Cisco Sourcefire

Sandro Chachanidze

Обратите внимание на них…

Все были умными. У всех была безопасность.
И всех их серьезно взломали.

Так что же изменилось?

Хакерство изменилось.

Хакинг, 21st век
Цепочка атаки

Обследование — Обследование защиты жертвы

Разработка — Написание специализированного софта для конкретных условий жертвы

Тестирование — Проверяем и убеждаемся что Malware обходит защиту жертвы

Запуск — Размещение Malware. Распространение внутри, установление связей наружу

Завершение

Миссия: Извлечение данных, сбор доказательств, компрометация.

Что бы вы изменили, зная что Вас взломают?

IPS
Нового Поколения!

Что делает SourceFire NGFW уникальным?

- Контекст
- Скорость
- Точность
- Гибкость
- Значимость

Каким образом SourceFire обеспечивает непревзойденную безопасность

УПРАВЛЕНИЕ

FireSIGHT™

Центр управления

FireCLOUD™

COLLECTIVE SECURITY INTELLIGENCE

ДЕТЕКТИРОВАНИЕ И БЛОКИРОВКА

FirePOWER™

NGIPS | NGFW

IPSx | Virtual | SSL

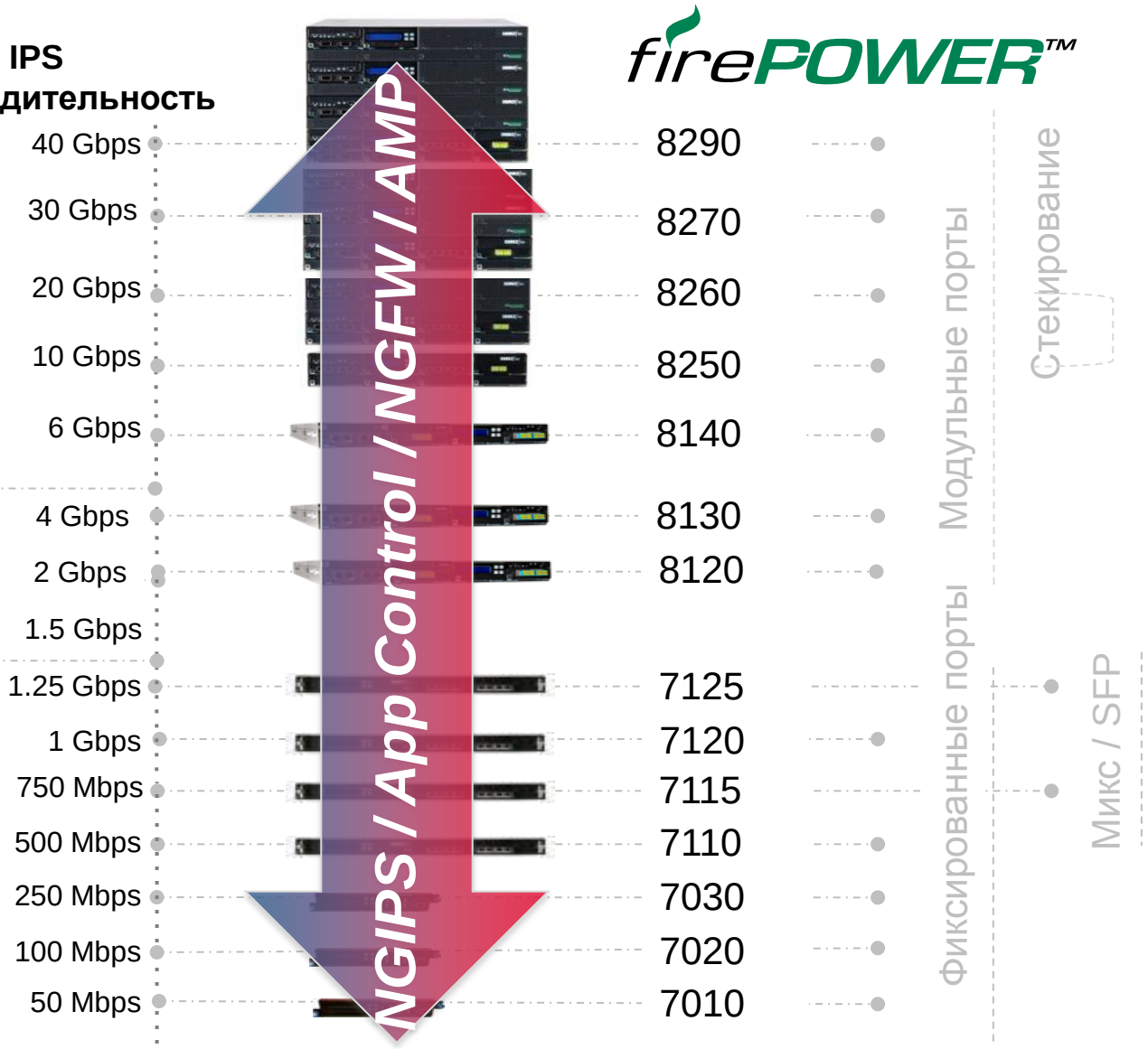
FireAMP™

Advanced Malware Protection

Лучшие технологии для полноценной защиты

Устройства FirePOWER™

Все устройства имеют:
- Интегрированную светодиодную индикацию
- Технологии Акселерации SourceFire
- LCD дисплей



SourceFire

FirePower (NGIPS) - Архитектура решения

Архитектура развертывания

Система Sourcefire предлагает защиту от сложных (ATP) угроз, контроля доступа и приложений и фаервола. Эти функции могут быть развернуты в различных видах архитектур:

- **Single interface** конфигурация позволяет использовать устройство как inline IPS. Данный режим можно использовать совместно с коммутаторами, использующими Spanning Tree Protocol (STP).

  → ***Routed*** - Маршрутизируемые интерфейсы, роутинг (Static/OSPF/RIP)

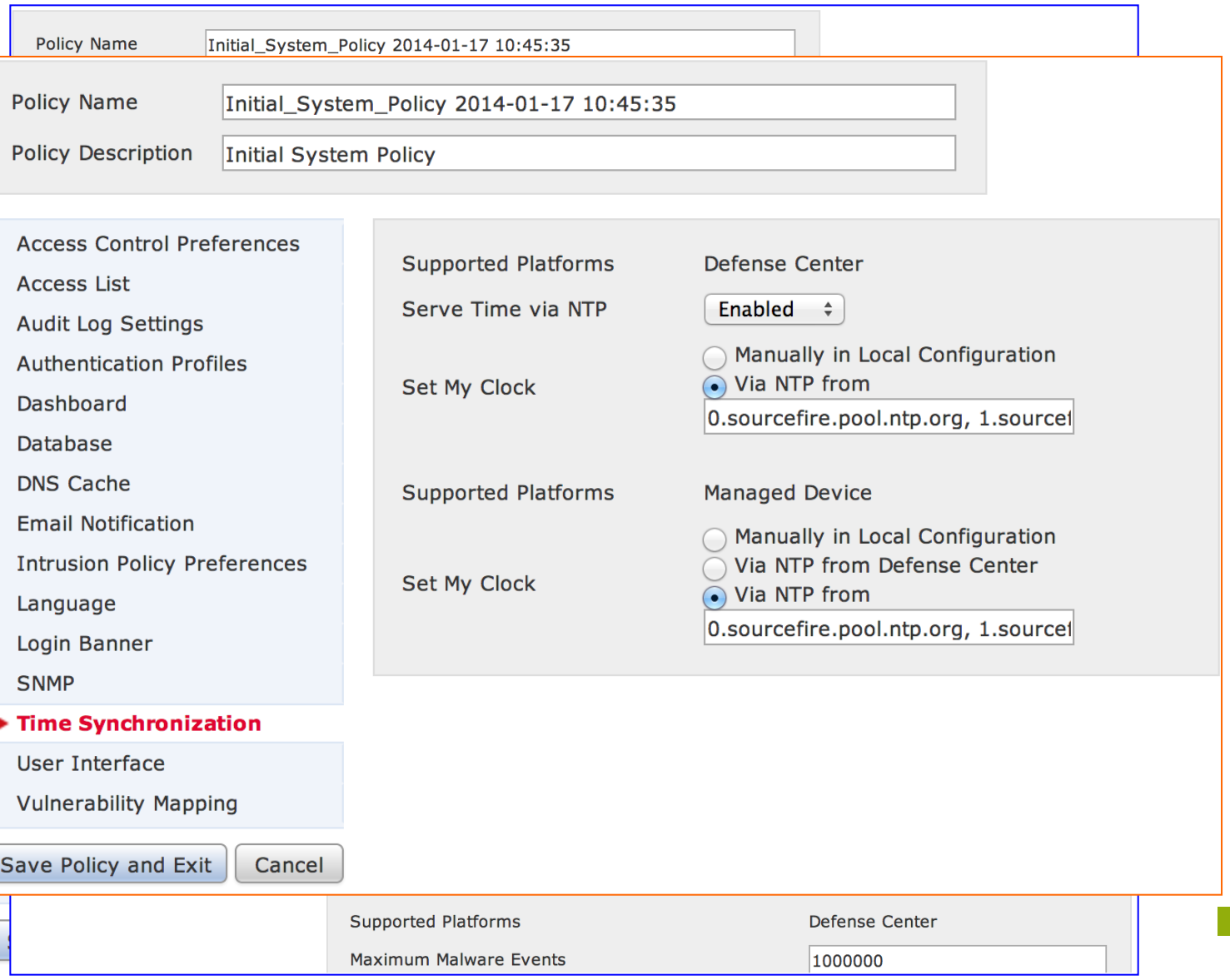
  → ***Switched*** - Layer2 Группы портов, проброс Trunk. Использование/Отключение STP

  → ***Passive*** - Возможность анализа зеркальной копии трафика

- **Clustered high availability (HA)** обмен статусом позволяет устройствам или стекам в кластере синхронизировать статусы. Если любое устройство отказывает, сосед принимает работу без потери потока трафика.

- **Stacking** комбинирует два или более устройства используя сетевую конфигурацию на одном основном устройстве и CPU и RAM на остальных устройствах стека.

Системная политика



Системная политика используется для настройки всех аспектов Defence Center, которые должны быть общими на всех устройствах

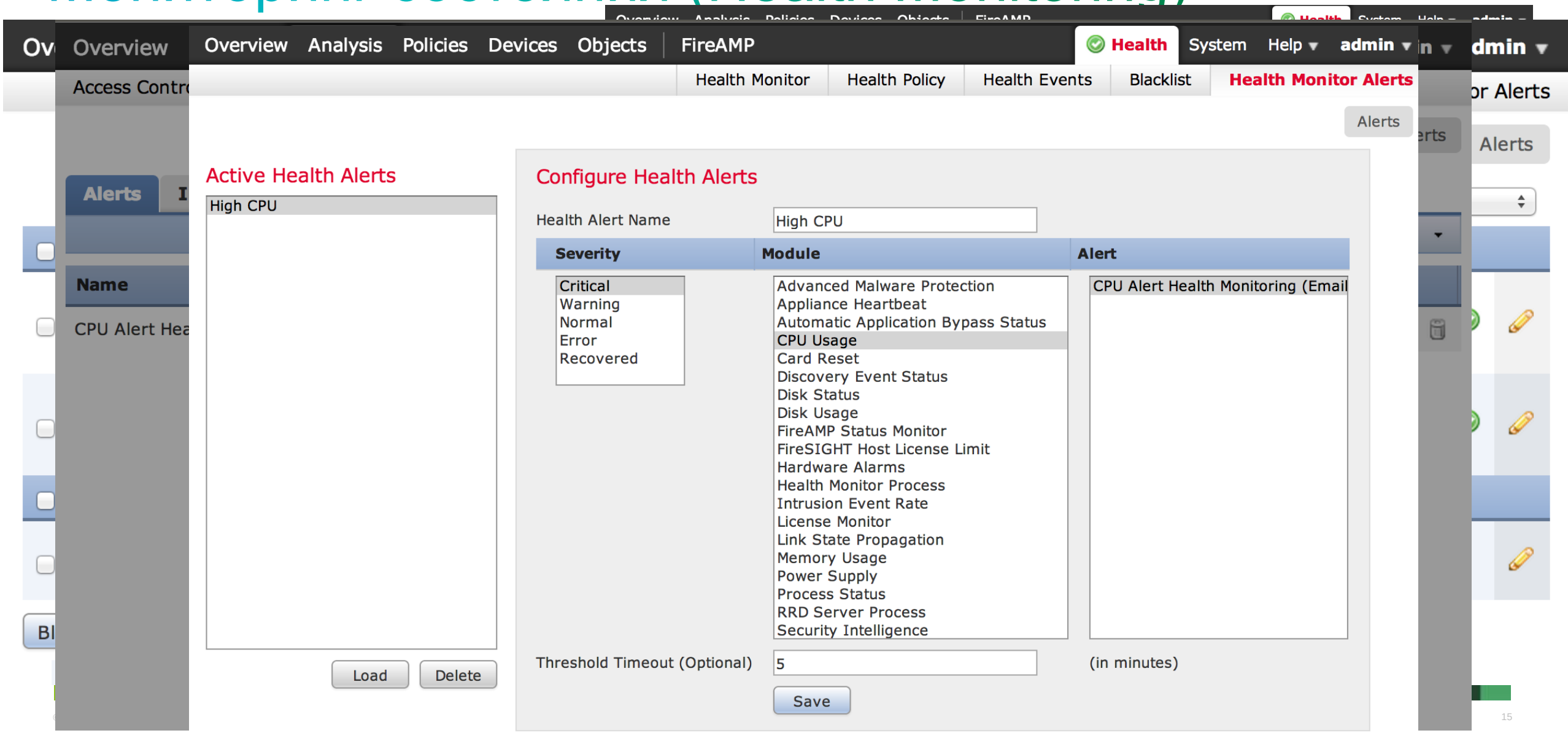
Мониторинг состояния (Health Monitoring)

Можно использовать SourceFire System’s Health Monitor для наблюдения за статусом критически важных функций внутри системы SourceFire. Вы создаете и применяете Health Policy к вашим устройствам, которые наблюдают за важными параметрами функционирования системы, включая статусы Hardware и Software. Health Monitor выбираемые модули в политики запускают серии тестов для определения состояния системы

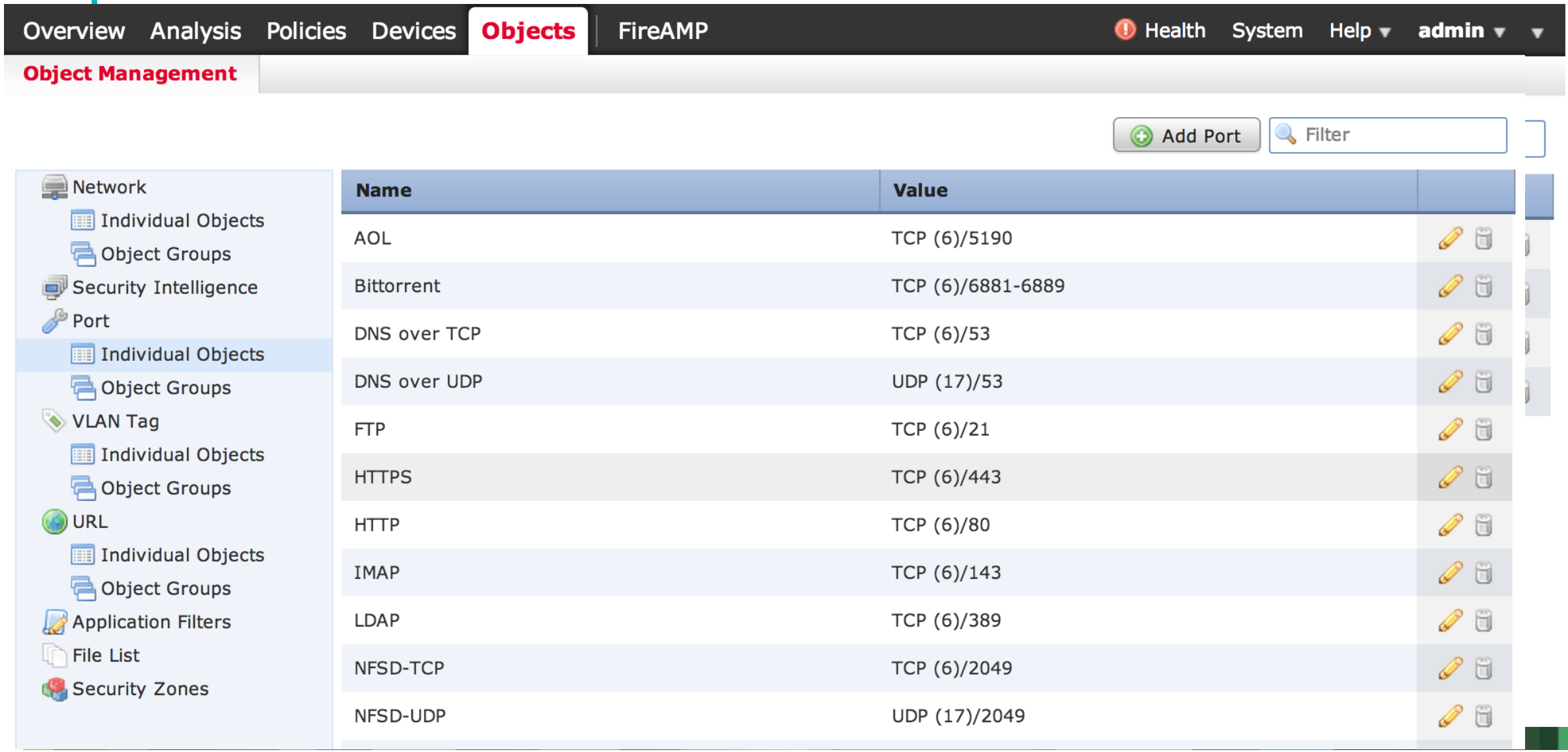
Health Monitor:

- Политики здоровья для устройства/системы в целом;
- Уведомление по событию для системы/устройства;
- Получение статусной информации о состоянии всех компонент системы;
- Статусный Dashboard (экран статистики) с суммарной информацией по систем;

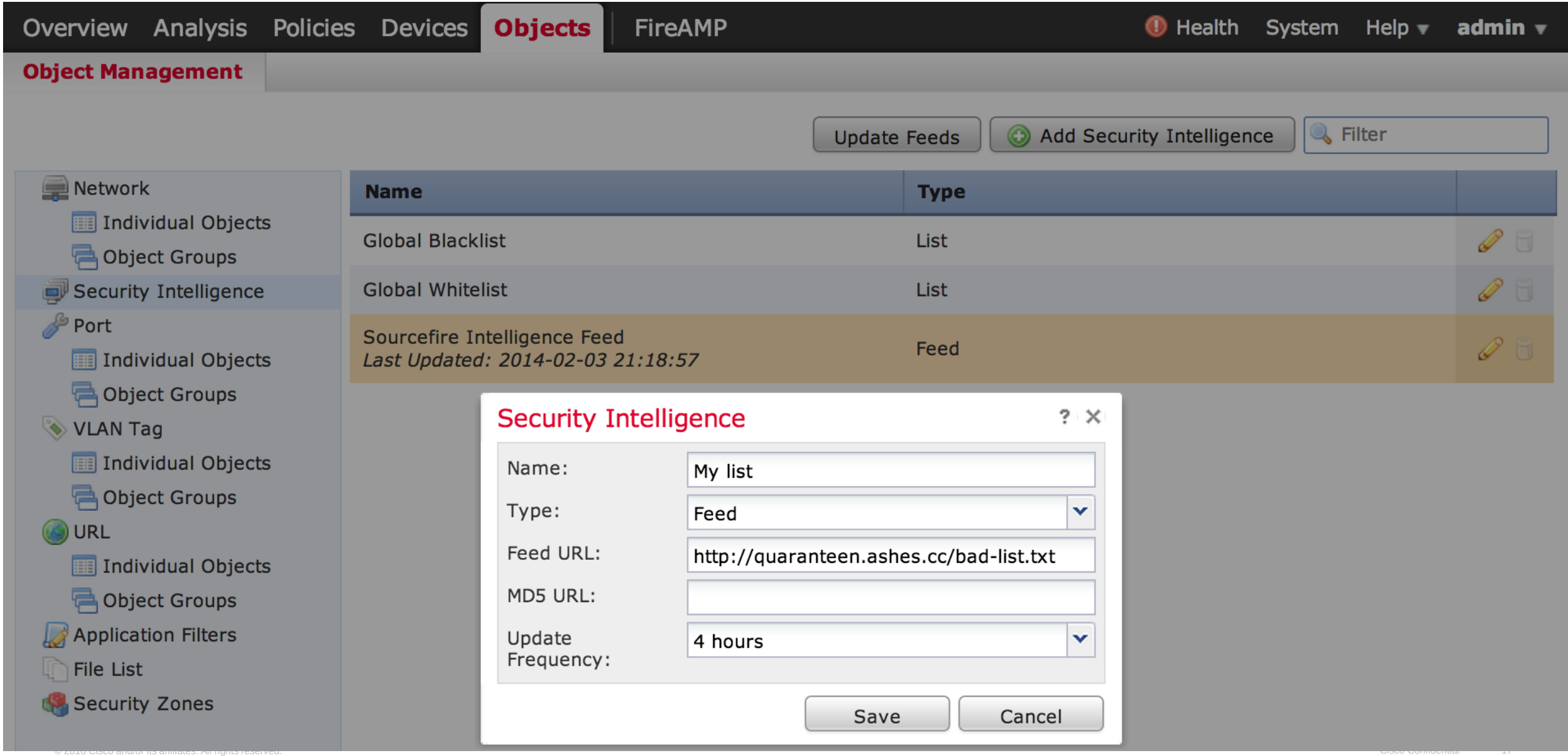
Мониторинг состояния (Health Monitoring)



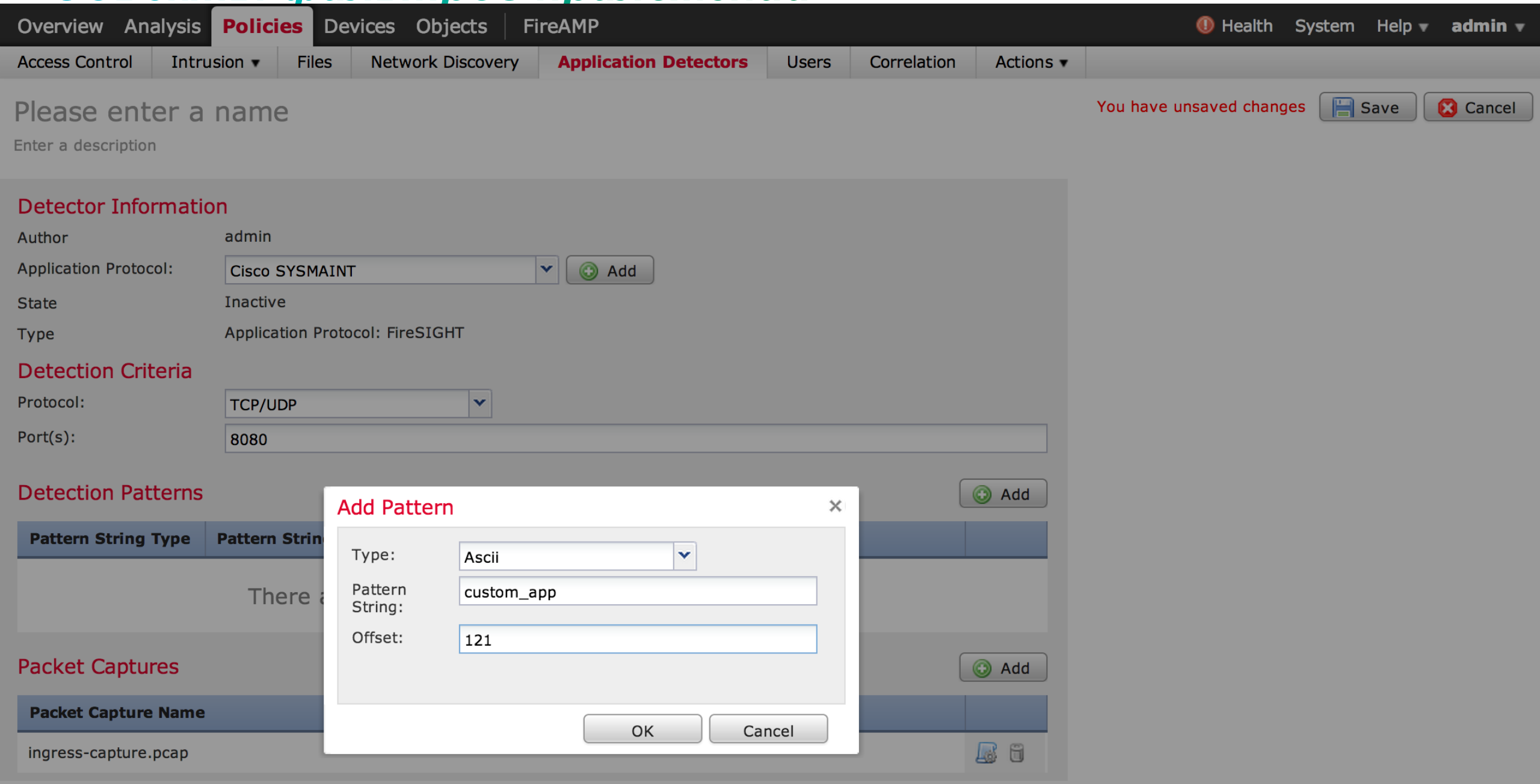
Управление объектами



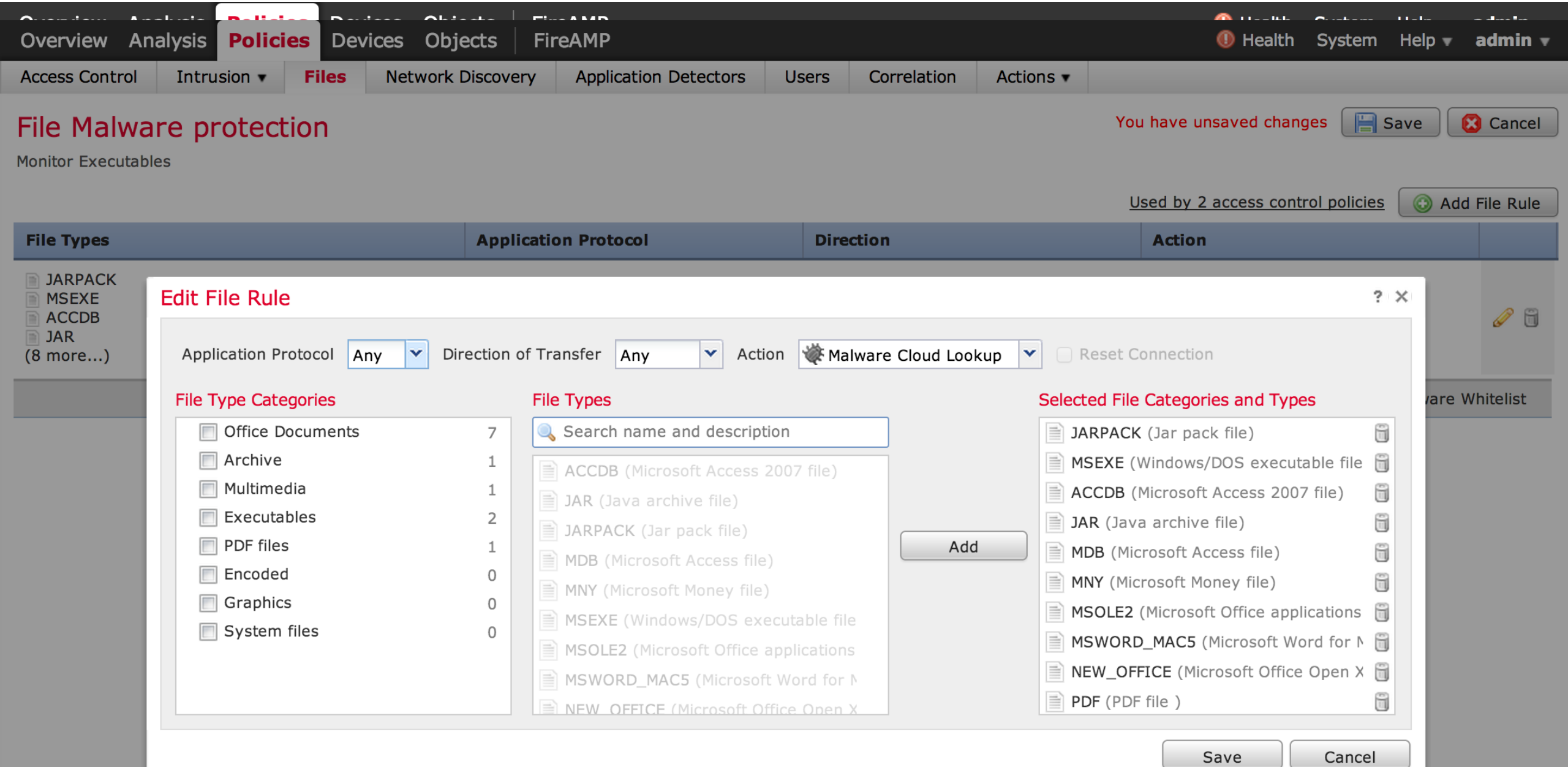
Security Intelligence

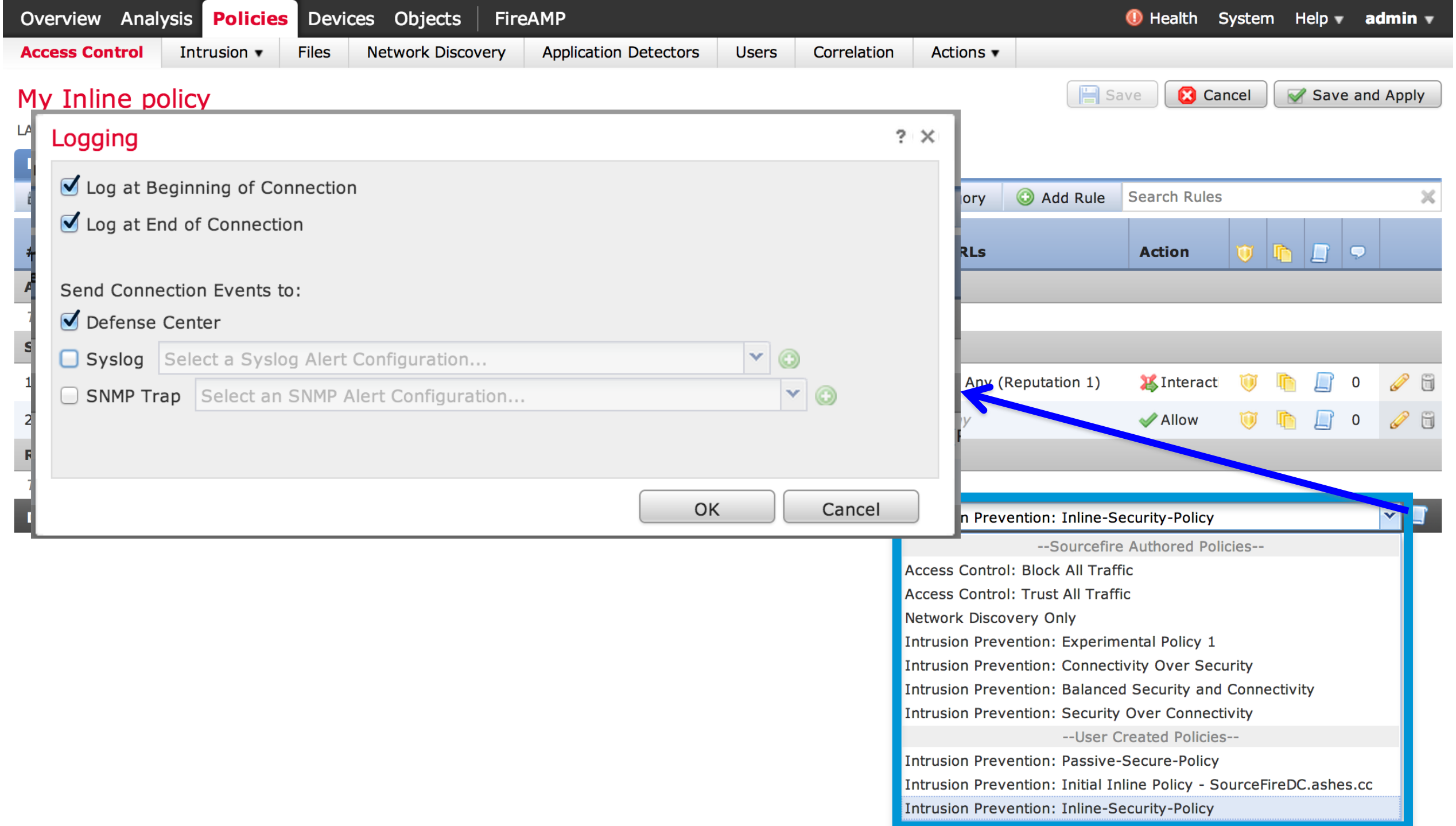


Объекты фильтров приложений

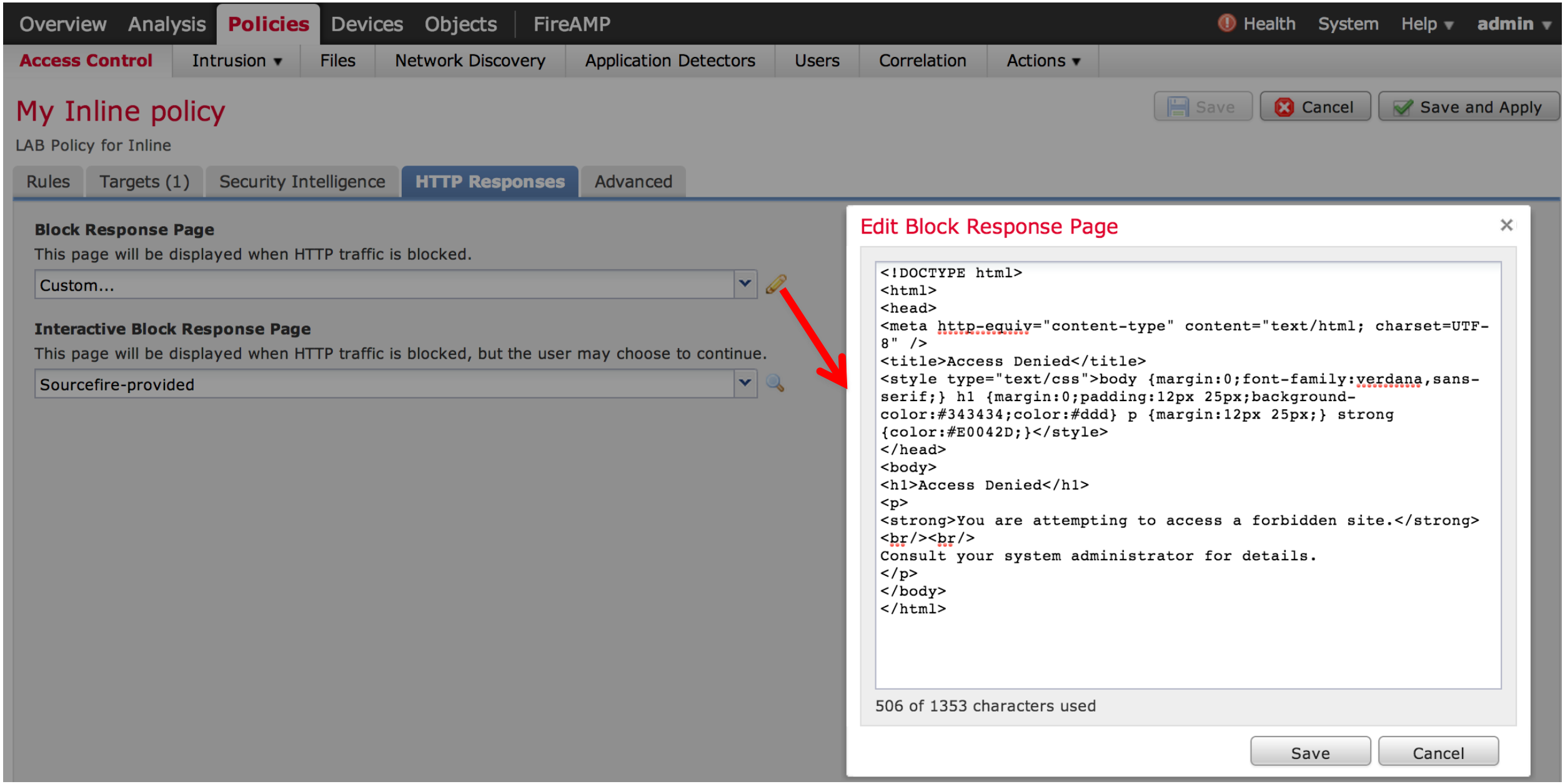


Политика доступа (Access Control Policy)




Overview
Analysis
Policies
Devices
Objects
FireAMP
Health
System
Help
admin
Access Control
Intrusion
Files
Network Discovery
Application Detectors
Users
Correlation
Actions
My Inline policy
Save
Cancel
Save and Apply
Logging
Log at Beginning of Connection
Log at End of Connection
Send Connection Events to:
Defense Center
Syslog
Select a Syslog Alert Configuration...
SNMP Trap
Select an SNMP Alert Configuration...
OK
Cancel
Add Rule
Search Rules
Action
Any (Reputation 1)
Interact
Allow
n Prevention: Inline-Security-Policy
--Sourcefire Authored Policies--
Access Control: Block All Traffic
Access Control: Trust All Traffic
Network Discovery Only
Intrusion Prevention: Experimental Policy 1
Intrusion Prevention: Connectivity Over Security
Intrusion Prevention: Balanced Security and Connectivity
Intrusion Prevention: Security Over Connectivity
--User Created Policies--
Intrusion Prevention: Passive-Secure-Policy
Intrusion Prevention: Initial Inline Policy - SourceFireDC.ashes.cc
Intrusion Prevention: Inline-Security-Policy

HTTP Ответы


Overview
Analysis
Policies
Devices
Objects
FireAMP
Health
System
Help
admin
Access Control
Intrusion
Files
Network Discovery
Application Detectors
Users
Correlation
Actions
My Inline policy
LAB Policy for Inline
Save
Cancel
Save and Apply
Rules
Targets (1)
Security Intelligence
HTTP Responses
Advanced
Block Response Page
This page will be displayed when HTTP traffic is blocked.
Custom...
Interactive Block Response Page
This page will be displayed when HTTP traffic is blocked, but the user may choose to continue.
Sourcefire-provided
Edit Block Response Page
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8" />
<title>Access Denied</title>
<style type="text/css">body {margin:0;font-family:verdana,sans-serif;} h1 {margin:0;padding:12px 25px;background-color:#343434;color:#ddd} p {margin:12px 25px;} strong {color:#E0042D;}</style>
</head>
<body>
<h1>Access Denied</h1>

You are attempting to access a forbidden site.

Consult your system administrator for details.

</body>
</html>
506 of 1353 characters used
Save
Cancel

Sourcefire FireSIGHT® Technology

FireSight!

Система SourceFire вошла в эру, где обнаружение тесно связано с знанием окружения с целью обеспечения более точного и релевантного предупреждения. Коллекция технологий, которые это обеспечивают называется FireSight. FireSight применяет 3 основный типа обнаружения для понимания сети, которую защищает SourceFire:

- **Discovery** – Тип обнаружения, который сообщает информацию о хостах, операционных системах, сервисах, протоколах и приложениях в выделенном окружении.

- **Connection** – Этот тип обнаружений является мониторингом соединений и хранит все что происходит, все связи хостов, как много данных проходило за время соединений и если применимо, какие URL запрашивались.

- **Users** – Этот тип обнаружения и мониторинга Ваших сетей за пользовательской активностью и записи их IP адресов. Также интегрируется с LDAP серверами для предоставления большей информации о обнаруживаемых пользователях. Также может интегрироваться с Microsoft Active Directory серверами для записи пользователей.

FireSight!

С настолько детальным представлением окружений SourceFire может подставлять IPS события в контектст где они происходят и мониторить подозрительную активность. Комбинация враждебной активности, сетевого поведения и детальное знание окружения позволяет SourceFIre проводить корреляцию событий для достижения следующих результатов:

События по уровню воздействия – Хост, который пытается использовать уязвимость актуальную для жертвы произведет высокий приоритет события; Если же жертва не имеет используемой в атаке уязвимости, событие все еще будет выдаваться, однако уровень угрозы будет ниже в силу невозможности нанести урон жертве.

Автоматическая подстройка – может быть достигнута в силу того, что система может выбирать правила и опции конфигурации основываясь на известном окружении. Это динамический процесс, в котором обнаруживаемые изменения в окружении детектируются и рапортуются как только обнаруживаются. Таким образом политики и конфигурация может обновляться самостоятельно без привлечения администратора.

Сетевое поведение – автоматически анализирует отклонение от нормального поведения хоста и на основании отклонений может вызвать событие.

Compliance - соответствие с Вашей корпоративной политикой безопасности может отслеживаться и рапортоваться.

User awareness – позволяет понимать что ваши пользователи делают в сети. Также можно отследить в какие атаки и активности были вовлечены пользователи и использовать эти знания в политике корелляции.

Discovery

Данная компонента SourceFire отвечает за пассивный мониторинг вашей сети. **Может быть дополнено активными сетевыми сканерами, либо прямым импортом информации об окружении через выделенный API.**

Следующая информация собирается об окружении:

- Хосты
- Операционные системы
- Сервисы
- Клиентские приложения
- Уязвимости, которые могут присутствовать
- Сетевое мапирование

Хостовые профили

- **Host** – Первый информационный блок на хостовом профиле и он содержит базовую информацию: Имя, операционную систему, IP address, MAC address и тип хоста.
- **Operating System** – Если прошло достаточно трафика до и от машины, определяется его ОС.
- **Servers** – Все сервисы, обнаруженные на хосте.
- **Applications** – Все приложения, обнаруженные на хосте.
- **Users** – Все пользователи, ассоциированные с хостом .
- **Attributes** – Аттрибуты, ассоциированные с хостом.
- **Host Protocols** – Протоколы замеченные на хосте.
- **Vulnerabilities** – Уязвимости, основываяст на сервисах, клиентских приложениях, протоколах и операционной системе хоста сисиема может заключить об их актуальности и перечислит их в профиле;

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	wnload
Patch	MacOSXUpd10.6.1.dmg	wnload
Patch	MacOSXServerUpd10.6.1.dmg	wnload
Patch	SecUpd2009-005.dmg	wnload
Patch	SecUpdSrvr2009-005.dmg	nload
Patch	SecUpd2009-005Intel.dmg	Intel wnload

Профили соединений

События соединений это записи происходящих соединений и если не записываются сами передаваемые данные, то фиксируются метаданные соединений время, source-destination, протоколы и количество переданных данных

Отслеживание активных соединений дает системе возможность мониторинга сетевого поведения и уведомления с исправлением подохрительной активности.

- First Packet
- Last Packet
- Action
- Initiator IP
- Responder IP
- Initiator User
- Initiator Port
- Responder Port
- Protocol
- Application
- Client
- Version
- TCP Flags
- Connection Type
- NetBIOS Domain
- Initiator Packets
- Responder Packets
- Initiator Bytes
- Responder Bytes
- URL
- URL Category
- URL Reputation
- Source Device
- Access Control Policy
- Ingress Security Zone
- Egress Security Zone
- Device
- Ingress Interface
- Egress Interface

Connection Summary

Provides tables and charts of the activity on your monitored network segment organized by different criteria

Connections × | Traffic × | Geolocation × | +

Show the Last 1 hour

Add Widgets

Traffic by Application (switch workflow)

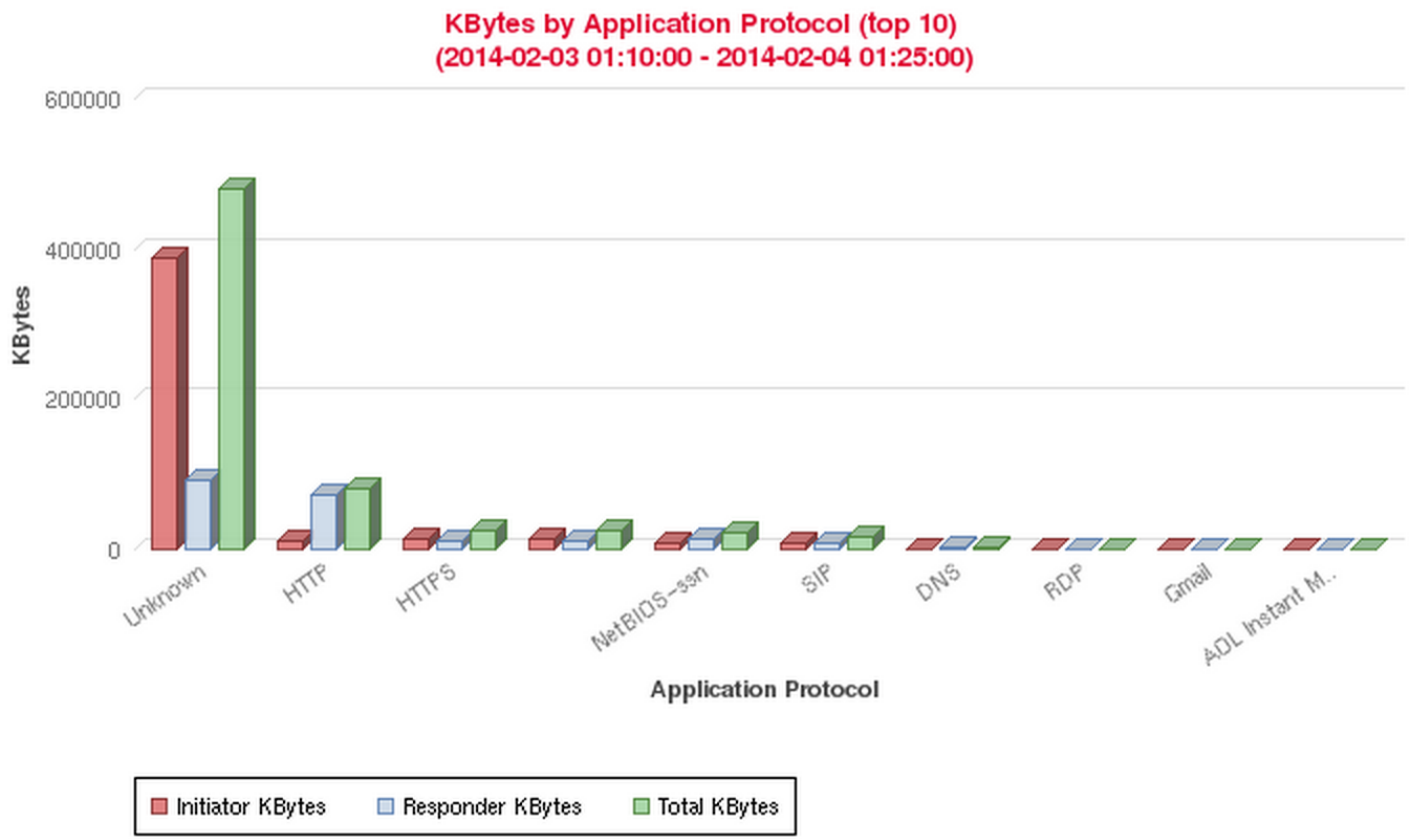
Top 10 Applications by Traffic › Table View of Connection Events

2014-02-03 01:14:00 - 2014-02-04 01:25:27
Expanding

No Search Constraints (Edit Search)

Connections | Intrusion | Malware | Files | Hosts | Applications | Application Details | Servers | Host Attributes | More ▾

X-Axis | Y-Axis | Datasets | Switch to Pie | Export Data | Detach



Обнаружение пользователей

Данная функция дает возможность коррелировать угрозы с хостами и пользователями. Сенсоры идентифицируют источник угроз, нарушения политик и сетевых уязвимостей. Путем связывания сетевого поведения, трафика и событий напрямую с пользователями, система SourceFire помогает бороться с угрозами, блокировать пользователей или их активности, а также защищать других от воздействия.

LDAP User Metadata Collection - Соединение с MS AD сервером или сервером, поддерживающим LDAP (Sun Directory Services or OpenLDAP)для сбора списка пользователей и их метаданных.

Следующая информация включается в обнаружение:

- first name
- last name
- email
- department
- phone number

Правила и политики корреляции

Defence Center можно настроить на запуск различных действий в ответ на нарушение политики или событие Network Discovery.

Эти действия включают ремедиацию, такую как блокирование хоста на фаерволе при обнаружении атаки. Когда срабатывает действие, генерируется событие о ремедиации.

Компонента ремедиации политики и соответствующие действия предоставляют гибкий API, который позволяет создавать и загружать собственные модули ремедиации и отвечать на события безопасности.

Еще один вариант ответа – это запуск уведомления.

- Email
- SNMP
- Syslog

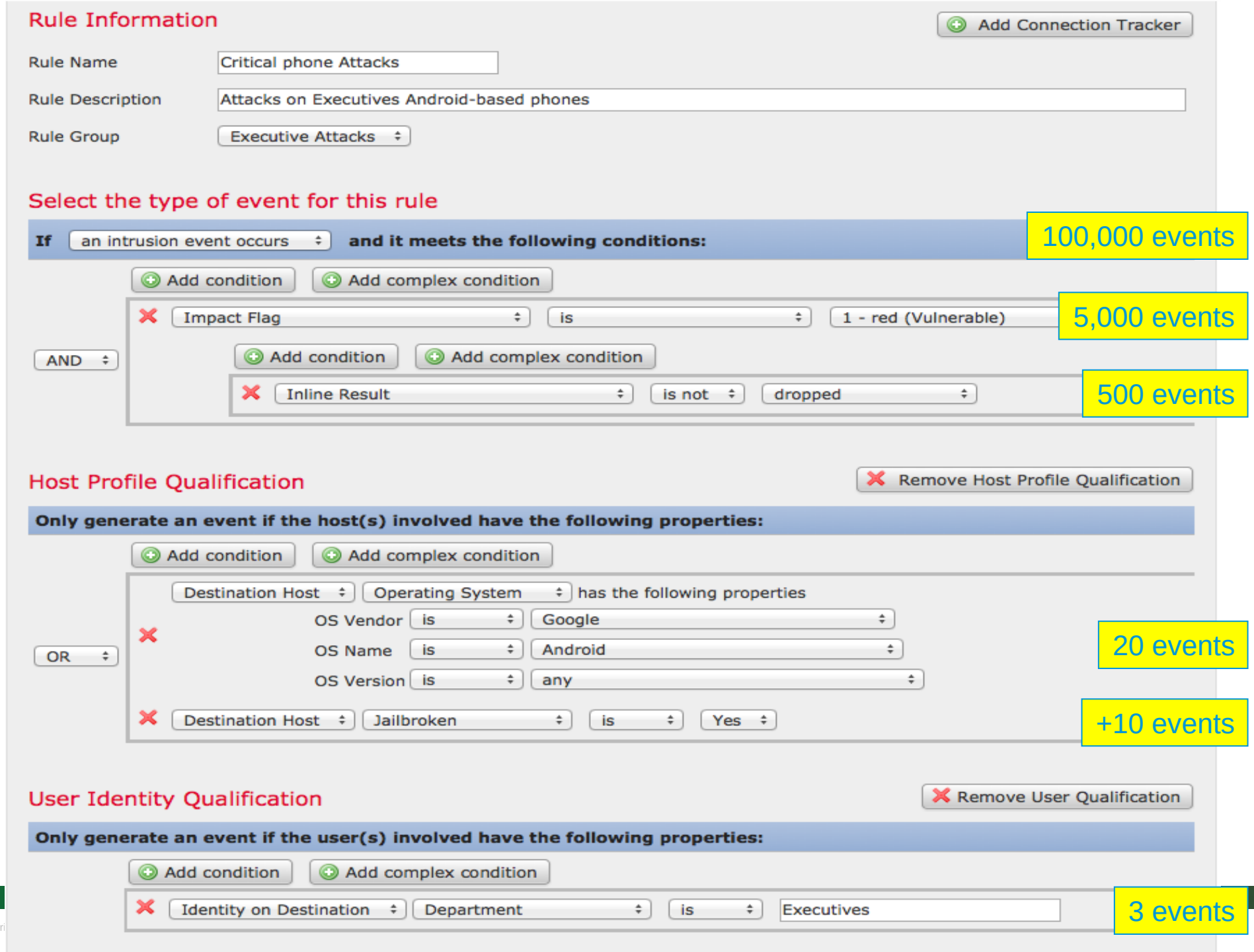
Также есть возможность добавить атрибут на хост, атрибуты и из типы можно задавать самостоятельно.

Собственный модуль ремедиации

В дополнение к стандартным модулям, которые поставляются с системой можно применять свои собственные модули. Модуль ремедиации это программа или скрипт, упакованный с ассоциированными файлами, который написан с целью совершения действий в ответ на определенные условия.

Скрипт ремедиации может быть написан на любом из указанных языков:

- Bash
- Tcsh
- Perl
- C - If you write your remediation module program in C, it must be pre-compiled and statically linked, with the exception of links to routines



Edit Policy: Inline-Security-Policy

Rules

< Back

Filter: MicrosoftVulnerabilities:"MS00-031"

Filter returned 1 result

Rule State | Event Filtering | Dynamic State | Alerting | Comments | Policy

GID	SID	Message
1	1021	SERVER-IIS ism.dll attempt

Hide details

1 of 1

Attack	Simple. No exploit software required.
False Positives	None Known
False Negatives	None known
Corrective Action	Check server logs for signs of compromise.
Contributors	Original rule writer unknown Original document author unkown Sourcefire Vulnerability Research Team Nigel Houghton <nigel.houghton@sourcefire.com>
References	Bugtraq page Common Vulnerabilities and Exposures Page Nessus Page Microsoft security bulletin
SRU	Sourcefire Rule Update 2013 06 17 001 vrt

Edit Policy: Inline-Security-Policy

HTTP Configuration

< Back

Consecutive Small Chunks	5 (0 - 255. When Small Chunk Size > 0, number of consecutive small chunks that is excessive.)
HTTP Methods	CONNECT, DELETE, HEAD, OPTIONS, PUT, TRACE
No Alerts	☐
Normalize HTTP Headers	☑
Inspect HTTP Cookies	☑
Normalize Cookies in HTTP Headers	☐
Allow HTTP Proxy Use	☐
Inspect URI Only	☐
Inspect HTTP Responses	☑
Normalize UTF Encodings to UTF-8	☑
Inspect Compressed Data	☑
Unlimited Decompression	☐ (Enabling this option sets Maximum Compressed Data Depth and Maximum Decompressed Data Depth to 65535 during commit)
Normalize JavaScript	☐ (Maximum allowed consecutive encoded spaces inside JavaScript)
Extract Original Client IP Address	☑
Log URI	☑
Log Hostname	☑
Profile	◉ All ○ Apache ○ IIS ○ Custom

Revert to Defaults

This configuration is contained in the base policy: Security Over Connectivity

Препроцессоры транспортного/сетевого уровней

SourceFire предоставляет препроцессоры, которые детектируют эксплоиты на сетевом и транспортных уровнях. Эти препроцессоры детектируют атаки, направленные на IP фрагментацию, валидацию чексуммы, TCP и UDP обработку сессий. До отсылки пакета в препроцессор пакетный декодер конвертирует заголовки пакета и данные в формат, доступный препроцессору и движку правил, далее детектирует аномальное поведение в заголовках пакетов.

Имеются следующие advanced configuration опции:

- **Checksum Verification**
- **Detection Settings**
- **Inline Normalization**
- **IP Defragmentation**
- **Packet Decoding**
- **TCP Stream Configuration**
- **UDP Stream Configuration**

Управление пользователями

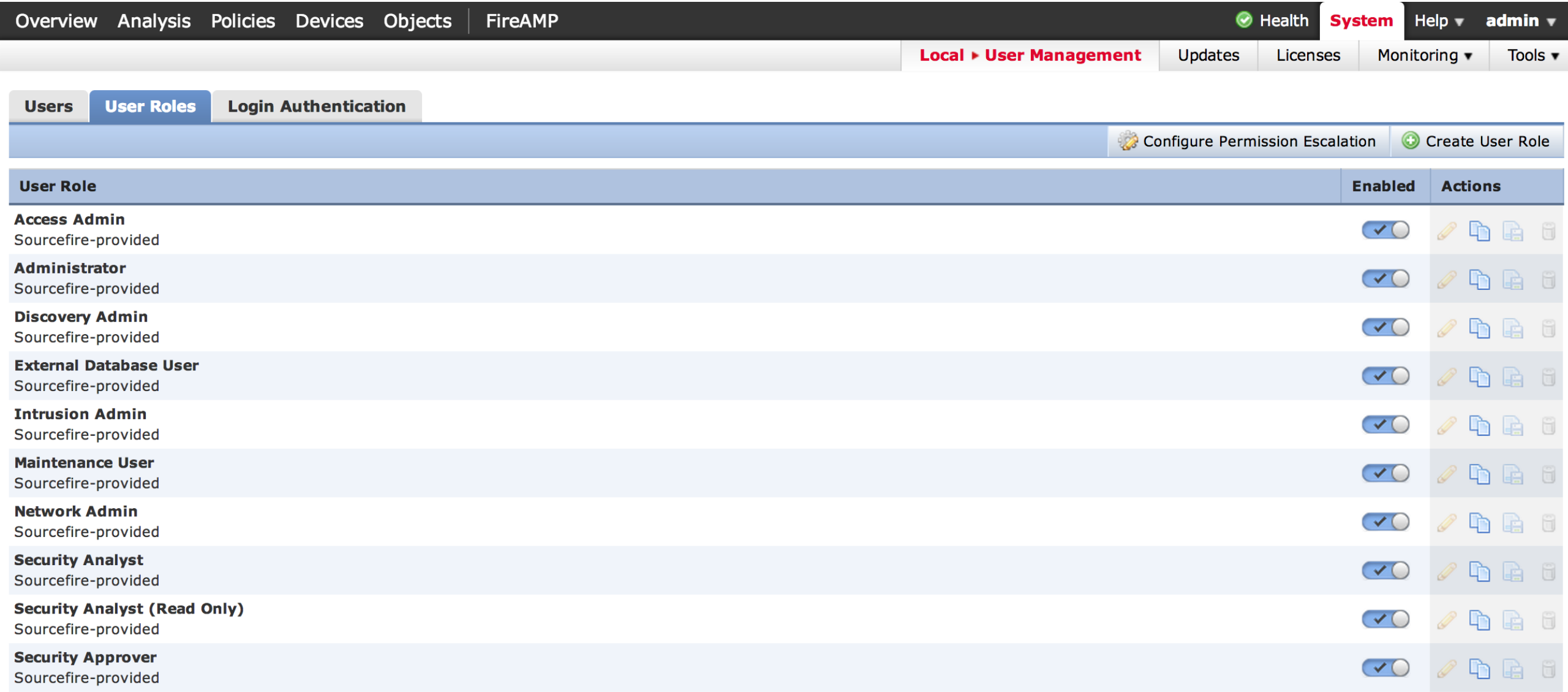
Доступна внешняя и внутренняя база аутентификации пользователей

На странице логина пользователь вводит свои учетные данные:

- Если пользователь настроен как внутренний пользователь, устройство проверяет свою локальную базу пользователей со всеми сопутствующими атрибутами.

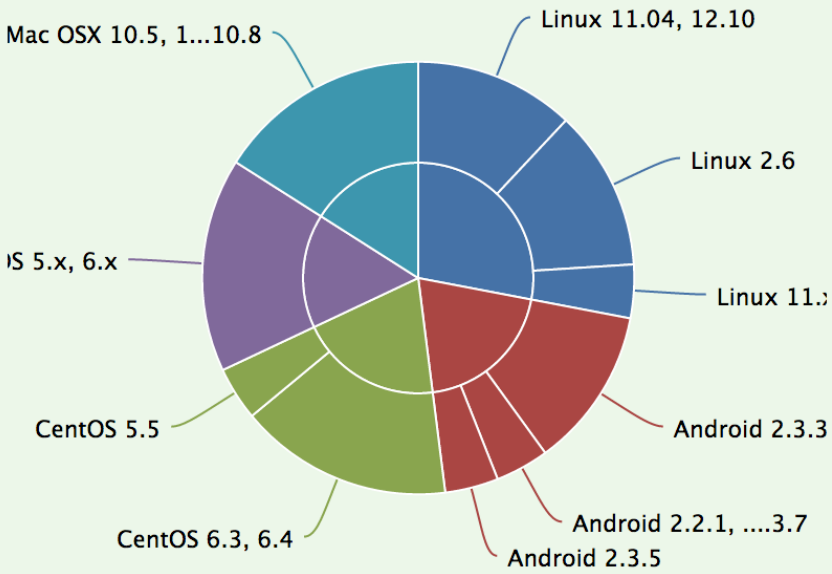
- Если пользователь заведен как внешний, система проверяет существует ли логин во внутренней базе и находит атрибуты, которые надо применить. Если пользователя нет во внутренней базе, система идет во внешний репозиторий, LDAP и RADIUS поддерживаются. Проверяются учетные данные и если они верны, предоставляется доступ.

Пользовательские роли

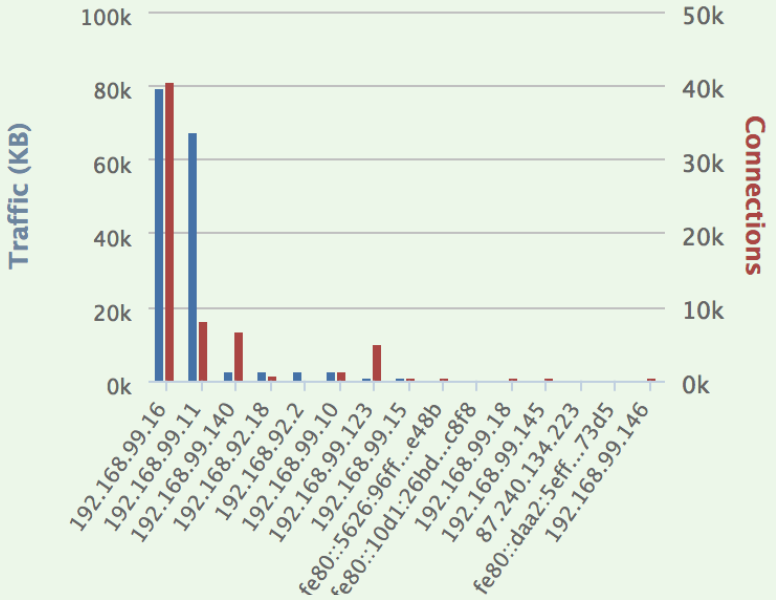


Network Information

Operating Systems



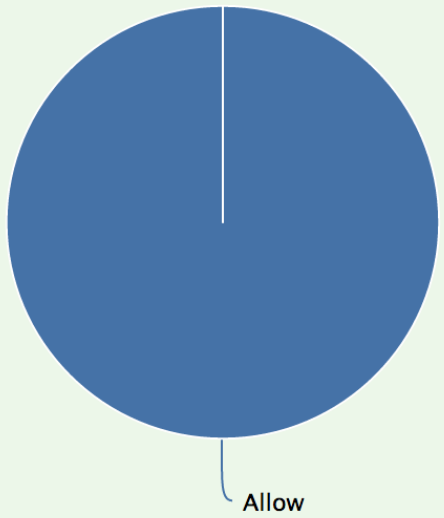
Traffic by Source IP



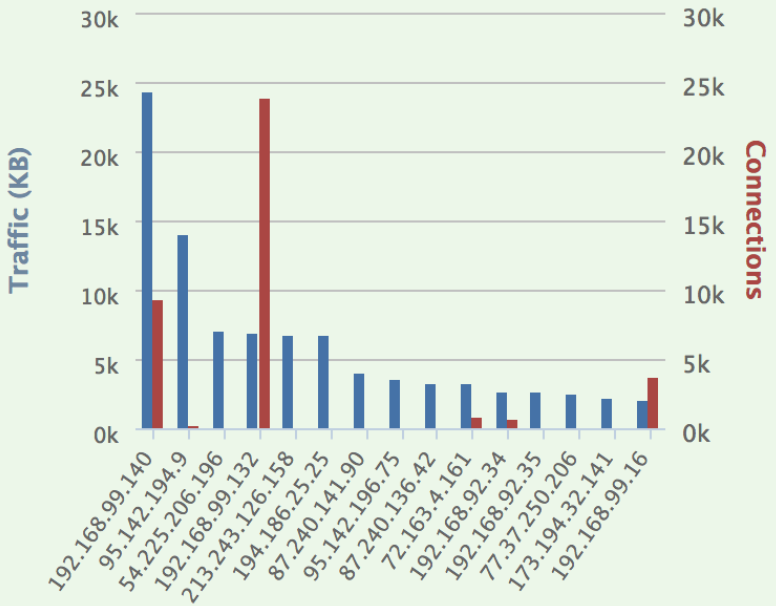
Traffic by Source User

No Data

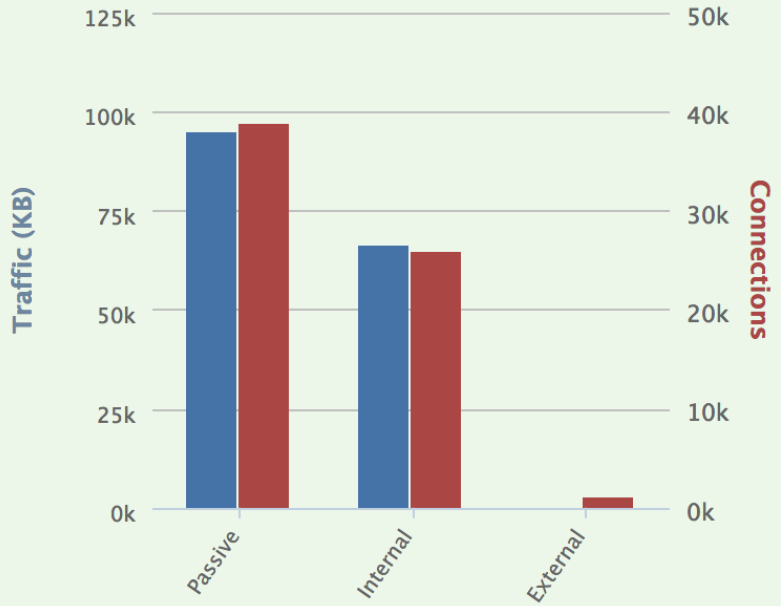
Connections by Access Control Action



Traffic by Destination IP



Traffic by Ingress Security Zone



Браузер контекста (Context Explorer)

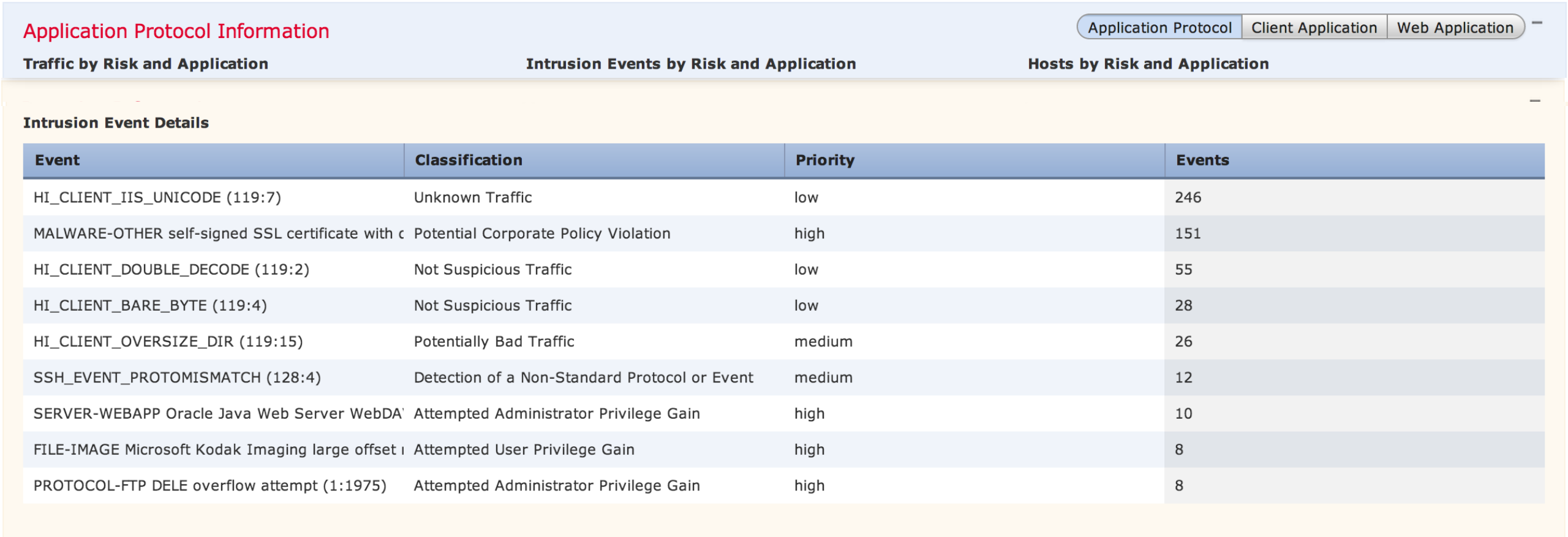
Статистика приложений

Секция информации о приложениях в браузере контекста состоит из трех интерактивных графиков и таблицы-списка:

-- Траффик

-- События безопасности

-- Хосты ассоциированные с приложениями и организованные по риску для бизнеса.

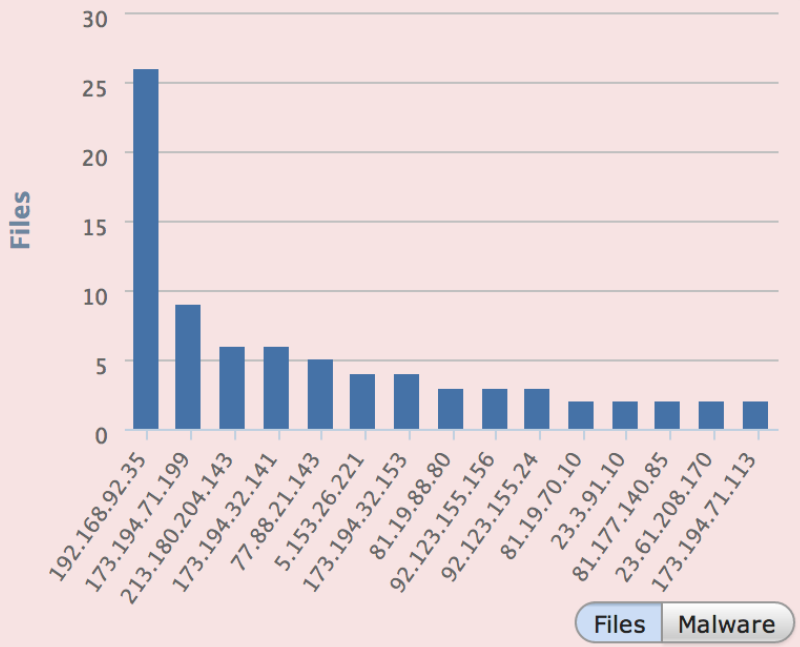


Event	Classification	Priority	Events
HI_CLIENT_IIS_UNICODE (119:7)	Unknown Traffic	low	246
MALWARE-OTHER self-signed SSL certificate with c	Potential Corporate Policy Violation	high	151
HI_CLIENT_DOUBLE_DECODE (119:2)	Not Suspicious Traffic	low	55
HI_CLIENT_BARE_BYTE (119:4)	Not Suspicious Traffic	low	28
HI_CLIENT_OVERSIZE_DIR (119:15)	Potentially Bad Traffic	medium	26
SSH_EVENT_PROTOMISMATCH (128:4)	Detection of a Non-Standard Protocol or Event	medium	12
SERVER-WEBAPP Oracle Java Web Server WebDA'	Attempted Administrator Privilege Gain	high	10
FILE-IMAGE Microsoft Kodak Imaging large offset i	Attempted User Privilege Gain	high	8
PROTOCOL-FTP DELE overflow attempt (1:1975)	Attempted Administrator Privilege Gain	high	8

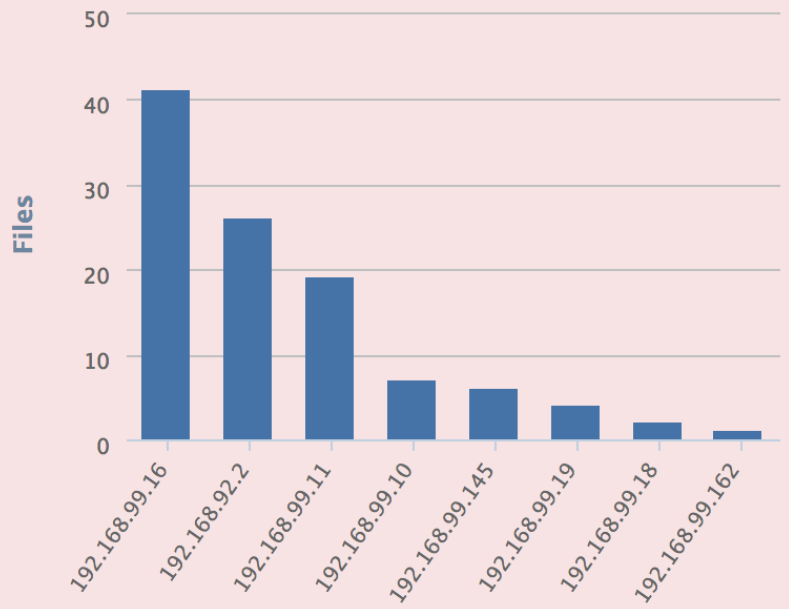
Браузер контекста (Context Explorer)

Статистика файлов

Top Hosts Sending Files



Top Hosts Receiving Files



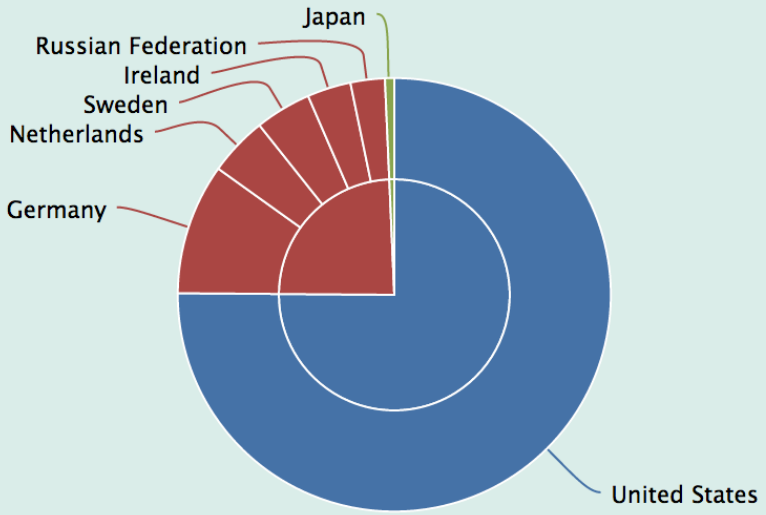
Top Malware Detections

No Data

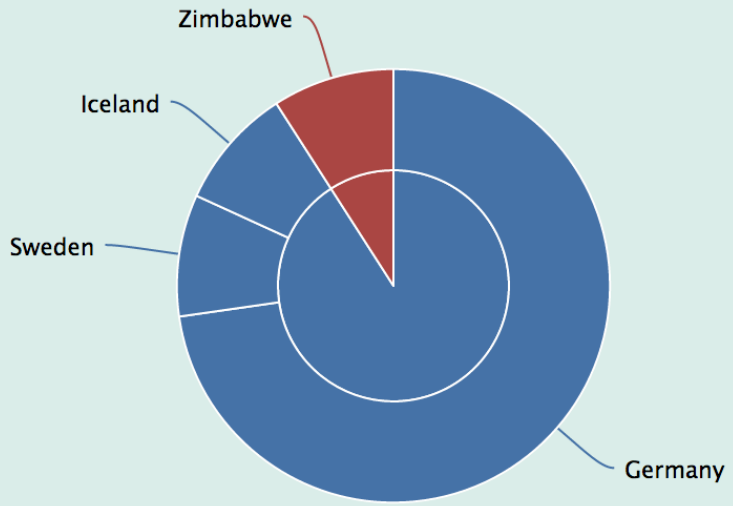
Браузер контекста (Context Explorer)
Геолокация

Geolocation Information

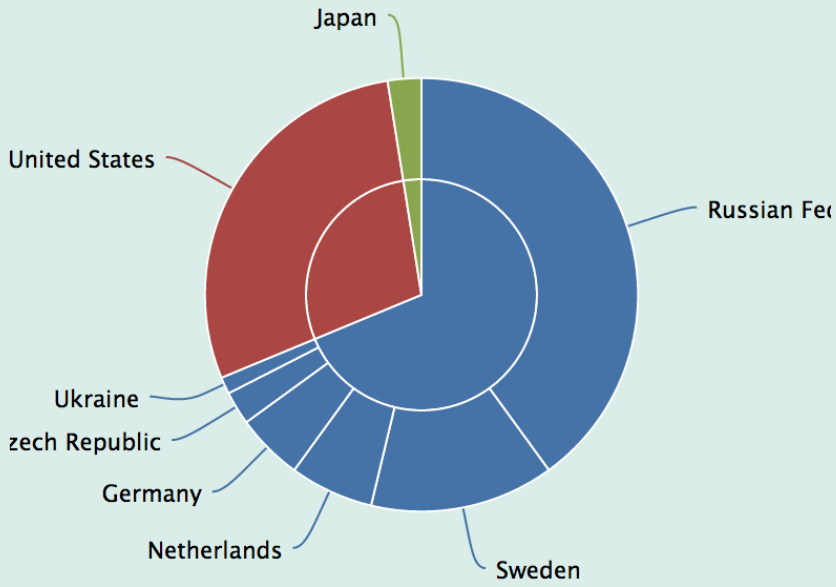
Connections by Initiator Country



Intrusion Events by Source Country



File Events by Sending Country

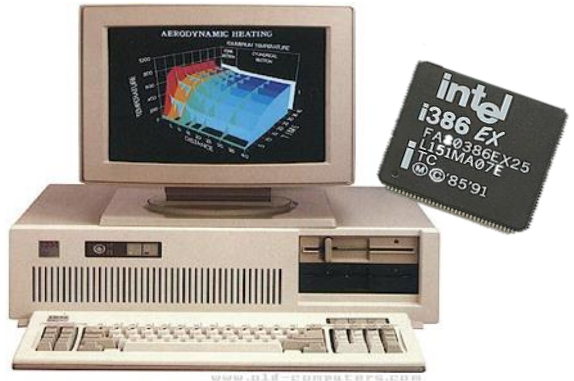


Advanced Malware Protection

Антивирус как средство от Malware

- Весьма ограничено:
  - Может использовать 2-5% от имеющегося CPU.
  - Ограниченный набор правил
  - Ограничено покрытие
  - Оперирует в точке времени.
- **Зачем доверять безопасность 386-му компьютеру?**

To your AV, this …



… looks like this.

Что если защита от Malware реализуется так?

- Петафлопы производительности
- Петабайты хранилища
- Big data аналитика
- Постоянный анализ
- Интеллектуальные алгоритмы поиска Malware

“Now, *that’s* what I’m talkin’ about!”

Детектирование malware дело не легкое….

- Не рассматривайте разрозненные объекты.
- Думайте об экосистеме Malware, смотрите за сцену, ищите скрытых актеров
- Отслеживайте праекторию Malware до пациента 9, в другом случае вы снова заразитесь

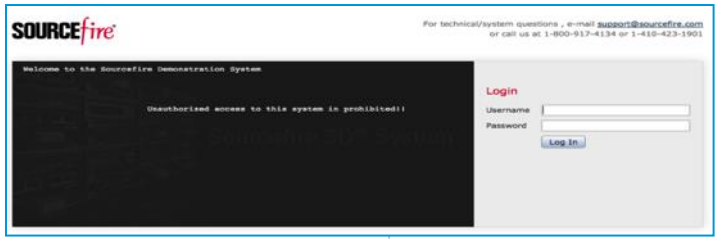
Диспозиция файлов:
- Known bad
- Known good
- Unknown

Unknown drops known bad
75%

Known bad drops unknown
70%

Наш подход к advanced malware protection

AMP for Networks



FireSIGHT Management Center

Sourcefire Sensor

AMP Malware license

Detection Services & Big Data analytics

SSL:443 | 32137

Heartbeat: 80

AMP for Endpoints

SaaS Manager

Модель работы Endpoint

File data

Hash tracked files

Check local cache

Query for Disposition

Block malicious dispositions

Network data

Capture Network Traffic

Log connection data for tracked files

System data

Host Name

Host IP Address

Heartbeat

Login Name

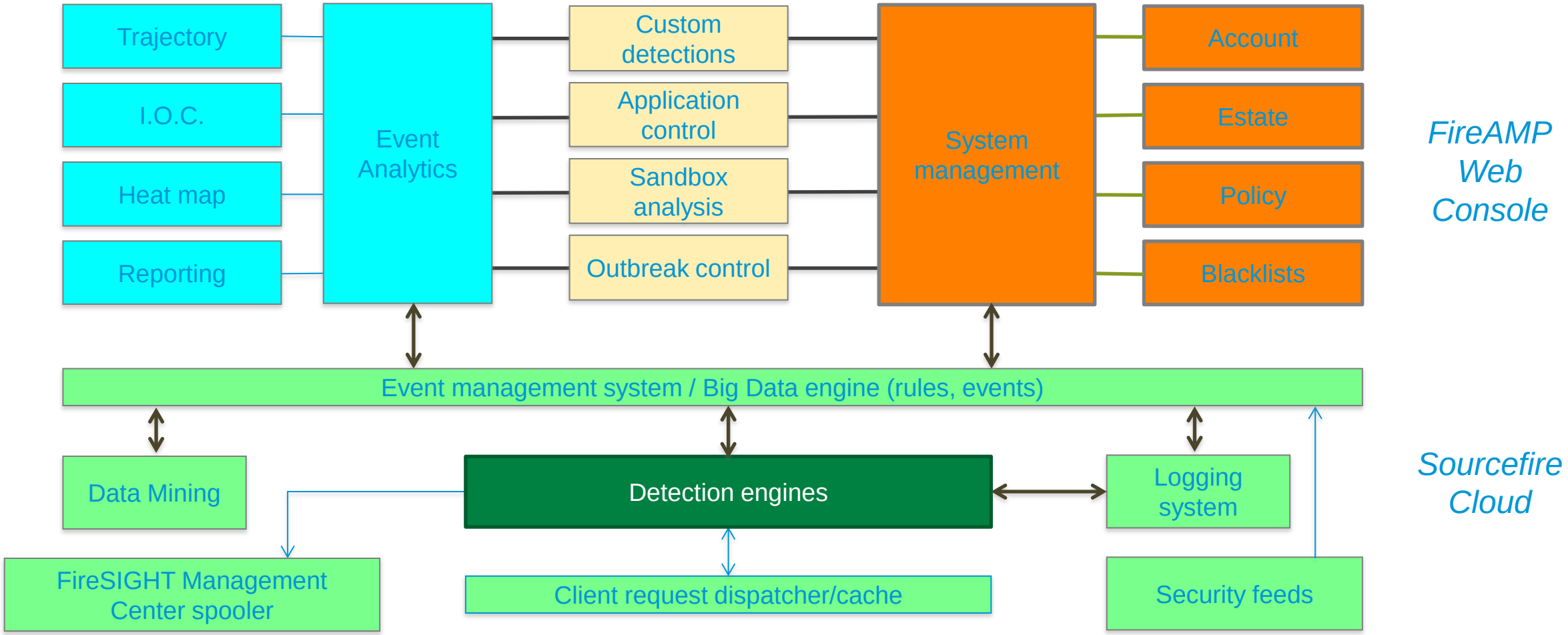
Legend

No Personally Identifiable Information (PII)

Optional PII

PII

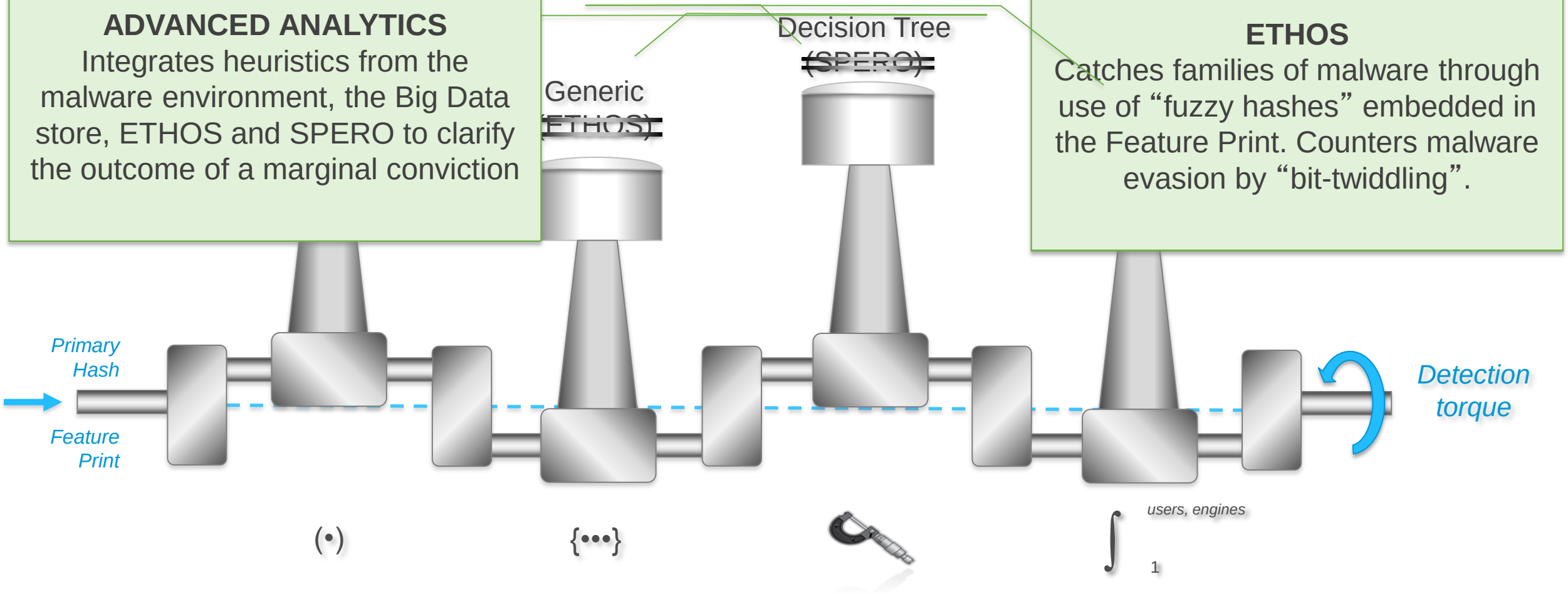
Все самое умное находится в облаке



Движки детектирования в AMP

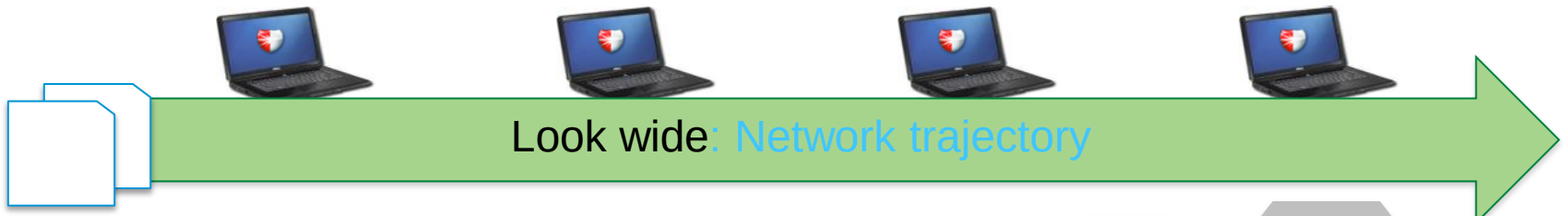
ADVANCED ANALYTICS
Integrates heuristics from the malware environment, the Big Data store, ETHOS and SPERO to clarify the outcome of a marginal conviction

ETHOS
Catches families of malware through use of “fuzzy hashes” embedded in the Feature Print. Counters malware evasion by “bit-twiddling”.

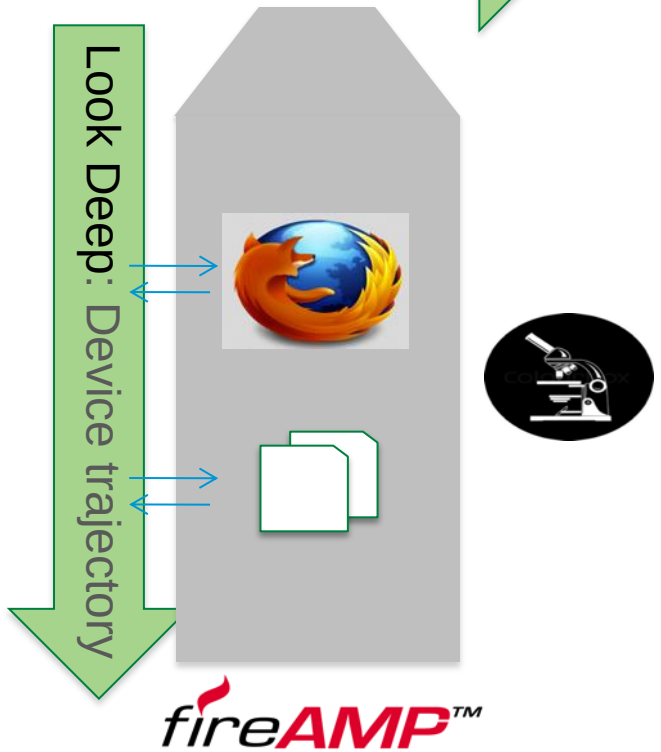


Поиск пациента 0: Анализ Траектории

Смотрите шире (AMP for Networks), глубже (AMP for Endpoints)



- Какие системы заражены?
- Когда это произошло?
- Где пациент №0?
- Что еще он с собой принес?



Thank you.

Questions ?

Sandro Chachanidze
achachan@cisco.com