TOMORROW starts here.

Межсетевые экраны следующего поколения Cisco ASA с сервисами FirePower – борьба с современными угрозами, архитектура решения и варианты применения

Руслан Иванов
Системный инженер-консультант
ruivanov@cisco.com

26.11.14

Cisco Connect

Проблемы с традиционной моделью «эшелонированной» безопасности

Точечные продукты

Высокая сложность, меньшая эффективность

Ручные и статичные механизмы

Медленная реакция, ручное управление, низкая результативность

Слабая прозрачность

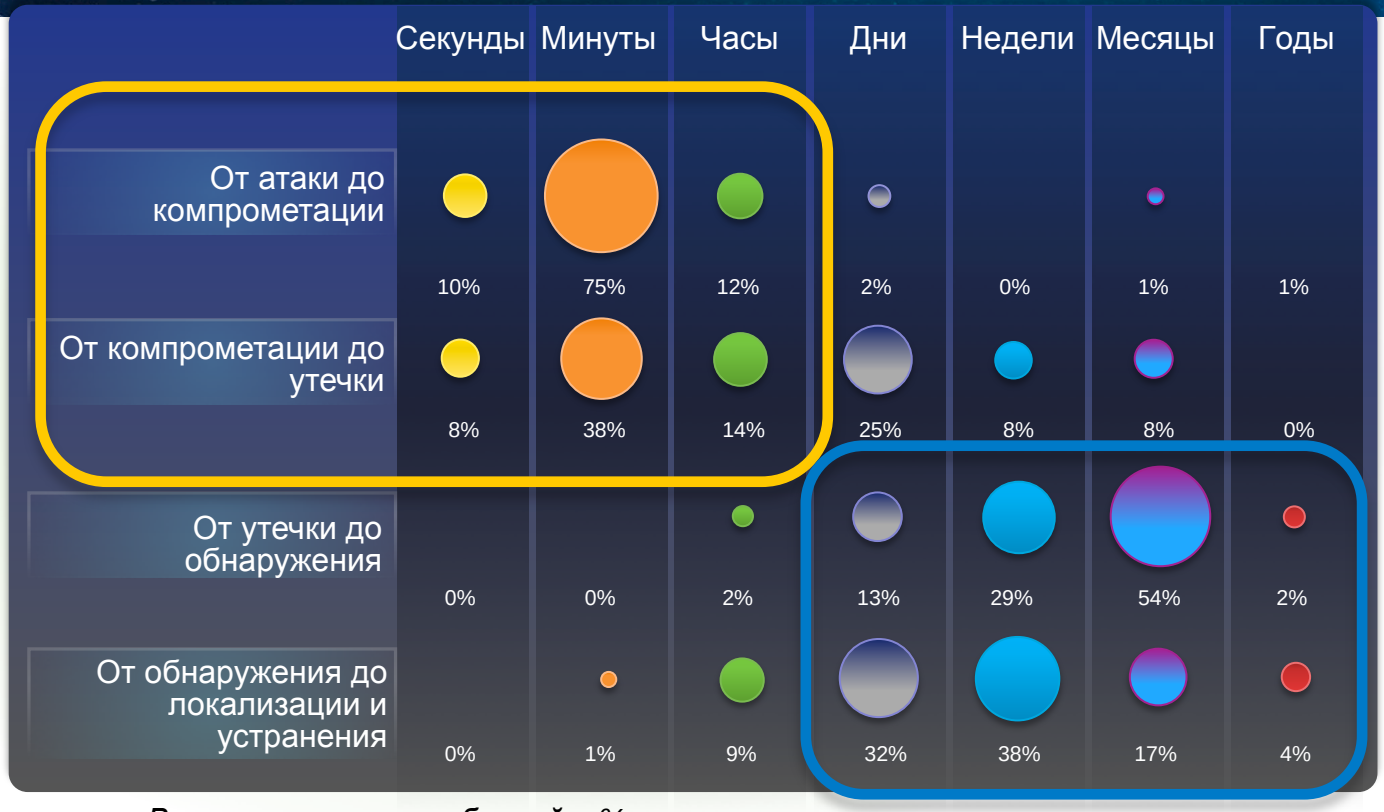
Многовекторные и продвинутые угрозы остаются незамеченными

Cisco Connect

Результат печален – такая защита проигрывает

Взломы осуществляются за минуты

Обнаружение и устранение занимает недели и месяцы

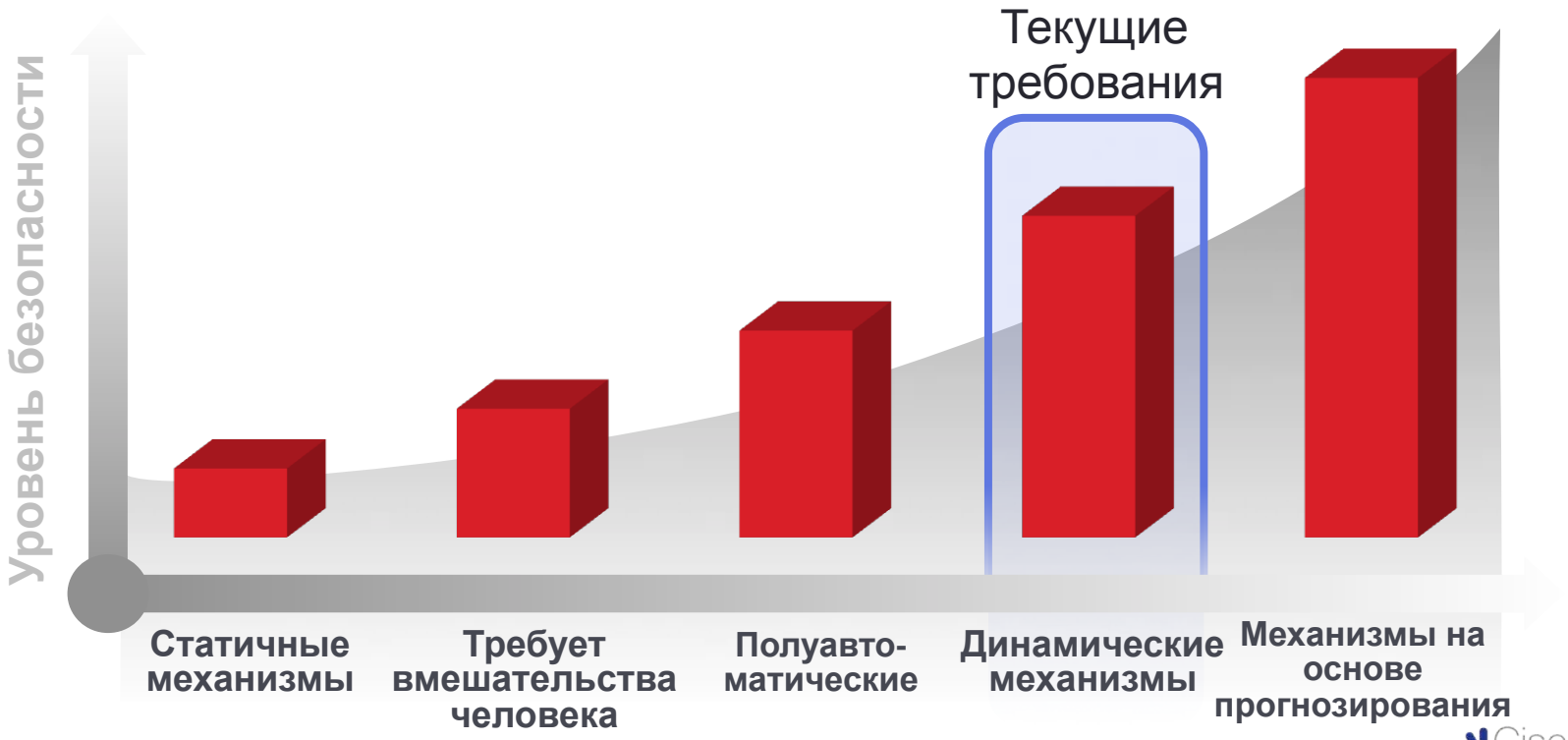


Временная шкала событий в % от общего числа взломов

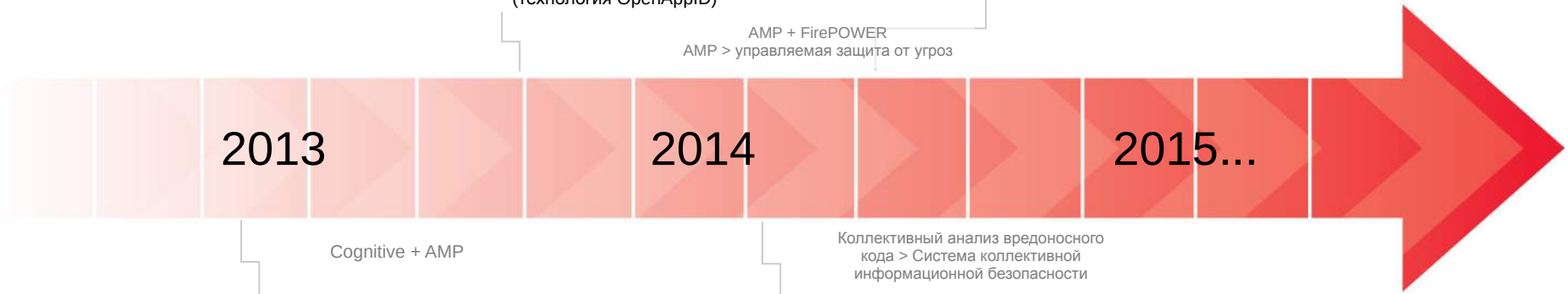
Источник: 2012 Verizon Data Breach Investigations

Cisco Connect

Эволюция механизмов безопасности



Cisco: информационная безопасность в центре внимания



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

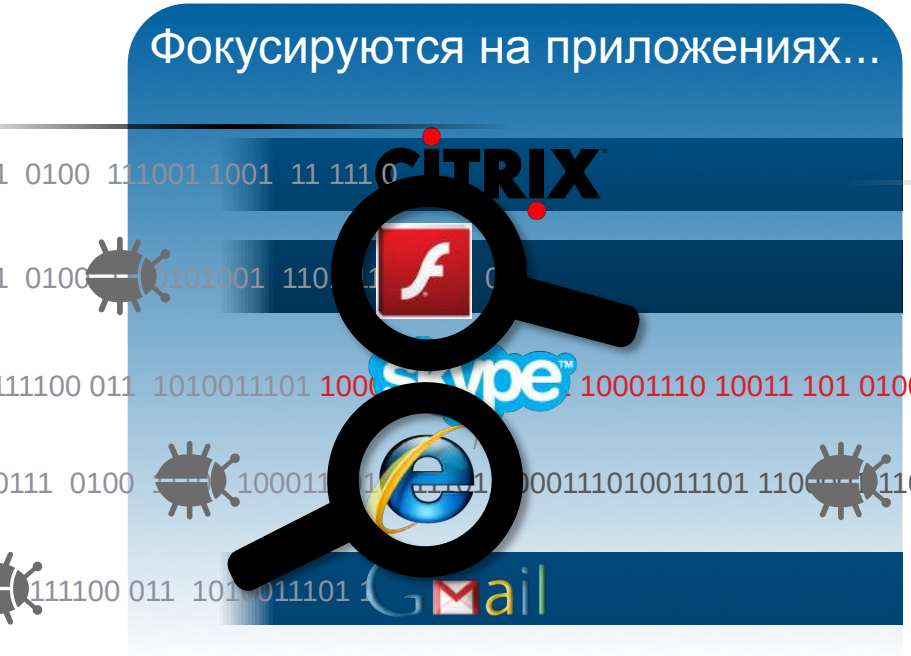
Коллективный анализ вредоносного кода > Система коллективной информационной безопасности

Приобретение компании ThreatGRID

- Коллективный анализ вредоносного кода
- Анализ угроз

Cisco Connect

Что не так с современными межсетевыми экранами?

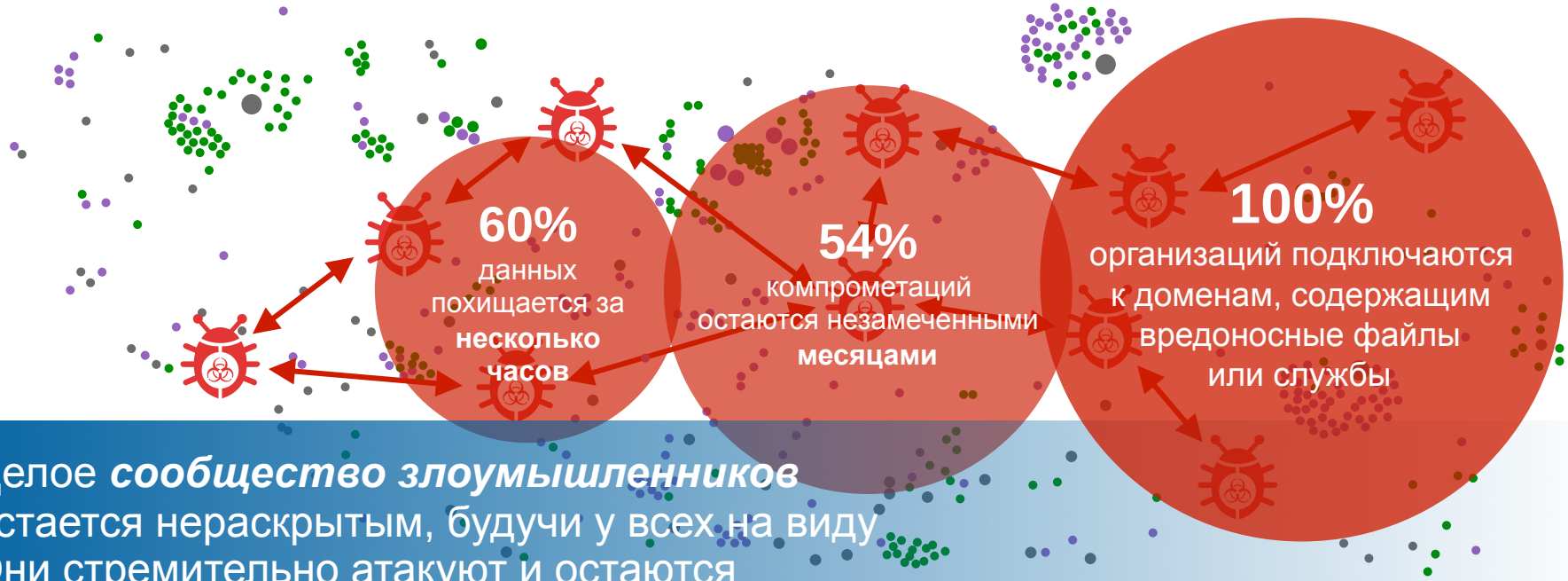


Но полностью упускают из вида угрозы

МСЭ нового поколения могут уменьшить область атаки, но усовершенствованный вредоносный код часто обходит защитные механизмы.

Cisco Connect

Современный ландшафт угроз требует большего, чем просто контроль приложений



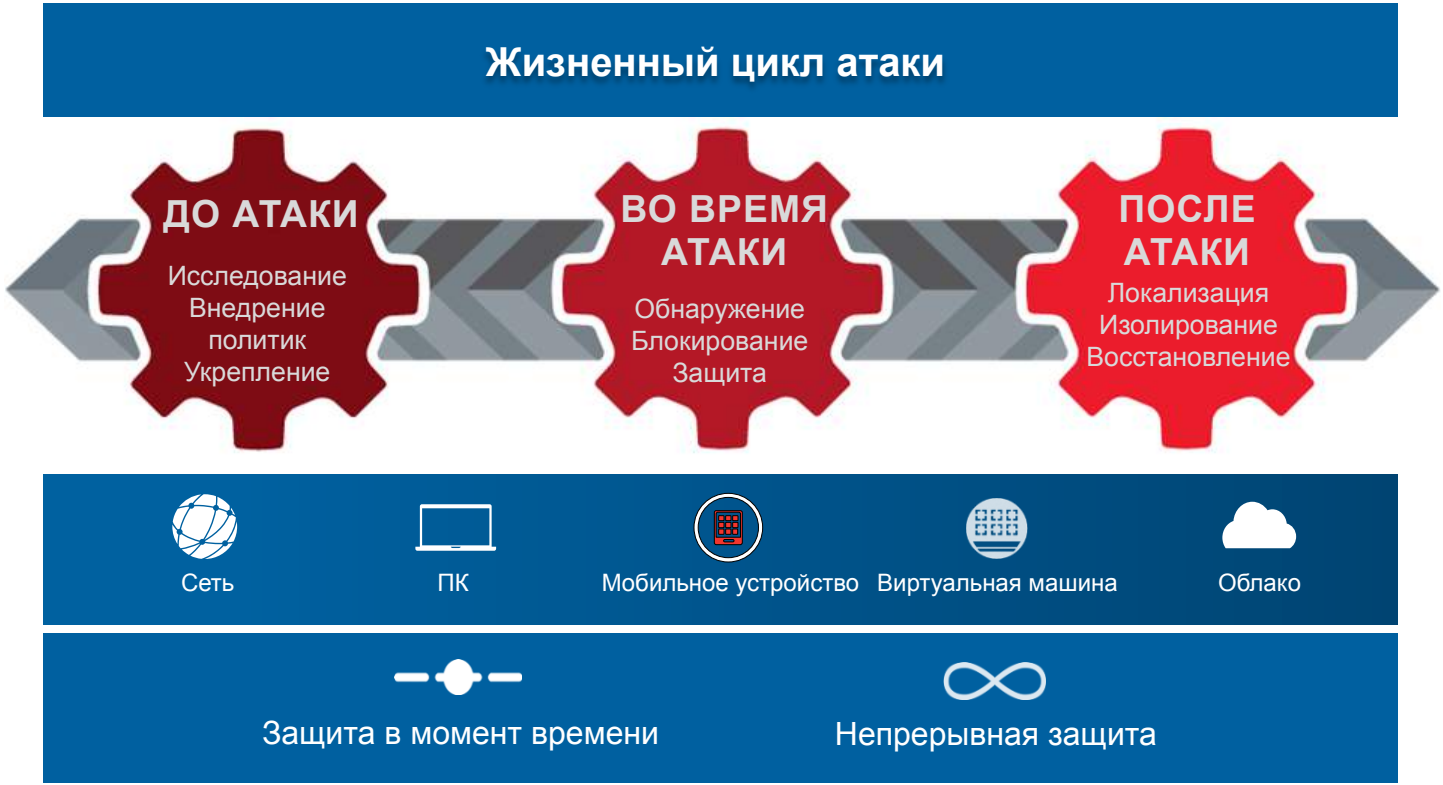
Целое ***сообщество злоумышленников*** остается нераскрытым, будучи у всех на виду
Они стремительно атакуют и остаются неуловимыми

Cisco Connect

«Будь неуловимым, почти бесформенным. Будь скрытным, почти беззвучным. Тогда ты сможешь направлять судьбу врага как тебе угодно»

Сунь Цзы. Искусство войны.

Комплексная защита от угроз для всего жизненного цикла атаки



Cisco Connect

Комплексная многоуровневая защита на основе межсетевого экрана Cisco ASA

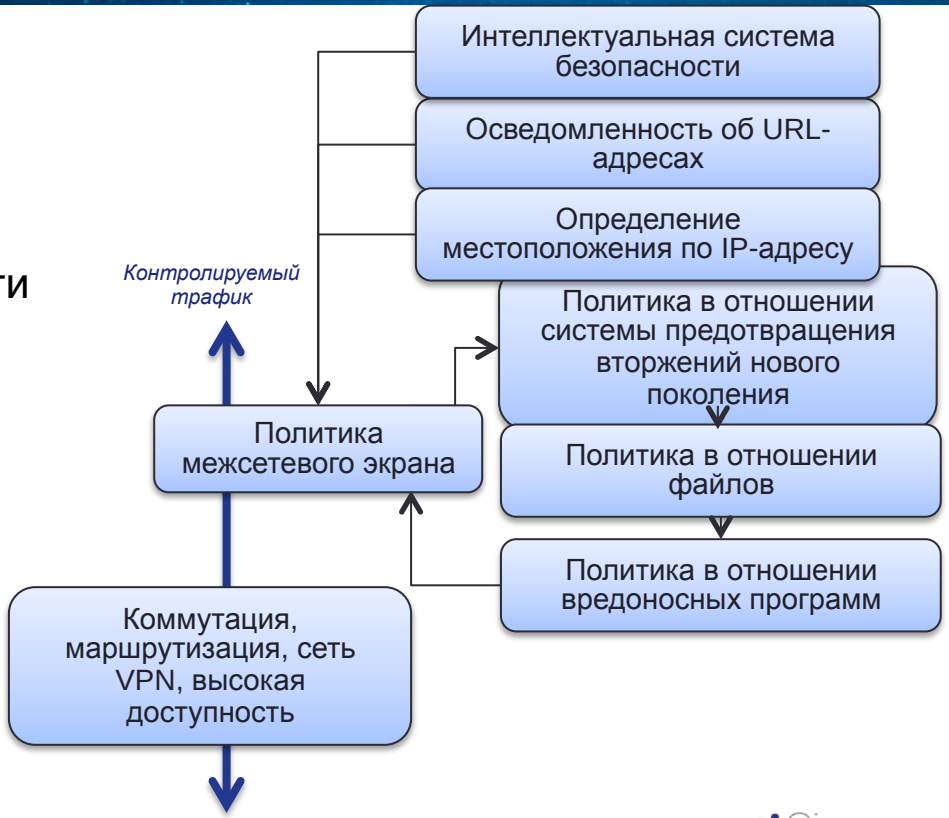
- Самый популярный межсетевой экран корпоративного класса с функцией контроля состояния соединений
- Детальный мониторинг и контроль приложений (Cisco® AVC)
- Ведущая в отрасли система предотвращения вторжений следующего поколения (NGIPS) с технологией FirePOWER
- Фильтрация URL-адресов на основе репутации и категоризации
- Система защиты от вредоносного кода Advanced Malware Protection с функциями ретроспективной защиты

В основе лежит платформа Cisco ASA 5500-X и 5585-X

- Высокопроизводительная масштабируемая платформа
- Высокая доступность, надежность и отказоустойчивость
- Интеллектуальные сетевые сервисы
- Виртуализация, прозрачность функционирования
- Широкий модельный ряд
- Сертификация производства в ФСТЭК по 3-му и 4-му классу для МСЭ

Что такое FirePOWER Services?

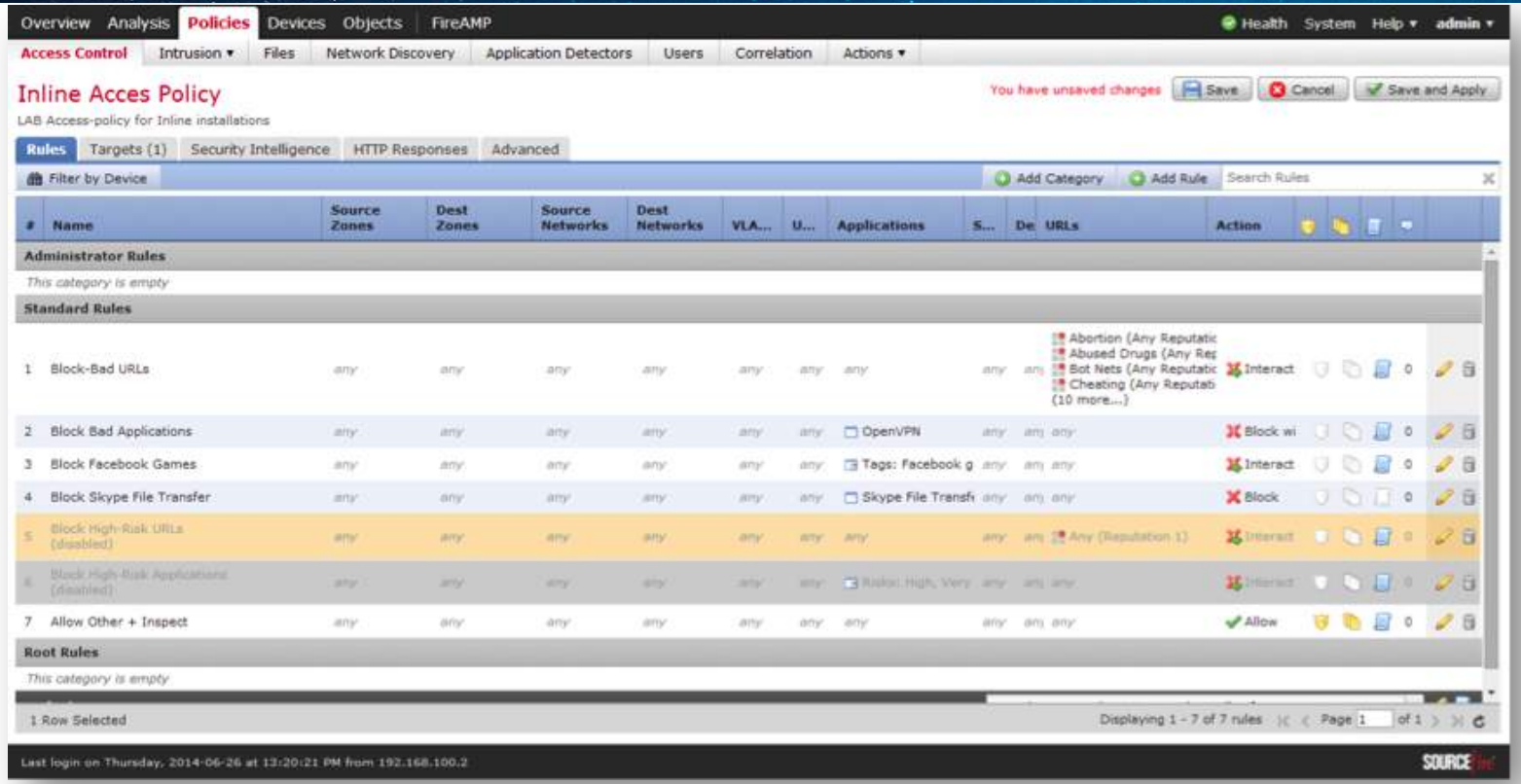
- Система предотвращения вторжений нового поколения – проверка содержимого
- Учет контекста
- Интеллектуальная система безопасности – управление черными списками
- Полный контроль доступа:
  - По зоне сети, VLAN, IP, порту, протоколу, приложению, пользователю, URL-адресу
- И все эти компоненты прекрасно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



Максимальная прозрачность сетевой активности

Категории	Технологии FirePOWER	Обычные IPS	МСЭ нового поколения
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	✓	✗	✗

Как выглядит пример политики NGFW?

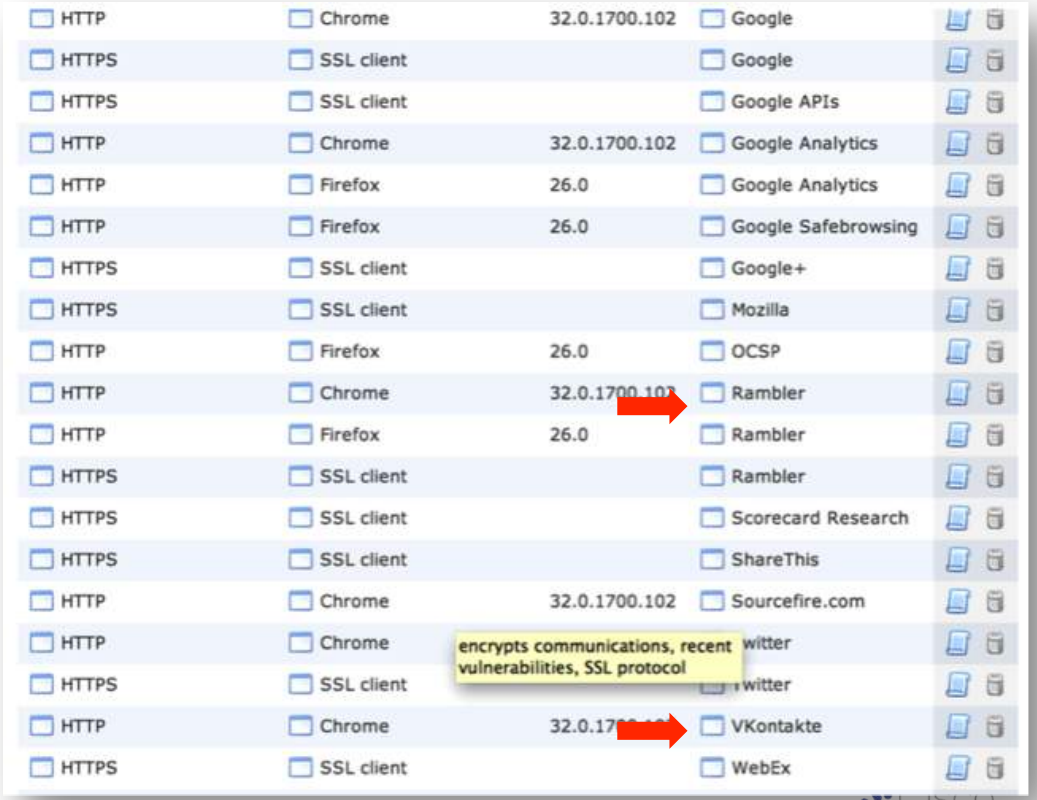


Cisco Connect

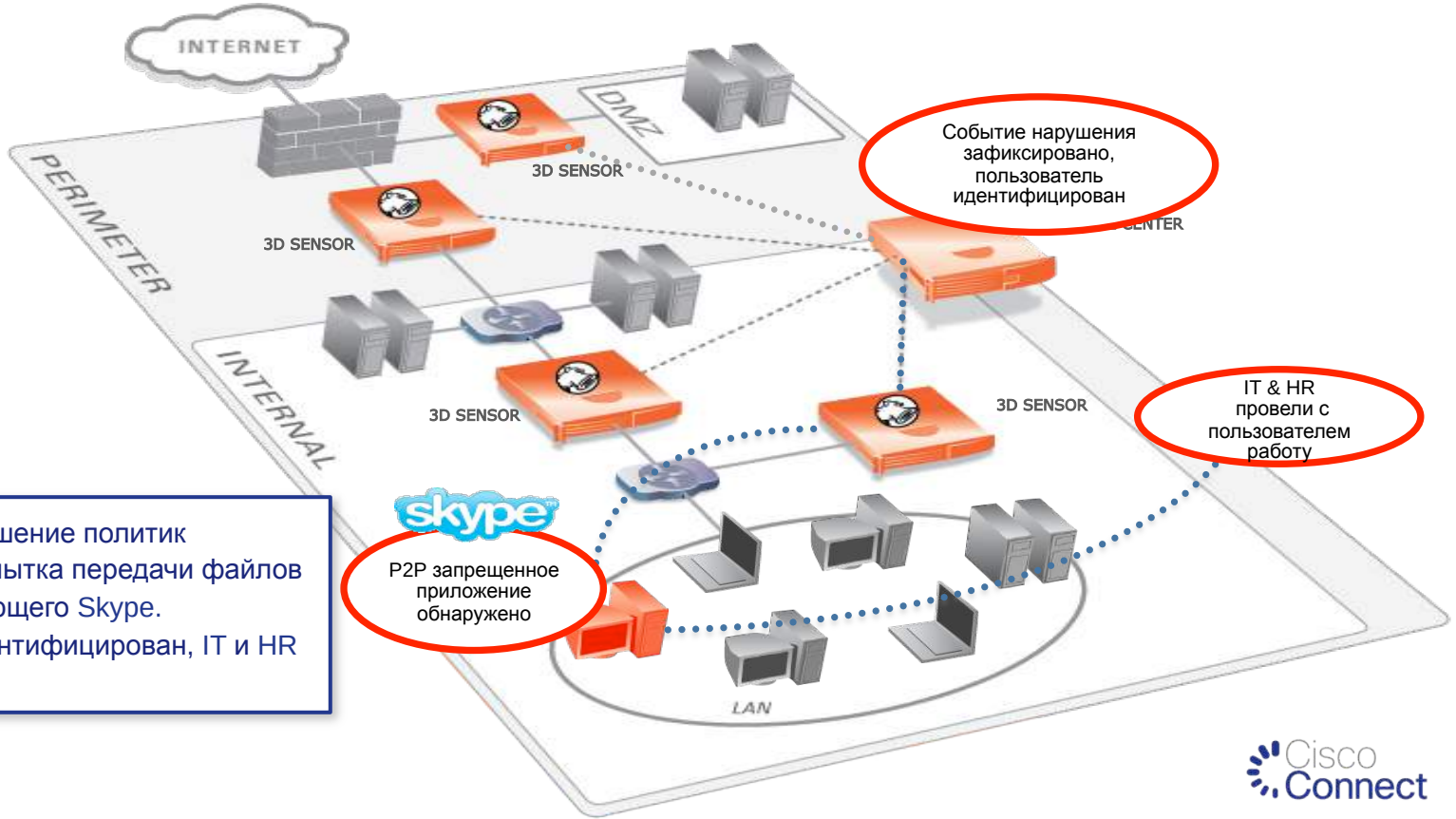
Распознавание приложений

- Анализ сетевого трафика позволяет распознавать широкий спектр различных приложений, которые затем можно использовать в правилах политики безопасности
- FirePOWER for ASA распознает приложения, используемые в России:

VKontakte, Rambler, Yandex и т.д.



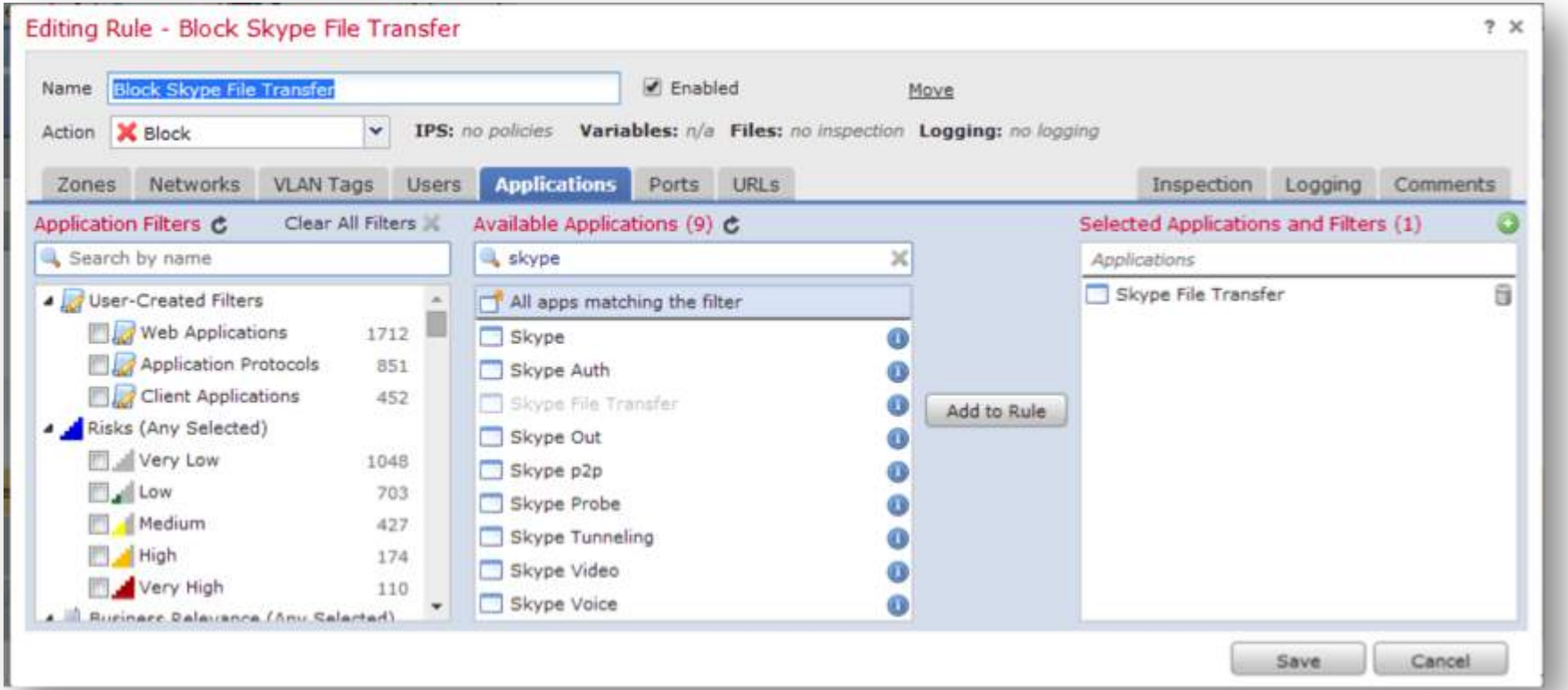
Идентификация приложений «на лету»



Обнаружено нарушение политик безопасности: Попытка передачи файлов с хоста, использующего Skype. Пользователь идентифицирован, IT и HR уведомлены.

Cisco Connect

Блокирование передачи файлов через Skype

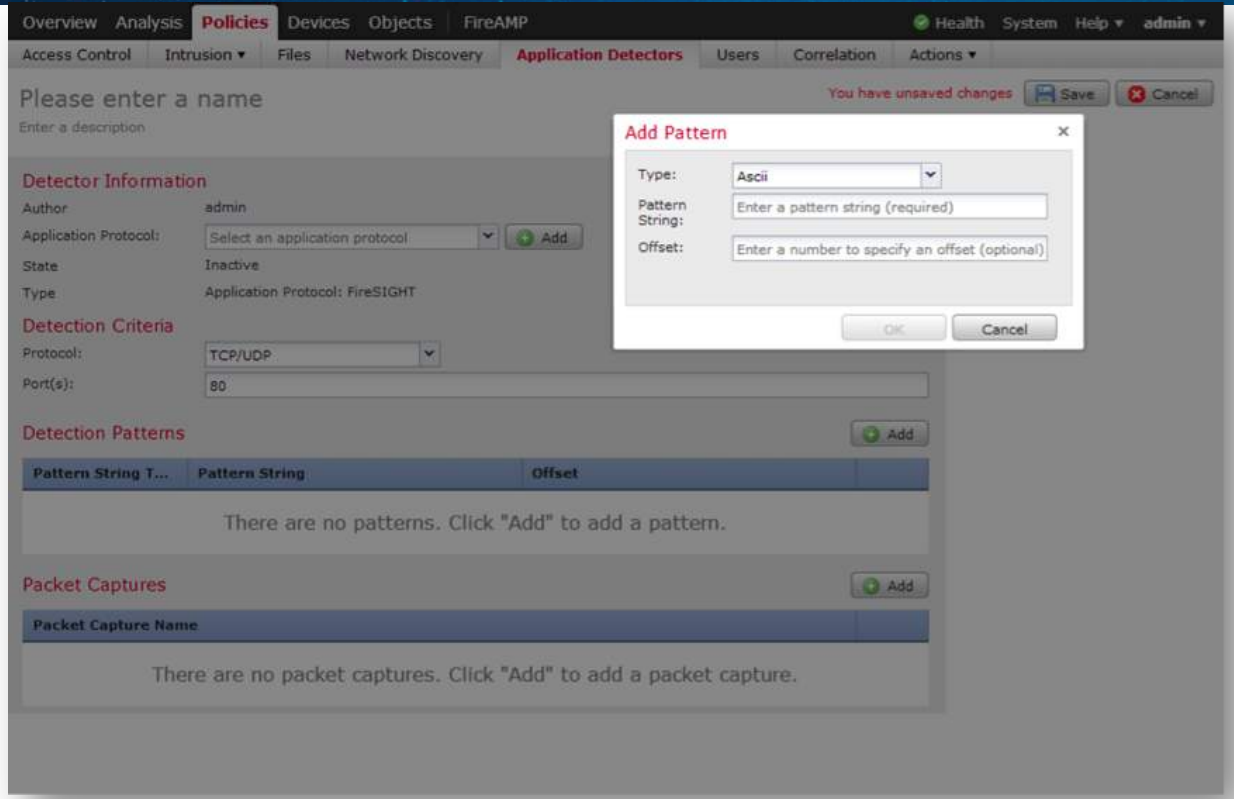


Cisco Connect

Описание собственных приложений

Приложения могут быть описаны с помощью шаблонов следующих форматов:

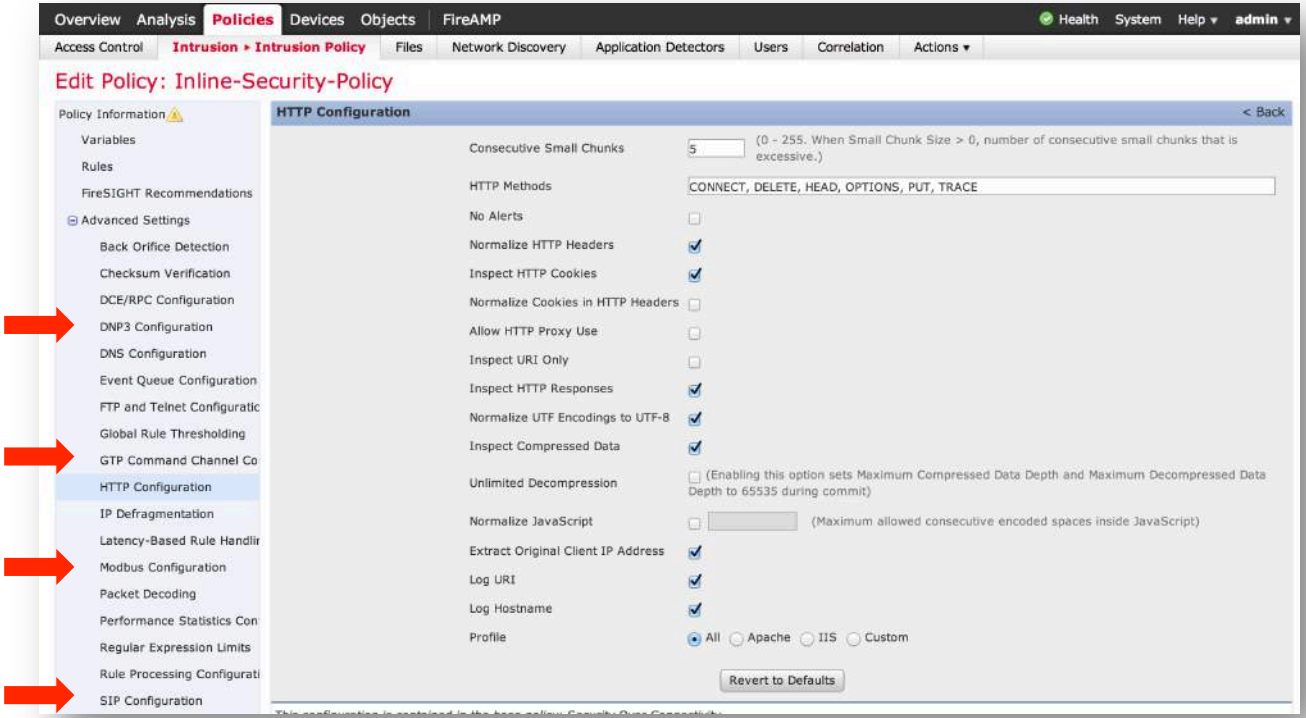
- ASCII
- HEX
- PCAP-файл



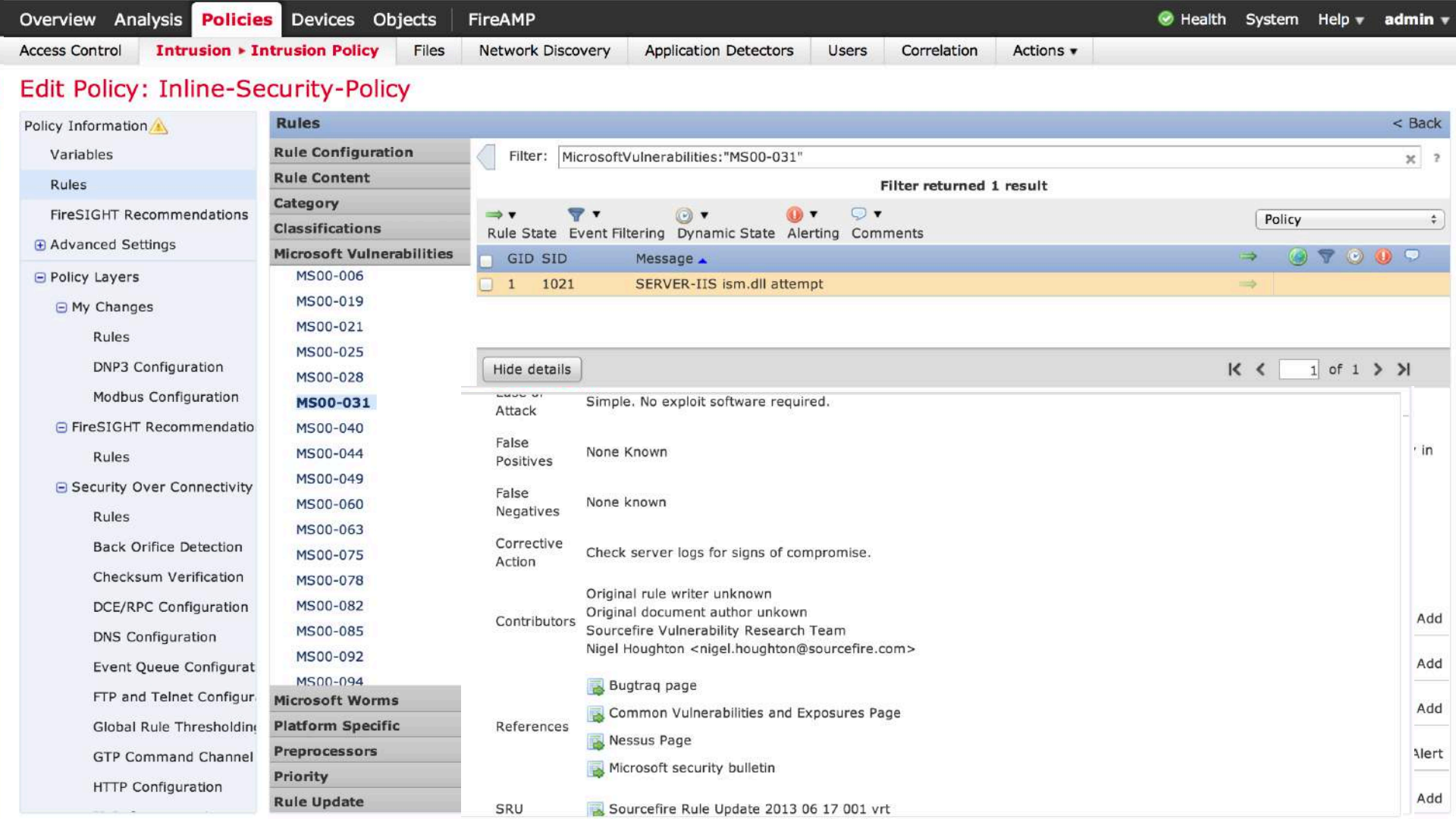
Cisco Connect

Система предотвращения вторжений: Препроцессоры для отдельных протоколов

- DCE/RPC
- DNS
- FTP и Telnet
- HTTP
- Sun RPC
- SIP
- GTP
- IMAP
- POP
- SMTP
- SSH
- SSL
- Modbus / DNP3

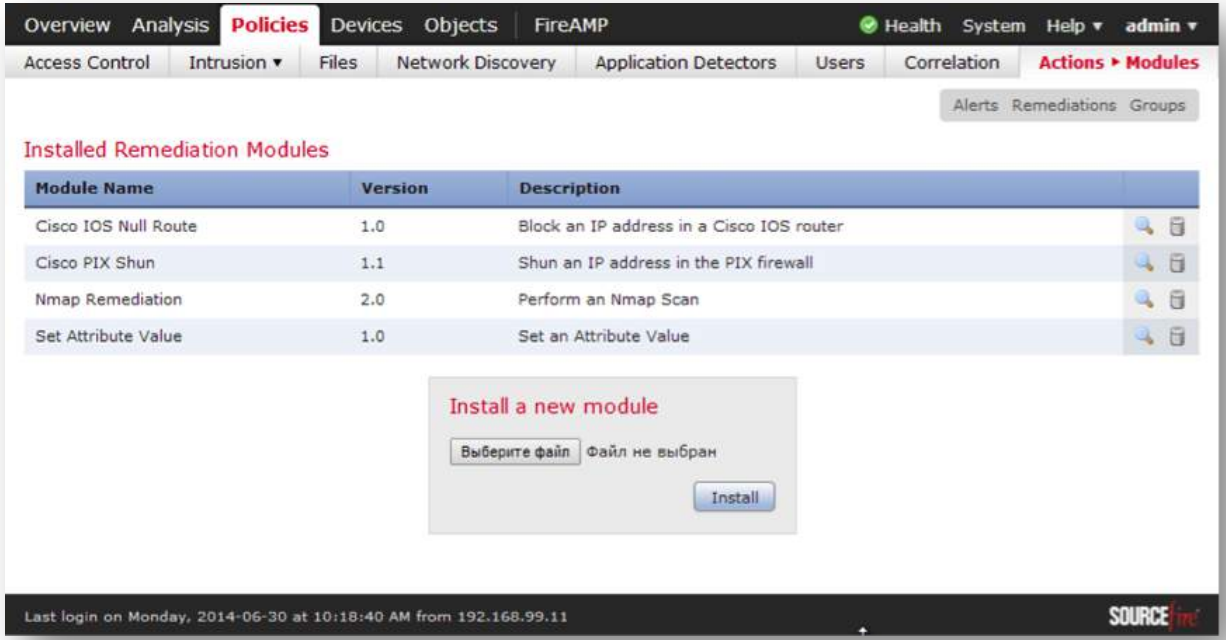


Cisco Connect


Overview Analysis Policies Devices Objects FireAMP
Health System Help admin
Access Control Intrusion ▸ Intrusion Policy Files Network Discovery Application Detectors Users Correlation Actions
Edit Policy: Inline-Security-Policy
Policy Information
Variables
Rules
FireSIGHT Recommendations
Advanced Settings
Policy Layers
My Changes
Rules
DNP3 Configuration
Modbus Configuration
FireSIGHT Recommendatio
Rules
Security Over Connectivity
Rules
Back Orifice Detection
Checksum Verification
DCE/RPC Configuration
DNS Configuration
Event Queue Configurat
FTP and Telnet Configur
Global Rule Thresholdin
GTP Command Channel
HTTP Configuration
Rules
< Back
Rule Configuration
Rule Content
Category
Classifications
Microsoft Vulnerabilities
MS00-006
MS00-019
MS00-021
MS00-025
MS00-028
MS00-031
MS00-040
MS00-044
MS00-049
MS00-060
MS00-063
MS00-075
MS00-078
MS00-082
MS00-085
MS00-092
MS00-094
Microsoft Worms
Platform Specific
Preprocessors
Priority
Rule Update
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
Add
Add
Add
Add

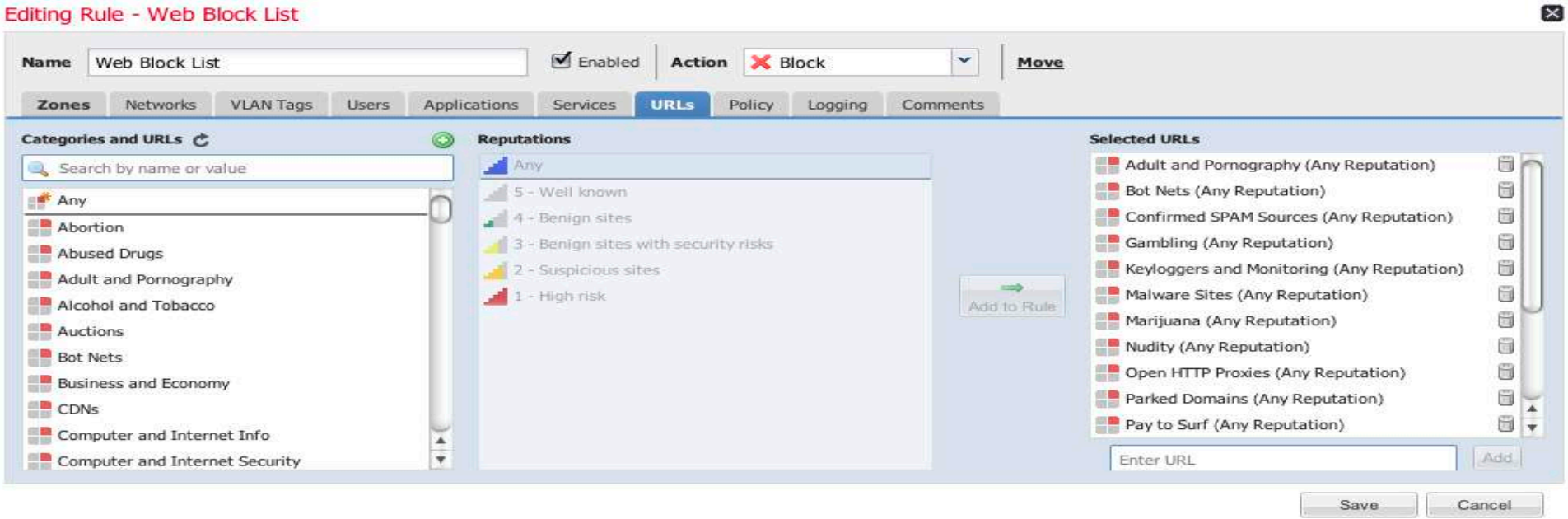
Реагирование на события

- Запуск сканирования NMAP с заданными параметрами на источник/направление атаки;
- Блокировка нарушителя на маршрутизаторе Cisco (RTBH);
- Блокировка нарушителя на МСЭ Cisco ASA;
- Установка необходимого атрибута на хост;
- Уведомление администратора посредством Email/SNMP/Syslog;
- Выполнение самописной программы, написанной на C, BASH, TCSH, Perl, с возможностью передачи переменных из события.



Cisco Connect

Фильтрация URL

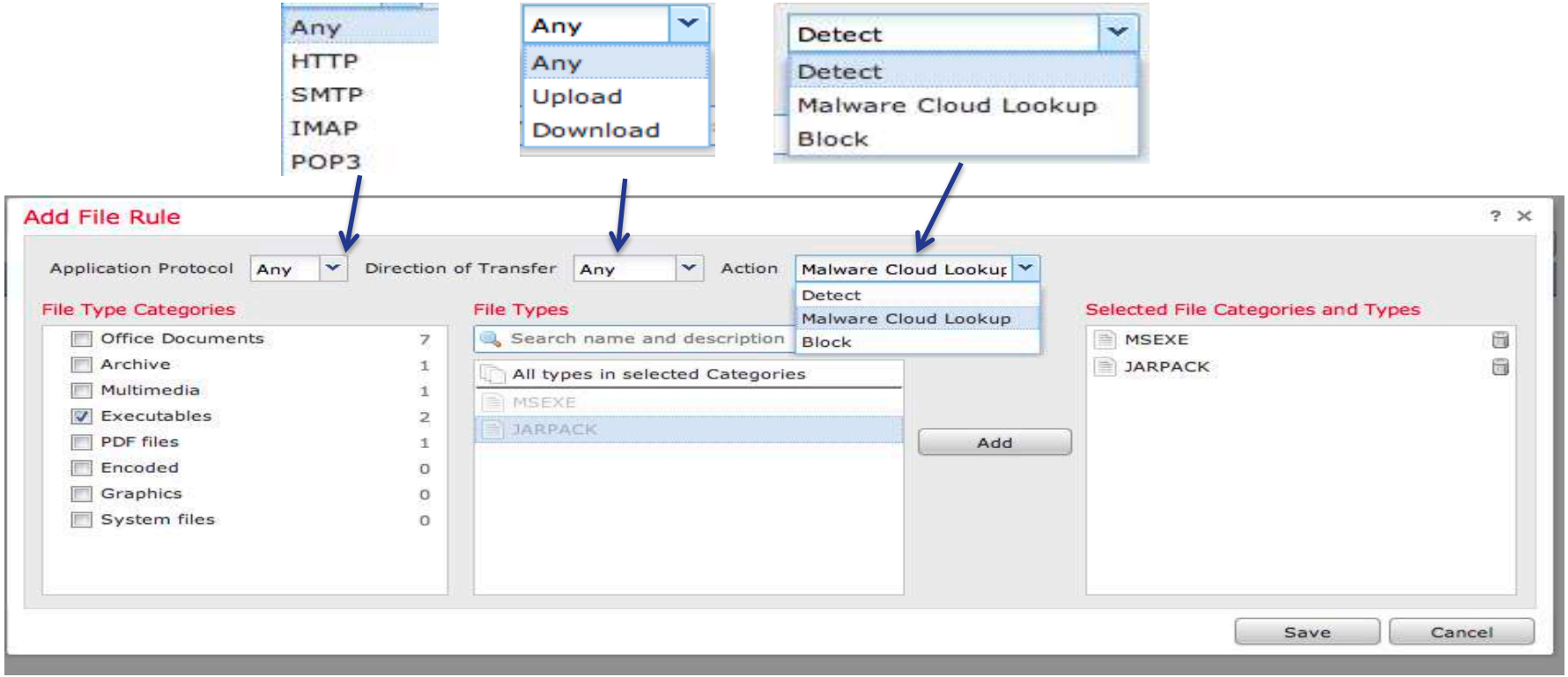


Различные категории URL

URLs категорированы по уровню рисков

Cisco Connect

Контроль по типам файлов и направлению передачи



Cisco Connect

Геолокация и визуализация местонахождения атакующих

Bad Guys

Top Events by Source Country

Country Name	Count
United States	162
Germany	36
China	18
Japan	13
France	11
Russia	4
North Korea	2
Pakistan	1
Iraq	1
Iran	1

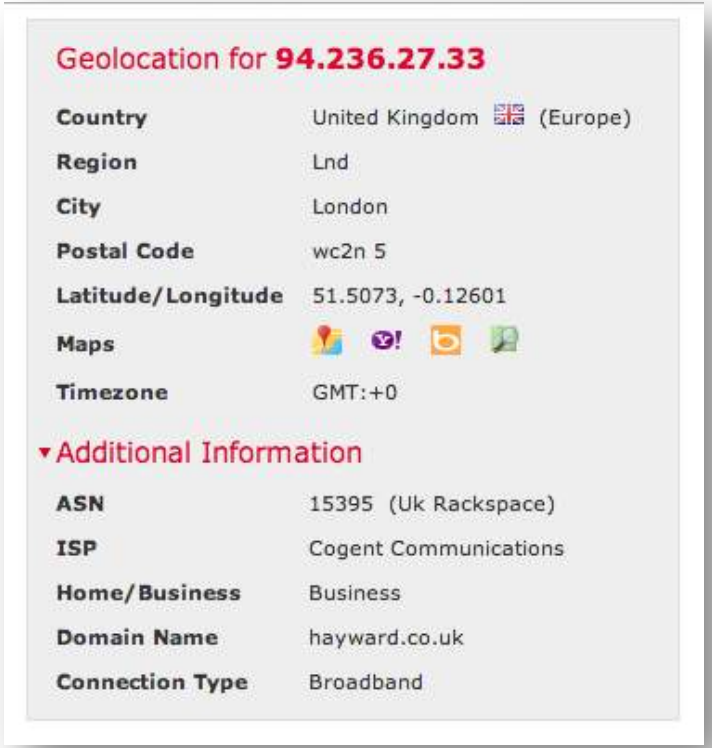
Last updated 1 minutes ago

Initiator IP	Initiator Location	Responder IP
76.100.209.66	USA	10.4.32.112
10.4.10.131		10.4.32.112
10.4.10.131		10.4.32.112
10.4.33.95		10.5.32.206
89.188.101.82	ISR	10.5.32.206
200.189.215.85	BRA	10.4.33.44
10.4.31.237		10.5.32.206
10.4.11.216		10.5.39.206

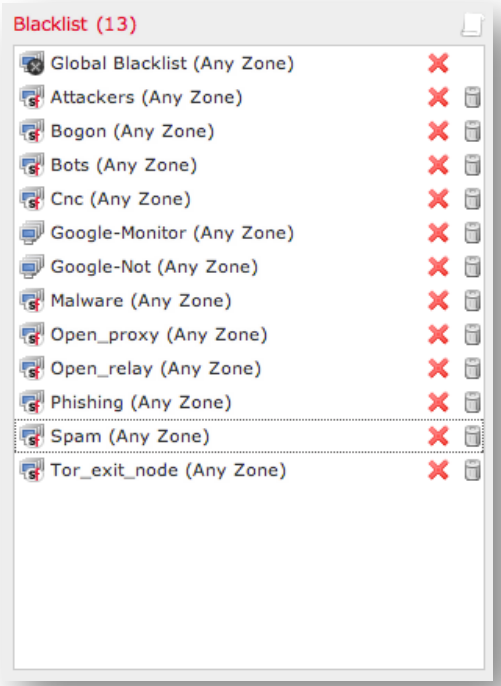
Визуализация карт, стран и городов для событий и узлов

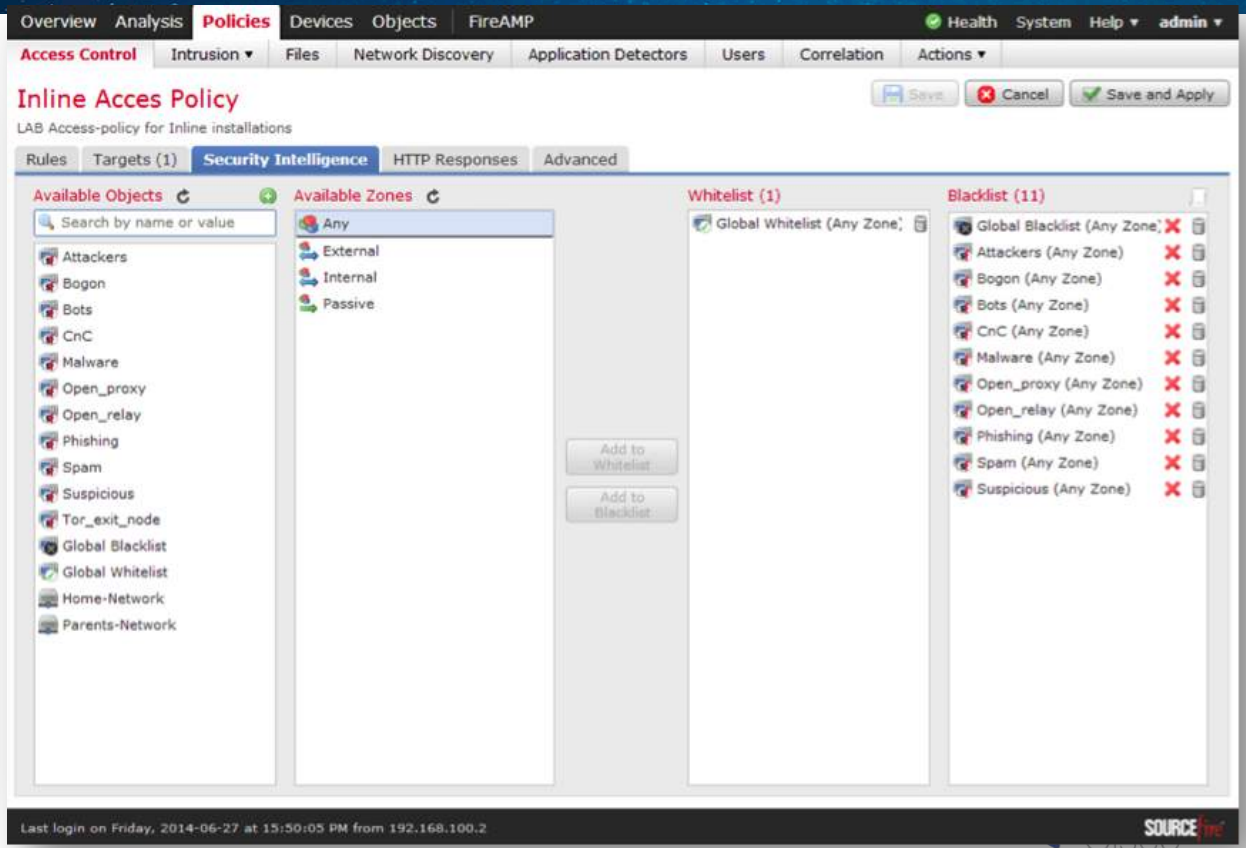
Детальная геолокация

- 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



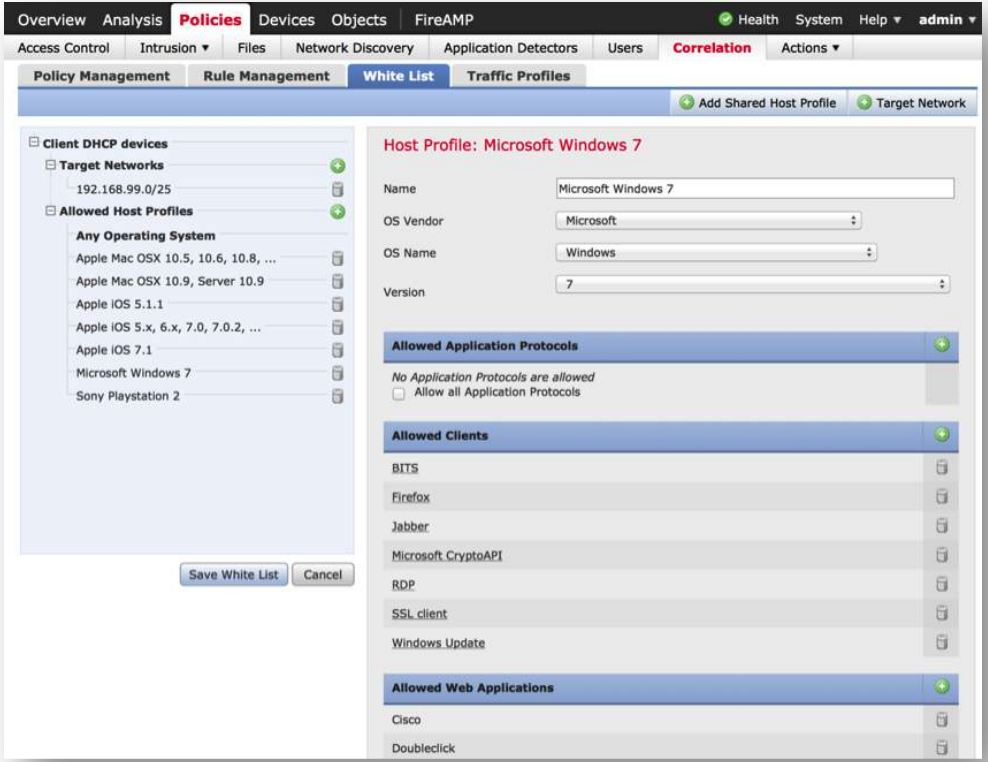
«Черные списки»: как свои, так и централизованные





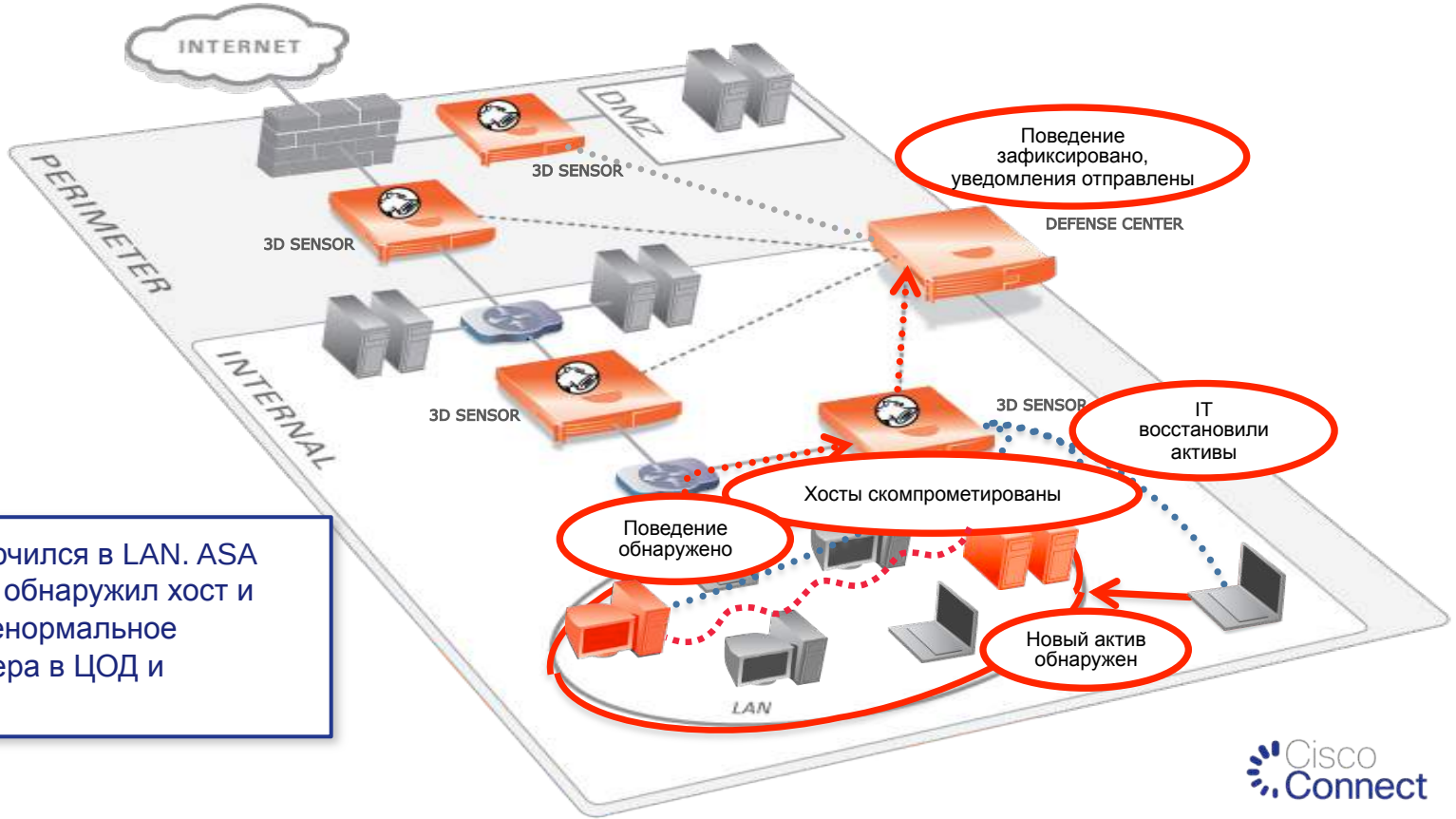
Создание «белых списков» / «списков соответствия»

- Разрешенные типы и версии ОС
- Разрешенные клиентские приложения
- Разрешенные Web-приложения
- Разрешенные протоколы транспортного и сетевого уровней
- Разрешенные адреса / диапазоны адресов
- И т.д.



Cisco Connect

Обнаружение «посторонних» / аномалий / несоответствий

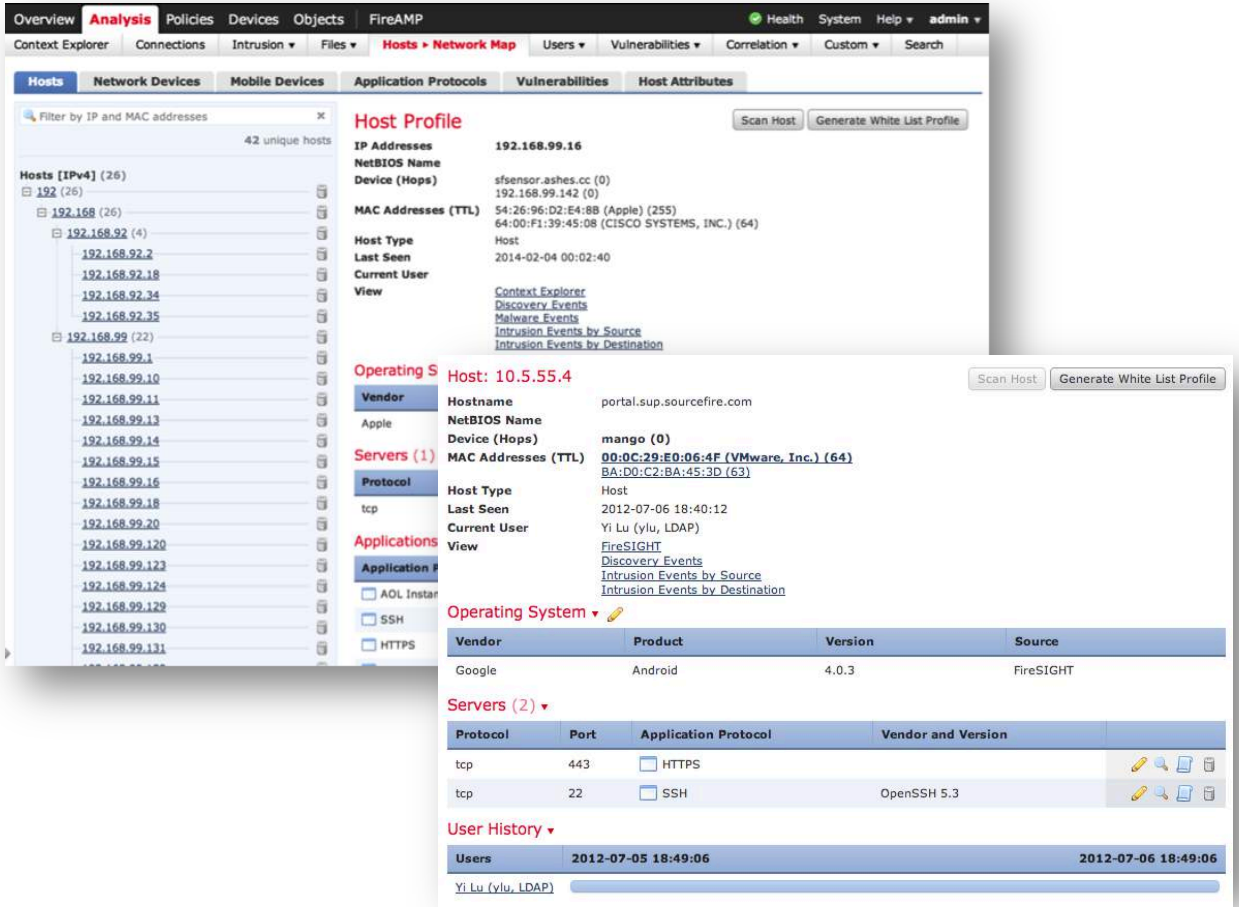


Новый хост включился в LAN. ASA with FirePOWER обнаружил хост и последующее ненормальное поведение сервера в ЦОД и уведомил IT.

Cisco Connect

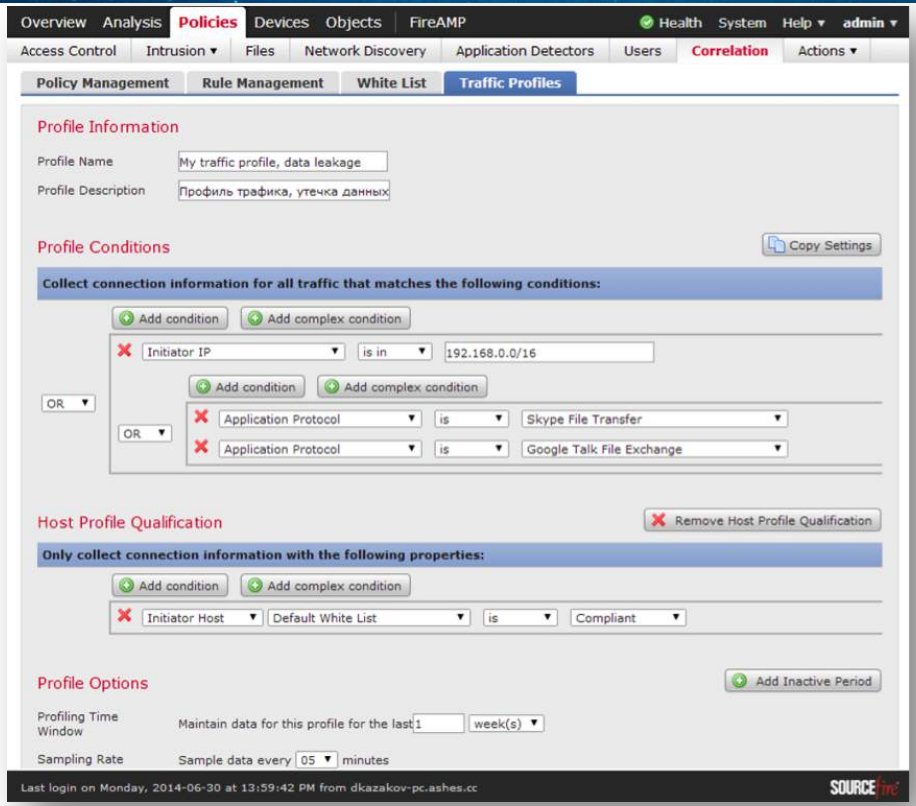
Инвентаризация и профилирование узлов

- 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



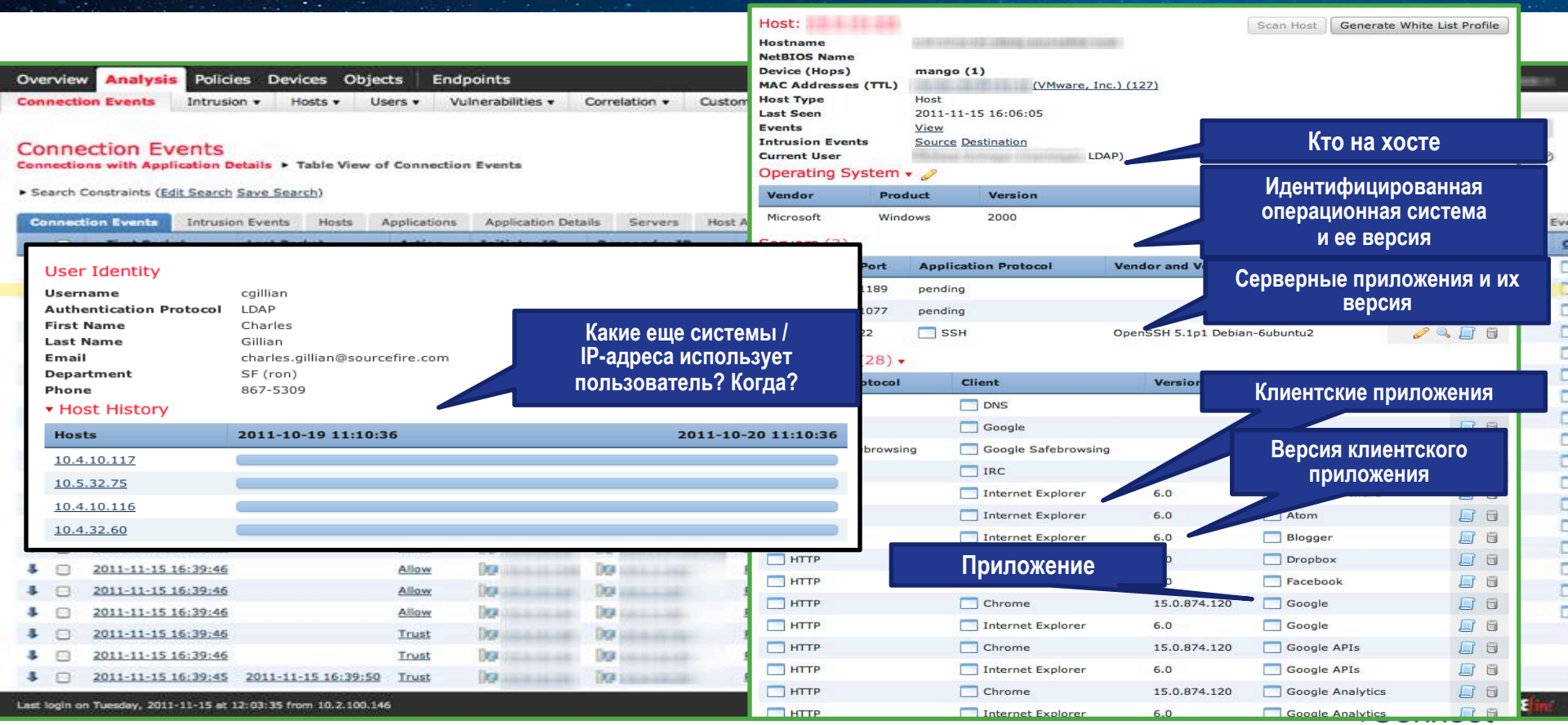
Профилирование трафика

- Профиль трафика может включать до 30 параметров соединения:
  - IP-, NetBIOS-, MAC-адреса
  - Сетевой протокол
  - Транспортный протокол
  - Прикладной протокол
  - И т.д.
- Позволяет устанавливать флаги состояний и т.д.

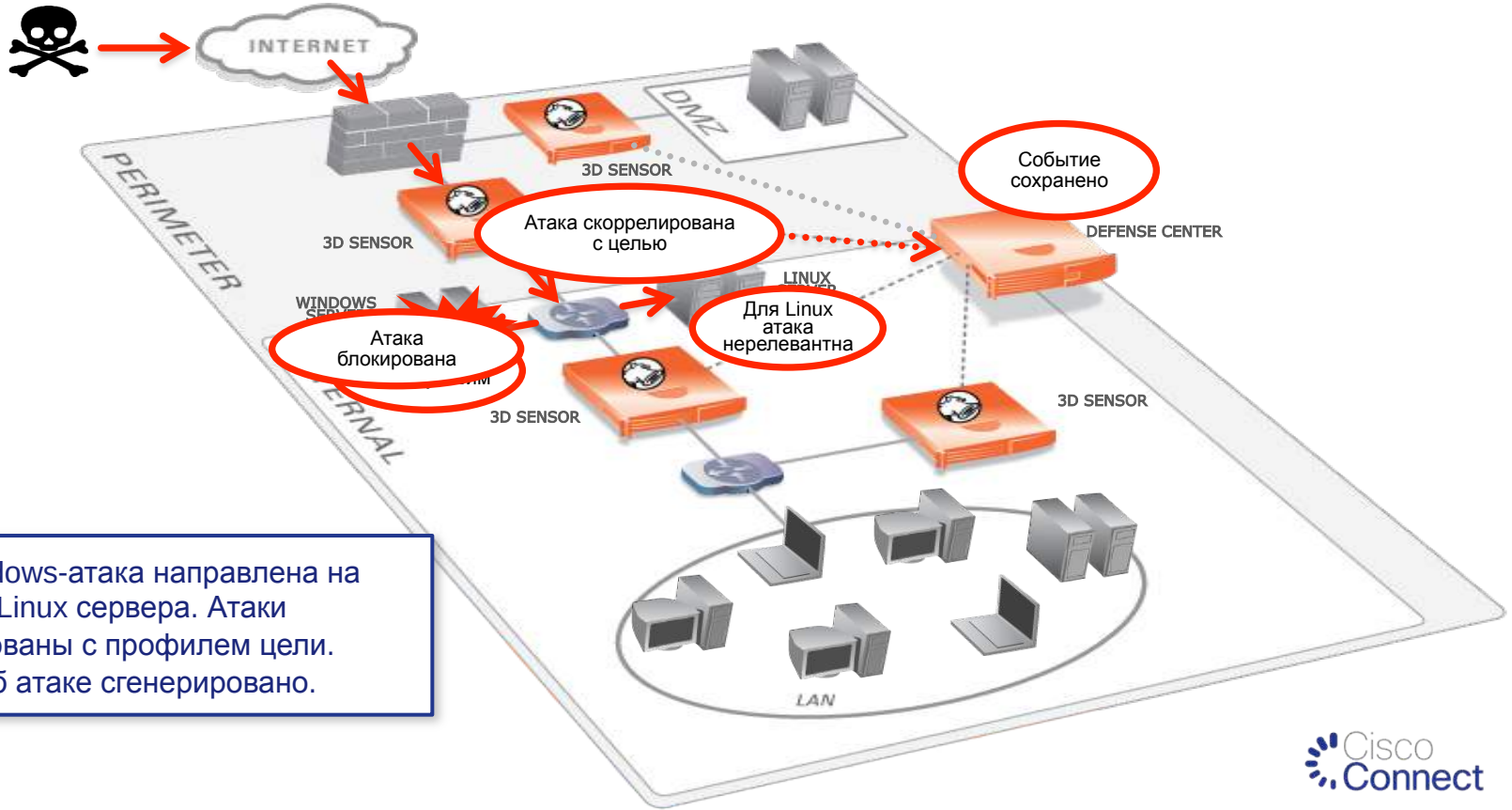


Cisco Connect

Анализ происходящего на узлах



Встроенная корреляция событий безопасности



Новая Windows-атака направлена на Windows и Linux сервера. Атаки скоррелированы с профилем цели. Событие об атаке сгенерировано.

Cisco Connect

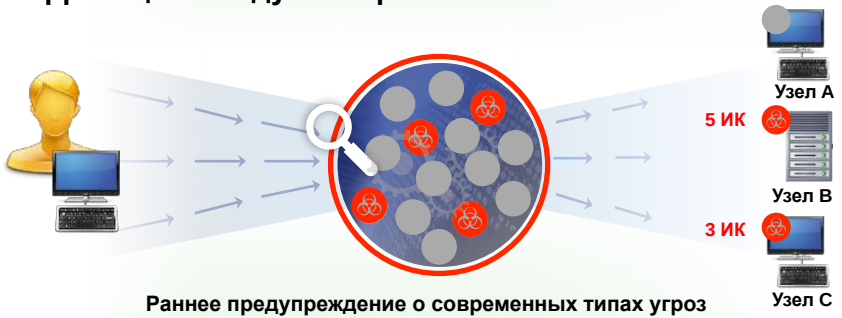
Автоматизированная, комплексная защита от угроз

Максимальная защита во время всего жизненного цикла атаки

Корреляция между контекстом и угрозами

Оценка вредоносного воздействия

Корреляция между векторами атаки

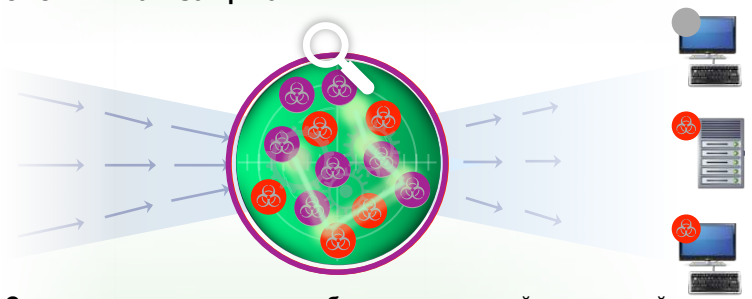


Раннее предупреждение о современных типах угроз

Динамические механизмы безопасности

Адаптация политик к рискам

Ретроспективная защита

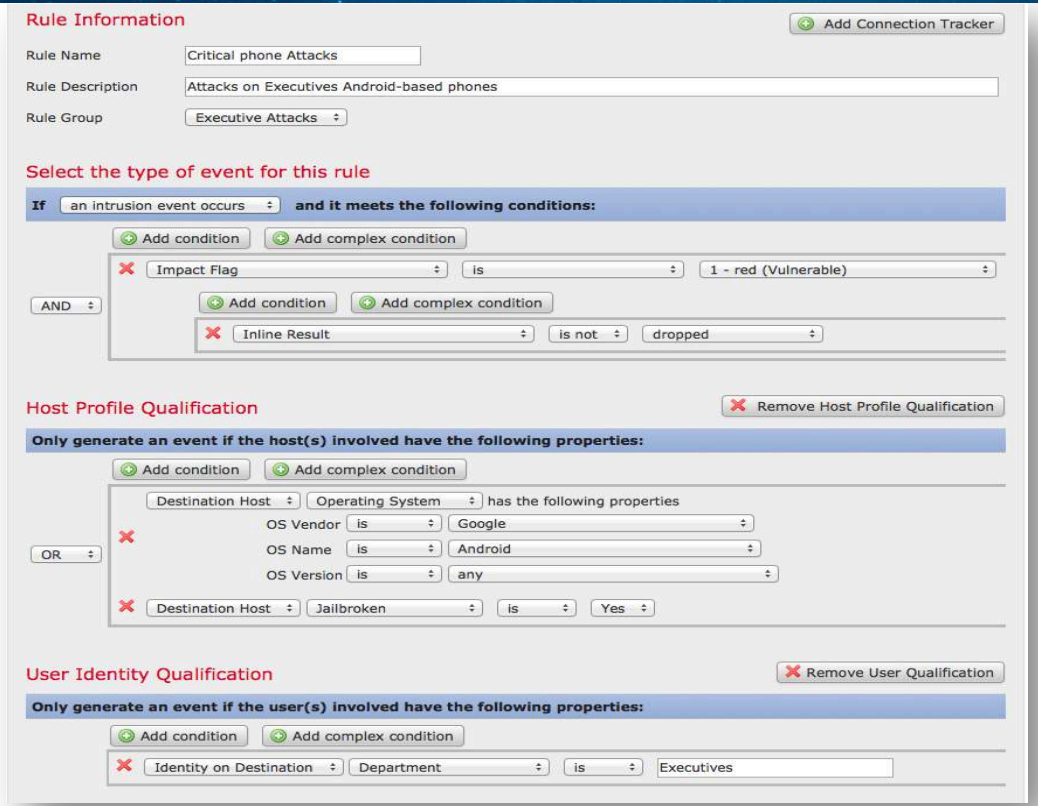


Сокращение времени между обнаружением и нейтрализацией

Cisco Connect

Встроенная система корреляции событий

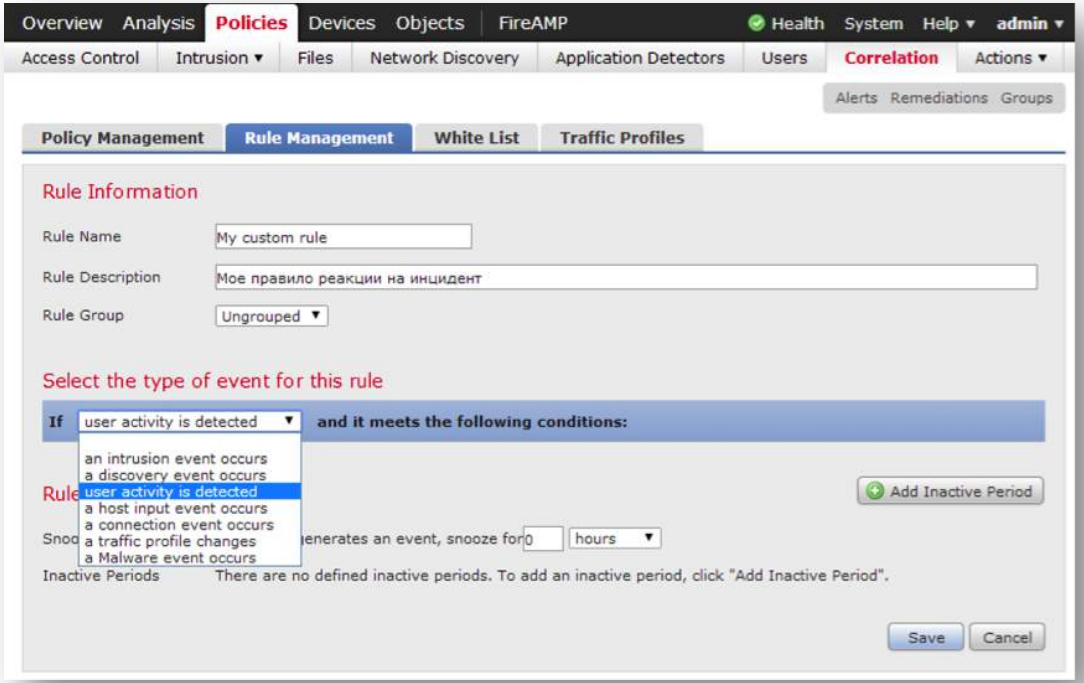
- Правила корреляции могут включать любые условия и их комбинации на базе идентифицированных в сети данных
  - Приложения
  - Уязвимости
  - Протоколы
  - Пользователи
  - Операционные системы
  - Производитель ОС
  - Адреса
  - Место в иерархии компании
  - Статус узла и т.п.



Cisco Connect

Встроенная система корреляции событий

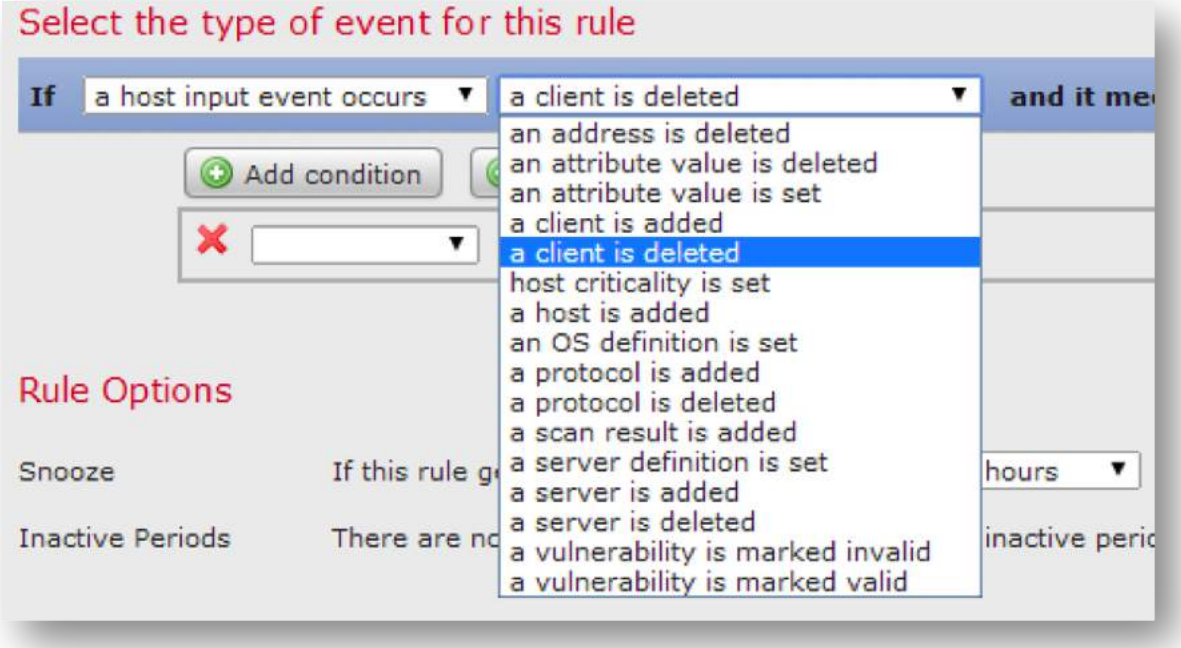
- Различные типы события для системы корреляции
  - Атаки / вторжение
  - Активность пользователя
  - Установлено соединение
  - Изменение профиля трафика
  - Вредоносный код
  - Изменение инвентаризационных данных (например, появление нового узла в сети или ОС на узле)
  - Изменение профиля узла
  -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



Cisco Connect

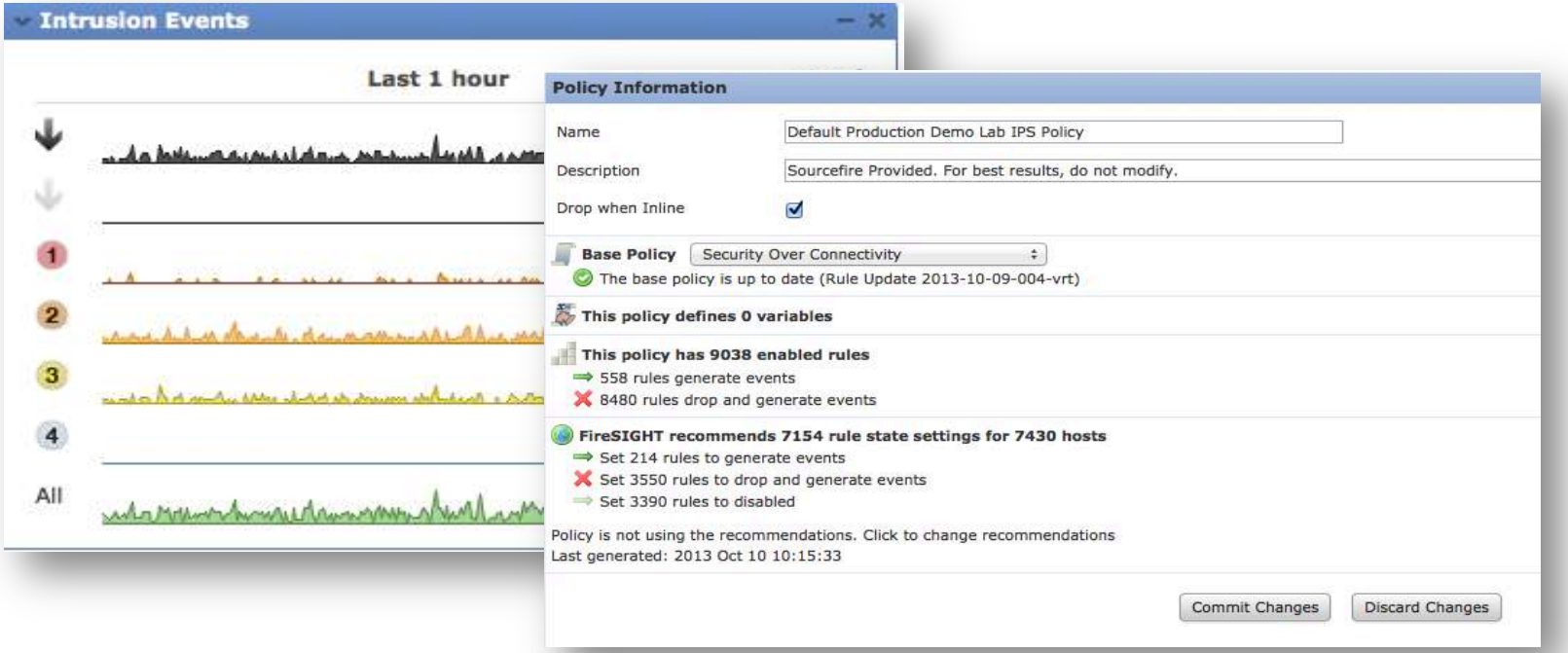
Встроенная система корреляции событий

- В зависимости от типа события могут быть установлены дополнительные параметры системы корреляции
- Возможность создания **динамических** политик безопасности



Cisco Connect

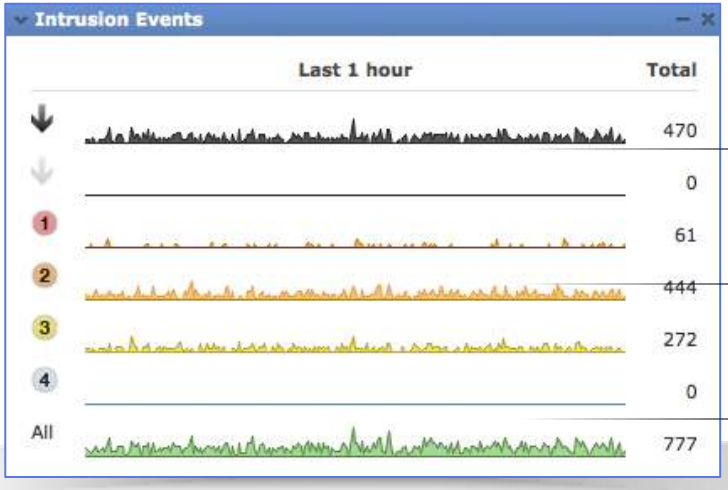
Автоматизация создания и настройки политик



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

Cisco Connect

Оценка вредоносного воздействия



Каждой попытке вторжения или событию 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

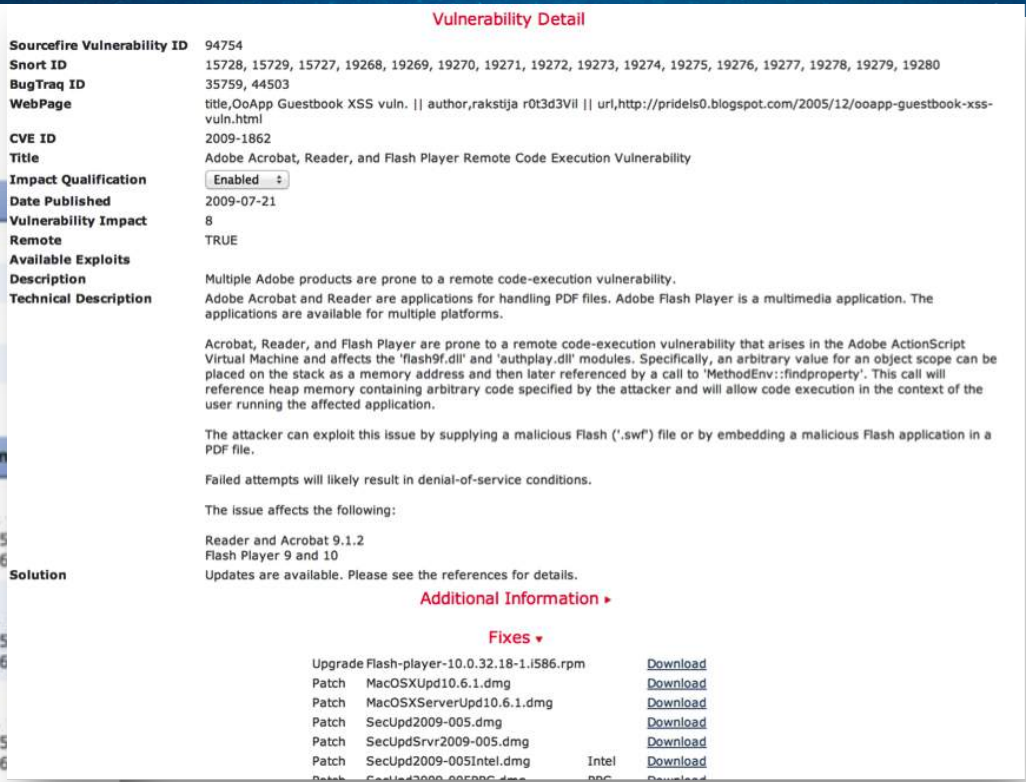
Host Criticality None

Host Protocols

Protocol	Layer
icmp	Transport
tcp	Transport
udp	Transport
IP	Network

Vulnerabilities (362)

Name	Remote	Componen
Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability	Yes	Mac OSX 10.5, 10.6, Server 10.5 Server 10.6
Adobe Flash Player and AIR 'intf_count' Integer Overflow Vulnerability	Yes	Mac OSX 10.5, 10.6, Server 10.5 Server 10.6
Adobe Flash Player and AIR (CVE-2009-1866) Stack Buffer Overflow Vulnerability	Yes	Mac OSX 10.5, 10.6, Server 10.5 Server 10.6



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

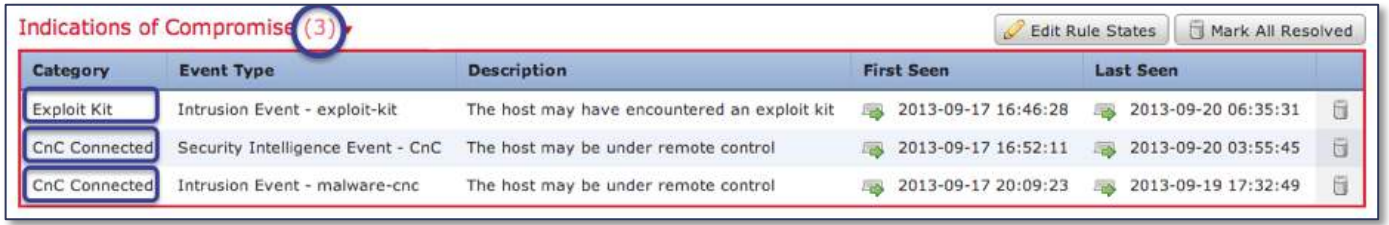
Fixes

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

Cisco Connect

Признаки компрометации

- **События СОВ**
  - Бэкдоры
  - Наборы эксплойтов
  - Атаки на веб-приложения
  - Подключения к серверам управления и контроля ботнетов
  - Получение администраторских полномочий
- **События анализа ИБ**
  - Подключения к известным IP серверов управления и контроля ботнетов
- **События, связанные с вредоносным кодом**
  - Обнаружение вредоносного кода
  - Компрометация Office/PDF/Java
  - Выполнение вредоносного кода
  - Обнаружение дроппера

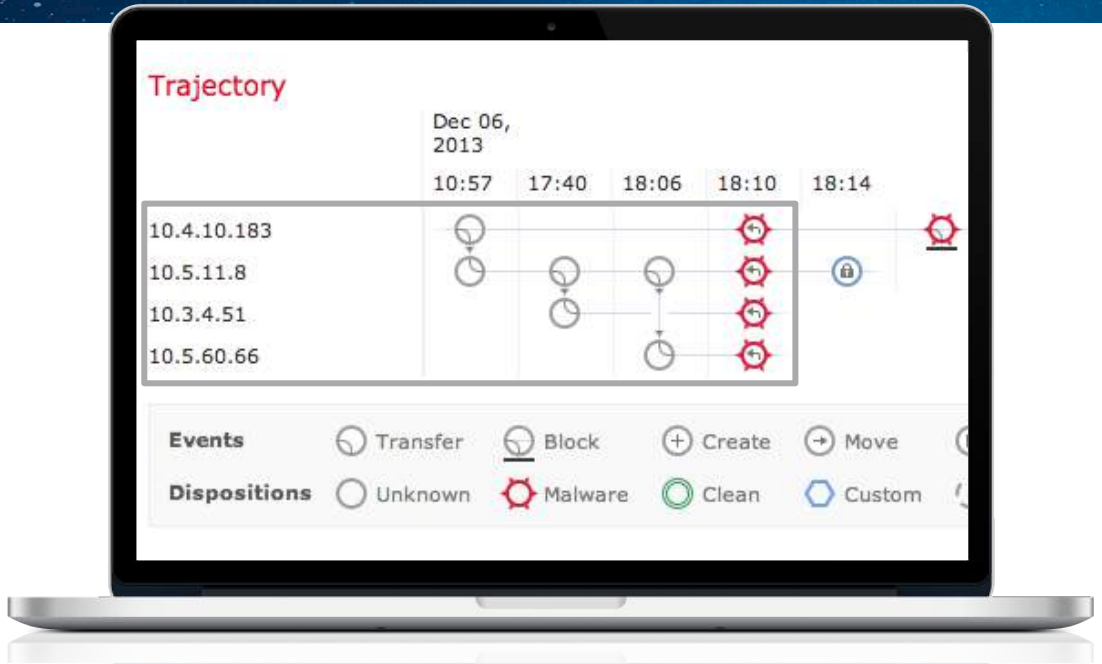


Анализ траектории движения вредоносных программ

Сеть

Конечные устройства

Контент



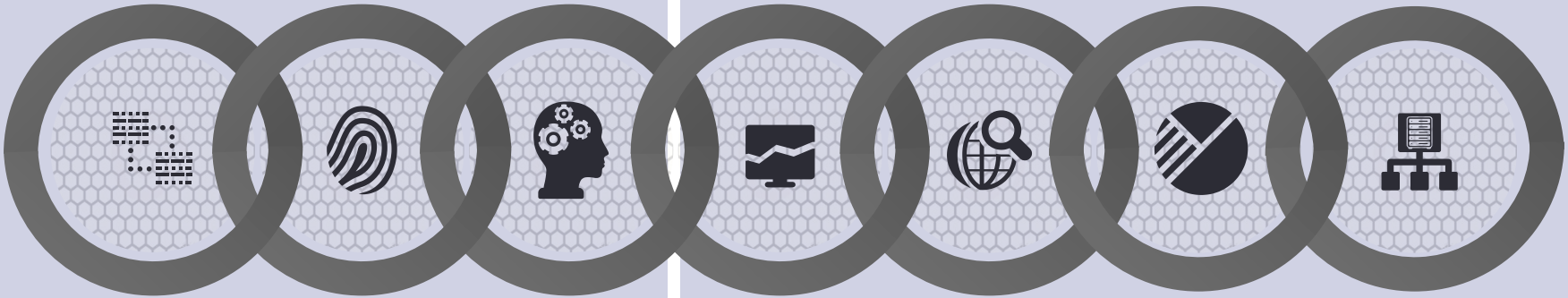
- Сетевая платформа использует признаки компрометации, анализ файлов и траекторию движения файла для того, чтобы показать, как вредоносный файл перемещается по сети, откуда он появился, что стало причиной его появления и кто еще пострадал от него

Cisco Connect

Обнаружение вредоносного кода с помощью AMP

Фильтрация по репутации

Поведенческое обнаружение



Идентичная сигнатура

Нечеткие идентифицирующие метки

Машинное обучение

Признаки компрометации

Динамический анализ

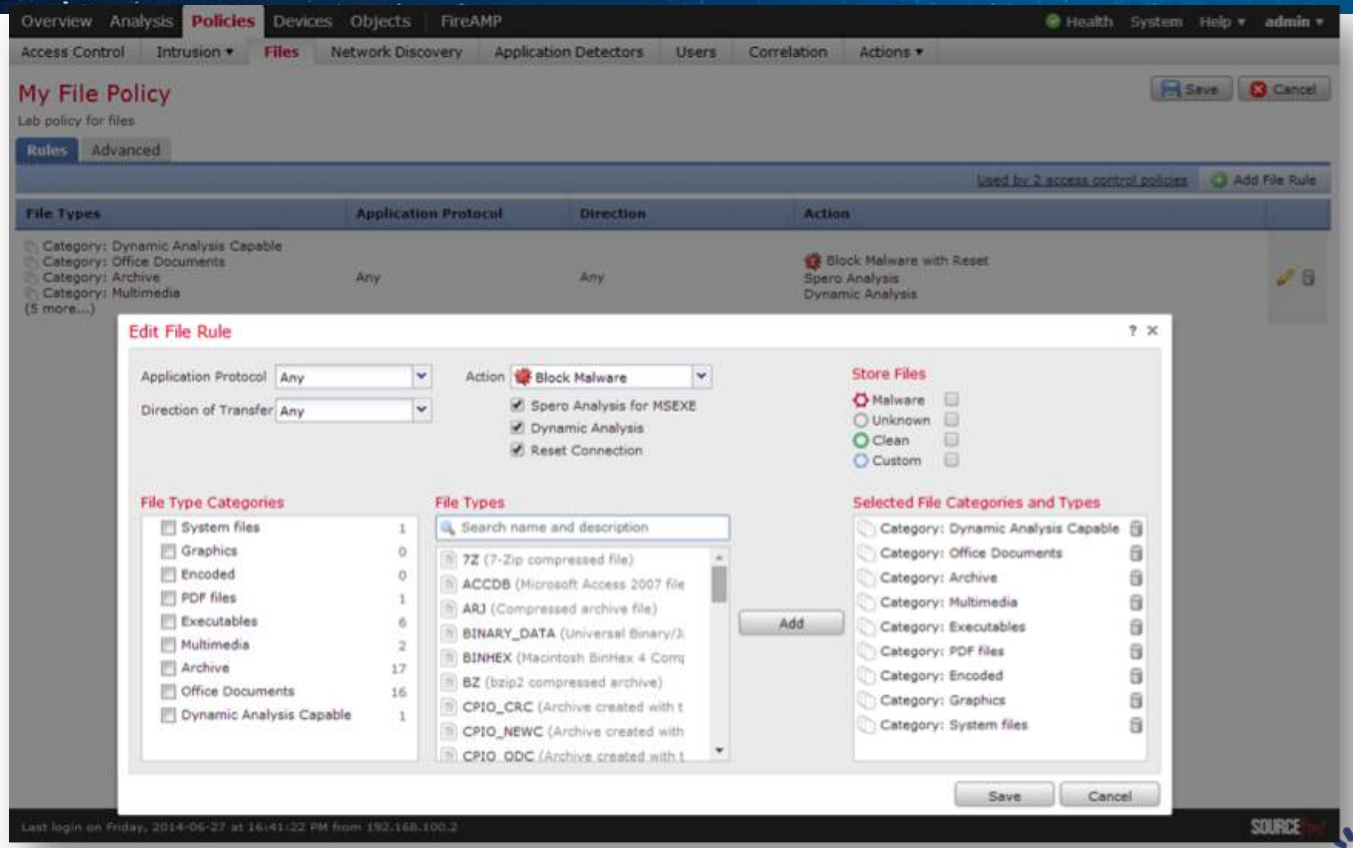
Расширенная аналитика

Сопоставление потоков данных с устройств

Cisco Connect

Блокирование вредоносного кода

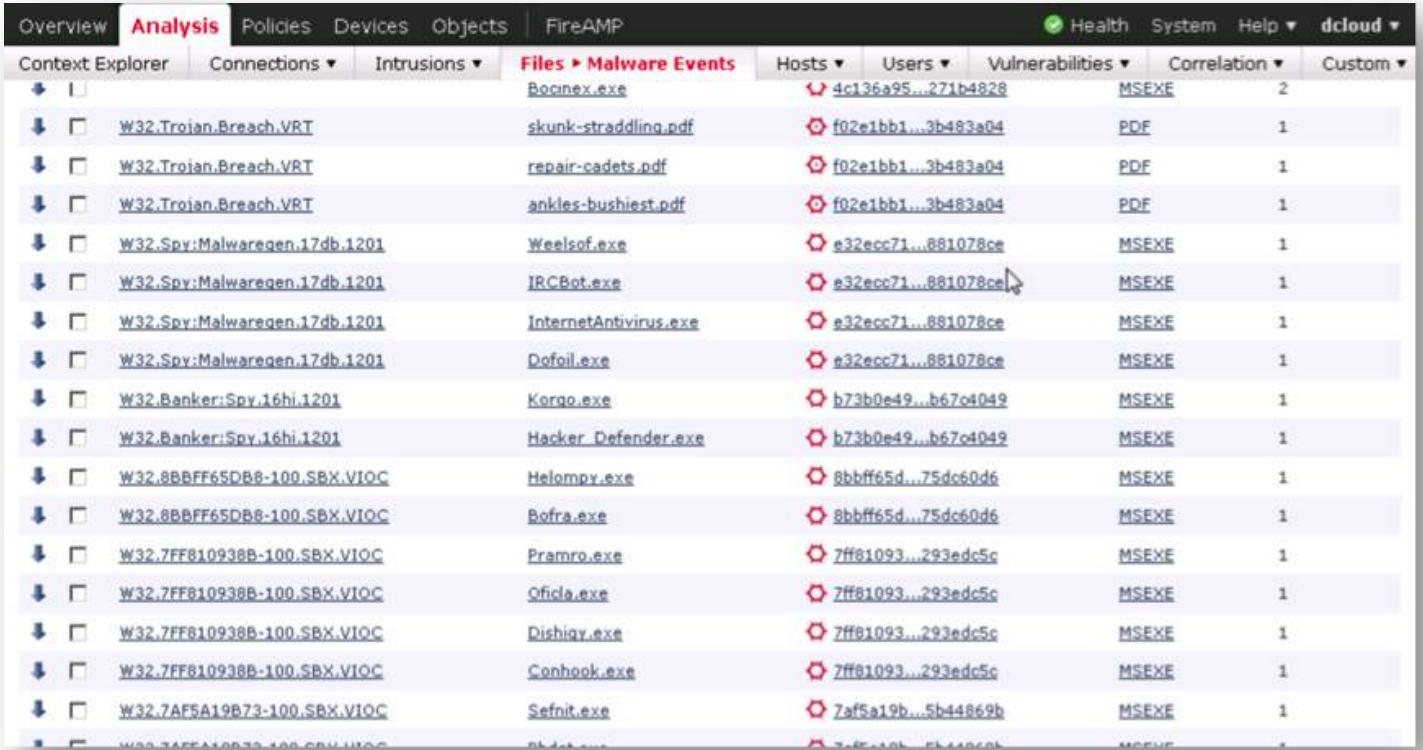
Bad Guys



Cisco Connect

Обнаружение известного вредоносного кода

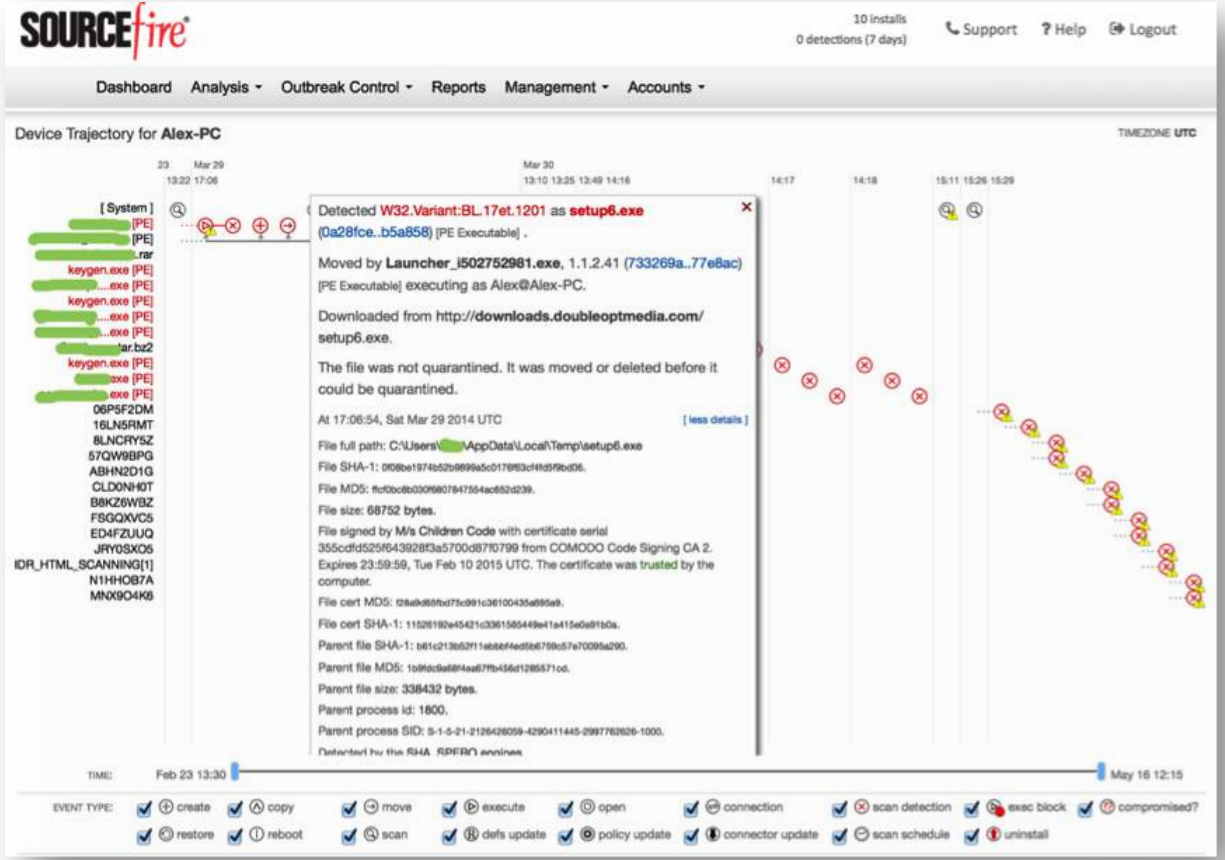
Bad Guys



Cisco Connect

Полная информация о вредоносном коде

Bad Guys



Cisco Connect

Если статус файла неизвестен, он отправляется в песочницу

Bad Guys

Warnings:	◦ Too many NtReadFile calls (excessive behavior) ◦ Too many NtUserPostMessage calls (excessive behavior) ◦ Too many NtProtectVirtualMemory calls (excessive behavior) ◦ Too many NtAllocateVirtualMemory calls (excessive behavior) ◦ Too many NtUserMessageCall calls (excessive behavior) ◦ Too many NtReadVirtualMemory calls (excessive behavior) ◦ Too many NtSetInformationFile calls (excessive behavior) ◦ Too many NtWriteFile calls (excessive behavior)

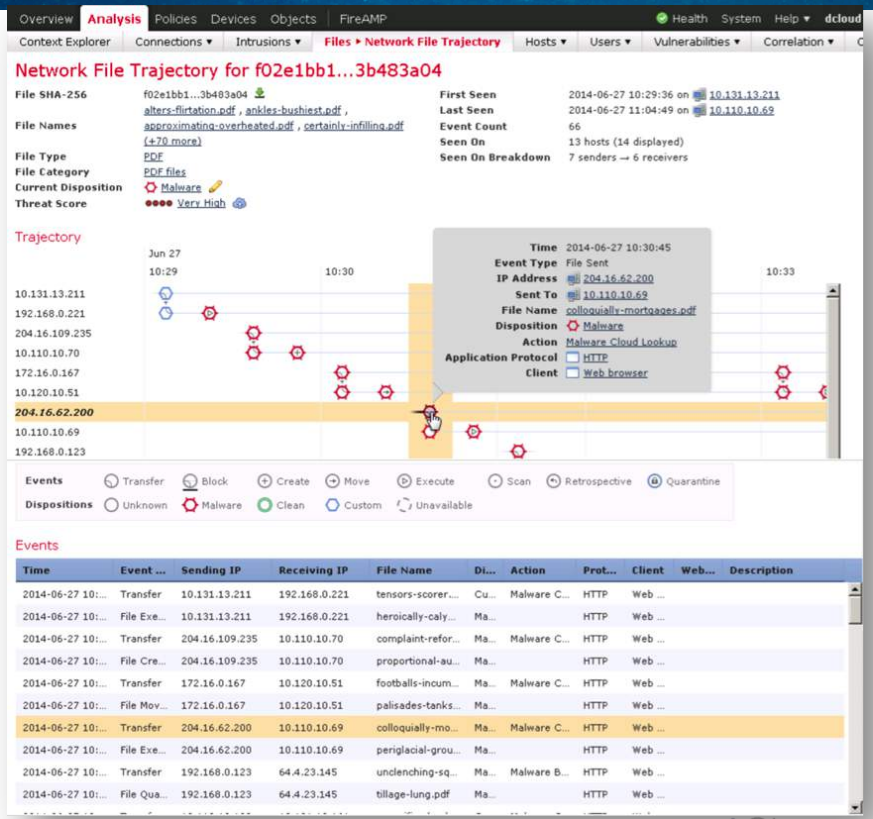
Classification / Threat Score

Persistence, Installation, Boot Survival :	
Hiding, Stealthiness, Detection and Removal Protection :	
Security Solution / Mechanism bypass, termination and removal, Anti Debugging, VM Detection :	
Spreading :	
Exploiting :	
Networking :	
Data spying, Sniffing, Keylogging, Ebanking Fraud :	

Cisco Connect

Анализ траектории вредоносного кода

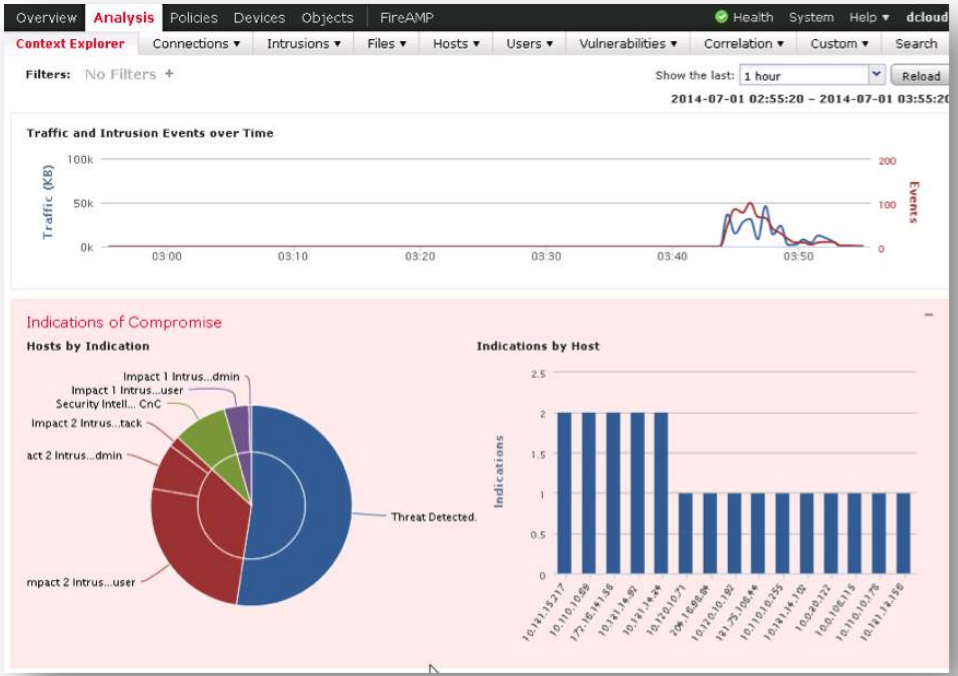
- Какие системы были инфицированы?
- Кто был инфицирован?
- Когда это произошло?
- Какой процесс был отправной точкой?
- Почему это произошло?
- Когда это произошло?
- Что еще произошло?



Cisco Connect

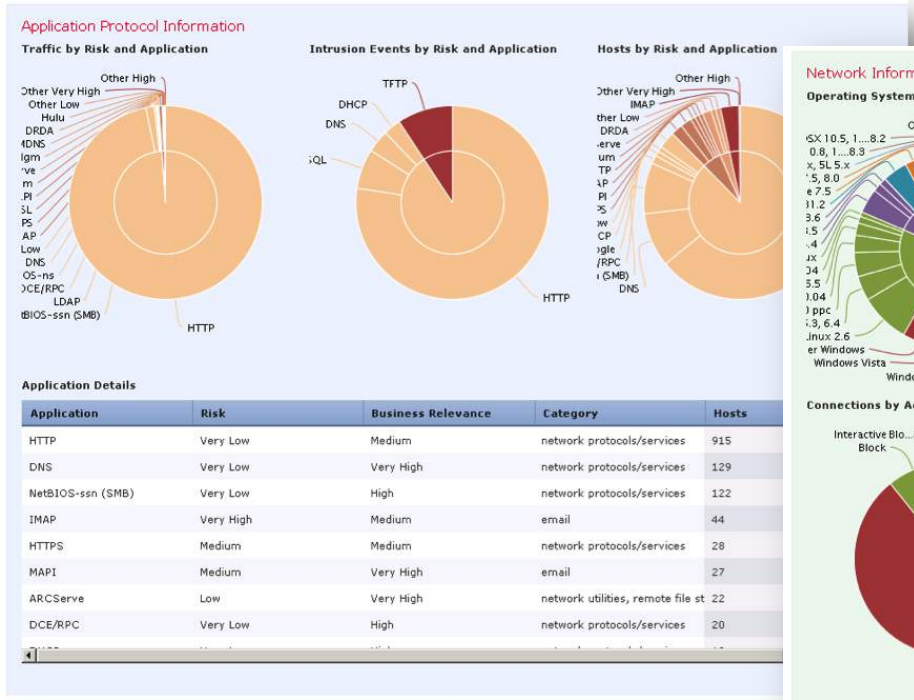
Мониторинг общей информации о сети

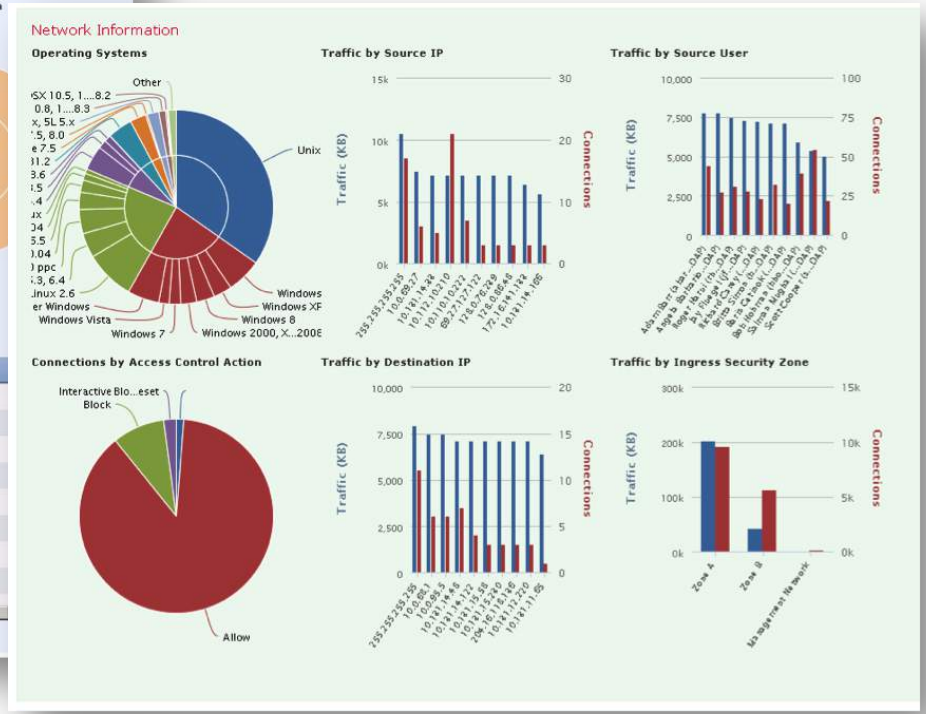
- Корреляция событий безопасности, трафика и вредоносного кода
- Активность конкретных пользователей и их приложений
- Используемые ОС и активность сетевого обмена
- Оценка событий по уровню воздействия и приоритета
- Статистика по вредоносному коду и зараженным файлам
- Геолокационные данные
- Категории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



Cisco Connect

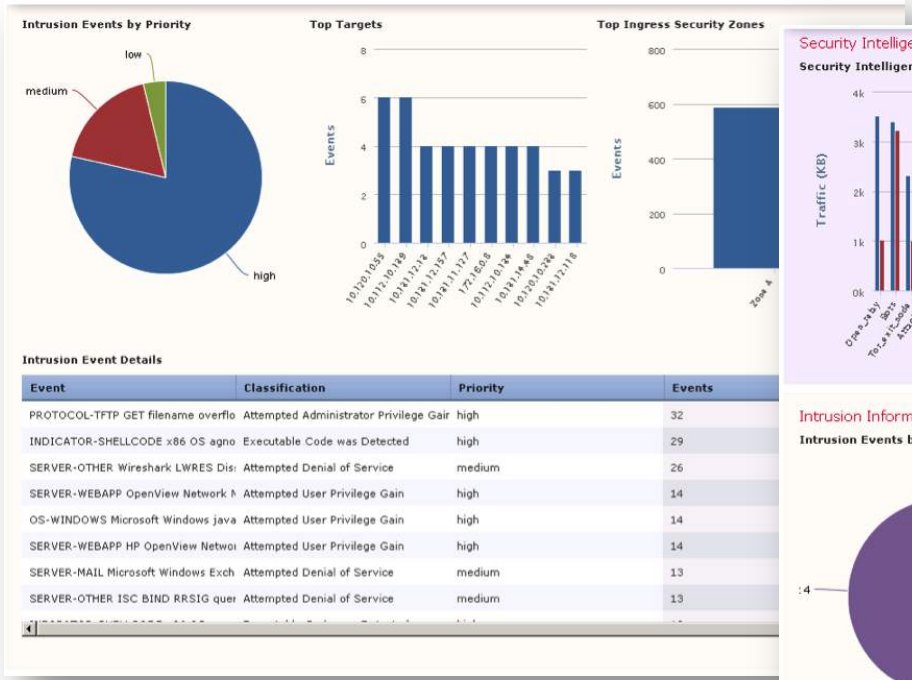
Мониторинг общей информации о сети





Cisco Connect

Мониторинг общей информации о сети



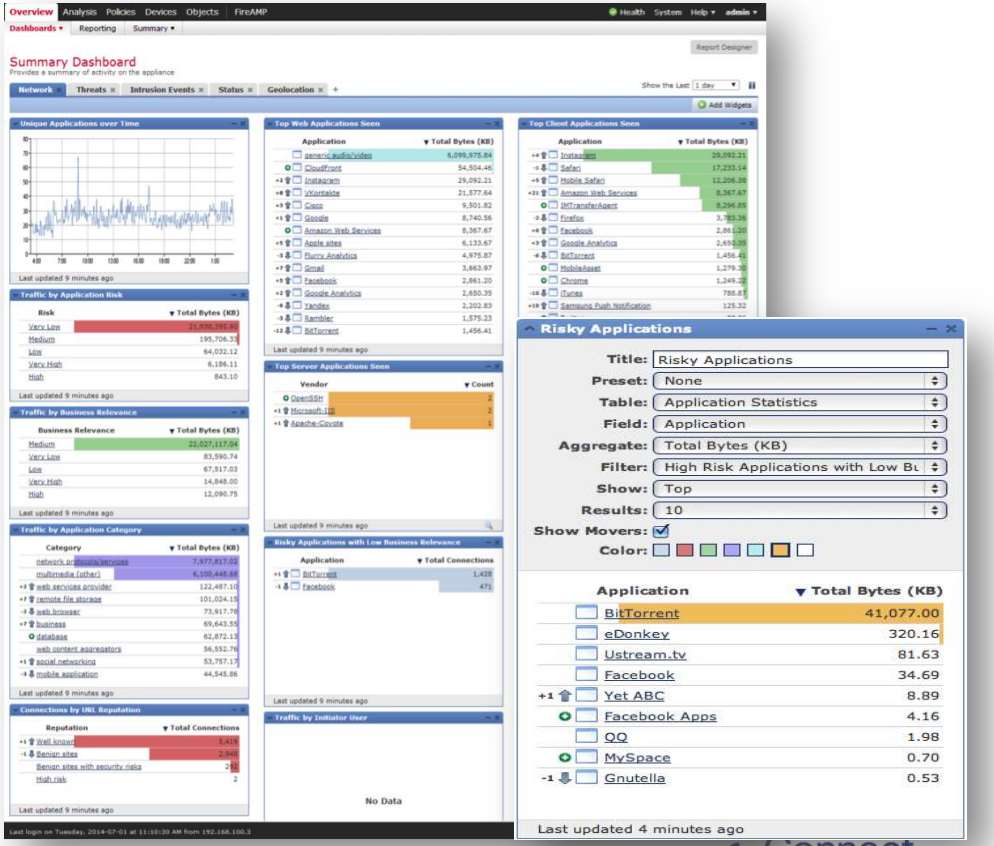
Cisco Connect

Мониторинг общей информации о сети

Cisco Connect

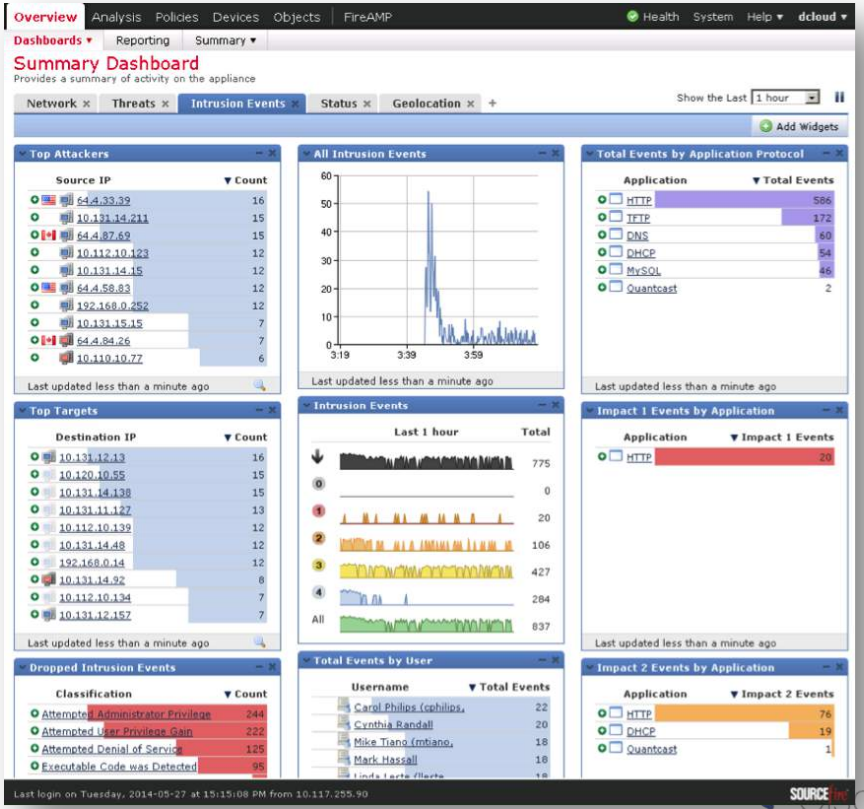
Мониторинг сетевых событий

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



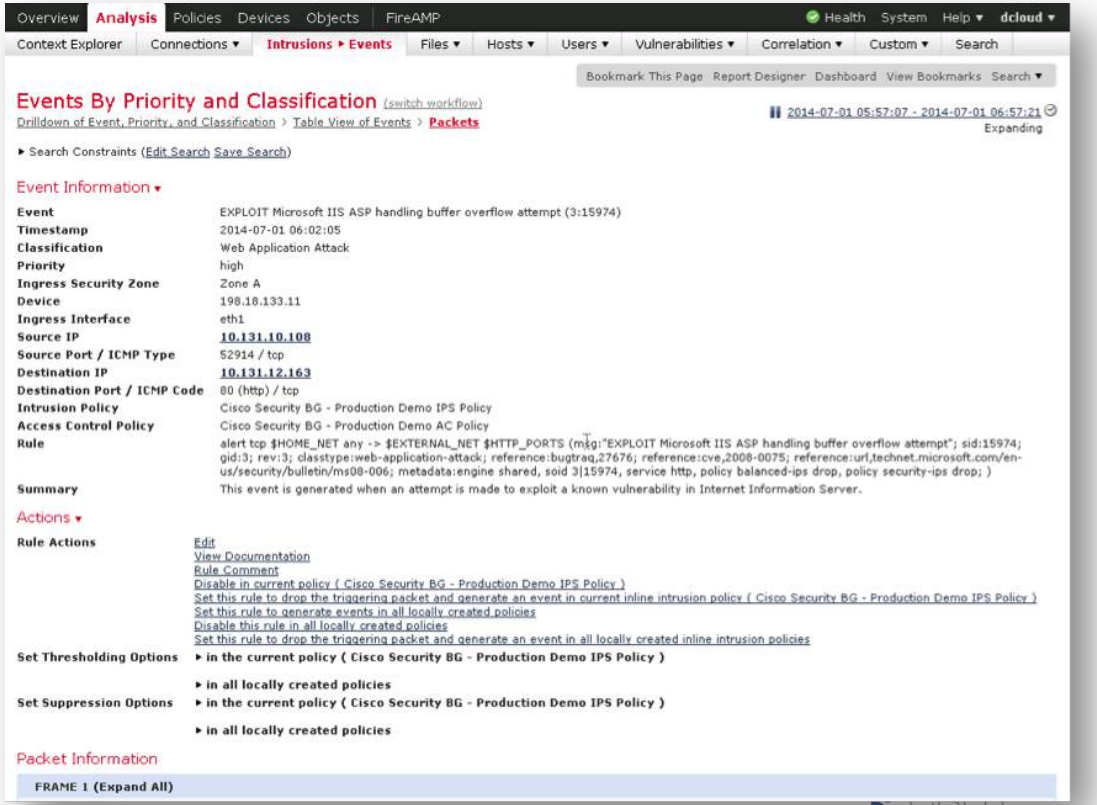
Мониторинг событий безопасности

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

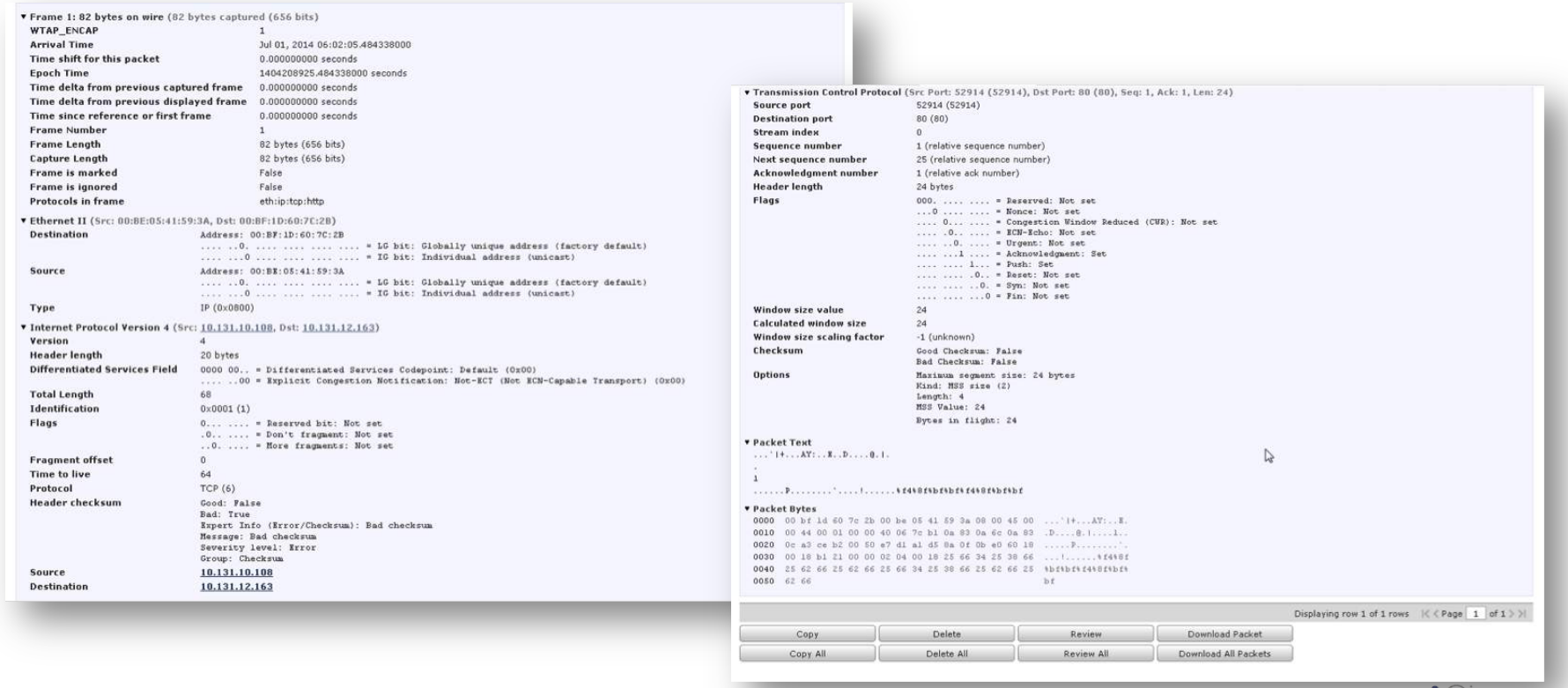


Детализация событий безопасности

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



Анализ сетевого дампа



▾ **Frame 1: 82 bytes on wire** (82 bytes captured (656 bits))

WTAP_ENCAP	1
Arrival Time	Jul 01, 2014 06:02:05.484338000
Time shift for this packet	0.000000000 seconds
Epoch Time	1404208925.484338000 seconds
Time delta from previous captured frame	0.000000000 seconds
Time delta from previous displayed frame	0.000000000 seconds
Time since reference or first frame	0.000000000 seconds
Frame Number	1
Frame Length	82 bytes (656 bits)
Capture Length	82 bytes (656 bits)
Frame is marked	False
Frame is ignored	False
Protocols in frame	eth:ip:tcp:http

▾ **Ethernet II** (Src: 00:BE:05:41:59:3A, Dst: 00:BF:1D:60:7C:2B)

Destination	Address: 00:BF:1D:60:7C:2B .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast)
Source	Address: 00:BE:05:41:59:3A .... ..0. .... = LG bit: Globally unique address (factory default) ....0 .... = IG bit: Individual address (unicast)
Type	IP (0x0800)

▾ **Internet Protocol Version 4** (Src: 10.131.10.108, Dst: 10.131.12.163)

Version	4
Header length	20 bytes
Differentiated Services Field	0000 00.. = Differentiated Services Codepoint: Default (0x00) .... ..00 = Explicit Congestion Notification: Not-ECT (Not ECN-Capable Transport) (0x00)
Total Length	68
Identification	0x0001 (1)
Flags	0... .... = Reserved bit: Not set .0.. .... = Don't fragment: Not set ..0. .... = More fragments: Not set
Fragment offset	0
Time to live	64
Protocol	TCP (6)
Header checksum	Good: False Bad: True Expert Info (Error/Checksum): Bad checksum Message: Bad checksum Severity level: Error Group: Checksum
Source	10.131.10.108
Destination	10.131.12.163

▾ **Transmission Control Protocol** (Src Port: 52914 (52914), Dst Port: 80 (80), Seq: 1, Ack: 1, Len: 24)

Source port	52914 (52914)
Destination port	80 (80)
Stream index	0
Sequence number	1 (relative sequence number)
Next sequence number	25 (relative sequence number)
Acknowledgment number	1 (relative ack number)
Header length	24 bytes
Flags	000. .... = Reserved: Not set ...0 .... = Nonce: Not set .... 0... .... = Congestion Window Reduced (CWR): Not set .... .0.. .... = ECN-Echo: Not set .... ..0. .... = Urgent: Not set ....1 .... = Acknowledgment: Set .... 1... = Push: Set .... .0.. = Reset: Not set ....0. = Syn: Not set ....0 = Fin: Not set
Window size value	24
Calculated window size	24
Window size scaling factor	-1 (unknown)
Checksum	Good Checksum: False Bad Checksum: False
Options	Maximum segment size: 24 bytes Kind: MSS size (2) Length: 4 MSS Value: 24 Bytes in flight: 24

▾ **Packet Text**

```
...'|+...AY:..E..D....@.|.
.
i
.....P........'....!.....%f4%8f%bf%bf%f4%48f%bf%bf
```

▾ **Packet Bytes**

```
0000  00 bf 1d 60 7c 2b 00 be 05 41 59 3a 08 00 45 00  ...`|+...AY:..E.
0010  00 44 00 01 00 00 40 06 7c b1 0a 83 0a 6c 0a 83  .D....@.|....l..
0020  0c a3 ce b2 00 50 e7 d1 a1 d5 8a 0f 0b e0 60 18  .....P........`.
0030  00 18 b1 21 00 00 02 04 00 18 25 66 34 25 38 66  ...!......%f4%8f
0040  25 62 66 25 62 66 25 66 34 25 38 66 25 62 66 25  %bf%bf%f4%8f%bf%
0050  62 66                                            bf
```

Displaying row 1 of 1 rows Page 1 of 1

Copy	Delete	Review	Download Packet
Copy All	Delete All	Review All	Download All Packets

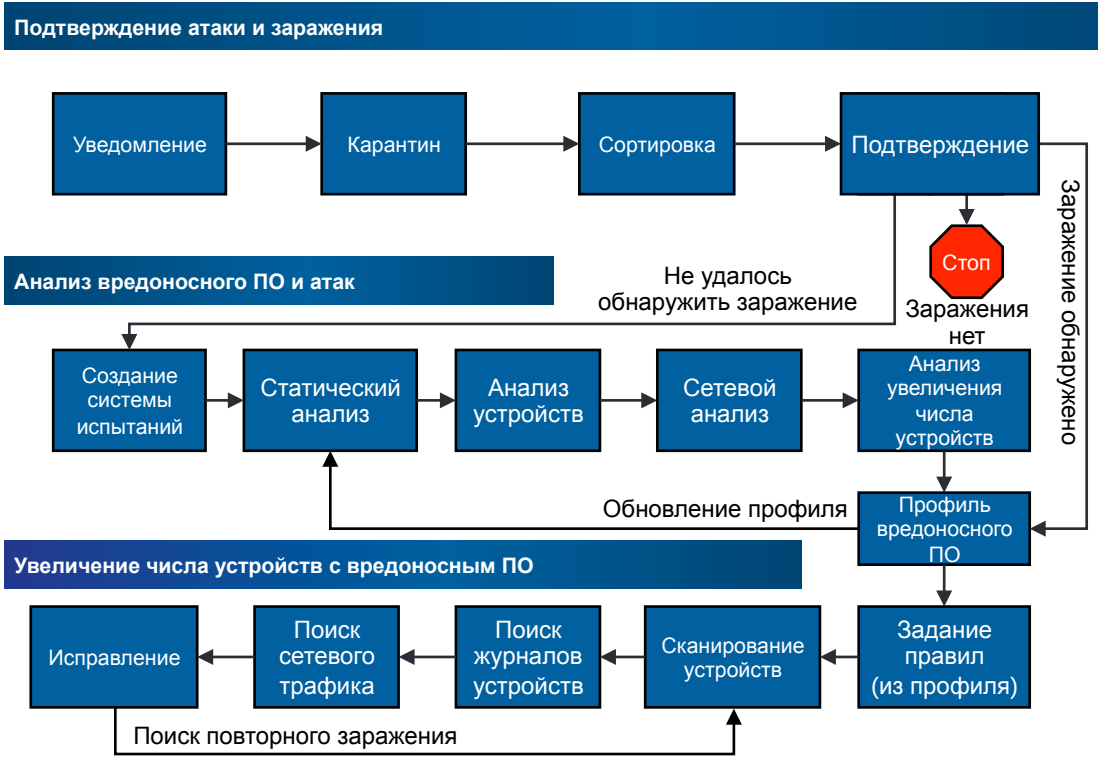
Cisco Connect

ASA с сервисами FirePOWER объединяет все вместе

Cisco Connect

Вопрос не в том, произойдет ли заражение, а как скоро мы его обнаружим, устраним и поймем причины

- С чего начать?
- Насколько тяжела ситуация?
- Какие системы были затронуты?
- Какой ущерб нанесла угроза?
- Как можно восстановить?
- Как можно предотвратить ее повторение?



Cisco Connect

Объединяя все вместе, ASA с сервисами FirePOWER...

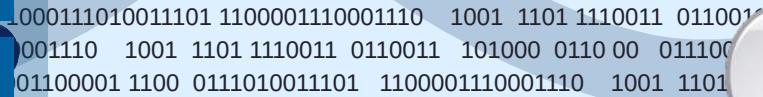
Все компоненты – контрольные точки

Эл. почта | Оконечные устройства | Интернет | Сеть | Система предотвращения вторжений IPS | Устройства

Поток телеметрических данных

- Идентифицирующие метки и метаданные файла
- Файловый и сетевой ввод/вывод
- Информация о процессе

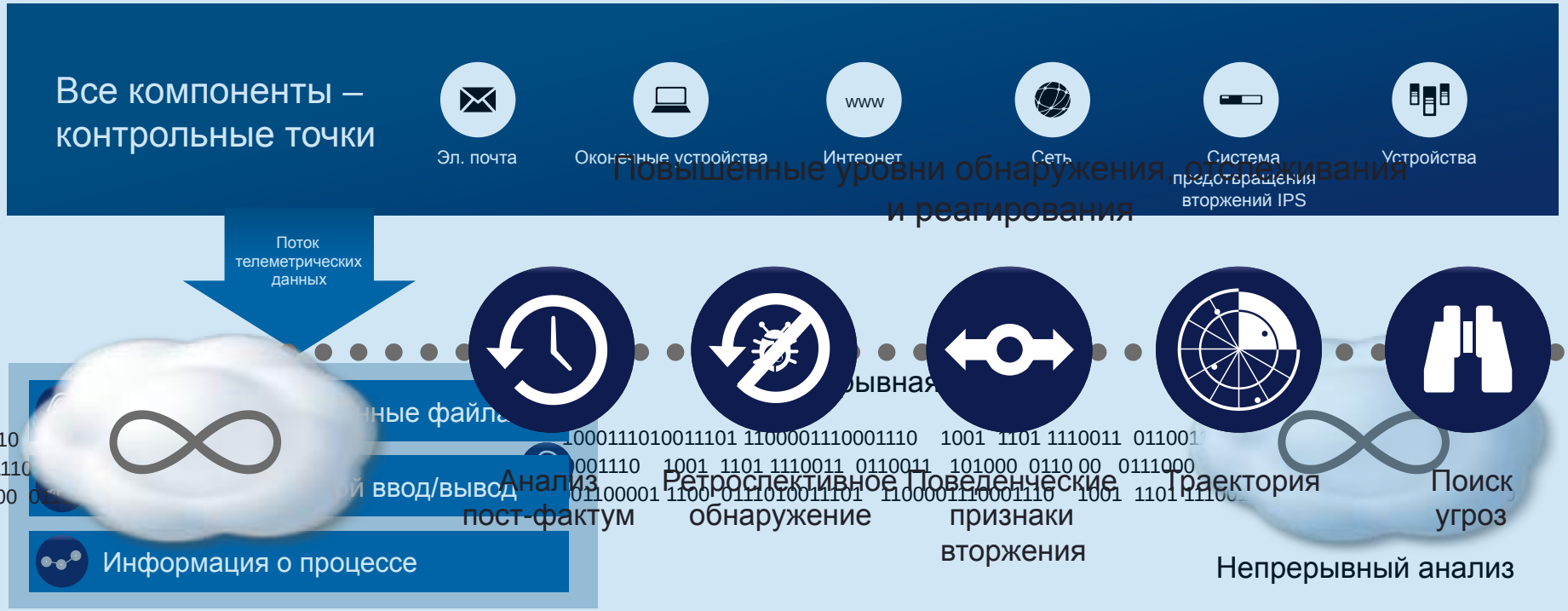
Непрерывная передача



Непрерывный анализ

Cisco Connect

…позволяет непрерывно анализировать широкий спектр угроз и реагировать на них…



...и даёт понимание того, что именно следует делать, чтобы решить проблему.

Кто

Сфокусируйтесь сначала на этих пользователях

Что

Эти приложения пострадали

Где

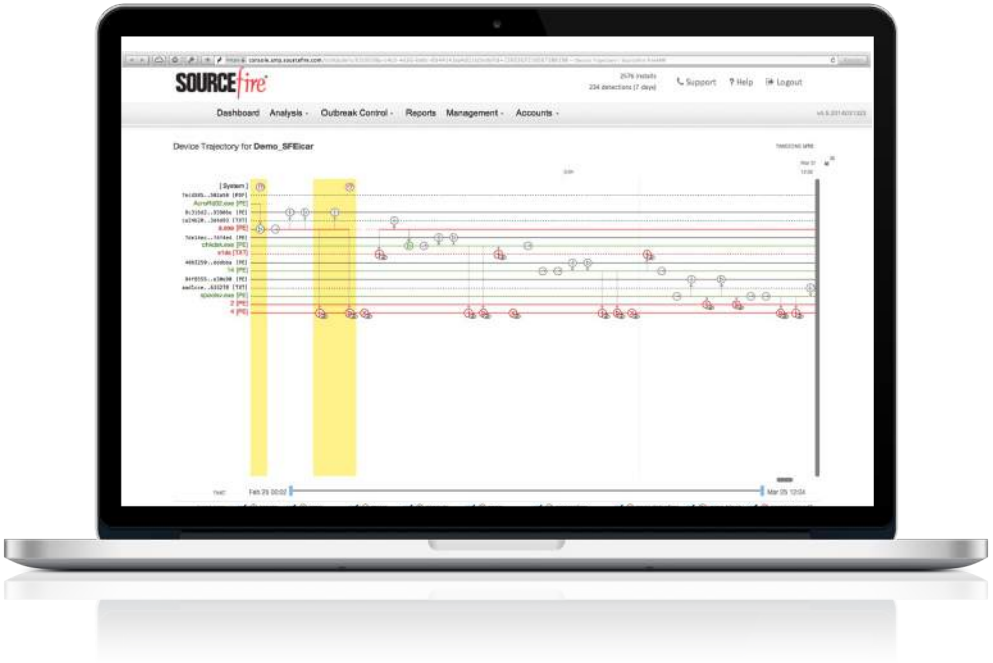
Взлом затронул эти области сети

Когда

Такова картина атаки по времени

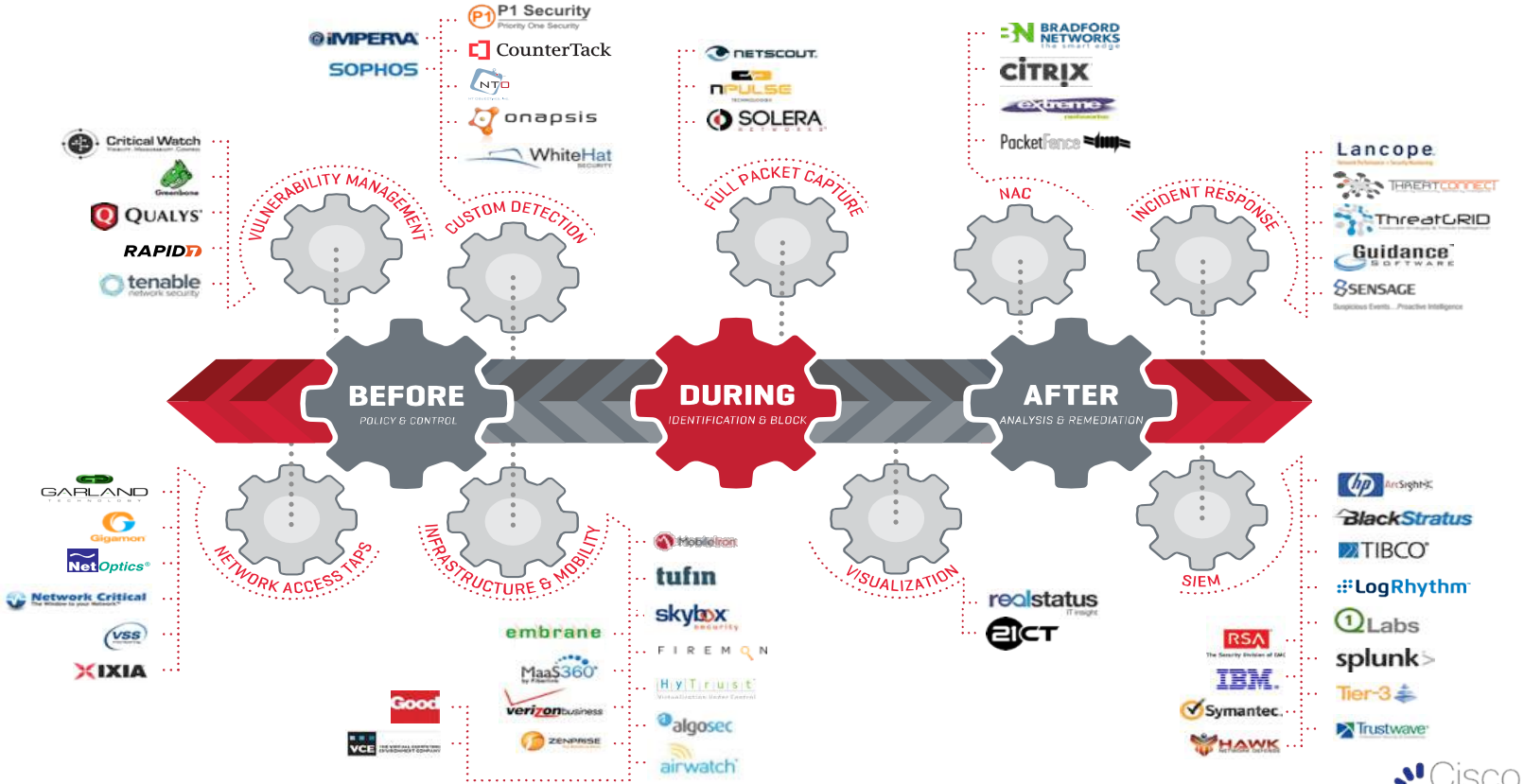
Как

Это источник угрозы и путь ее распространения



Cisco Connect

Экосистема Cisco ASA with FirePOWER



Cisco Connect

Варианты исполнения Cisco ASA with FirePOWER

FirePOWER Services for 5500-X (ПО)

ASA 5512-X, 5515-X, 5525-X, 5545-X, 5555-X

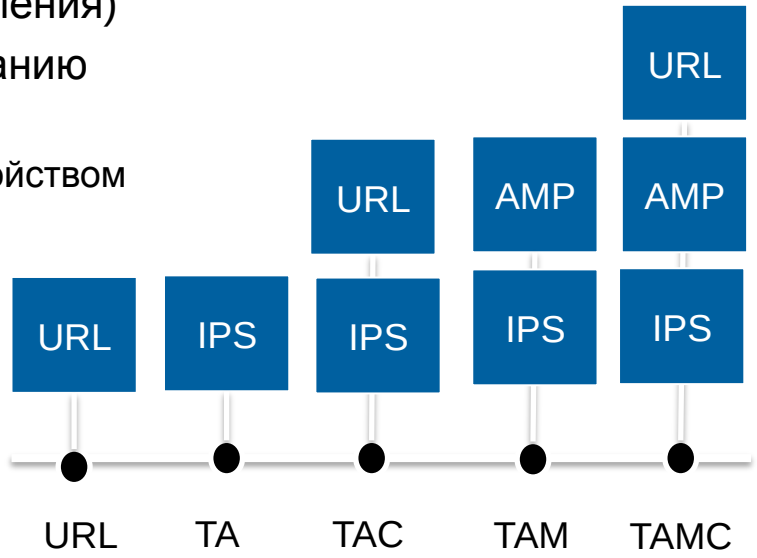
FirePOWER Services for 5585-X (модуль)

ASA 5585-X

Модульная функциональность

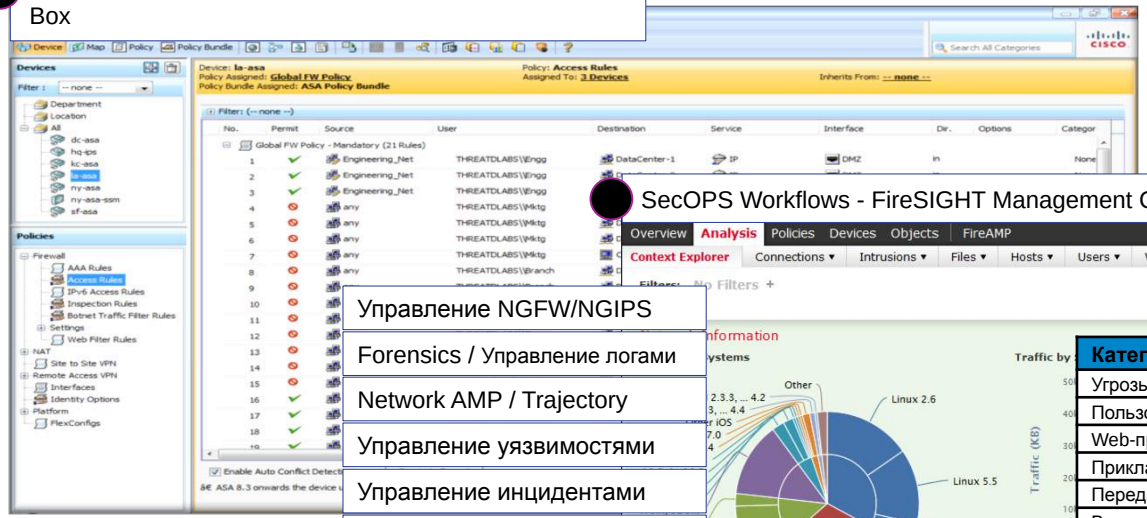
5 вариантов заказа защитных функций:

- Подписка на 1 или 3 года (включая обновления)
- Функция AVC (NGFW) включена по умолчанию
  - Активирует функции FirePOWER Services
  - Постоянная и поставляется вместе с устройством
- Обновления AVC включены в SMARTnet



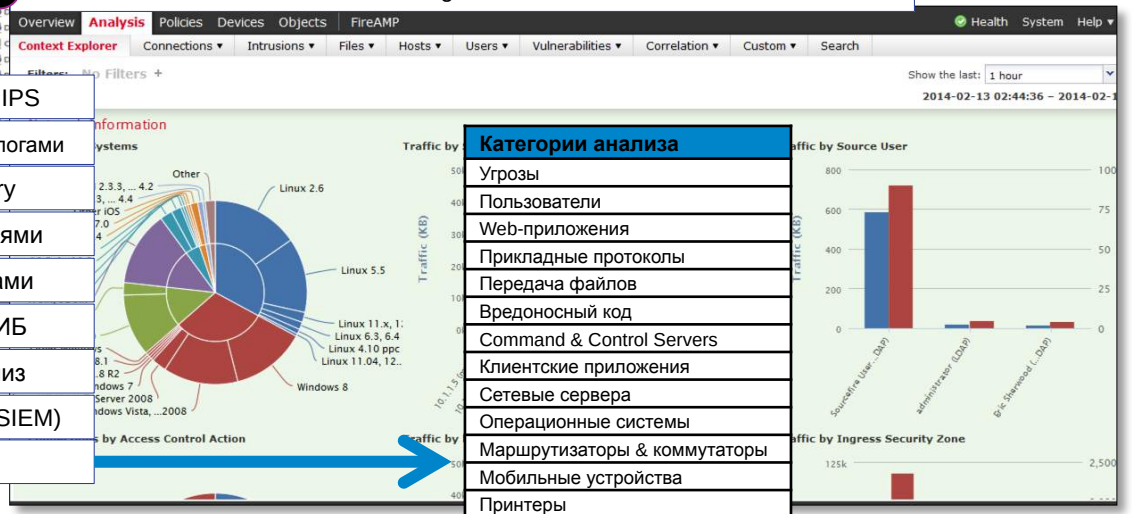
Что используется для управления ASA с сервисами FirePower?

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



FireAMP Connector (Управляется облачной 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
Маршрутизаторы & коммутаторы
Мобильные устройства
Принтеры
VoIP-телефоны
Виртуальные машины

Cisco Connect

Cisco ASA с функциями FirePOWER

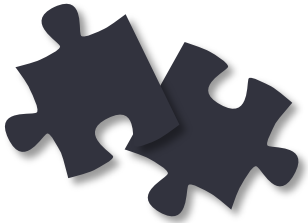
Реальная борьба с угрозами

Полная информация о происходящих в сети процессах

- 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

Cisco Connect

«Поэтому сказано, что тот, кто знает врага и знает себя, не окажется в опасности и в ста сражениях. Тот, кто не знает врага, но знает себя, будет то побеждать, то проигрывать. Тот, кто не знает ни врага, ни себя, неизбежно будет разбит в каждом сражении.»

Сунь Цзы. Искусство войны.

#CiscoConnectRu

Cisco Connect

Спасибо за внимание!
Пожалуйста, используйте код для оценки доклада:

3345

Руслан Иванов
Системный инженер-консультант
+7 (495) 961-1467
ruivanov@cisco.com

CiscoRu Cisco CiscoRussia