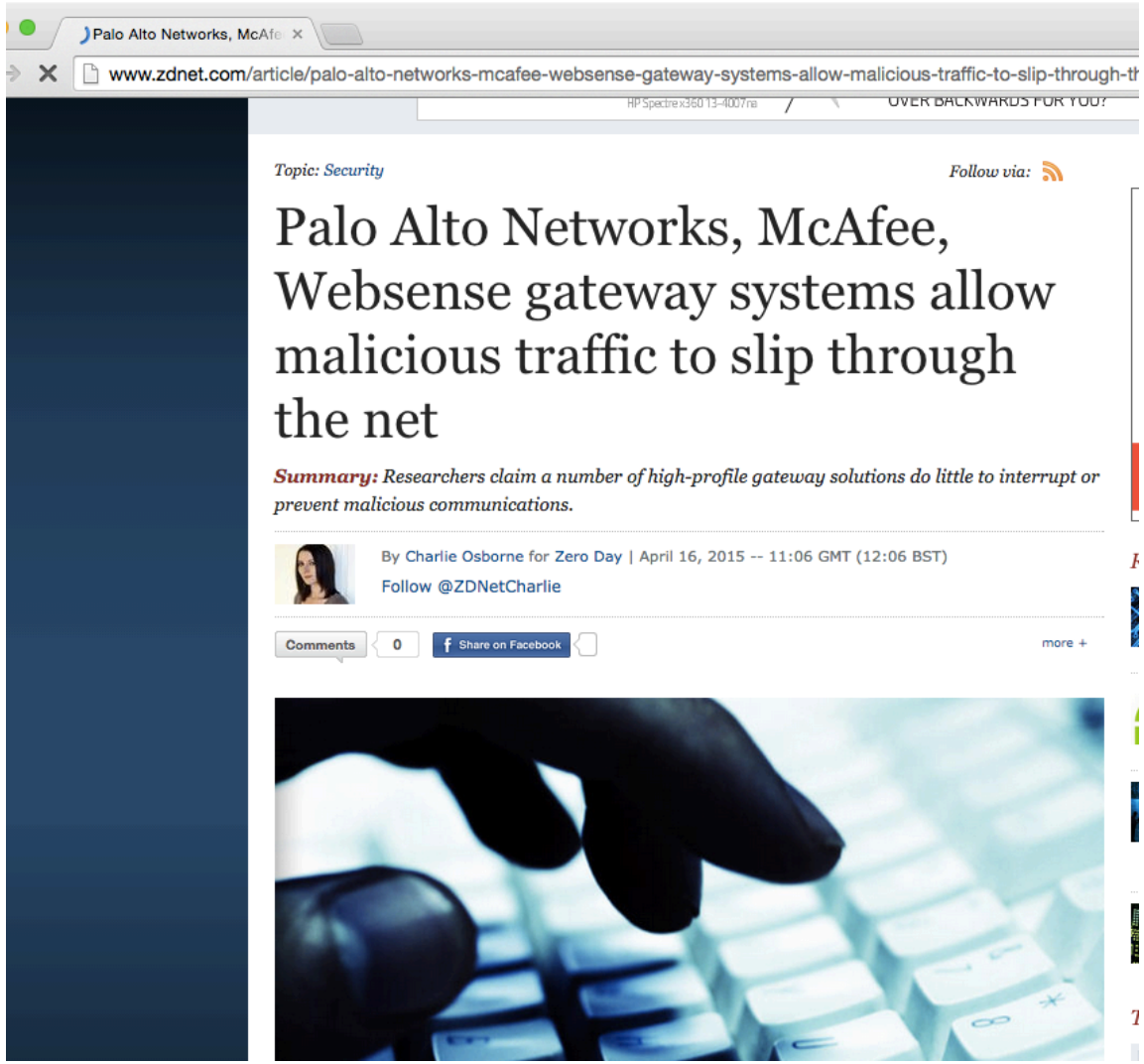


Приложения - это не все, что нужно

Они предотвращают атаки, но не эффективны во время и после ее реализации



А это подтверждение

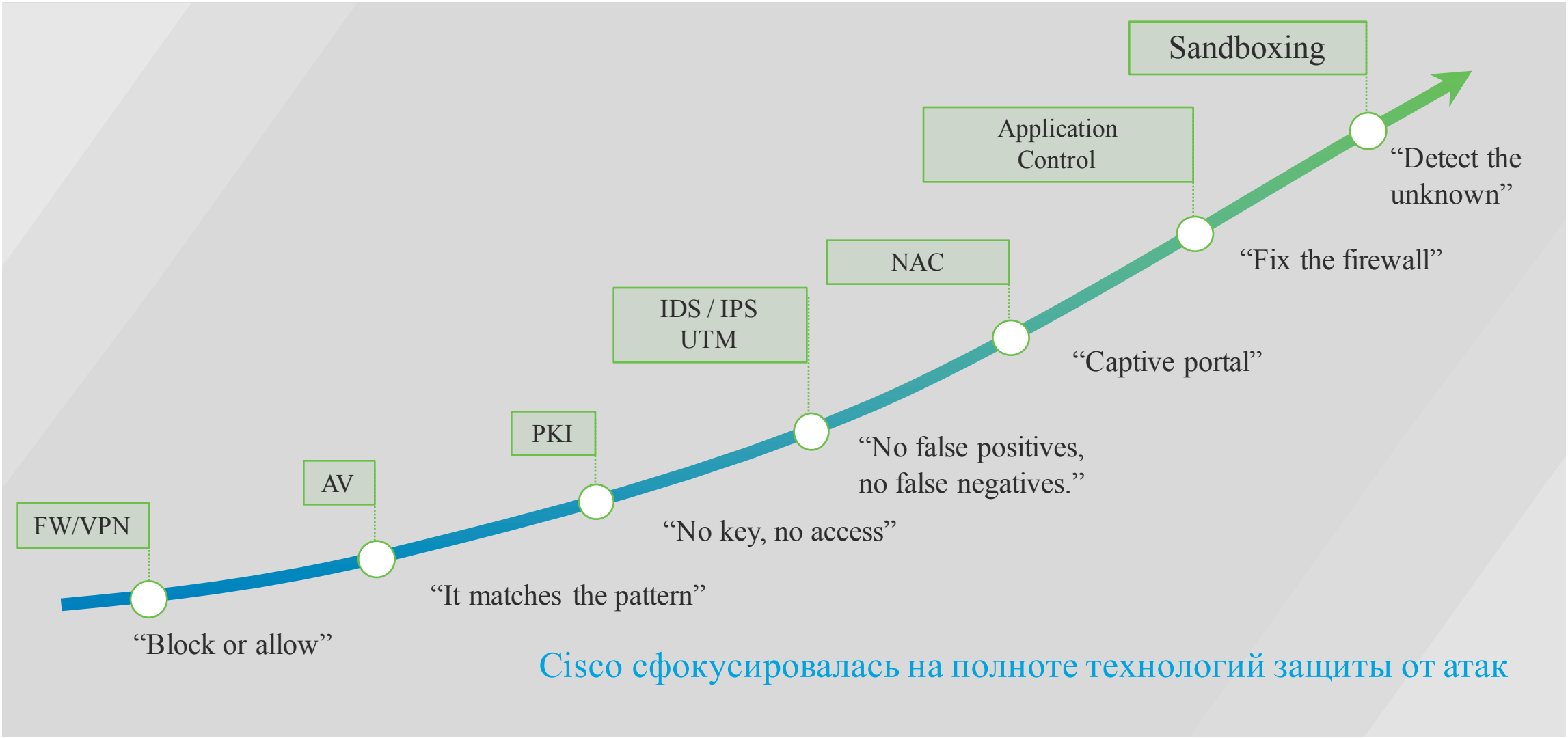


16 апреля 2015 года
http://www.zdnet.com/article/palo-alto-networks-mcafee-websense-gateway-systems-allow-malicious-traffic-to-slip-through-the-net/

Дело COBCEM не в названиях компаний, проблема в методологии

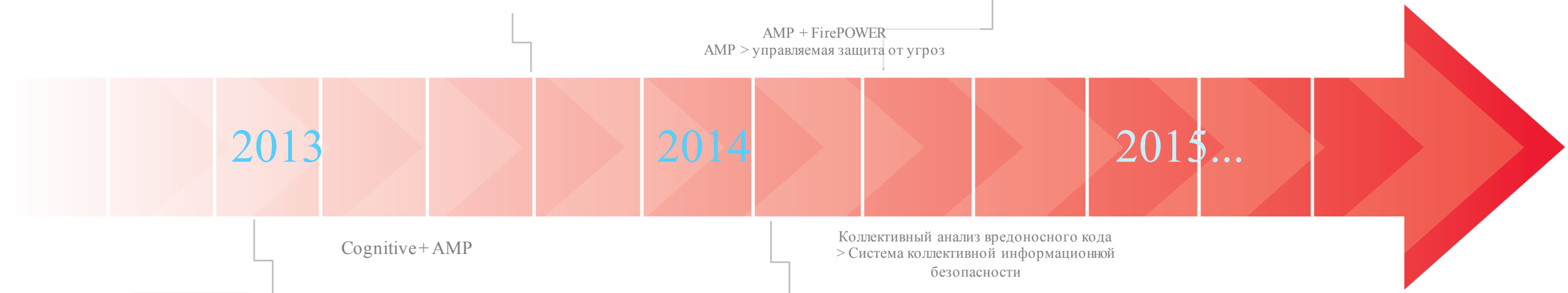
Создание межсетевого экрана нового поколения

В безопасности не существует единой серебрянной пули



Cisco сфокусировалась на полноте технологий защиты от атак

Cisco: в центре внимания — безопасность!



Приобретение компании Sourcefire Security

- Ведущие в отрасли СОПВ нового поколения
- Мониторинг сетевой активности
- Advanced Malware Protection
- Разработки отдела по исследованию уязвимостей (VRT)
- Инновации в ПО с открытым исходным кодом (технология OpenAppID)

Коллективные исследования Cisco – подразделение Talos по исследованию и анализу угроз

- Подразделение Sourcefire по исследованию уязвимостей — VRT
- Подразделене Cisco по исследованию и информированию об угрозах — TRAC
- Подразделение Cisco по безопасности приложений — SecApps

AMP + FirePOWER
AMP > управляемая защита от угроз

Cognitive+ AMP

Приобретение компании Cognitive Security

- Передовая служба исследований
- Улучшенные технологии поведенческого анализа в режиме реального времени

Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

Приобретение компании ThreatGRID

- Коллективный анализ вредоносного кода
- Анализ угроз

Cisco защищает на протяжении всего цикла атаки

ДО	ВО ВРЕМЯ	ПОСЛЕ
ASA NGFW	FirePOWER NGIPS и WIPS	Lancope Stealthwatch
ISE & TrustSec	WSA и CWS	Threat Grid
AnyConnect	ESA	Cognitive Threat Analytics
OpenDNS Investigate	Cloud Access Security	OpenDNS Investigate и CTA
	Advanced Malware Protection	
OpenDNS Umbrella		
Talos		

Начало: Cisco ASA с функцией FirePOWER

Первый в отрасли межсетевой экран нового поколения (NGFW), который смотрит шире и глубже

Анонсирован 16 сентября 2014 года

- Межсетевое экранирование Cisco® ASA в сочетании с системой предотвращения вторжений Sourcefire® нового поколения

МСЭ нового поколения, смотрящий шире и глубже других
ASA FirePOWER

Особенности

- Межсетевое экранирование Cisco® ASA в сочетании с системой предотвращения вторжений Sourcefire® нового поколения
- Усиленная защита от вредоносного кода Advanced Malware Protection (AMP)
- Лучшие в своем классе технологии анализа ИБ (SI), мониторинга и контроля приложений (AVC) и фильтрации URL-адресов

Преимущества

- Непревзойденная, многоуровневая защита от угроз
- Беспрецедентная прозрачность сетевой активности
- Комплексная защита от угроз на всем протяжении атаки
- Снижение стоимости и сложности систем

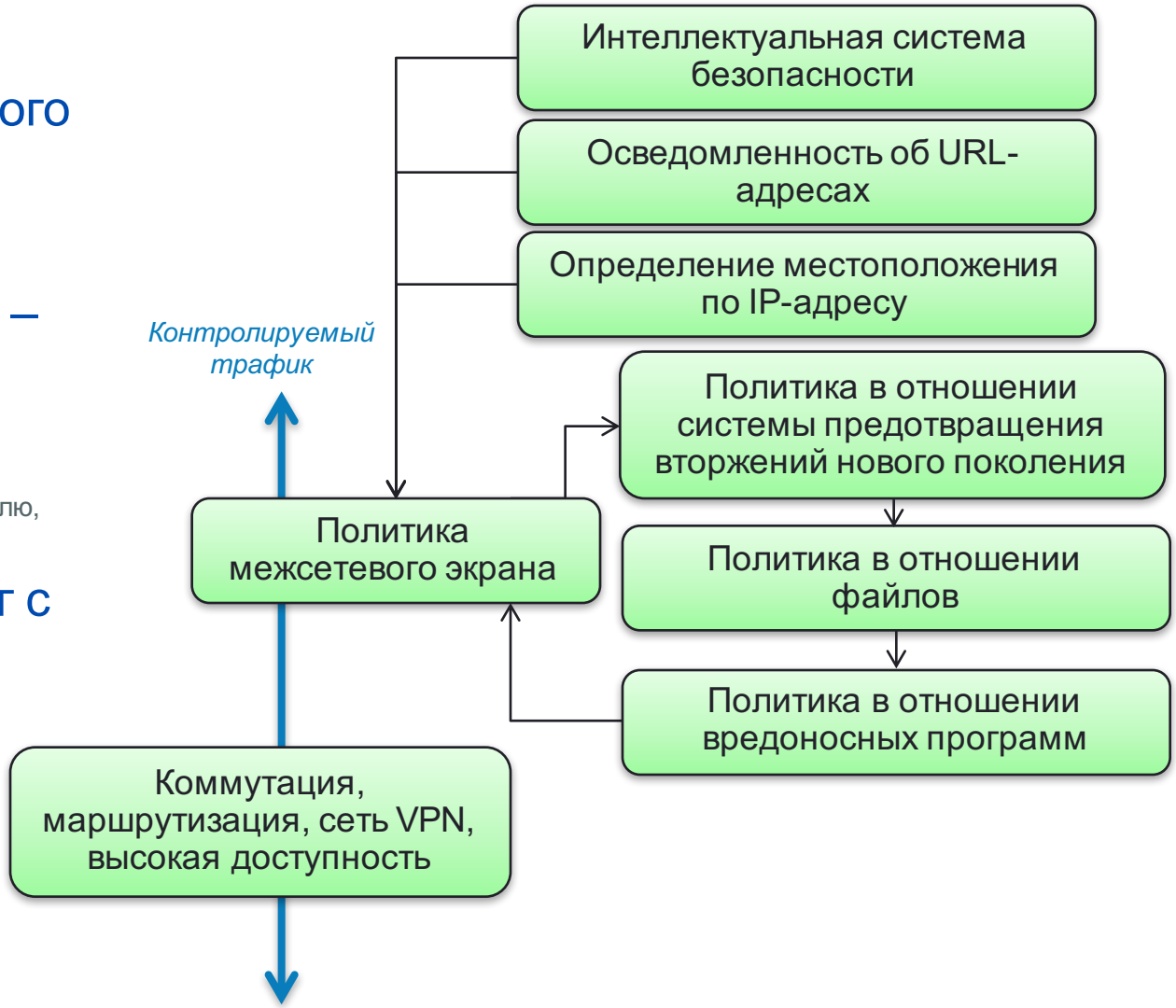
«С помощью многоуровневой защиты организации смогут расширить возможности для мониторинга, внедрить динамические механизмы безопасности и обеспечить усиленную защиту в течение всего жизненного цикла атаки»

Непревзойденная комплексная и многоуровневая защита

- Самый популярный межсетевой экран ASA корпоративного класса с функцией контроля состояния соединений
- Система гранулярного мониторинга и контроля приложений (Cisco® AVC)
- Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- Фильтрация URL-адресов на основе репутации и классификации
- Система Advanced Malware Protection с функциями ретроспективной защиты

Что умеет делать Firepower?

- Система предотвращения вторжений нового поколения – проверка содержимого
- Учет контекста
- Интеллектуальная система безопасности – управление черными списками
- Полный контроль доступа
  - По зоне сети, сеть VLAN, IP, порту, протоколу, приложению, пользователю, URL-адресу
- И все эти компоненты интегрируются друг с другом
  - Используются политики системы предотвращения вторжений
  - Политики контроля файлов

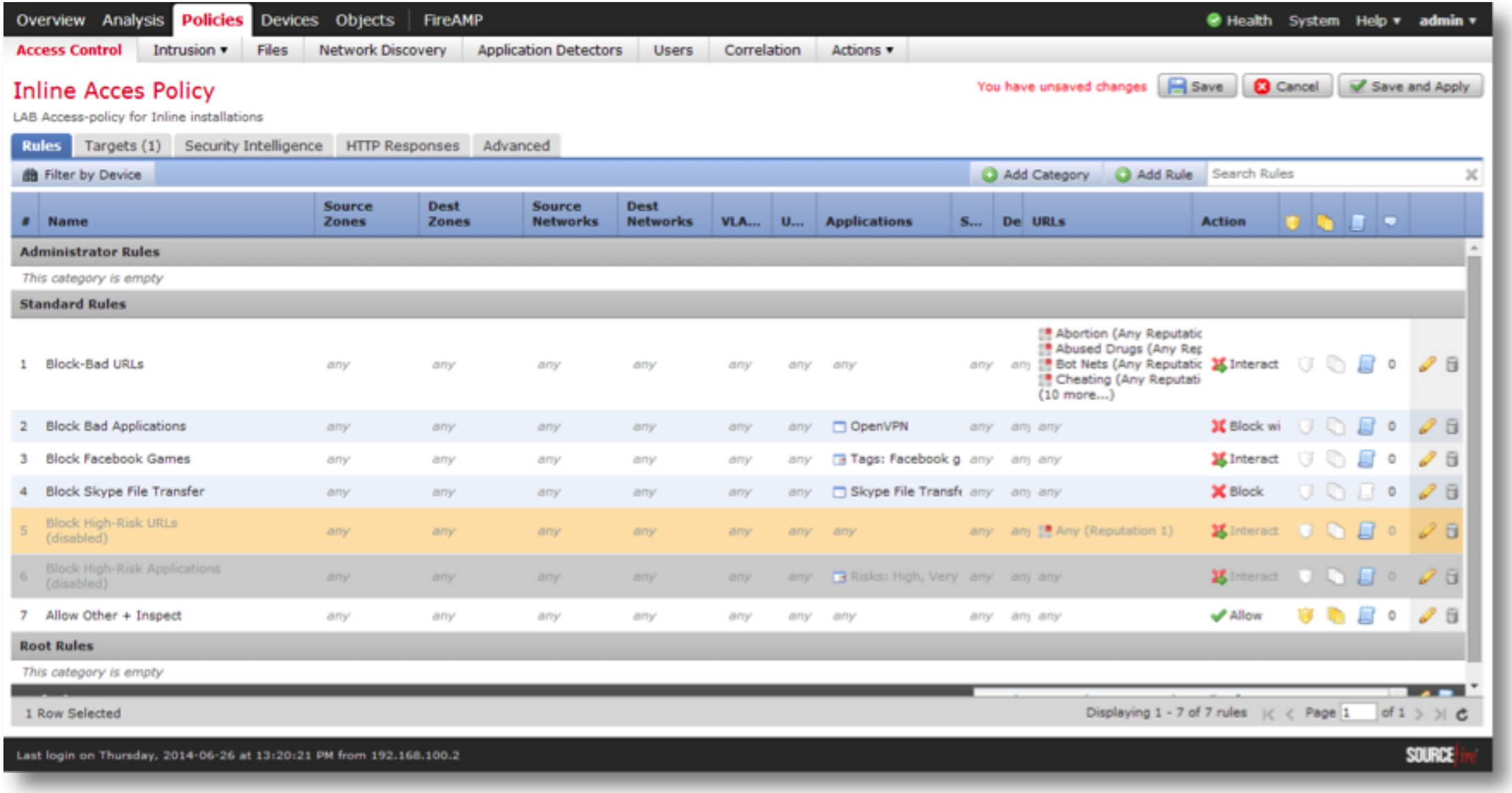


Беспрецедентная прозрачность сетевой активности

Категории	Технологии FirePOWER	Прежние IPS	Прежние МСЭ
Угрозы	✓	✓	✓
Пользователи	✓	✗	✓
Веб-приложения	✓	✗	✓
Протоколы приложений	✓	✗	✓
Передача файлов	✓	✗	✓
Вредоносный код	✓	✗	✗
Серверы управления и контроля ботнета	✓	✗	✗
Клиентские приложения	✓	✗	✗
Сетевые серверы	✓	✗	✗
Операционные системы	✓	✗	✗
Маршрутизаторы и коммутаторы	✓	✗	✗
Мобильные устройства	✓	✗	✗
Принтеры	✓	✗	✗
VoIP-телефония	✓	✗	✗
Виртуальные машины	✓	✗	✗

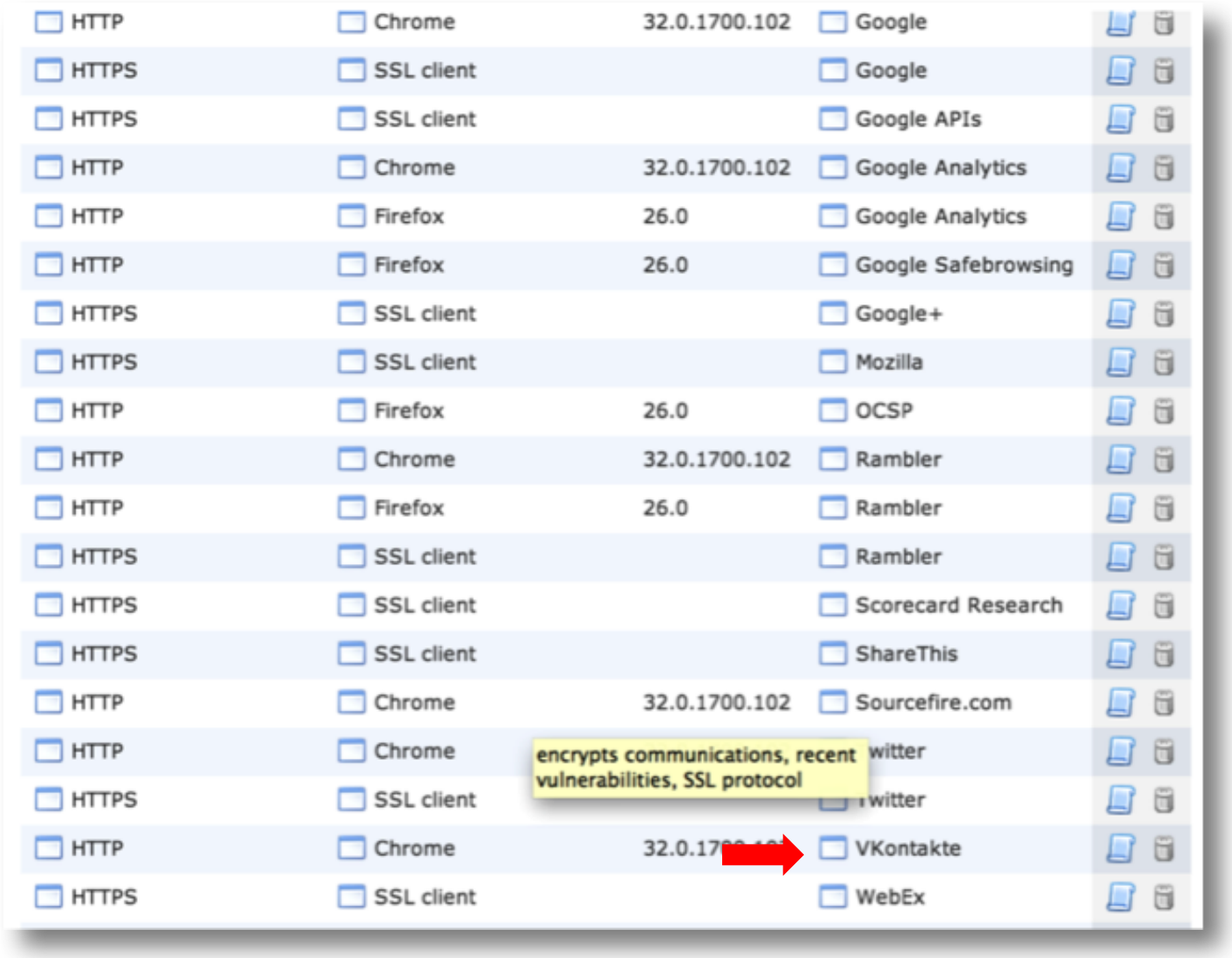
Особенности функционала. NGFW

Политика NGFW



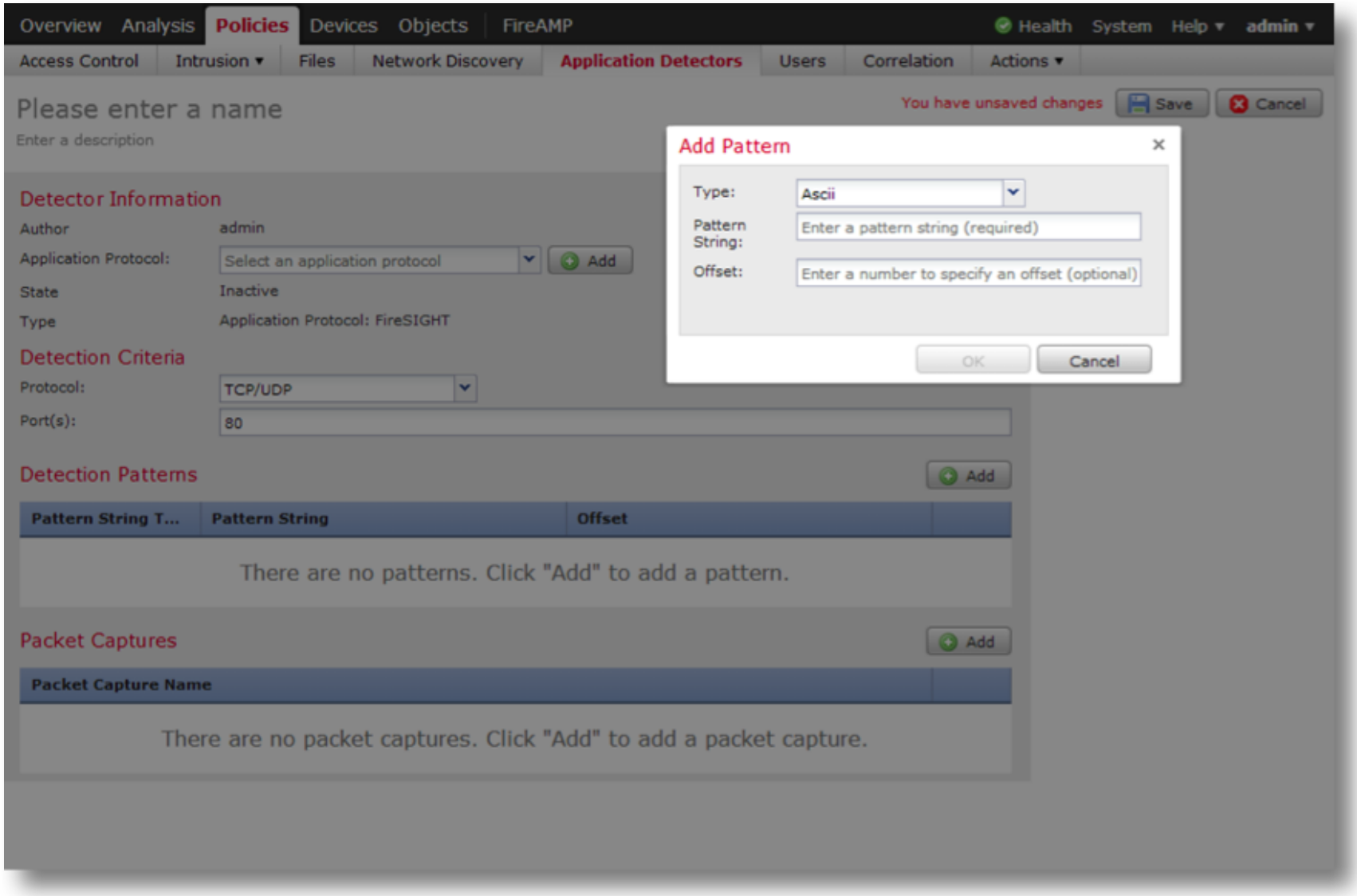
Распознавание приложений

- Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности
- FirePOWER for ASA распознает и «локальные» приложения

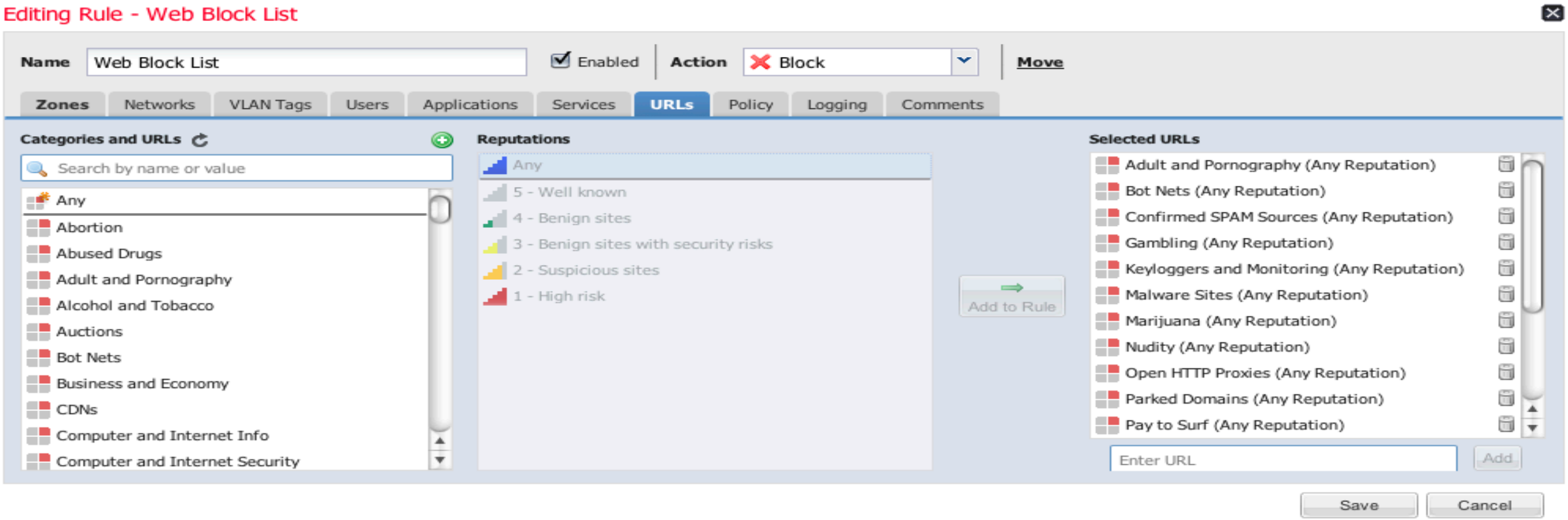


Описание собственных приложений

- Приложения могут быть описаны шаблонами
  - ASCII
  - HEX
  - PCAP-файл



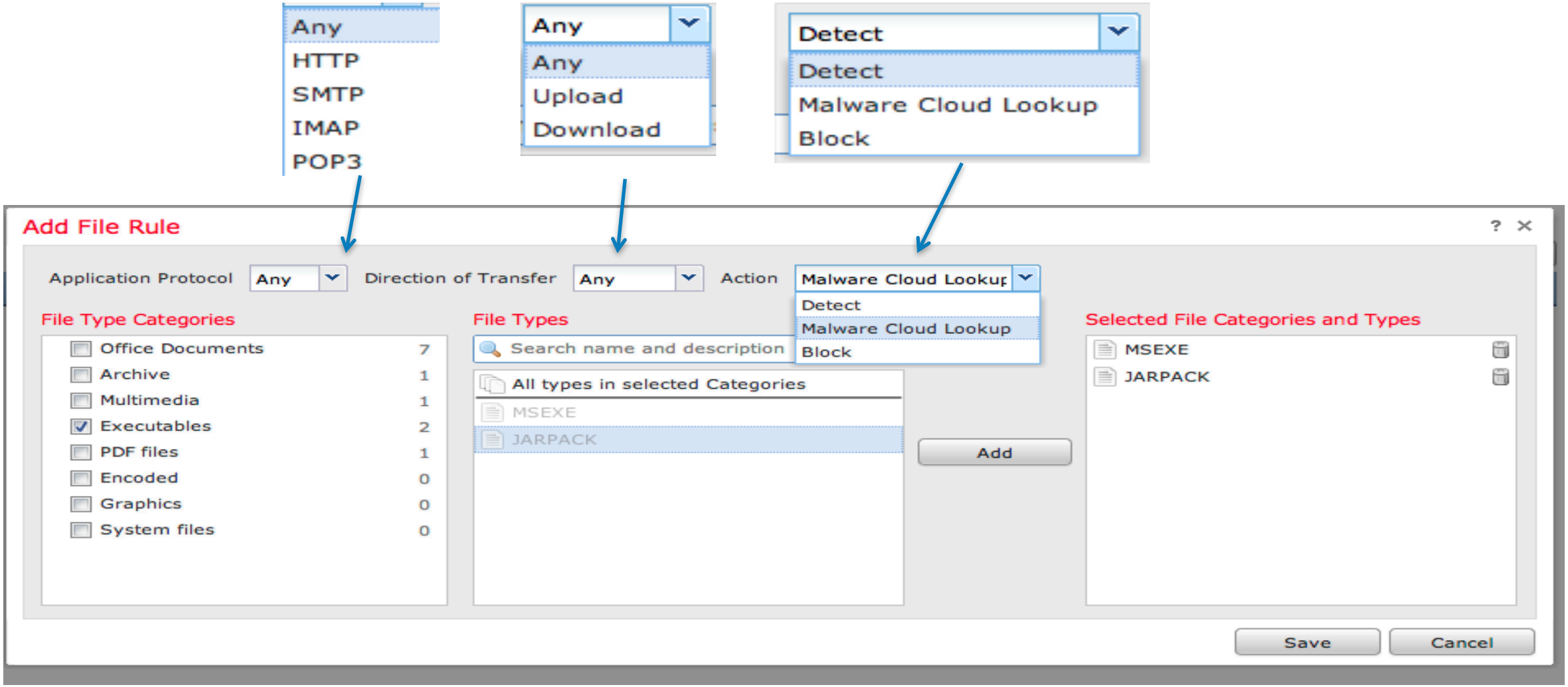
Фильтрация URL



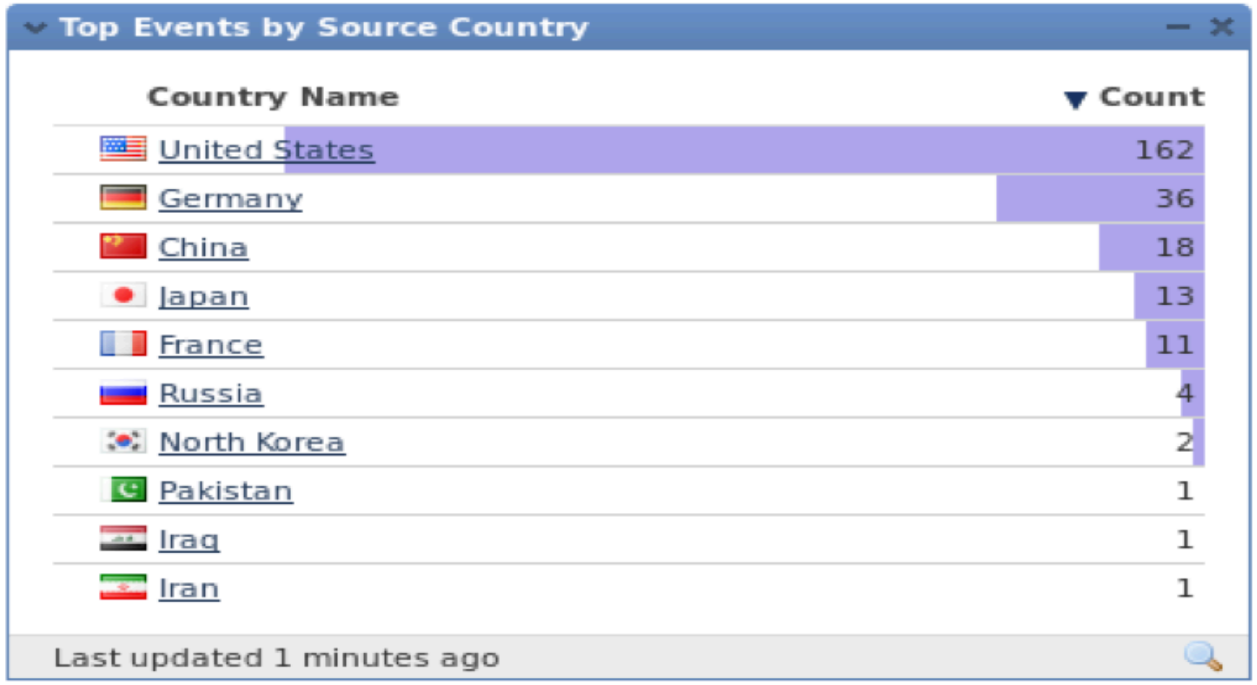
Различные категории URL

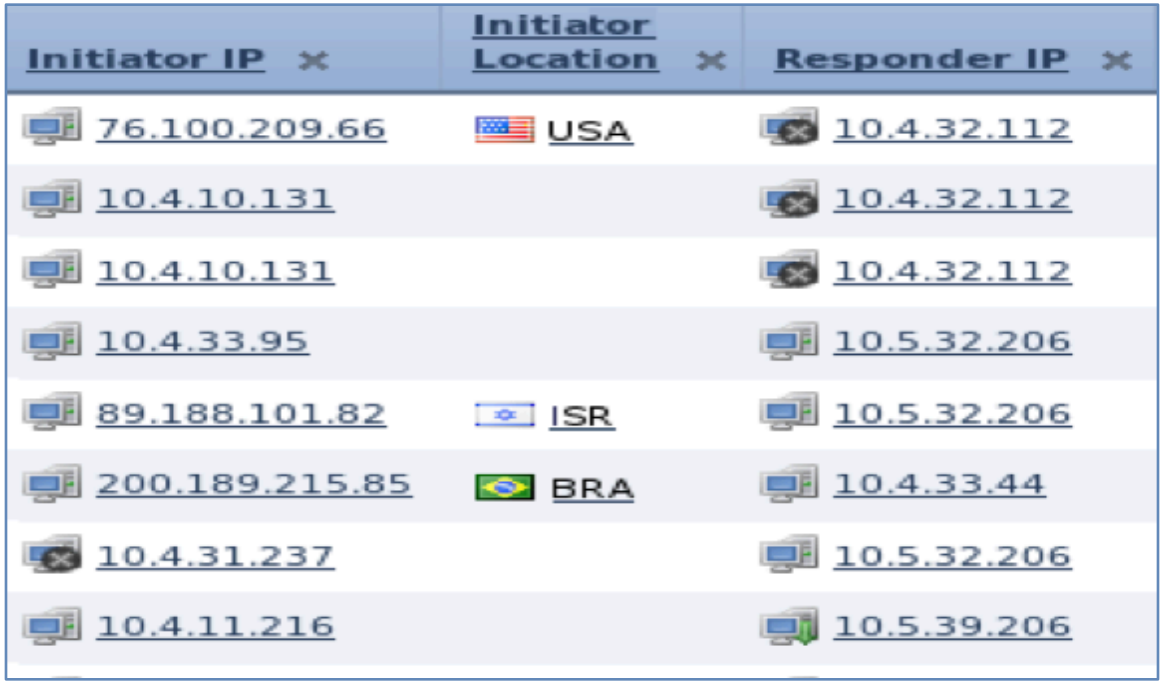
URLs категорированы по уровню рисков

Контроль по типам файлов и направлению передачи



Геолокация и визуализация местонахождения атакующих

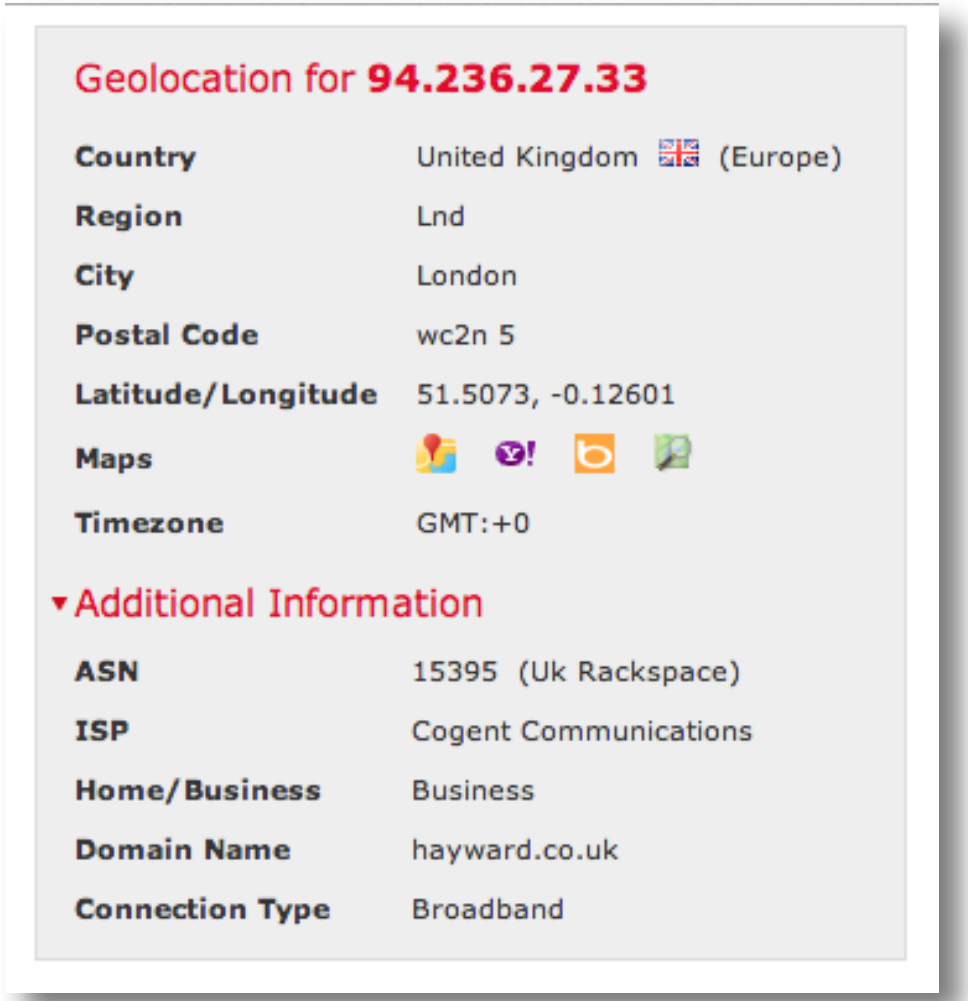




- Визуализация карт, стран и городов для событий и узлов

Детали по геолокации

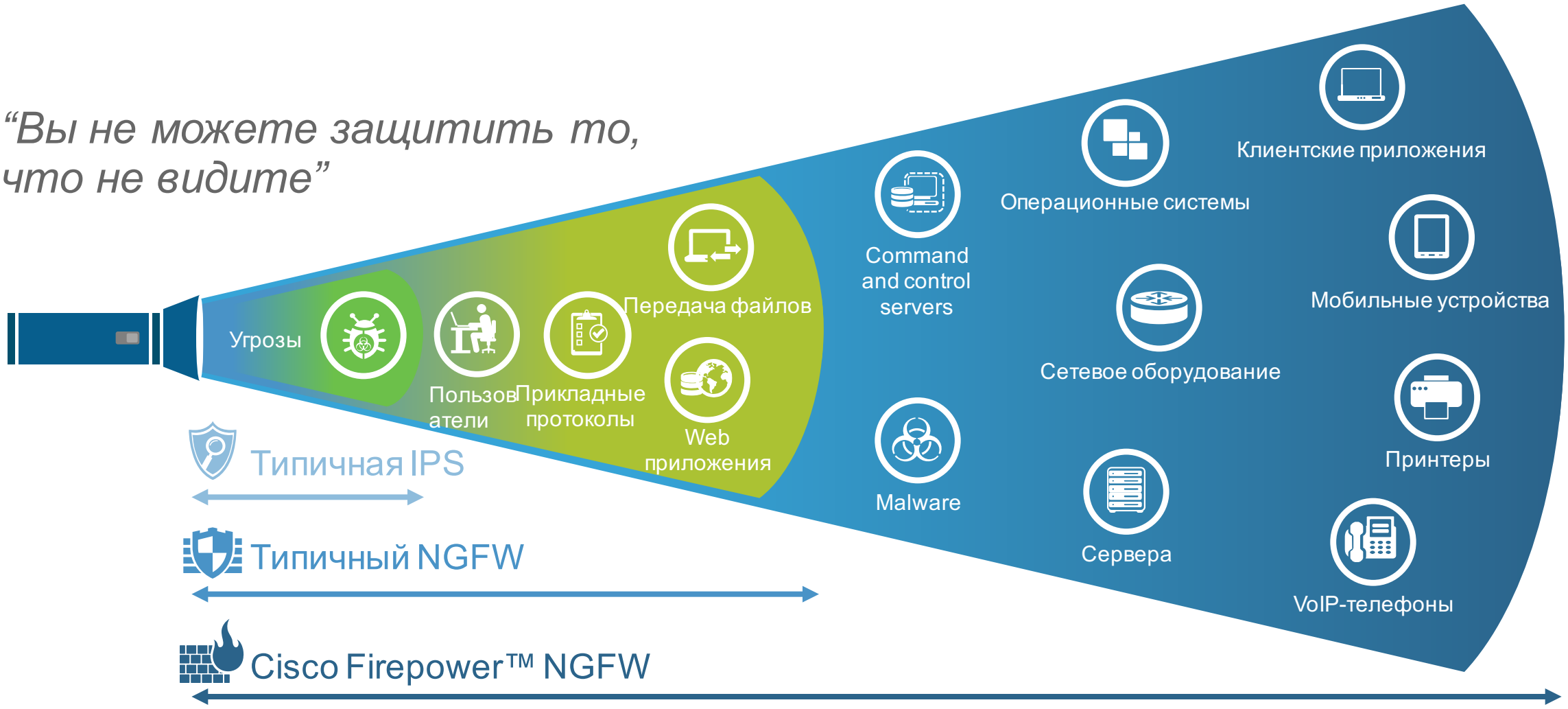
- IP –адреса должны быть маршрутизируемыми
- Два типа геолокационных данных
  - Страна – включено по умолчанию
  - Full – Может быть загружено после установки:
    - Почтовый индекс, координаты, TZ, ASN, ISP, организация, доменное имя и т.д.
    - Ссылки на карты (Google, Bing и другие)
- Страна сохраняется в запись о событии
  - Для источника & получателя



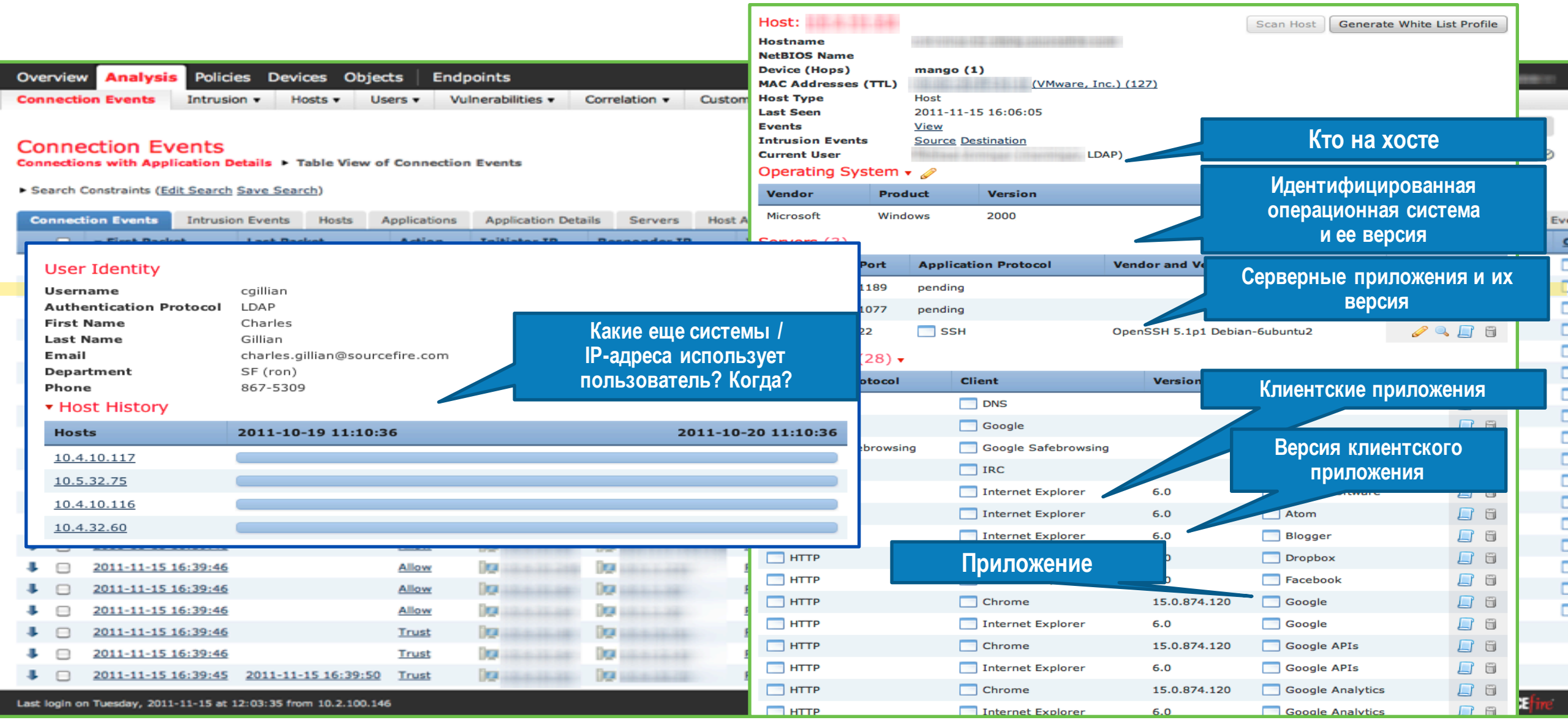
Особенности функционала. NGIPS

Смотреть глубже и шире

“Вы не можете защитить то, что не видите”

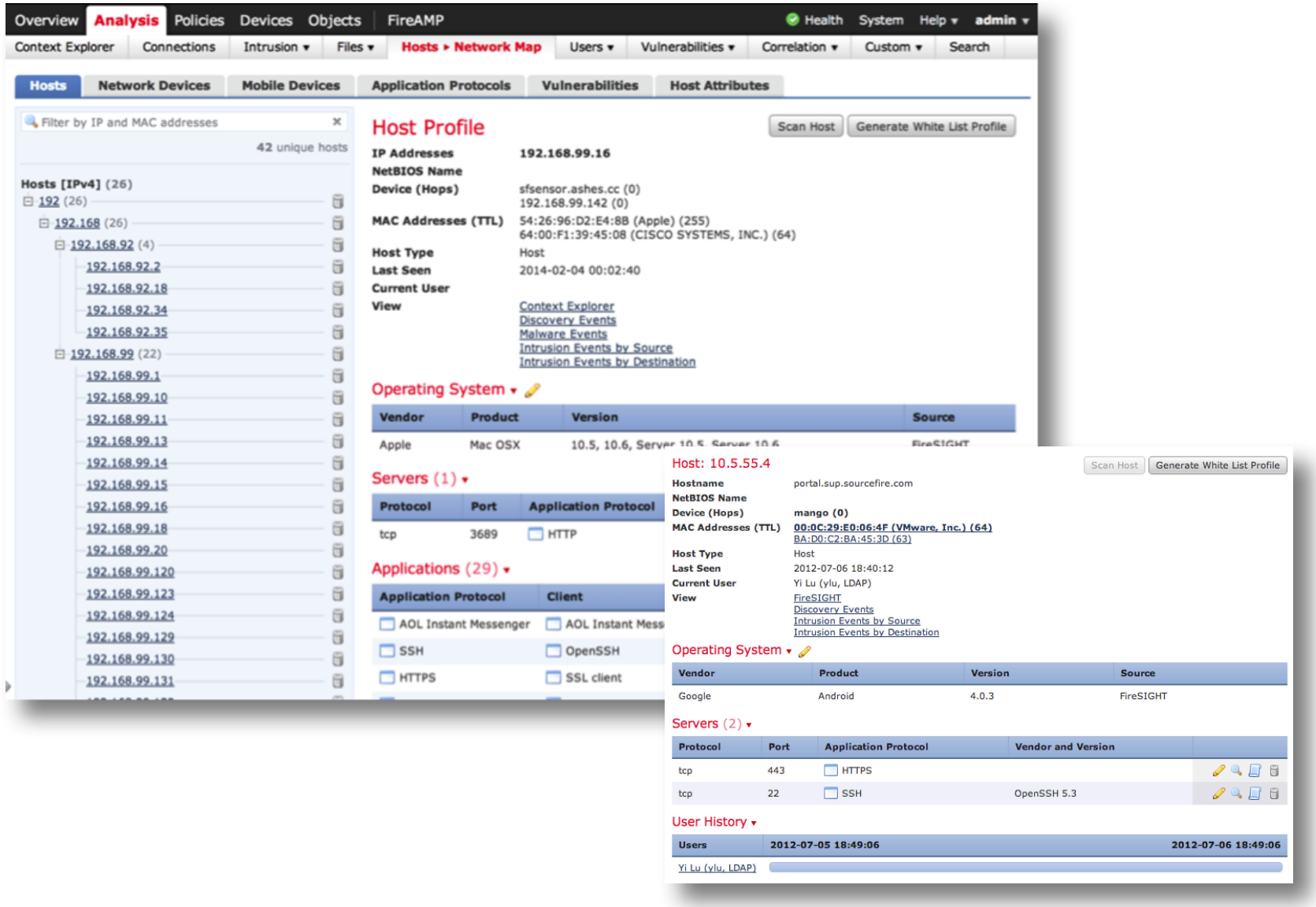


Анализ происходящего на узлах

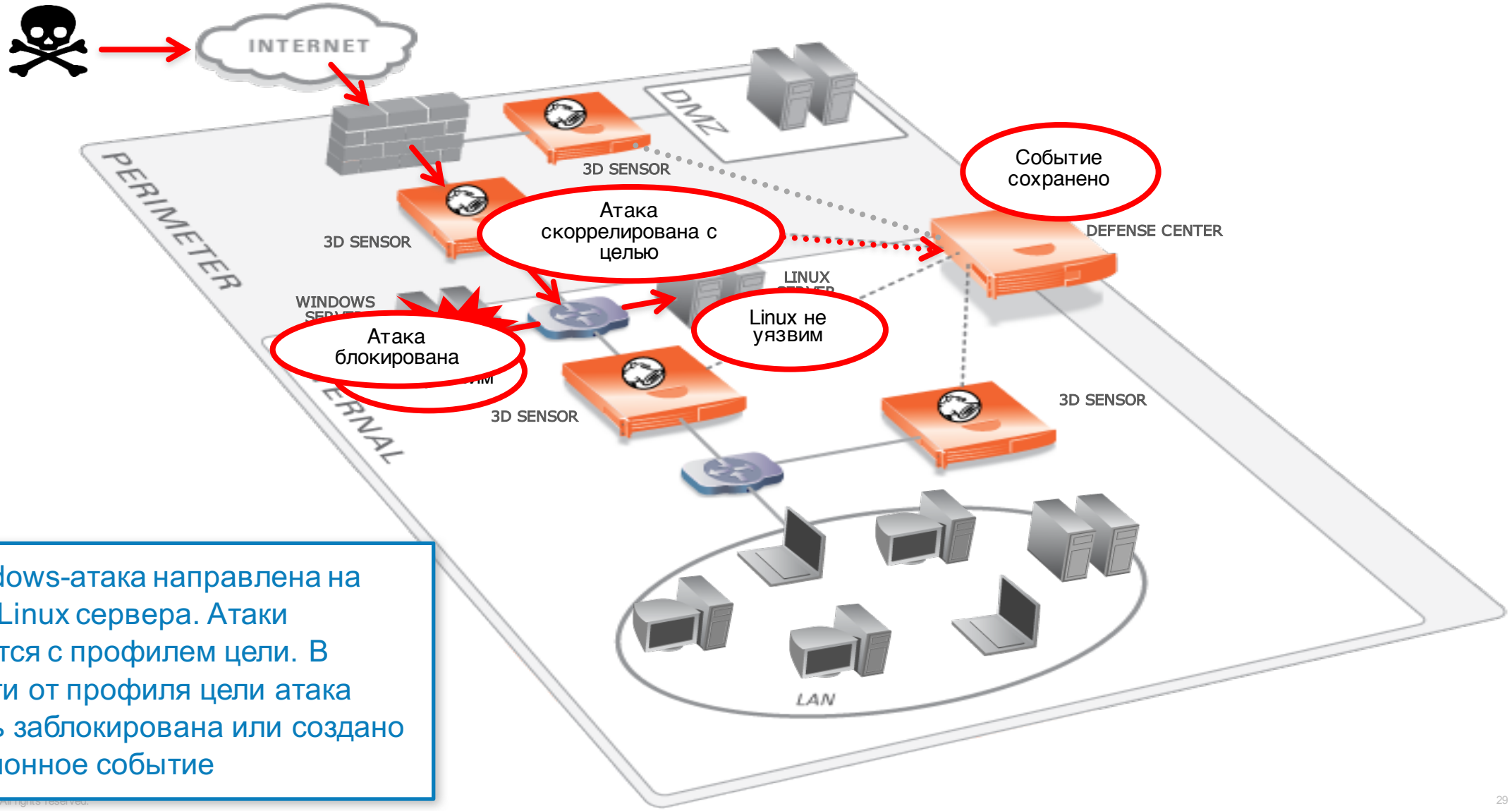


Инвентаризация и профилирование узлов

- Профиль хоста включает всю необходимую для анализа информацию
  - IP-, NetBIOS-, MAC-адреса
  - Операционная система
  - Используемые приложения
  - Зарегистрированные пользователи
  - И т.д.
- Идентификация и профилирование мобильных устройств



Корреляция событий безопасности



Новая Windows-атака направлена на Windows и Linux сервера. Атаки сравниваются с профилем цели. В зависимости от профиля цели атака может быть заблокирована или создано информационное событие

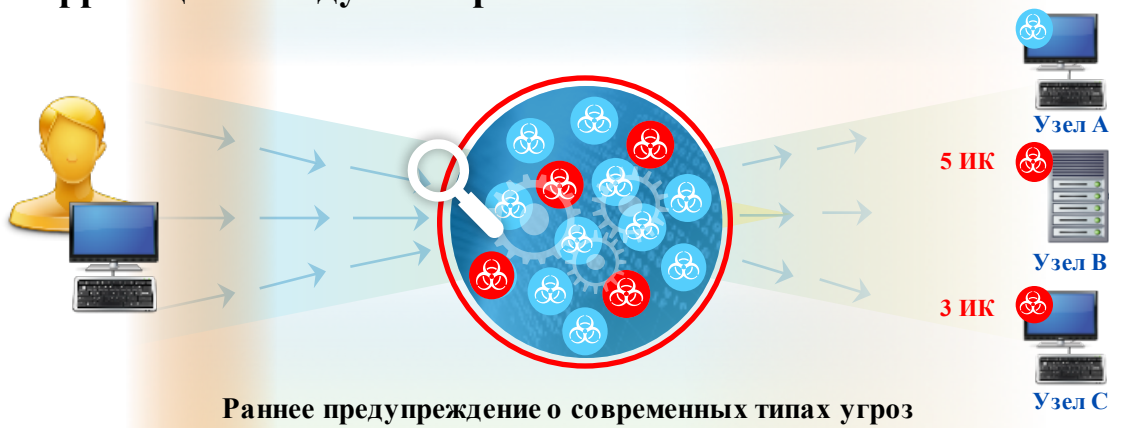
Автоматизированная, комплексная защита от угроз

Непревзойденная защита в течение всего жизненного цикла атаки

Корреляция между контекстом и угрозами

Оценка вредоносного воздействия

Корреляция между векторами атаки

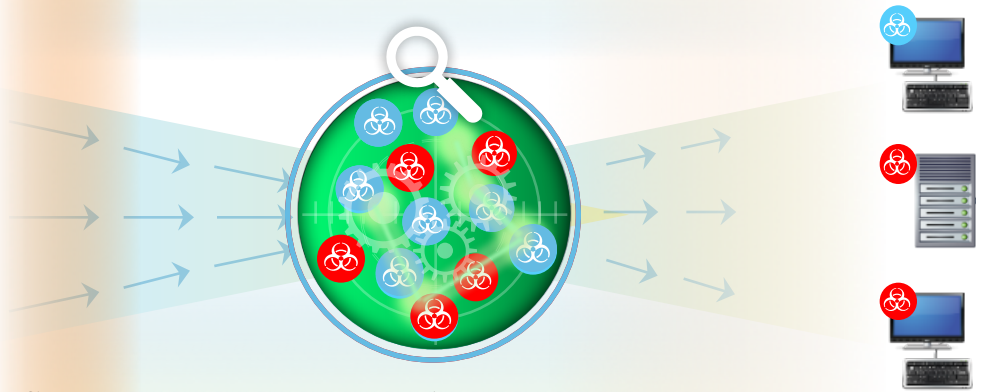


Раннее предупреждение о современных типах угроз

Динамические механизмы безопасности

Адаптация политик к рискам

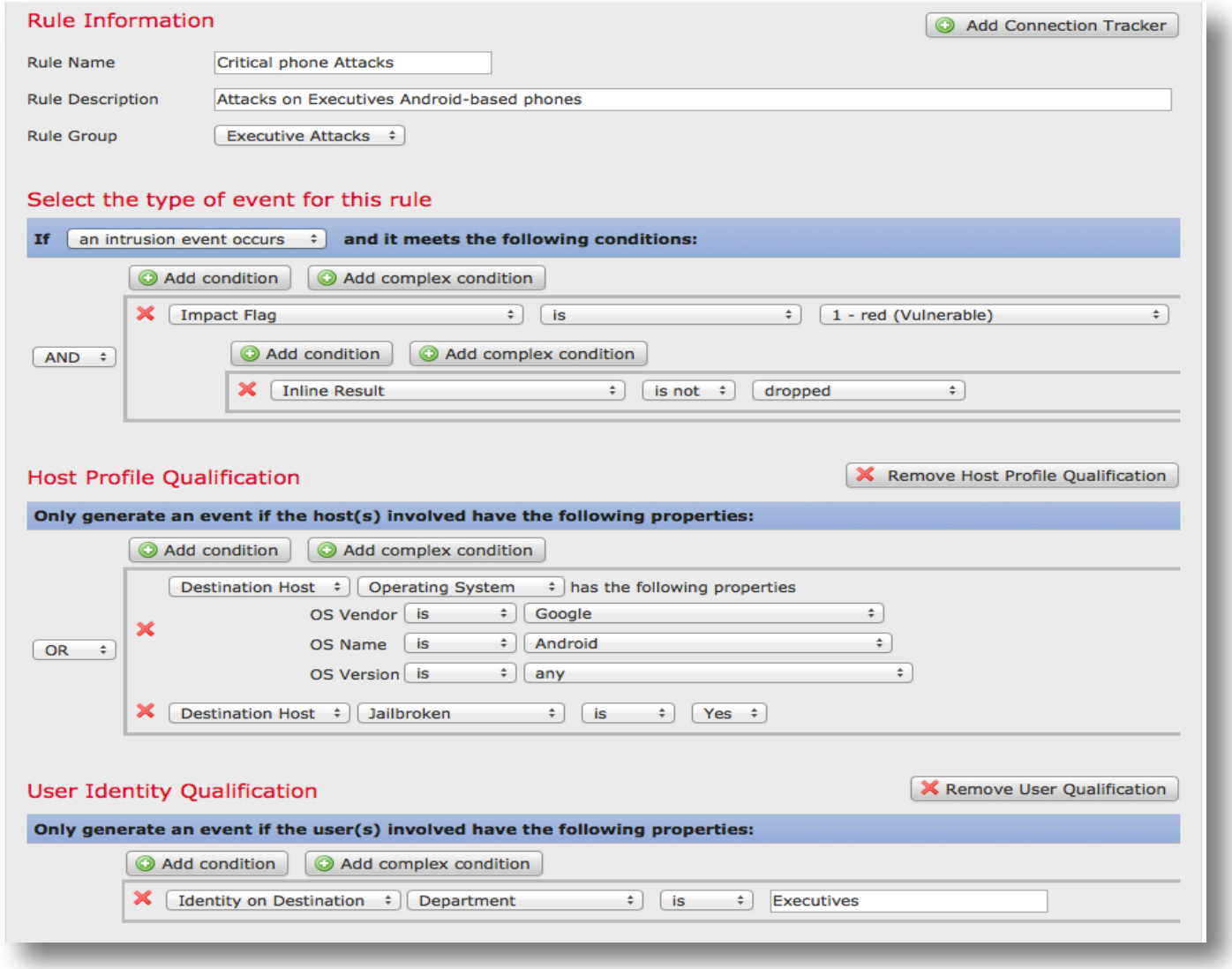
Ретроспективная защита



Сокращение времени между обнаружением и нейтрализацией

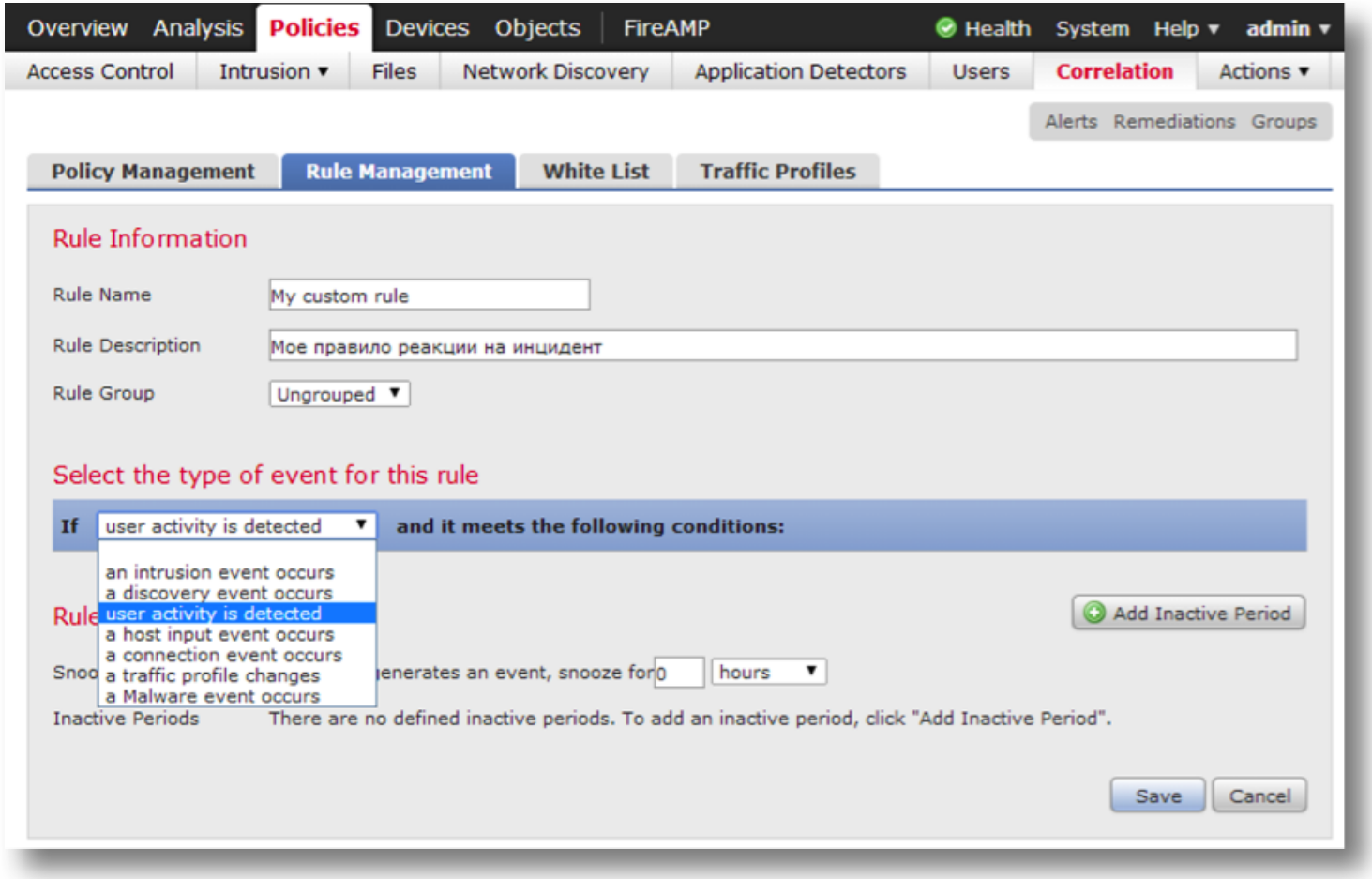
Система корреляции событий

- Правила корреляции могут включать любые условия и их комбинации на базе идентифицированных в сети данных
  - Приложения
  - Уязвимости
  - Протоколы
  - Пользователи
  - Операционные системы
  - Производитель ОС
  - Адреса
  - Место в иерархии компании
  - Статус узла и т.п.

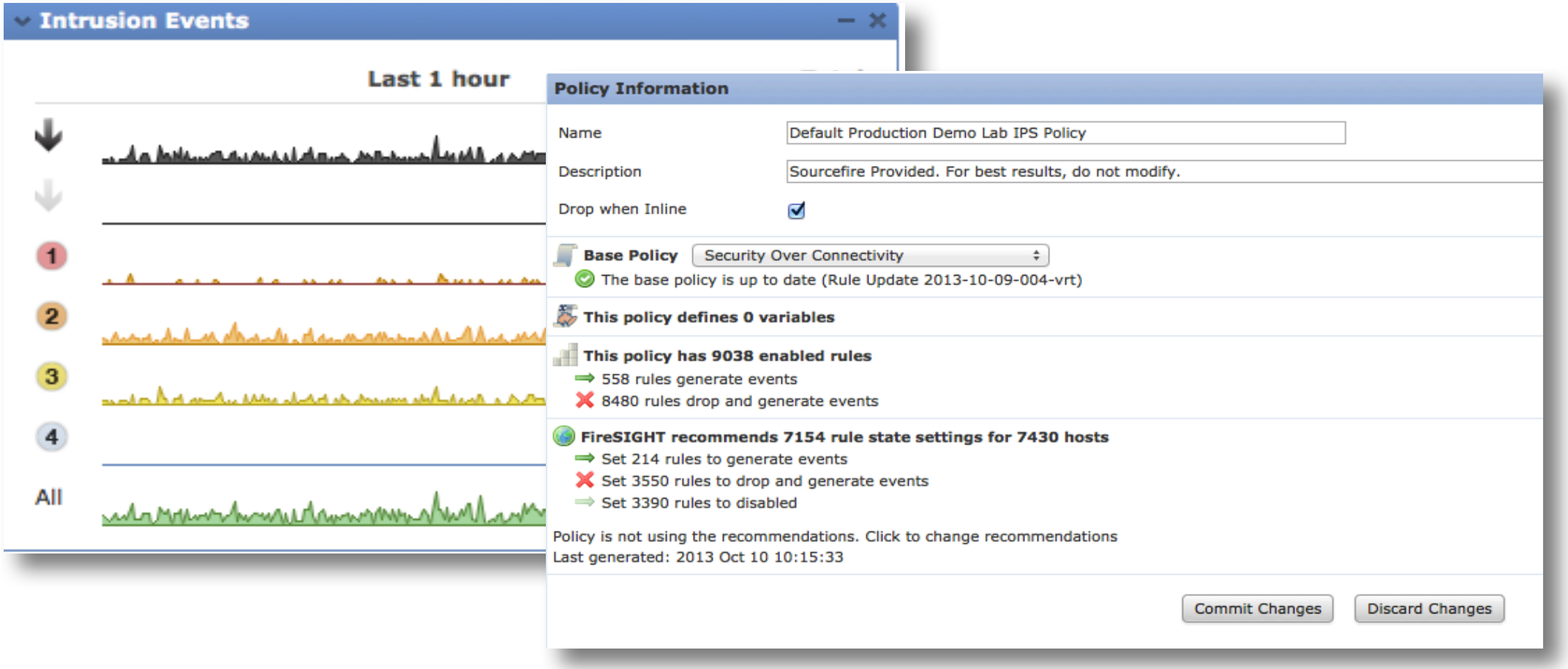


Дополнительная система корреляции событий

- Различные типы события для системы корреляции
  - Атаки / вторжение
  - Активность пользователя
  - Установлено соединение
  - Изменение профиля трафика
  - Вредоносный код
  - Изменение инвентаризационных данных (например, появление нового узла в сети или ОС на узле)
  - Изменение профиля узла
  - Появление новой уязвимости



Автоматизация создания и настройки политик



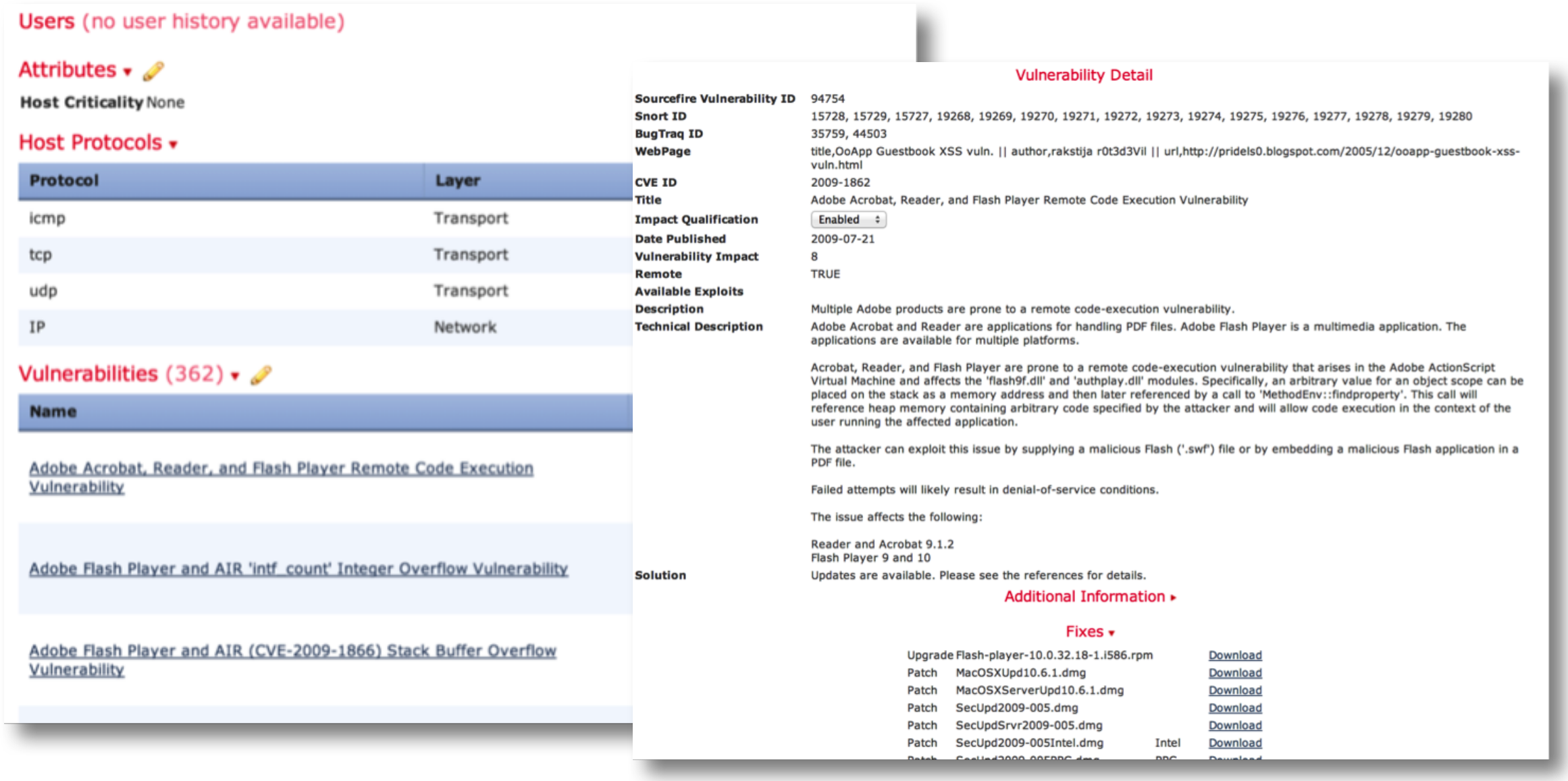
Анализ сети, протоколов, приложений, сервисов, устройств, ОС, уязвимостей и др. позволяет автоматизировать создание политик и правил МСЭ и IPS

Оценка вредоносного воздействия

Каждому событию вторжения присваивается уровень воздействия атаки на объект

УРОВЕНЬ ВОЗДЕЙСТВИЯ	ДЕЙСТВИЯ АДМИНИСТРАТОРА	ПРИЧИНЫ
1	Немедленно принять меры, опасность	Событие соответствует уязвимости, существующей на данном узле
2	Провести расследование, потенциальная опасность	Открыт соответствующий порт или используется соответствующий протокол, но уязвимости отсутствуют
3	Принять к сведению, опасности пока нет	Соответствующий порт закрыт, протокол не используется
4	Принять к сведению, неизвестный объект	Неизвестный узел в наблюдаемой сети
0	Принять к сведению, неизвестная сеть	Сеть, за которой не ведется наблюдение

Использование информации об уязвимостях



Users (no user history available)

Attributes

Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

Vulnerabilities (362)

Name
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability
Adobe Flash Player and AIR (CVE-2009-1866) Stack Buffer Overflow Vulnerability

Vulnerability Detail

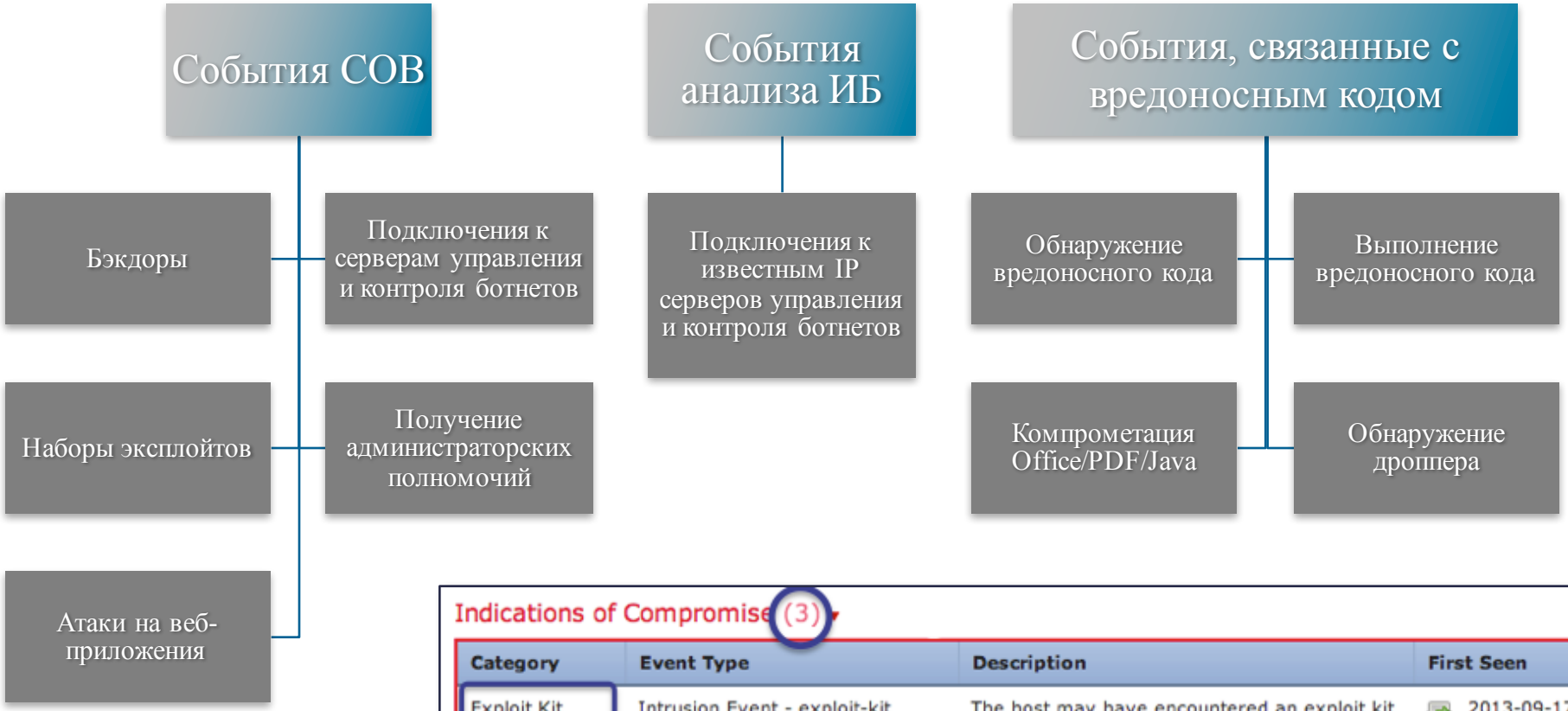
Sourcefire Vulnerability ID	94754
Snort ID	15728, 15729, 15727, 19268, 19269, 19270, 19271, 19272, 19273, 19274, 19275, 19276, 19277, 19278, 19279, 19280
BugTraq ID	35759, 44503
WebPage	title,OoApp Guestbook XSS vuln. || author,rakstija r0t3d3Vil || url,http://pridels0.blogspot.com/2005/12/ooapp-guestbook-xss-vuln.html
CVE ID	2009-1862
Title	Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability
Impact Qualification	Enabled
Date Published	2009-07-21
Vulnerability Impact	8
Remote	TRUE
Available Exploits	
Description	Multiple Adobe products are prone to a remote code-execution vulnerability.
Technical Description	Adobe Acrobat and Reader are applications for handling PDF files. Adobe Flash Player is a multimedia application. The applications are available for multiple platforms. Acrobat, Reader, and Flash Player are prone to a remote code-execution vulnerability that arises in the Adobe ActionScript Virtual Machine and affects the 'flash9f.dll' and 'authplay.dll' modules. Specifically, an arbitrary value for an object scope can be placed on the stack as a memory address and then later referenced by a call to 'MethodEnv::findproperty'. This call will reference heap memory containing arbitrary code specified by the attacker and will allow code execution in the context of the user running the affected application. The attacker can exploit this issue by supplying a malicious Flash ('.swf') file or by embedding a malicious Flash application in a PDF file. Failed attempts will likely result in denial-of-service conditions. The issue affects the following: Reader and Acrobat 9.1.2 Flash Player 9 and 10
Solution	Updates are available. Please see the references for details.

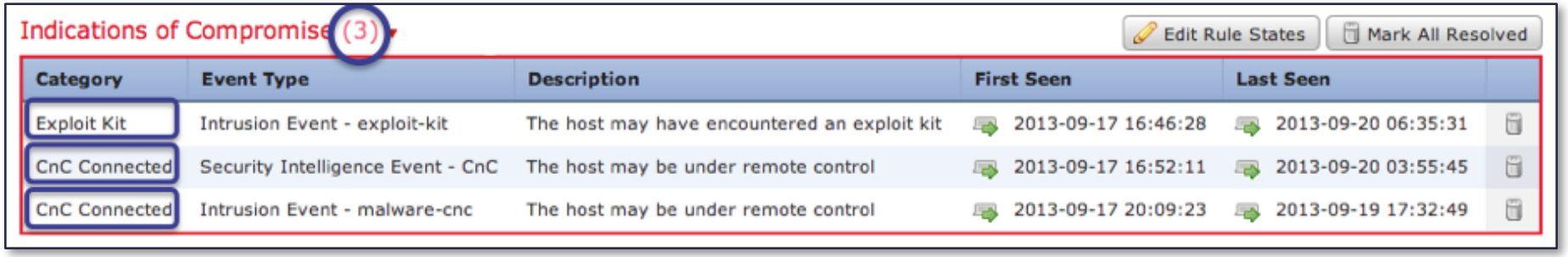
Additional Information

Fixes

Upgrade	Flash-player-10.0.32.18-1.i586.rpm		Download
Patch	MacOSXUpd10.6.1.dmg		Download
Patch	MacOSXServerUpd10.6.1.dmg		Download
Patch	SecUpd2009-005.dmg		Download
Patch	SecUpdSrvr2009-005.dmg		Download
Patch	SecUpd2009-005Intel.dmg	Intel	Download

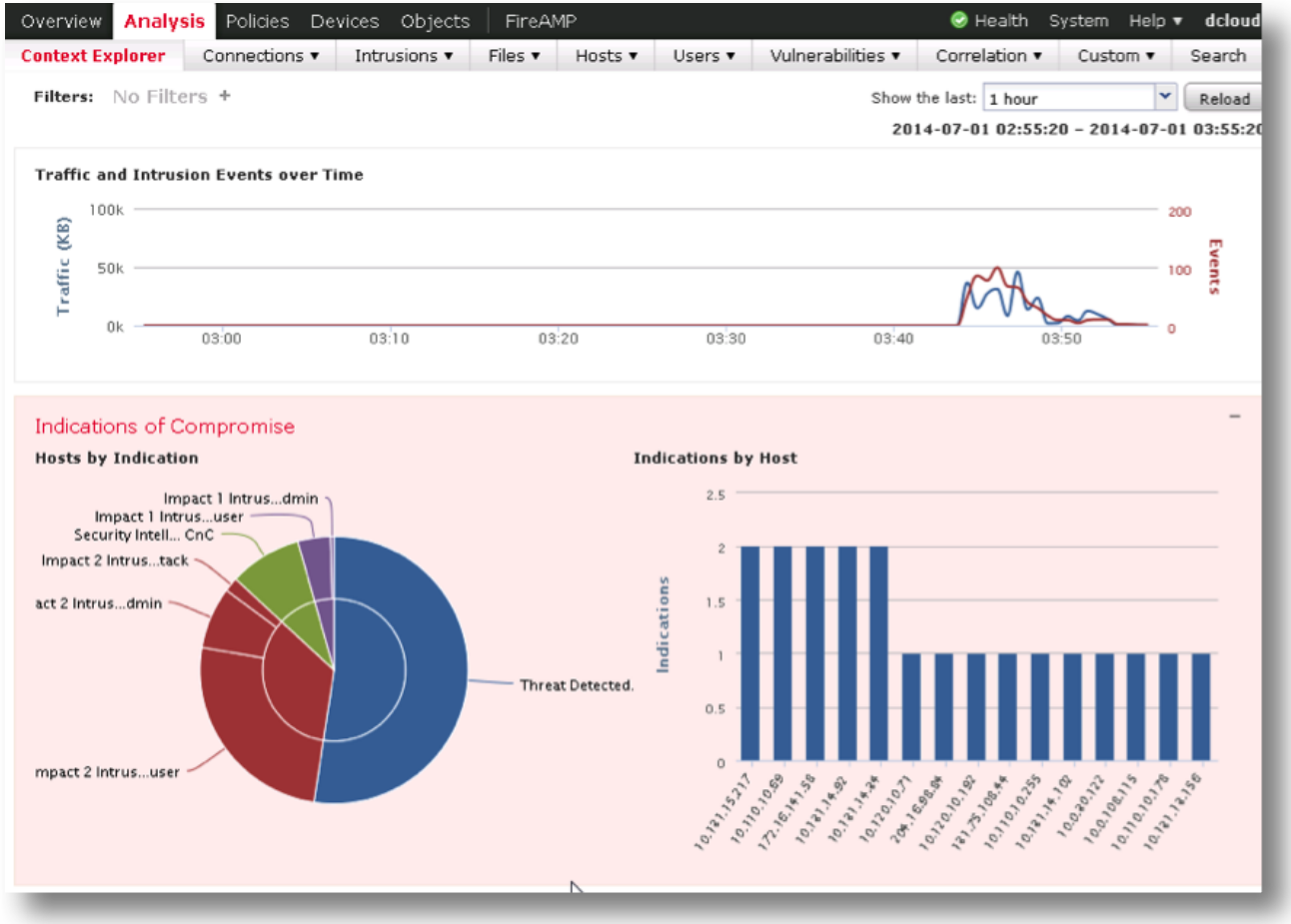
Признаки (индикаторы) компрометации





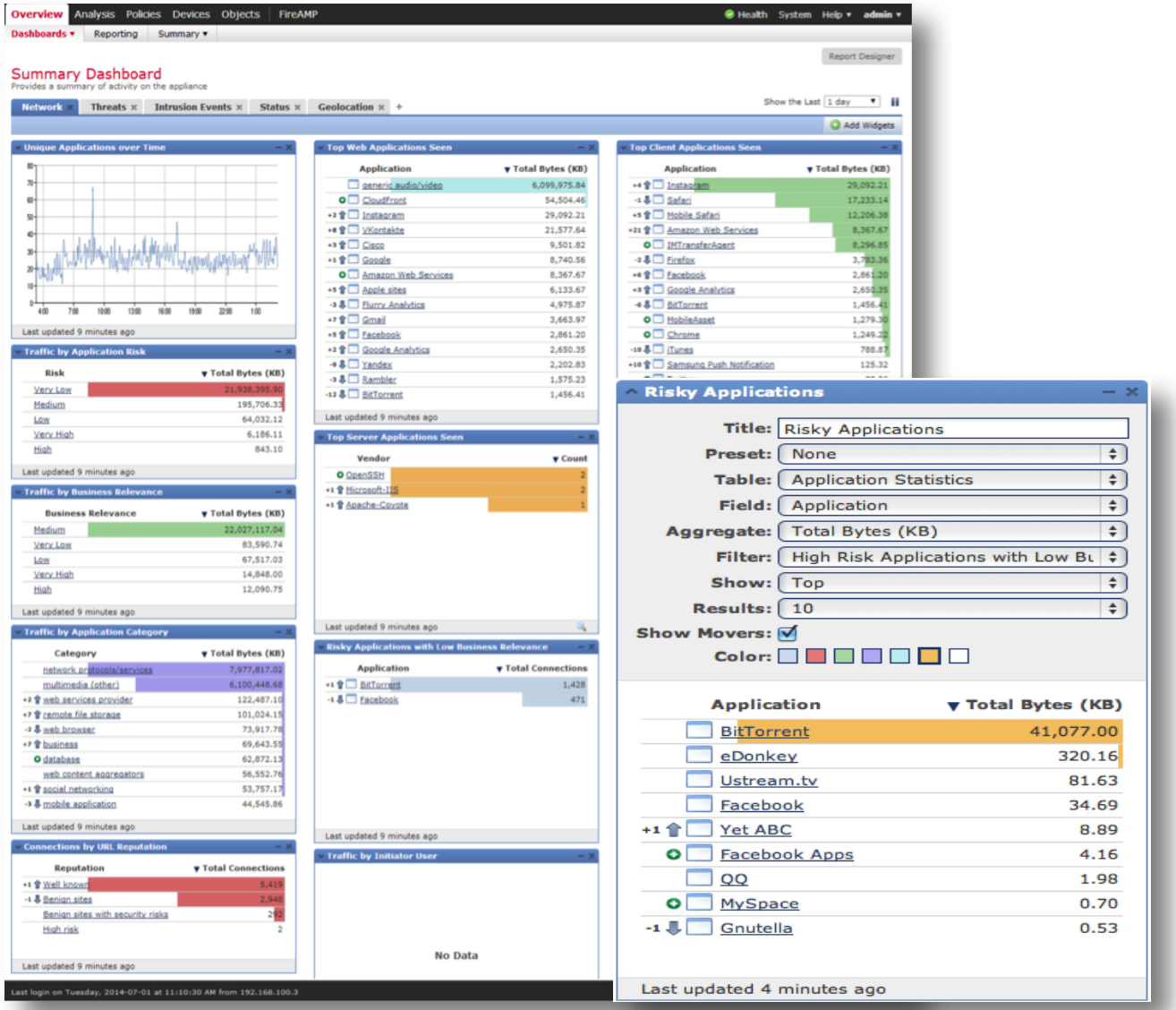
Мониторинг общей информации о сети

- Корреляция событий безопасности, трафика и вредоносного кода
- Активность конкретных пользователей и их приложений
- Используемые ОС и активность сетевого обмена
- Оценка событий по уровню воздействия и приоритета
- Статистика по вредоносному коду и зараженным файлам
- Геолокационные данные
- Категории сайтов и посещаемые URL



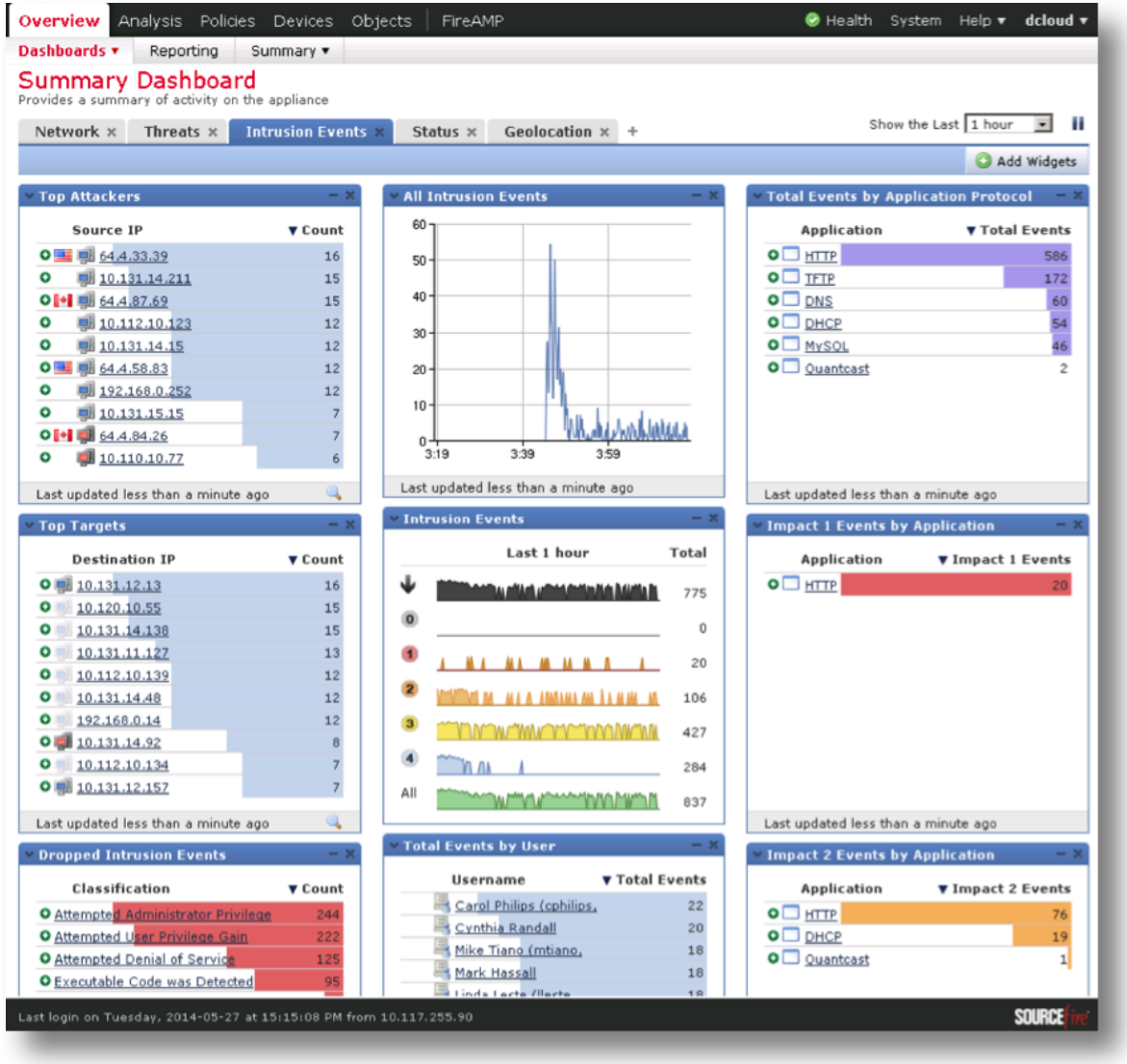
Мониторинг сетевых событий

- Использование сервисов
- Использование приложений
- Использование операционных систем
- Распределение соединений
- Активность пользователей
- Уязвимые узлы и приложения
- И т.д.



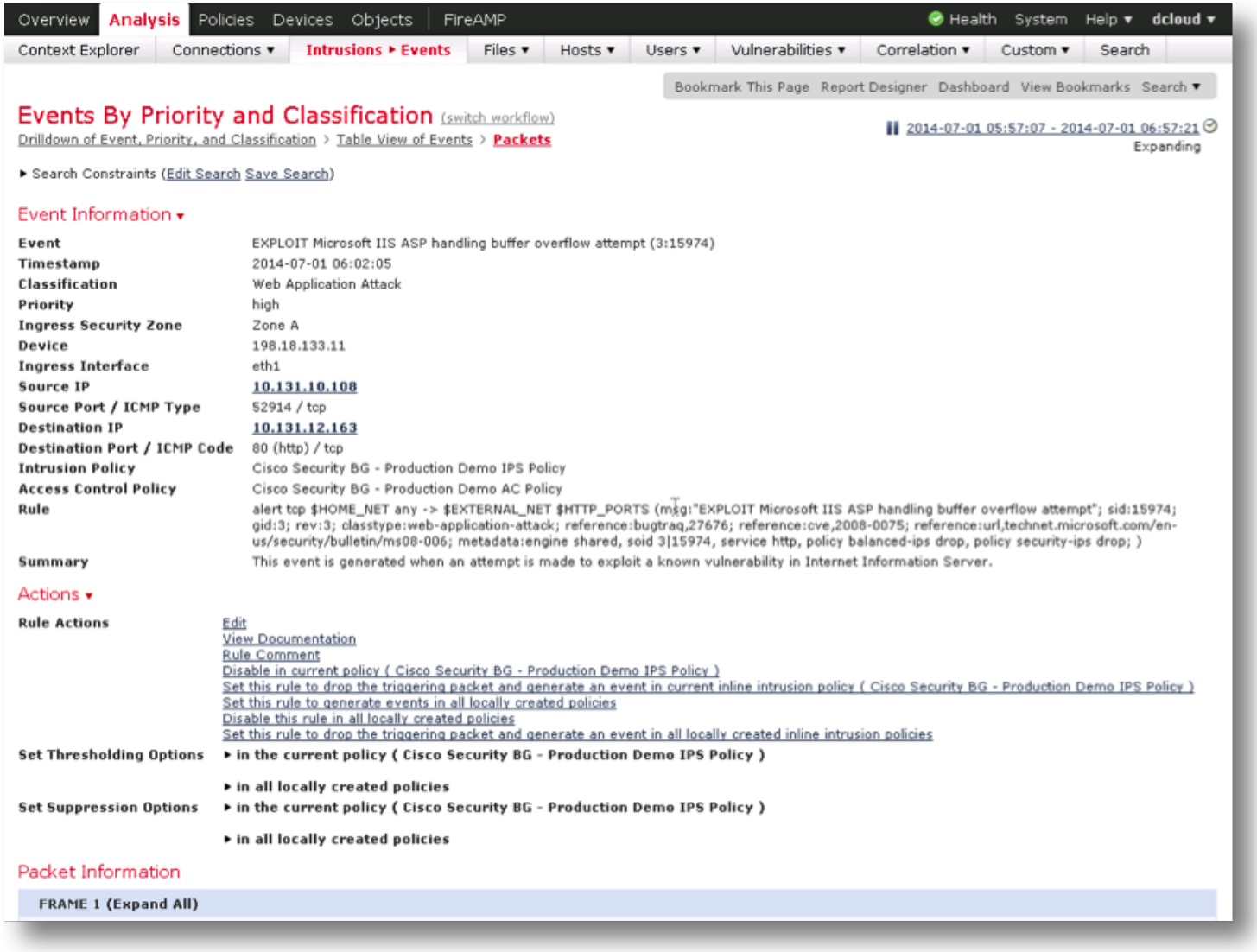
Мониторинг событий безопасности

- Основные нарушители
- Основные атаки
- Заблокированные атаки
- Основные цели
- Приоритет событий
- Уровень воздействия



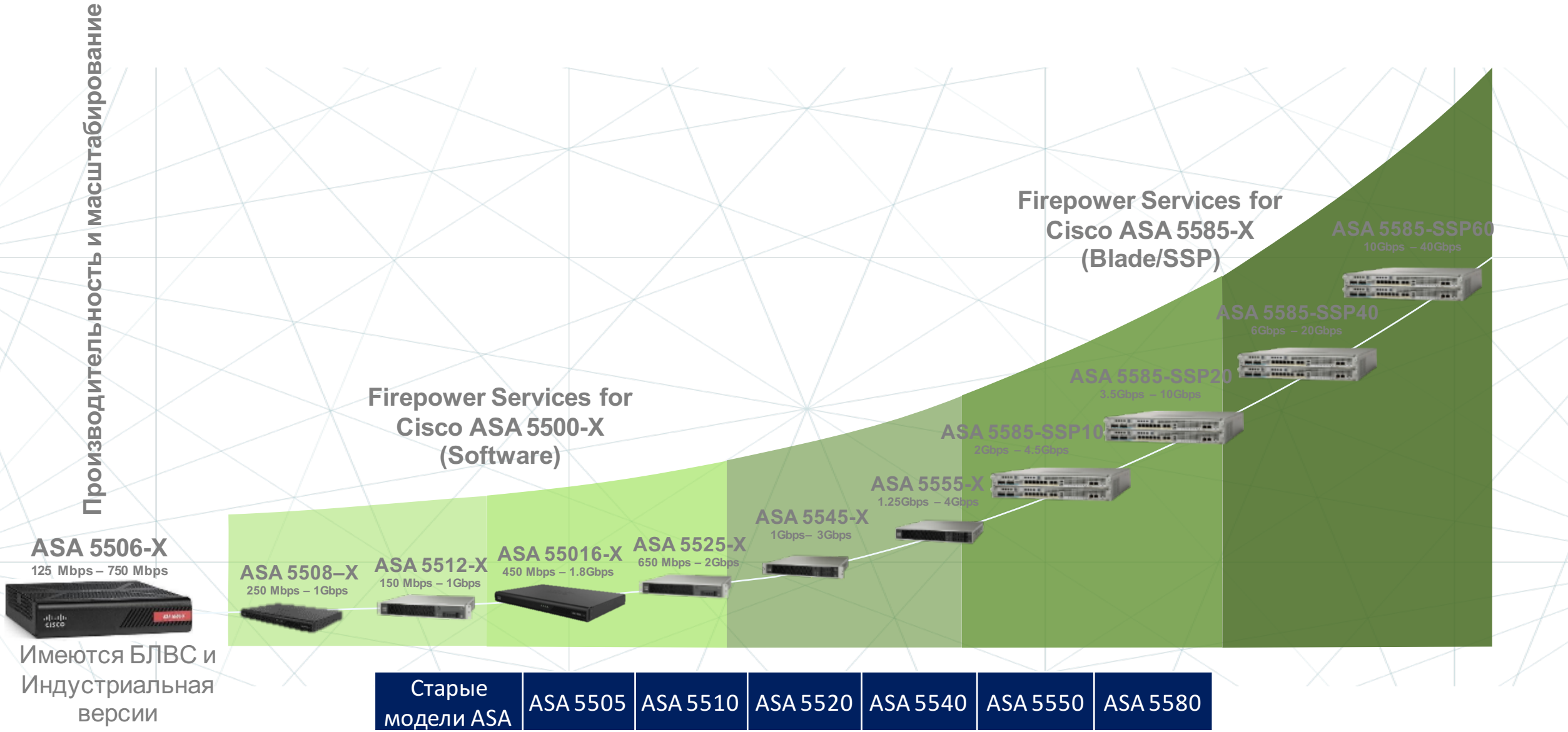
Детализация событий безопасности

- Подробная информация о событии безопасности
- Возможность изменения правил реагирования
- Возможность тюнинга правила / сигнатуры
- Сетевой дамп



Платформы

ASA Продуктовое портфолио



Новые модели Cisco ASA with FirePOWER Services

5506-X	5506W-X	5508-X 5516-X	5506H-X
Desktop Model	Integrated Wireless AP	Выше производительность	Для АСУ ТП
100% NGFW - поставляется с AVC	Wi-Fi может управляться локально или через Cisco WLC	1RU; новая платформа – лучшее сочетание цены и производительности	NGFW для критичных инфраструктур и объектов

Идеальна для замены Cisco® ASA 5505

Cisco ASA 5506H-X в защищенном исполнении

*** Конфигурация Cisco® ASA 5506-H идентична Desktop ASA 5506-X, исключая следующие параметры:

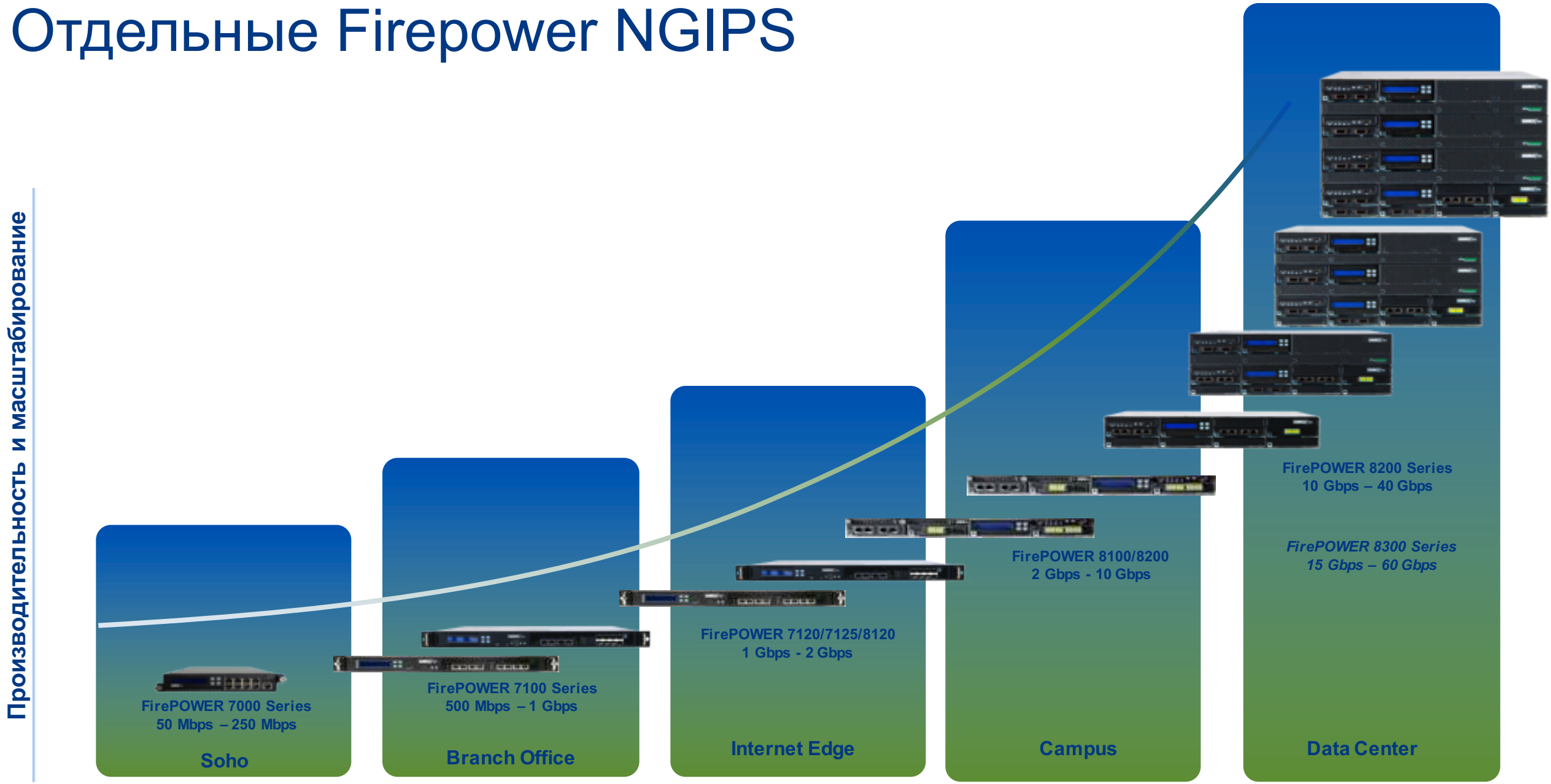
Параметр	Значение
Порты	4 x портов данных
Управление	1 порт, 10/100/1000BASE-T, 100BASE-FX, 1000BASE-X, SFP
Напряжение	5V (*** 5506 is 12V)
Диапазон температур	От –20 до 60°C (рабочий) От -40 до 85°C (обычный)
Монтаж	Wall-Mount, Horizontal Desk, Rack-Mount и DIN rail-mount

9 x 9.2 x 2.5 in.

Промышленный МСЭ/IDS Cisco ISA 3000

- Производительность: 2 Gbps
- Кол-во IPSec/SSL VPN: 25
- IPv4 MAC Security ACE: 1000
- Кол-во интерфейсов: 4x1GE или 2xGE, 2xFiber (SFP)
  - Медный: 4x10/100/1000BaseT
  - Оптический: 2x1GbE (SFP), 2x10/100/1000BaseT
- 4 ядра Intel Rangely, SSD 64 GB
- 8 GB DRAM, 16 GB Flash
- Питание DC
- Исполнение: -40C до 60C без обдува; -40C до 70C с 40LFM; -34C до 74C с 200LFM

Отдельные Firepower NGIPS



FirePower 8200 & 8300 Series

8250
10 Gbps
8350
15 Gbps

8260
20 Gbps
8360
30 Gbps

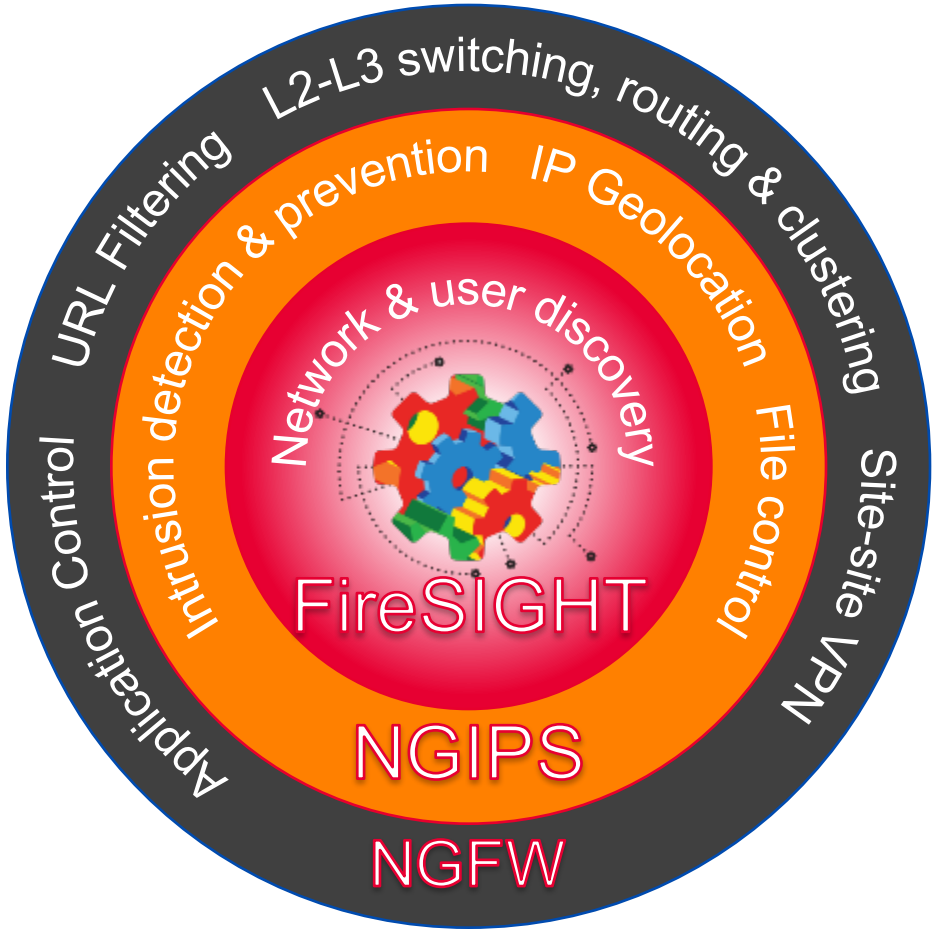
8270
30 Gbps
8370
45 Gbps

8290
40Gbps
8390
60 Gbps

- Обычно используется в ЦОД
- Стекируемая конфигурация
- Возможность расти с увеличением потребностей
- Каждая серия стекируется только с такой же моделью

FirePower Management Centre (FireSight)

- Контекст и пользователи коррелируются MC
- Контроль доступа осуществляется встроенным NGIPS
- Приложения и их контроль доступа, свичинг и роутинг осуществляется NGFW



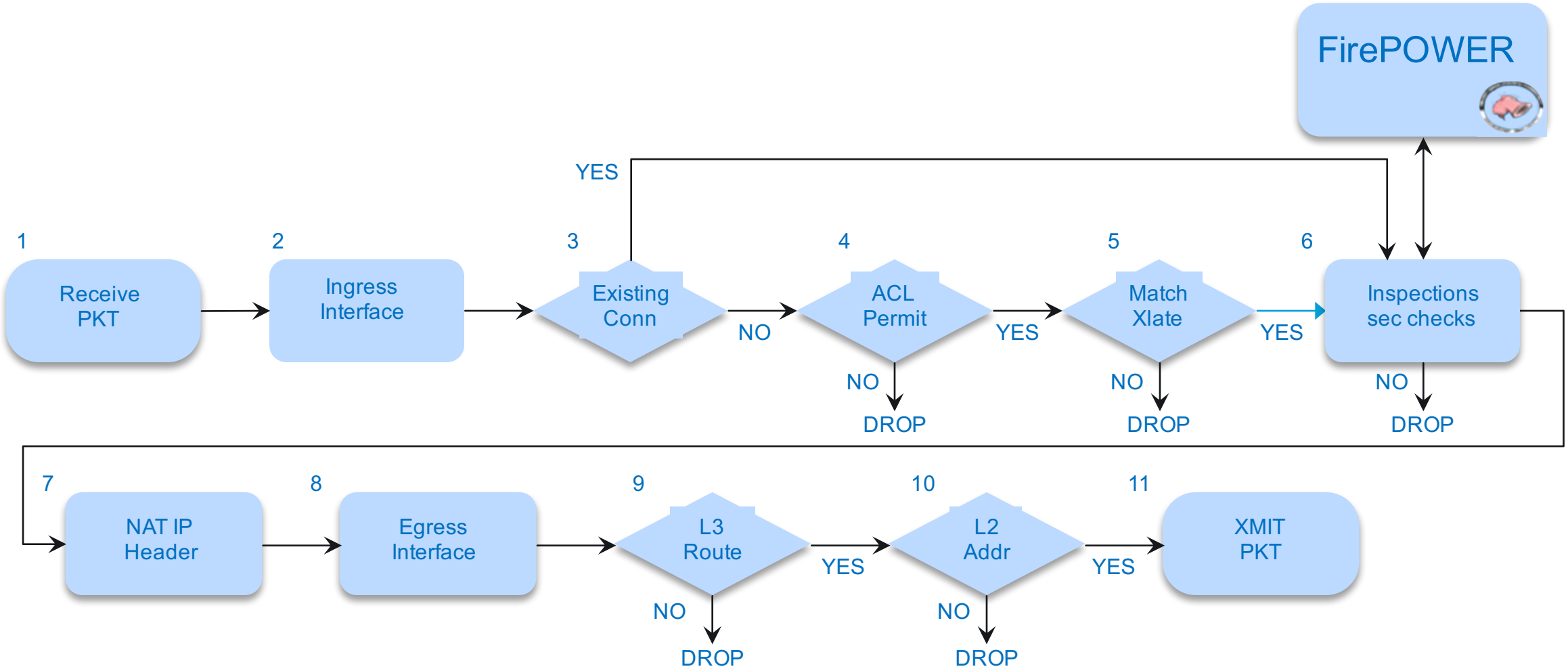
Cisco FirePower Management Center Models

Feature	FireSIGHT FS750	FireSIGHT FS1500	FireSIGHT FS2000	FireSIGHT FS3500	FireSIGHT FS4000	FireSIGHT FS-VMW-SW
Maximum number of sensors managed	10	35	70	150	300	25 10 2
Maximum number of IPS events	20 million	30 million	60 million	150 million	300 million	10 million
Event storage	100 GB	125 GB	1.8TB	400 GB	4.8 TB	250 GB
Maximum network map (hosts/users)	2,000/2,000	50,000/50,000	150,000/150,000	300,000/300,000	600,000/600,000	50,000/50,000
Maximum flow rate (flows per second)	2,000 fps	6,000 fps	12,000 fps	10,000 fps	20,000 fps	Varies*
Network Interfaces	2 x 1Gbps	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (Optional SFP's available via CCW)	2 x 1Gbps	2 x 1Gbps 2 x 10Gbps (Optional SFP's available via CCW	1 x 1Gbps
High availability	Lights-out management (LOM)	RAID 1, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	RAID 5, LOM, high-availability pairing	No

For ASA FP or Virtulal FP only

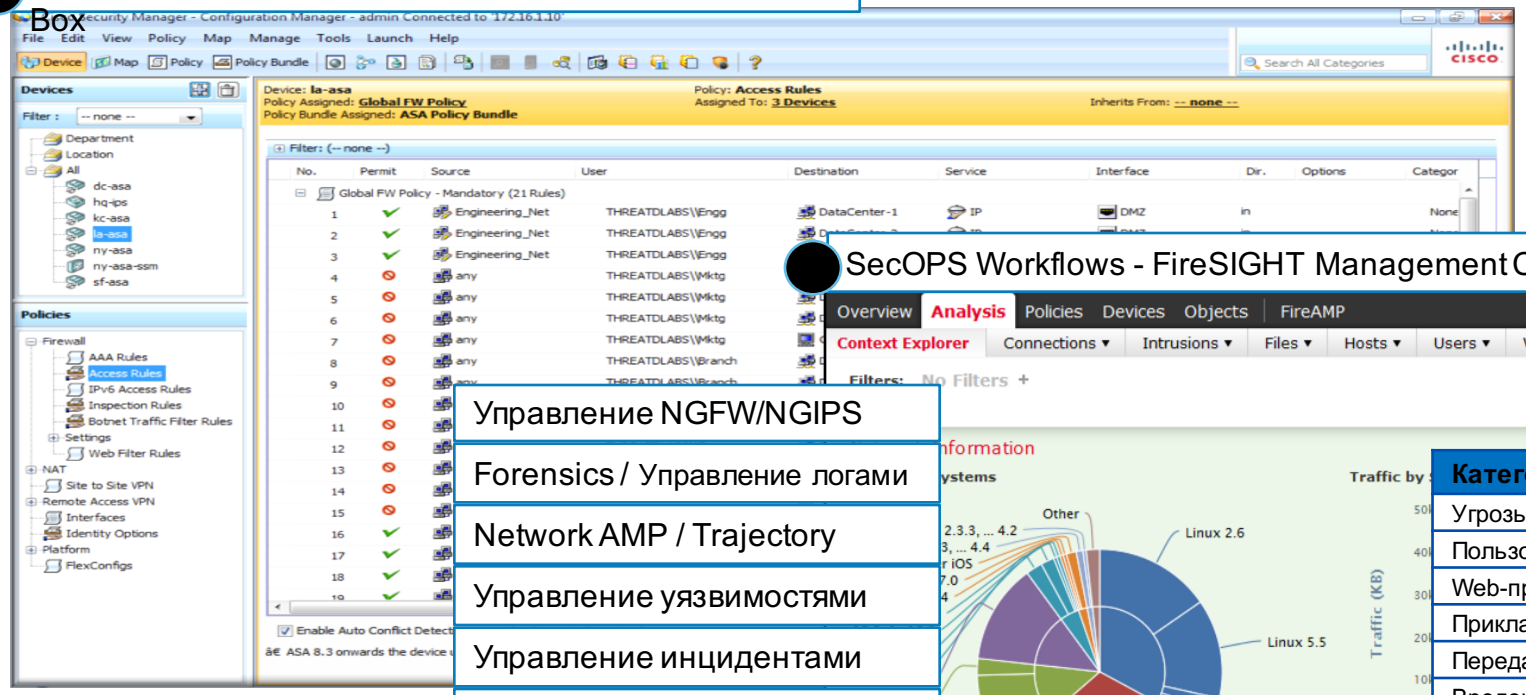
Развитие NGFW

ASA FirePower. Алгоритм обработки пакетов



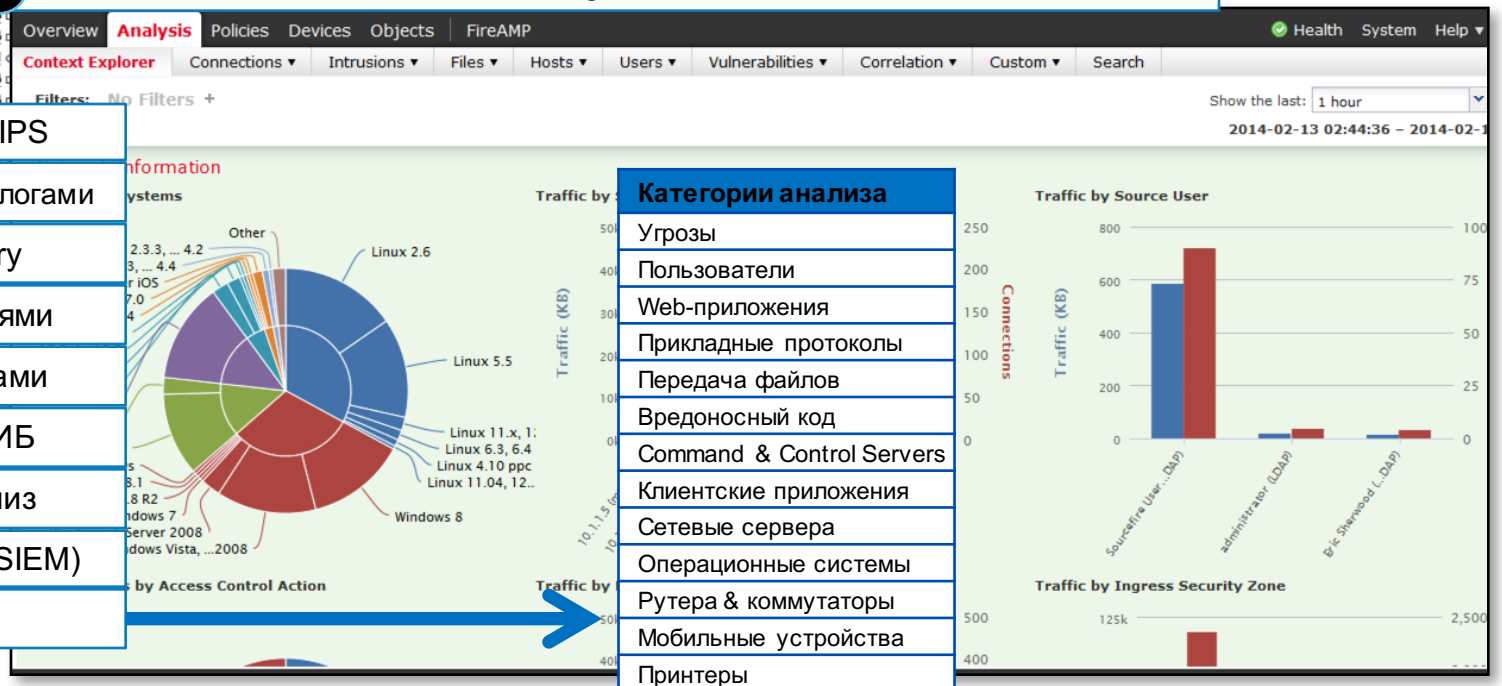
Управление ASA FirePower требует наличия двух систем!

- NetOPS Workflows - CSM 4.6/7 или ASDM-ASA-On-Box



FireAMP Connector
(Managed by FMC)

- SecOPS Workflows - FireSIGHT Management Center



- Управление NGFW/NGIPS
- Forensics / Управление логами
- Network AMP / Trajectory
- Управление уязвимостями
- Управление инцидентами
- Адаптивная политика ИБ
- Ретроспективный анализ
- Корреляция событий (SIEM)
- Распознавание

Категории анализа
Угрозы
Пользователи
Web-приложения
Прикладные протоколы
Передача файлов
Вредоносный код
Command & Control Servers
Клиентские приложения
Сетевые сервера
Операционные системы
Рутера & коммутаторы
Мобильные устройства
Принтеры
VoIP-телефоны
Виртуальные машины

Недостатки платформы

Для ASA FirePower

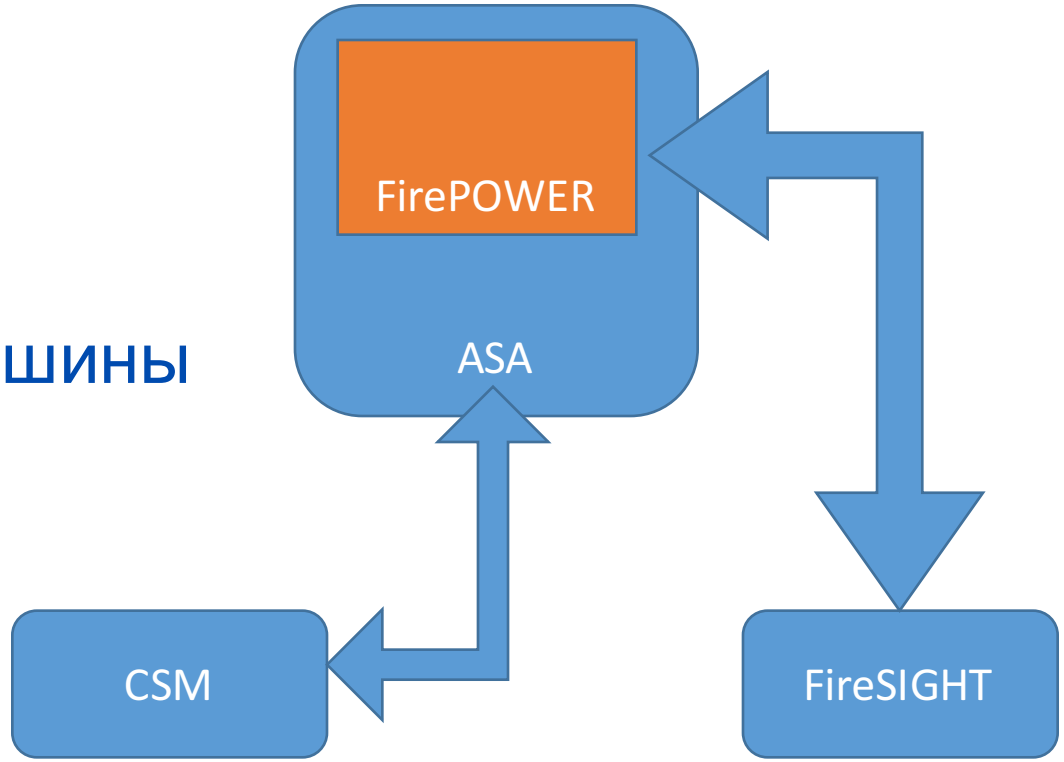
Разворачиваются два образа

Работают две OS

Пакеты проходят через виртуальные машины

Дублируется функционал

2 интерфейса управления

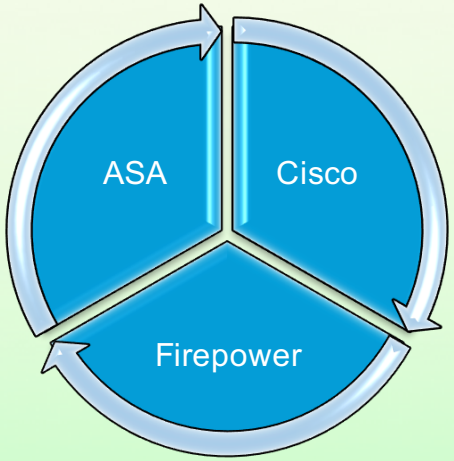


Развитие нашей стратегии безопасности

Унифицированное ПО

Routing, NAT, Identity, Firewall, Clustering / HA

Service Chaining & Orchestration

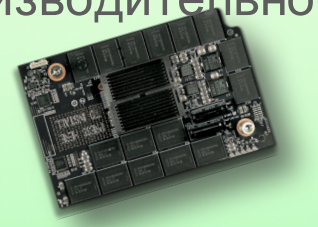


Threat prevention, advanced malware, and application visibility and control

Унифицированные устройства

Использование архитектуры Cisco

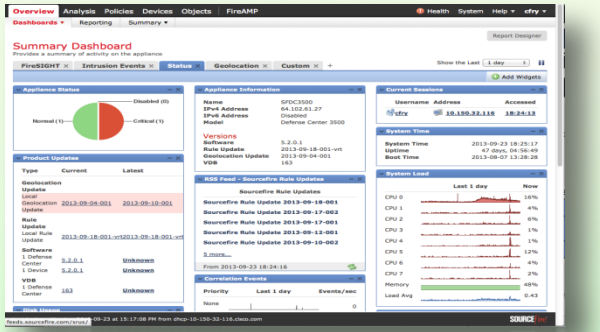
Ускорение для максимальной производительности



До мульти-100Гбит портов

Унифицированное управление

FireSIGHT UI C объединенным управлением



Firepower Threat Defense

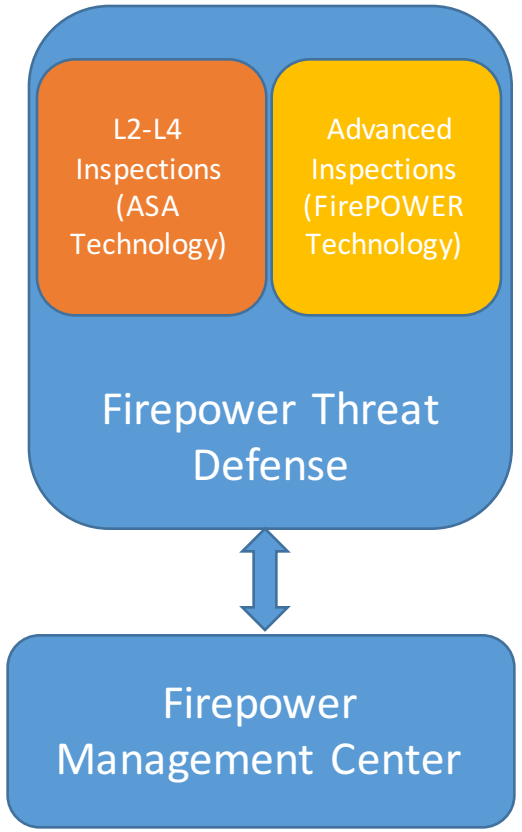
Новое предложение NGFW

Объединяет все лучшее от ASA и от FirePower

однопроходная инспекция

Не дублируется функционал*

Один интерфейс управления



Новые возможности в Firepower Threat Defense 6.0

Threat Innovation

DNS Inspection and Sinkholing

URL-based Security Intelligence

SSL Decryption

OpenAppID

Captive Portal and Active Auth

File Property Analysis and Local Malware Checks

ISE Identity/Device/SGT in Policy

Enterprise Management

Domains with Role-Based Access

Policy Inheritance

Firepower Threat Defense Image

Unified ASA and Firepower Rules and Objects

ASA Dynamic and Static NAT

ASA Routing Support: OSPF (not OSPFv3), BGP4, RIP, Static (not Multicast)

Syn Cookies, Anti-Spoofing

ASA ALGs (fixed configuration)

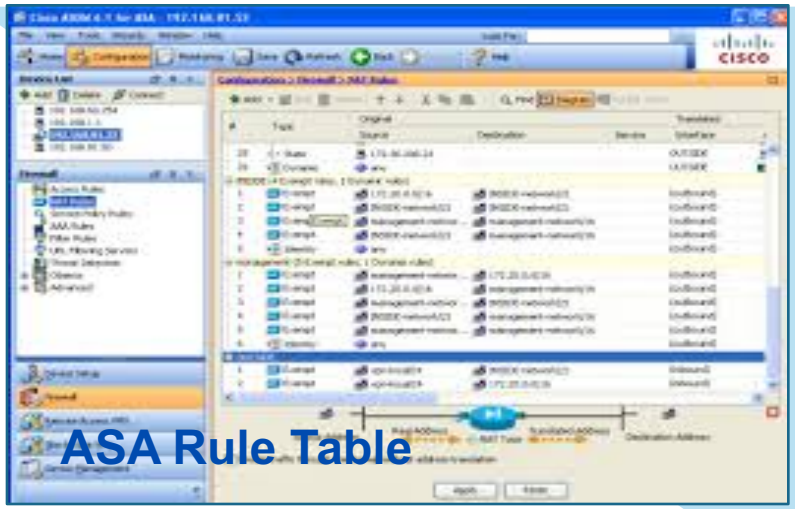
VMware and AWS Support

Smart Licensing Support

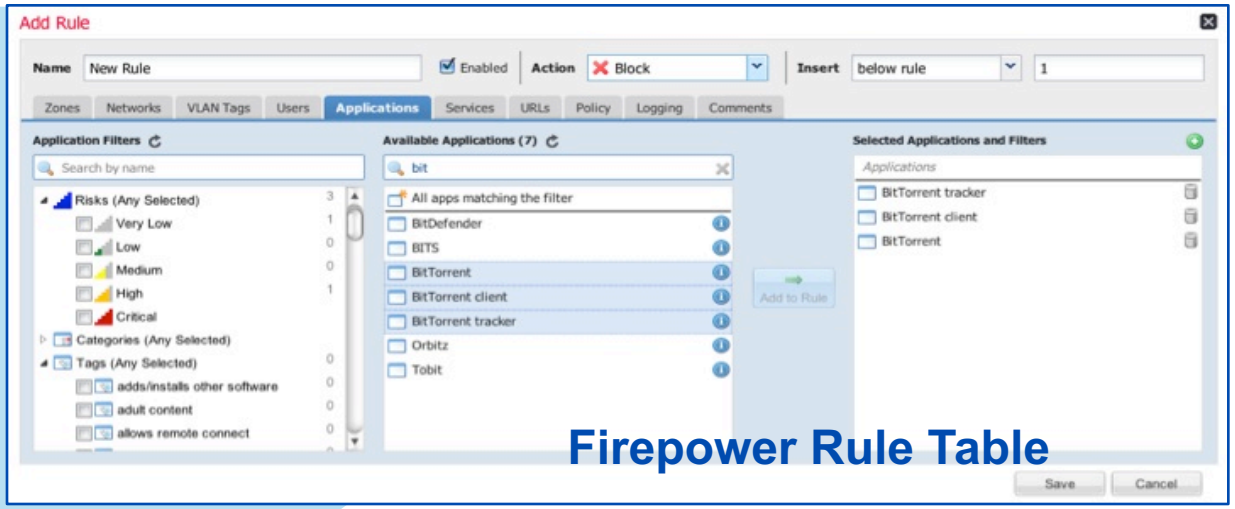
Общее для всех платформ FirePower

Только в FIREPOWER THREAT DEFENSE

Таблица правил с одной политикой (Firepower Threat Defense)



ASA Rule Table



Firepower Rule Table

One Rule Table

gence | HTTP Responses | Advanced

Add Category | Add Rule | Search Rules

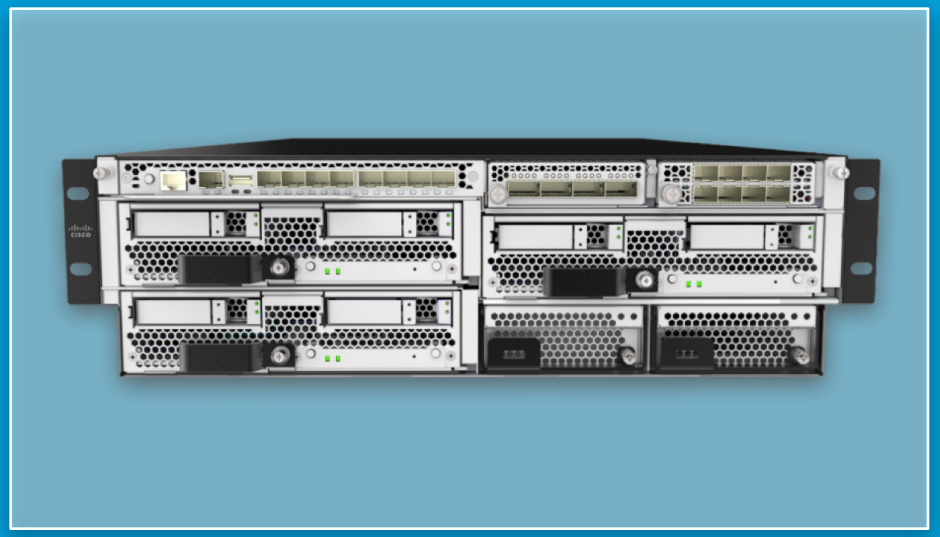
#	Name	Source Zones	Dest Zones	Source Networks	Dest Networks	VLAN Tags	Users	Applications	Src Ports	Dest Ports	URLs	Action					
Mandatory - acl (1-5)																	
1	test-rule	any	any	1.1.1.1 2.2.2.2	1.1.1.1 2.2.2.2	any	any	any	any	HTTPS	any	Block				0	
2	r2	any	any	IPv4-Private-1	any	any	any	any	any	any	any	Block				0	

Unified Policy and Objects

Сравнение функционала

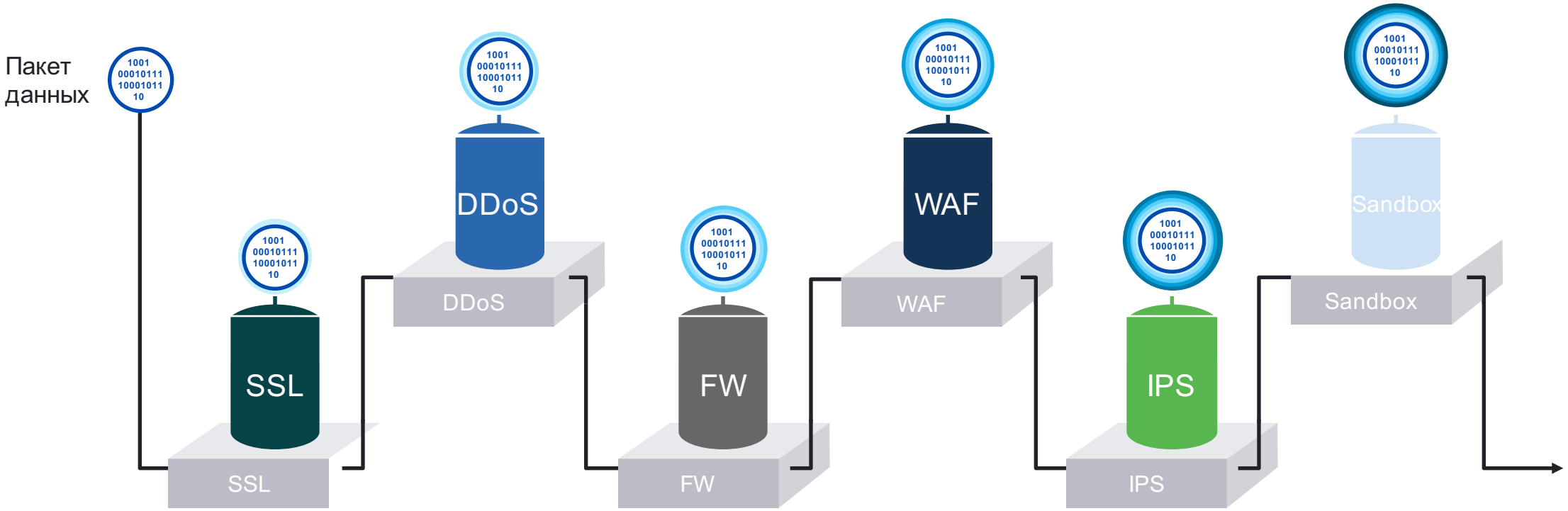
ASA with FirePOWER Services	Firepower Threat Defense
ALL ASA functionality, including: • Access Rules / Objects • Active/Passive HA & Clustering • Transparent & Routed Deployment • NAT (Dynamic & Static) • Unicast & Multicast Routing • Syn Cookies / Anti-Spoofing • Configurable ALGs • Site-to-Site & RA VPN • Multi-contexts	**Phase 1 of ASA functionality (at GA):** • ASA + Firepower Rules / Objects • Active/Passive HA • Transparent & Routed Deployment • NAT (Dynamic & Static) • Unicast Routing (OSPF, BGP, RIP, Static) • Syn Cookies / Anti-Spoofing • ALGs (fixed configuration)
ALL Firepower Functionality: • User / Host / App Visibility and Control • Security Intelligence: DNS/URL/IP • Malware file lookup / dynamic analysis / IOC • URL Category and Reputation Filtering • NGIPS	**ALL Firepower Functionality:** • User / Host / App Visibility and Control • Security Intelligence: DNS/URL/IP • Malware file lookup / dynamic analysis / IOC • URL Category and Reputation Filtering • NGIPS
Management: • Firepower Management Center for Firepower Services • Central Manager GUI & Full Config CLI • CSM / ADSM / CLI for ASA functions	**Management:** • Firepower Management Center - Unified Manager for all functionality

Примечание: список не полный, функциональность быстро расширяется



Высокопроизводительная безопасность

Устаревшая модель безопасности



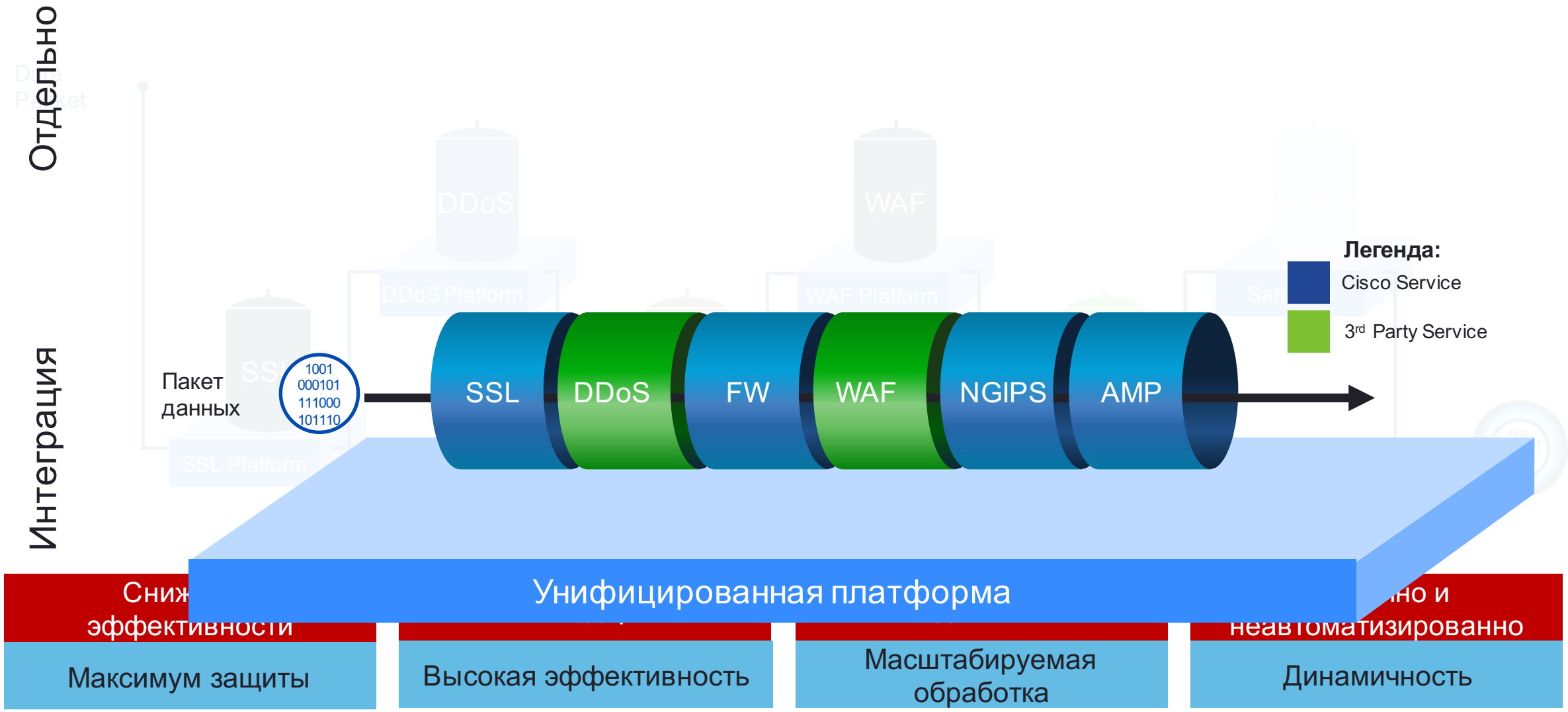
Снижение эффективности

Рост задержек

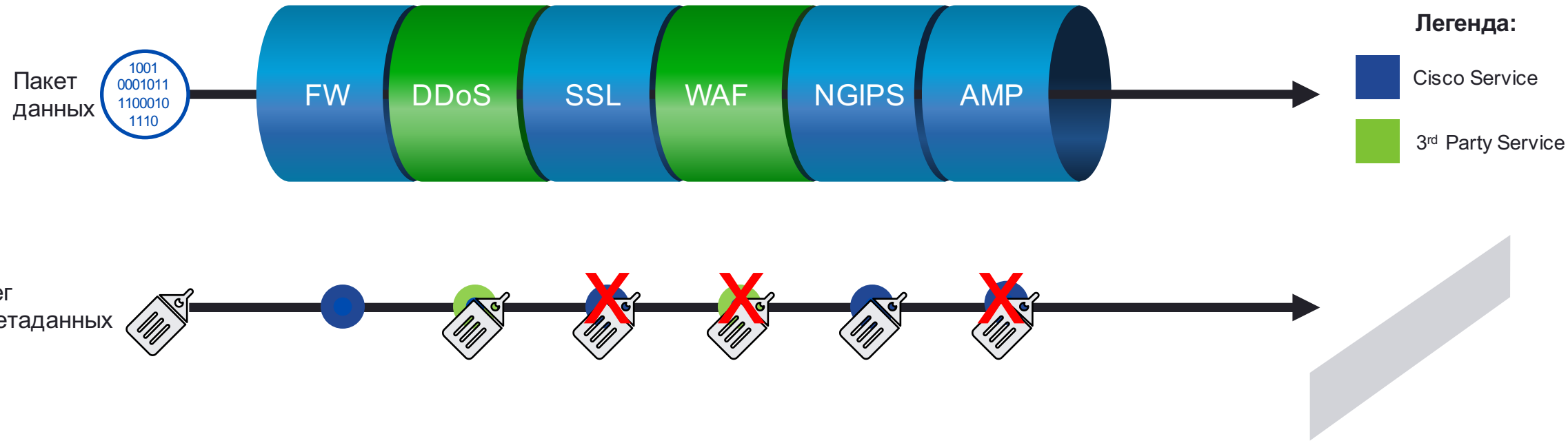
Замедление сети

Статично и неавтоматизированно

Cisco трансформирует интеграцию сервисов ИБ



Что впереди: интеллектуальная обработка



Теги определяют необходимость повторной инспекции или нет

Автоматизация разбора трафика в зависимости от задачи

Оптимизация безопасности через интеллектуальную сборку сервисов

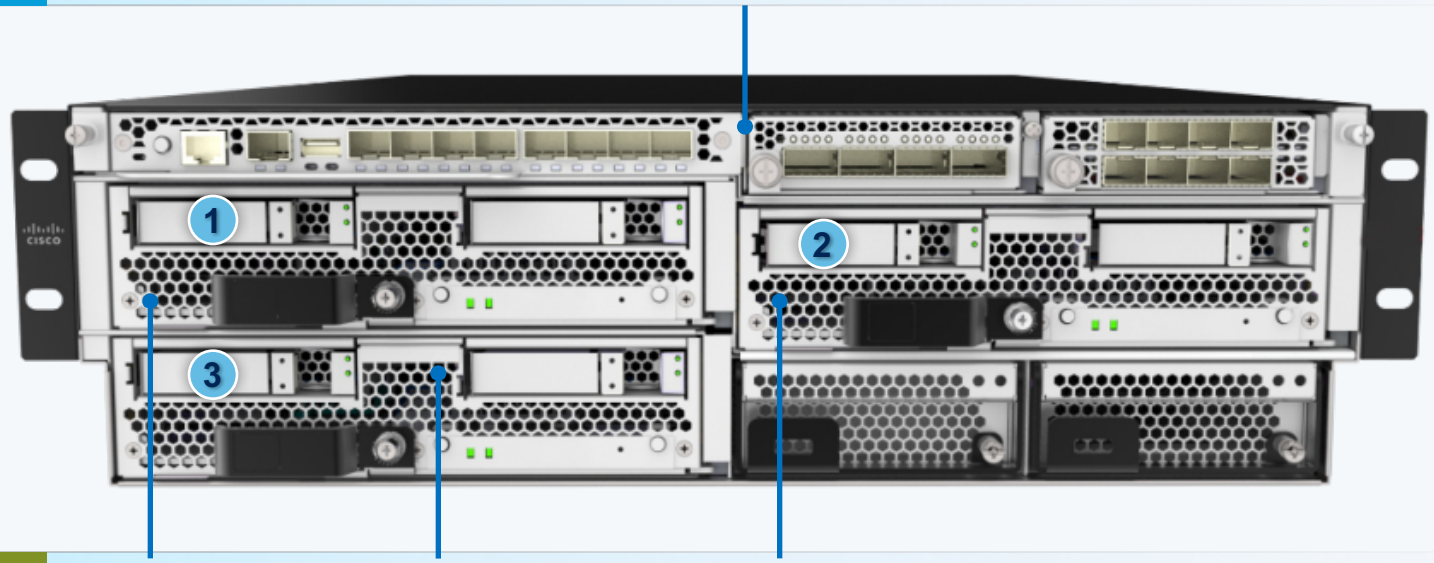
Платформа Firepower 9300

- Модульная платформа операторского класса с интерфейсами 10, 40, и 100 Гбит/с.
- Объединение сервисов безопасности компании Cisco и других компаний
- Эластичная масштабируемость за счет кластеризации
- Ускоренная обработка для доверенных приложений
- Функции ПО Cisco ASA для операторов связи
  - Эффективная защита на сетевом и транспортном уровне
  - Трансляция адресов операторского класса (Carrier-grade NAT)
  - Анализ протоколов GTPv1 и GTPv2 начиная с ASA 9.5(1)
  - Анализ SCTP и Diameter в планах

Обзор платформы Cisco Firepower 9300

Модуль управления

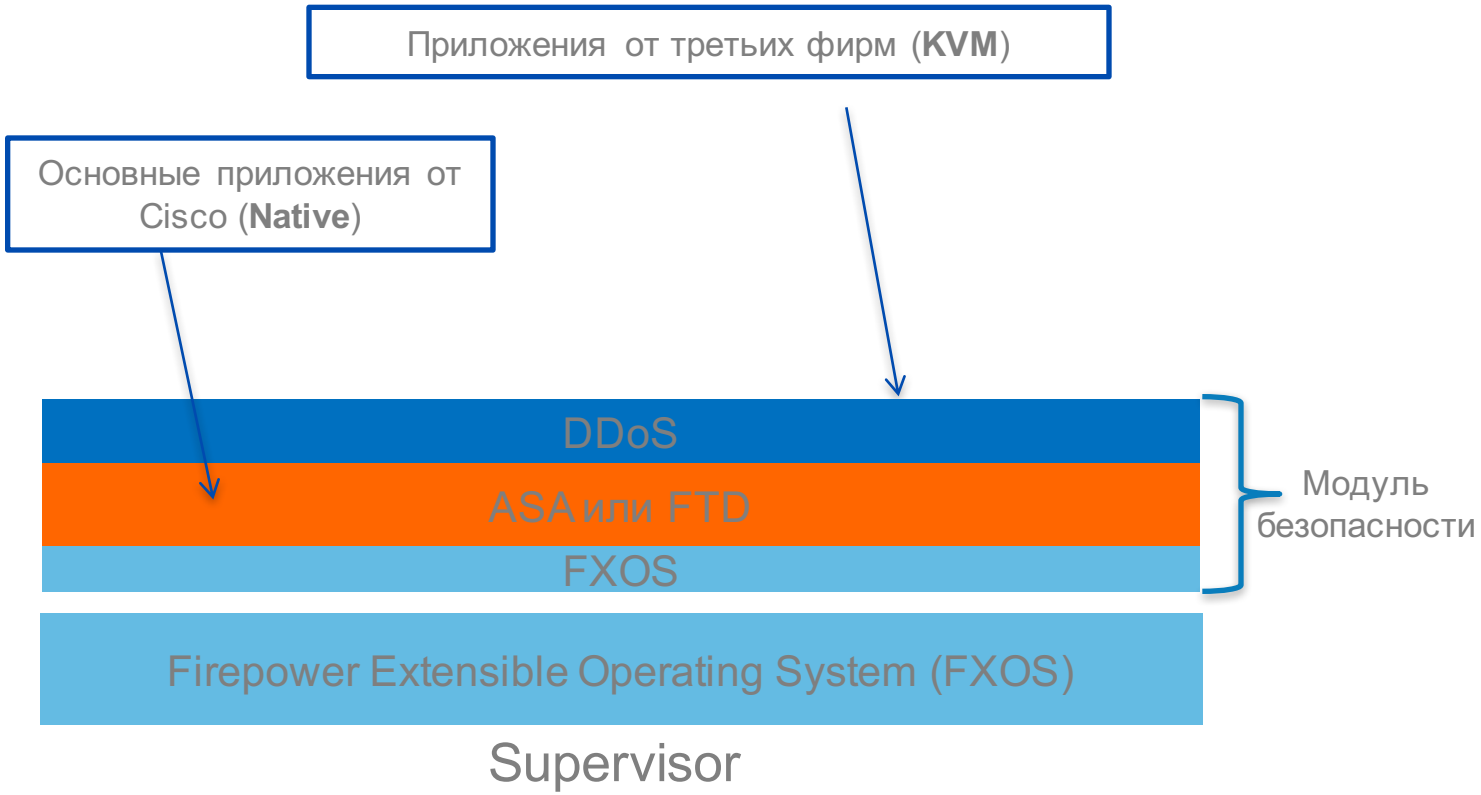
- Внедрение и управление приложениями
- Сетевые интерфейсы и распределение трафика
- Кластеризация для сервисов Cisco® ASA и прочих



Модули безопасности

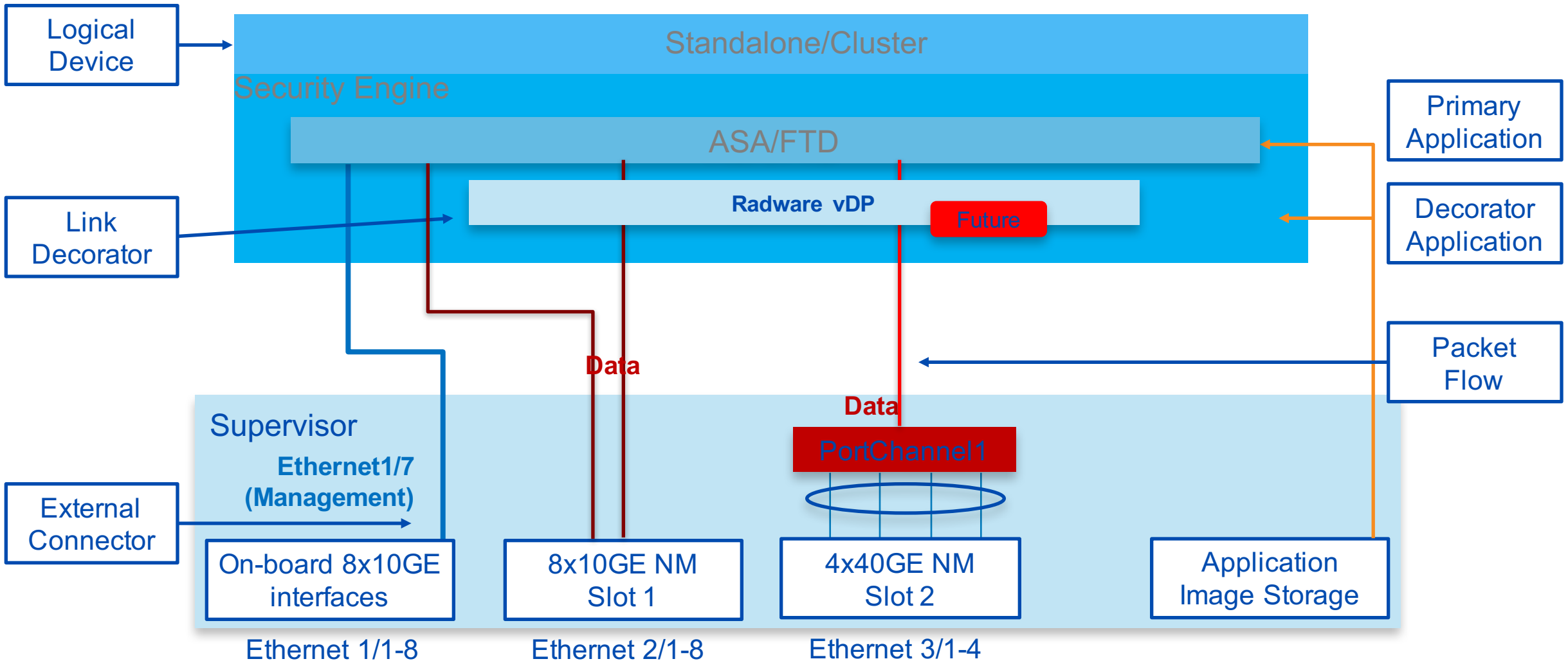
- Встроенный классификатор пакетов и потоков, а также ускоритель шифрования
- Приложения компании Cisco (МСЭ, СОВ, и т.п.) и 3-их компаний (защита от DDoS, балансировка)
- Работает отдельно или в кластере (до 240 Гбпс на шасси и более 1 Тбпс на кластер)

Программная архитектура



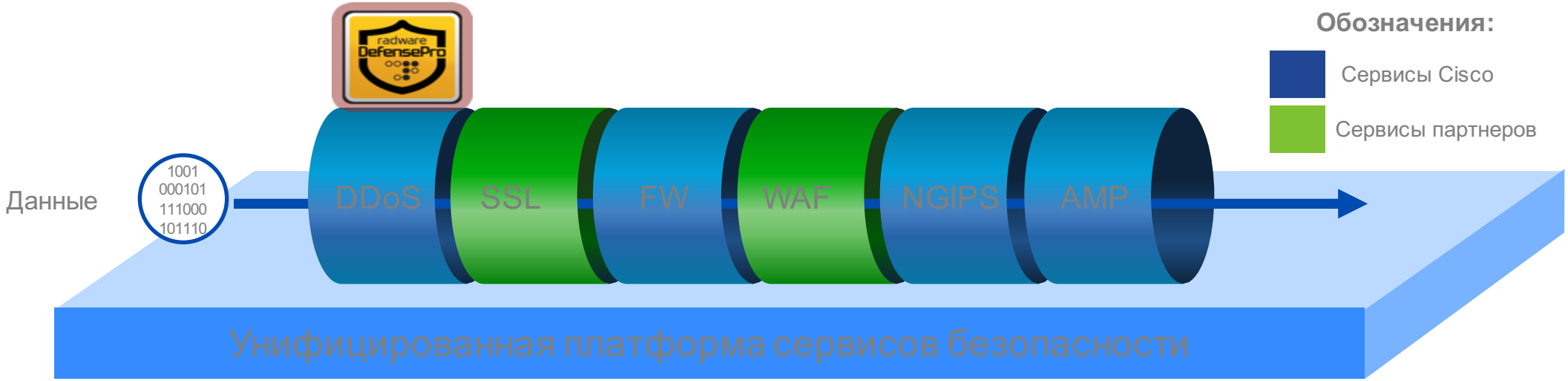
- FXOS обеспечивает интерфейс для управления устройство и его контроля для приложений безопасности на модулях безопасности
- Все имиджи подписаны и проверяются через Secure Boot
- Имиджи приложений безопасности в формате Cisco Secure Package (CSP)
  - Разные версии одних приложений могут быть сохранены на Supervisor. Они могут быть размещены на модулях безопасности по требованию
  - Содержит основные системы (например, ASA, FTD) и другие имиджи (например, ASDM, REST и др.)

Архитектура безопасности для новых платформ FirePower



Firepower 9300 изменяет модель интеграции сервисов

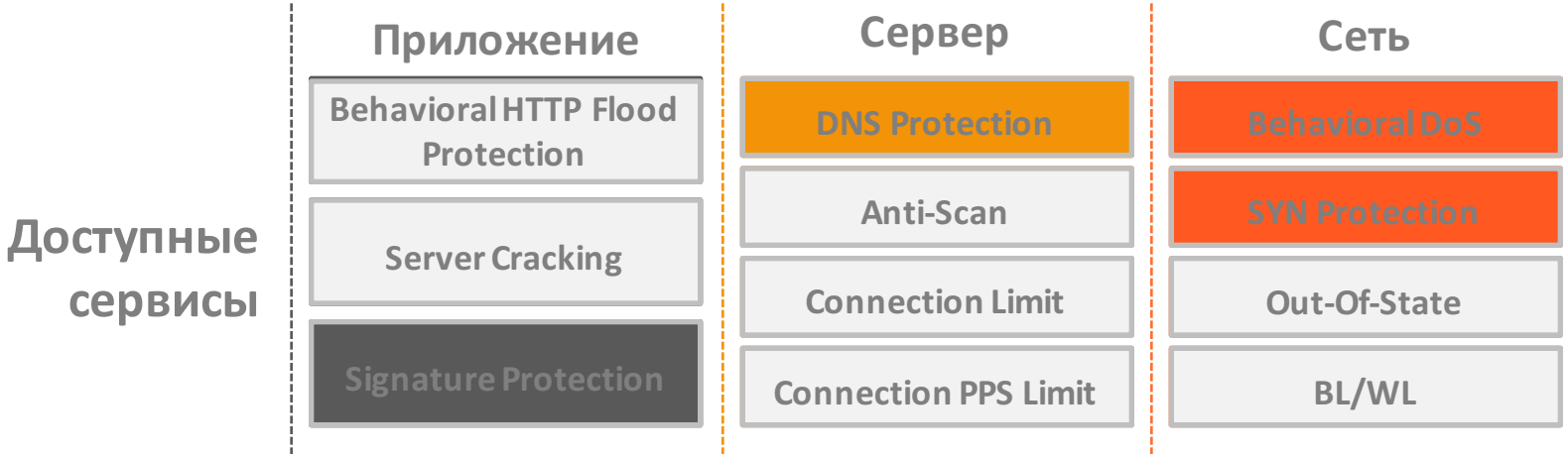
- Radware vDP – первое из приложений 3-х компаний, ставшее элементом новый архитектуры
- Защита от DDoS работает на входных интерфейсах Firepower 9300



Максимальная защита | Высокая эффективность | Масштабируемость | Гибкость

Обзор Radware vDefensePro

- Фокус на поведенческих DDoS-атаках, а не основанных на объеме

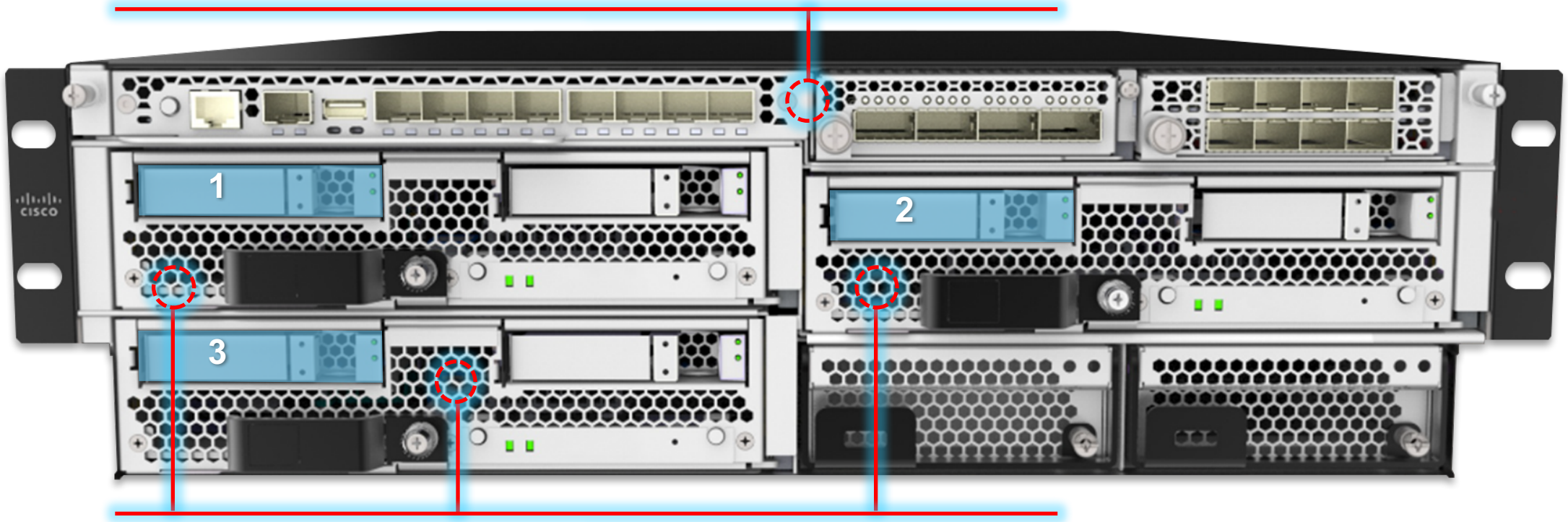


- До 10Gbps на модуль на 6 выделенных ядрах x86 CPU
- Внутришассийная кластеризация vDP позволяет обеспечить до 30Gbps на 3-х модулях

Обзор Firepower 9300

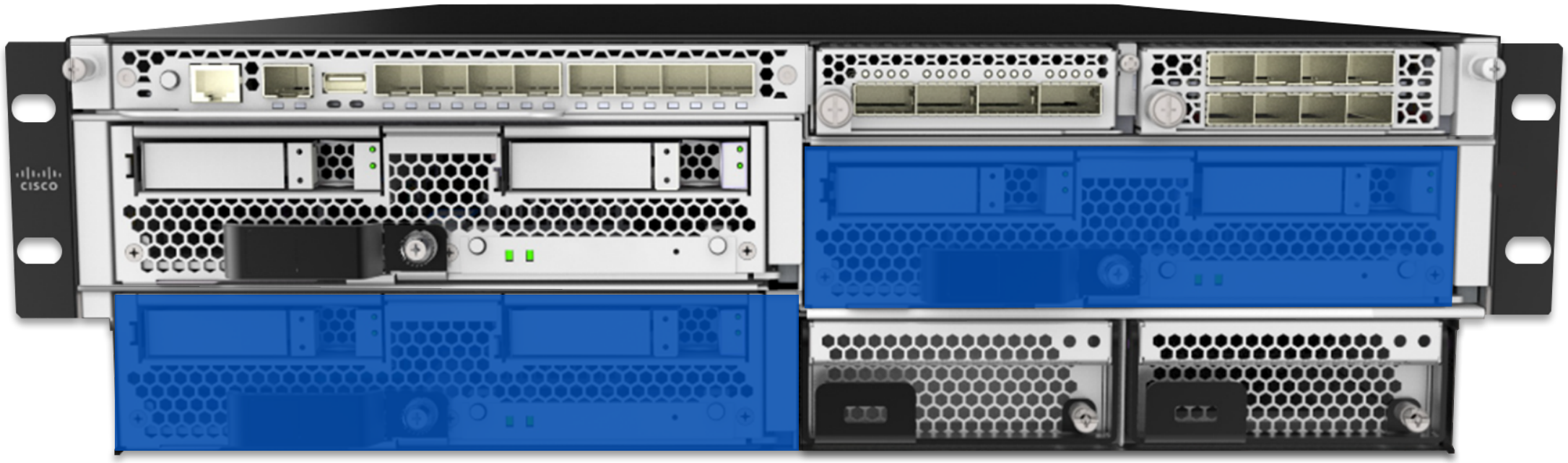
Supervisor

Внедрение и оркестрация защитных приложений
Управление сетевыми модулями (10GE/40GE) и движением трафика
Базовая кластеризация для ASA или Cisco NGFW

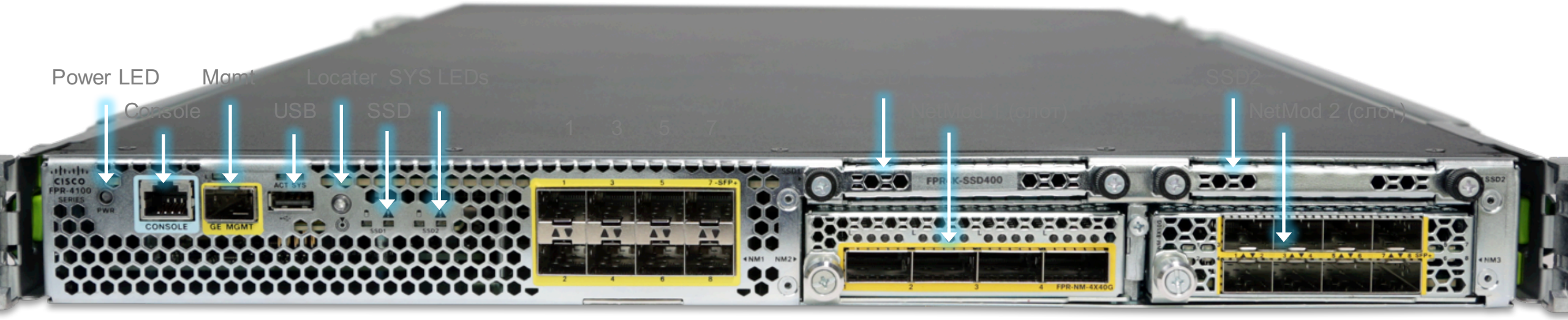


Модули безопасности

Встроенный классификатор пакетов/потоков (Smart NIC) и криптоакселератор
CPU с 24 или 36 физическими ядрами (48 или 72 с hyperthreading)
Стандартный или шасси (до 240Gbps) и на все кластер (1Tbps+)



И мы приходим к Firepower 4100 Series



Фиксированная конфигурация

- 8x SFP+ (10G) фиксированных портов
- Security Engine

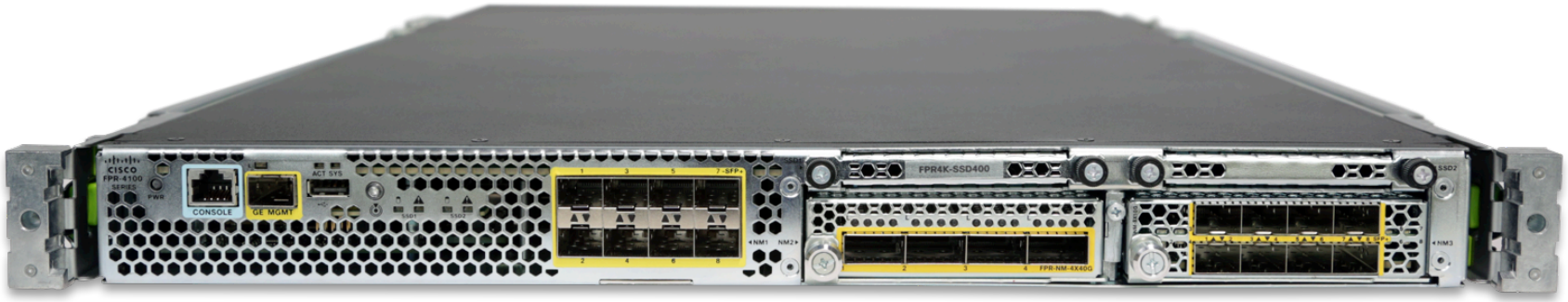
Модульная система

- 2x слота для сетевых модулей (NetMod)
- 2x слота для 2.5” SSD

Устройства Firepower 4100 Series

Разработан с использованием Security Services Platform (SSP)
- Инфраструктурная платформа для сервисов безопасности
- Интегрирует сервисы безопасности Cisco и сервисы ИБ третьих фирм
- Архитектура разработана для быстрого добавления новых сервисов по требованиям рынка

Разработан для:
- Периметра Интернет
- Периметра кампуса
- Периметра ЦОД



Аппаратная платформа для:
- Firepower NGFW
- Cisco AMP
- ASA

Firepower 4120/40/50 – аппаратные компоненты

Модуль Supervisor :

Консоль и порты управления

8 10G фиксированных Ethernet портов

2 x Network Modules (до 40 GE)

Модуль безопасности:

Два CPU, каждый подключен к **Smart NIC и** карте **Crypto accelerator**

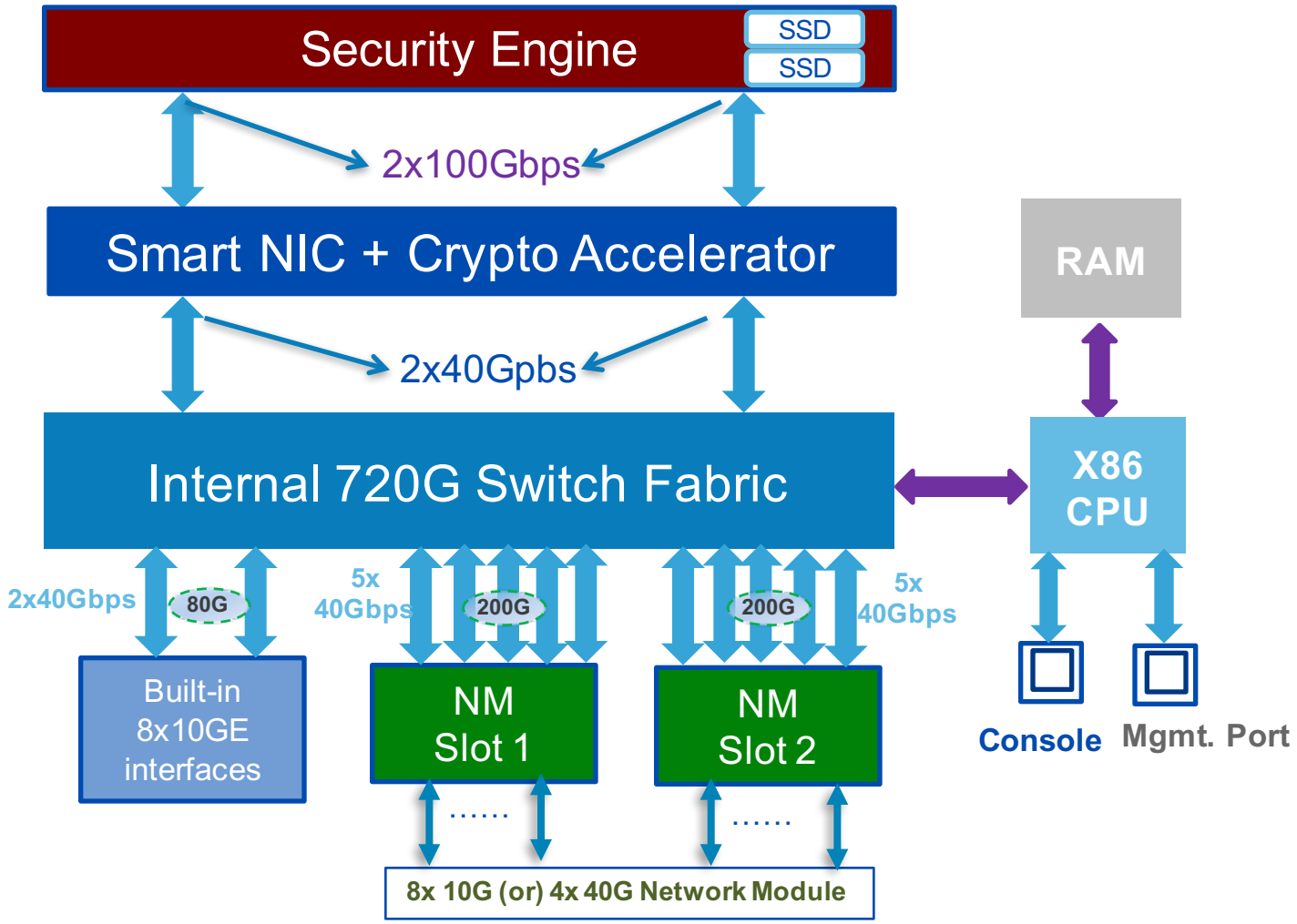
Два SSD - 1 основной + 1 дополнительный (для сервиса AMP)

Размер SSD

- 200GB для 4120
- 400GB для 4140

Backplane

80GB Backplane



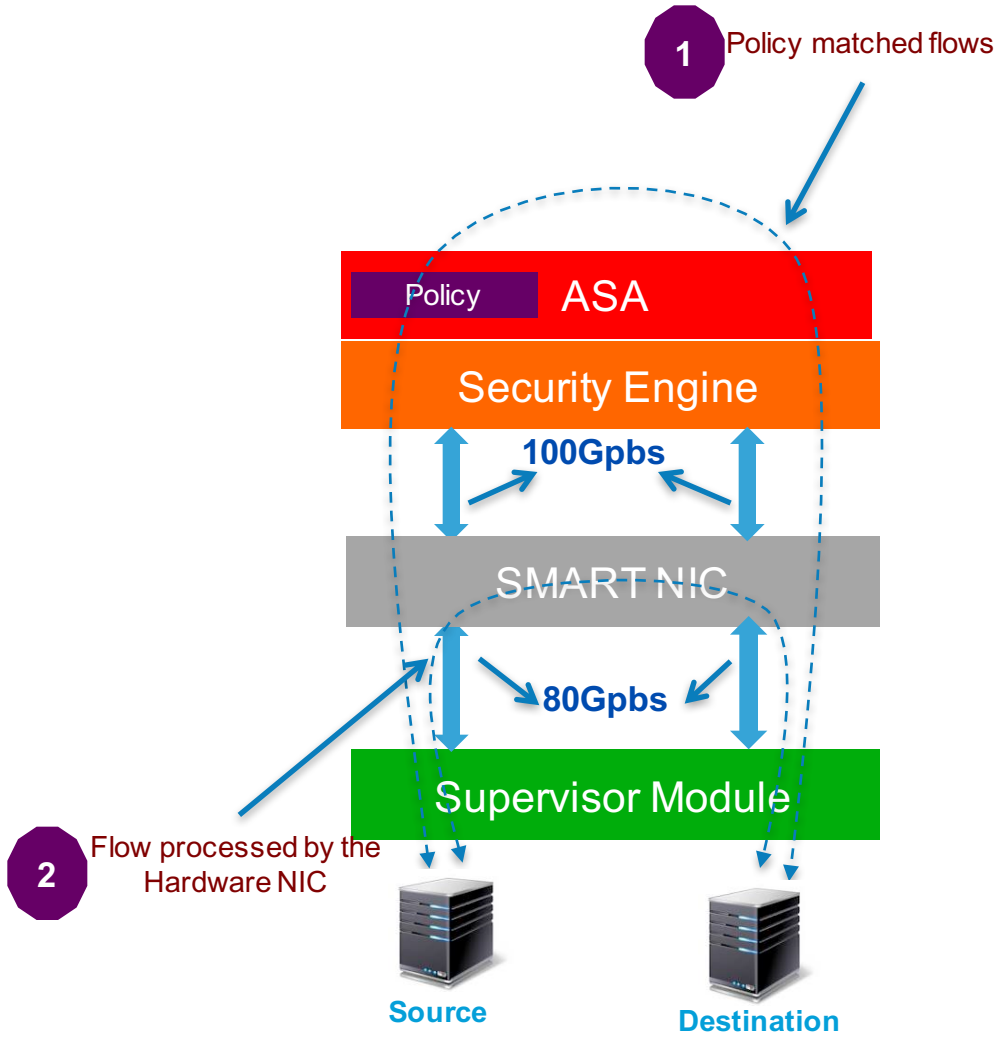
Операции разгрузки потоков

Обработка доверенных потоков на сверх высоких скоростях с помощью SMART NIC

- Аппаратная обработка без нагрузки x86
- 30-40 Гбит/с на один TCP/UDP поток , <5мкс задержка.

Использование:

- Потоковое медиа
- Высокопроизводительные вычисления
- Intra/Inter DC резервное копирование или синхронизация БД
- GRE туннелирование



От Cisco ASA к Cisco Firepower

Производительность и масштабируемость

FP 9300

FP 4100 Series

5585-X Series

ASA 5516-X

Предприятия & корпорации

ASA 5508-X

ASA 5506W
ASA 5506-X
ASA 5506H

SMB & филиалы

FTD производительность

	4110	4120	4140	SM-24	SM-36	SM-36x3
Max Throughput: Application Control (AVC)	12G	20G	25G	25G	35G	100G
Max Throughput: Application Control (AVC) and IPS	10G	15G	20G	20G	30G	90G
Sizing Throughput: AVC (450B)	4G	8G	10G	9G	12.5G	30G
Sizing Throughput: AVC+IPS (450B)	3G	5G	6G	6G	8G	20G
Maximum concurrent sessions w/AVC	4.5M	11M	14M	28M	29M	57M

ASA производительность

	4110	4120	4140	SM-24	SM-36	SM-36x3
Stateful inspection firewall throughput (maximum)	20G	40G	60G	75G	80G	225G
Stateful inspection firewall throughput (multiprotocol)	10G	20G	30G	50G	60G	100G
Concurrent firewall connections	10M	15M	25M	55M	60M	70M
New connections per second	150K	250K	350K	0.6M	0.9M	2M
Security contexts	250	250	250	250	250	250
Virtual Interfaces	1024	1024	1024	1024	1024	1024
IPSec 3DES/AES VPN Throughput	8G	10G	14G	15G	18G	18G

Платформы Cisco NGFW

New Appliances

Firepower 4100 Series and Firepower 9300	Firepower Services on ASA 5500-X	Firepower Services on ASA 5585-X

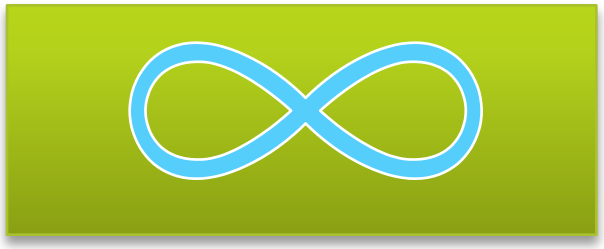
Все управляются с помощью FirePower Management Center

*5585-X management avail 2H ’16 (pre-commit date)

5 отличительных особенностей FirePOWER/AMP

1. Знаем КТО и ЧТО в сети
- Интеграция в Cisco ISE

2. Продвинутая система защиты от вирусов



3. Карта сети
- Видим приложения, уязвимости….

4. Автонастройка
- Проще внедрять и поддерживать

5. Open AppID
- Добавьте свое кастомное приложение

FirePOWER

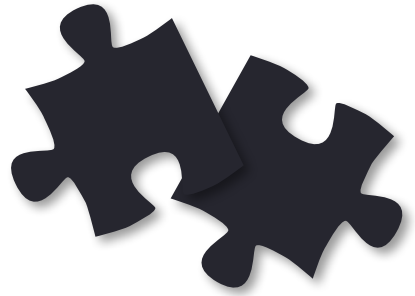
МСЭ нового поколения, смотрящий шире и глубже

Непревзойденная прозрачность

- Полная осведомленность о сетевом контексте для устранения уязвимостей

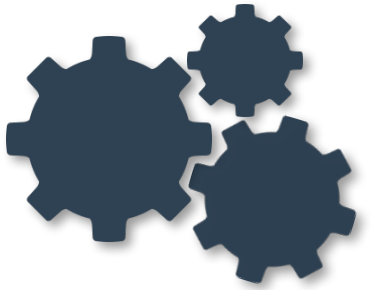
Комплексная защита от угроз

- Лучшая в своем классе многоуровневая защита в одном устройстве



Автоматизация

- Простота управления, динамическое реагирование и восстановление



Вопросы?

Thank you.