Инновации Cisco Security

Что нового в продуктах безопасности

Pavel Rodionov
CSE Security
14 ноября 2017

Инновации Firepower NGFW

Firepower NGFW: эволюция

2016

- Анонс Firepower Threat Defense
- Критический функционал Enterprise Edge
- Перенос ASA функционала

2017

- Новые платформы, RA VPN
- Улучшения работы системы , FDM расширения

6.2.3

Предыдущие релизы

МАЙ 2017

Firepower 6.2.1

- Анонс Firepower 2100
- Remote Access VPN (SSL и IPsec) для 2100

ASA 9.8.1

- MOBIKE (Mobile IKEv2)
- VTI
- ASAv50

СЕНТЯБРЬ 2017

Firepower 6.2.2

- Remote Access VPN для остальных платформ
- Threat Intelligence Director
- FDM для VMware NGFWv

ASA 9.8.2

- ASA для Firepower 2100

На всех устройствах Firepower может быть запущен ASA

2100 серия

Хорошее относшение ценаю/качество

NGFW дл Internet Edge,
10 GbE подключение

4100 серия

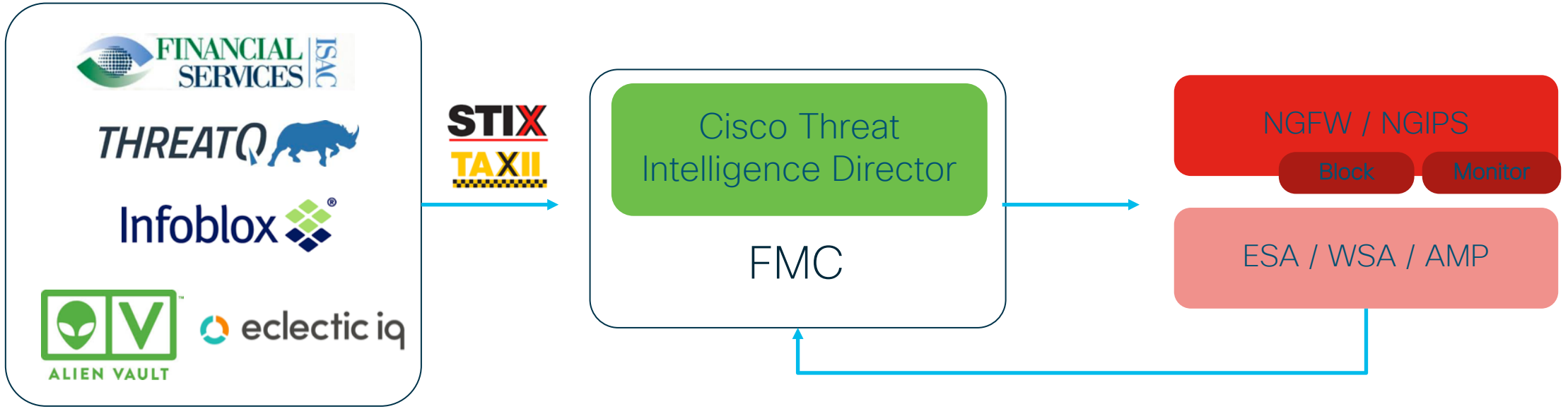
Высокопроизводительный 1RU
NGFW для ЦОД
40 GbE интерфейсы

9300 серия

Операторский класс
NGFW дл кампуса и SP
Подключения до 100 Gbps

На всех может работать как Firepower Threat Defence, так и ASA

Cisco Threat Intelligence Director (CTID)



Получите информацию Threat Intelligence (CTI)

Опубликуйте данные на сенсоры

Детектируйте инциденты

Управление NGFW

Расширение возможностей локального менеджера

Предназначен

- Для создания простой, но эффективной системы безопасности
- Клиентам с устройствами 5506-X-5555-X/2100

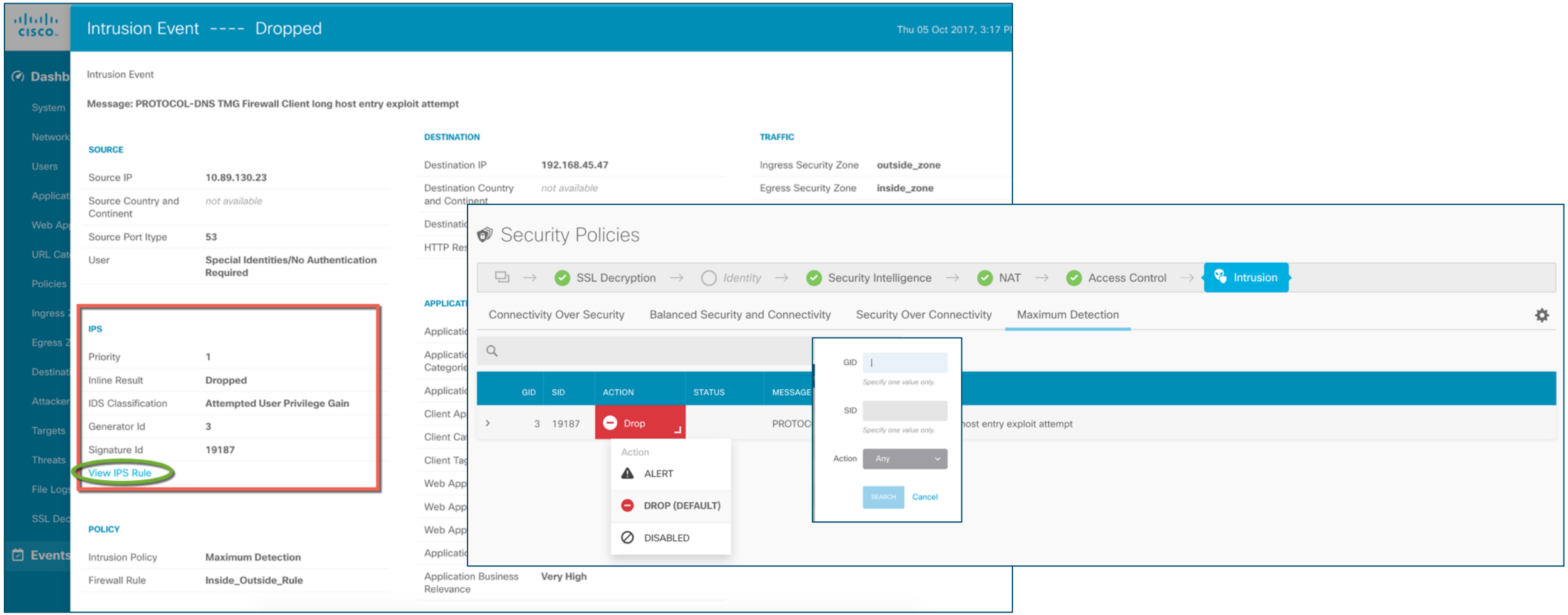
UX переработка

Управление процессом

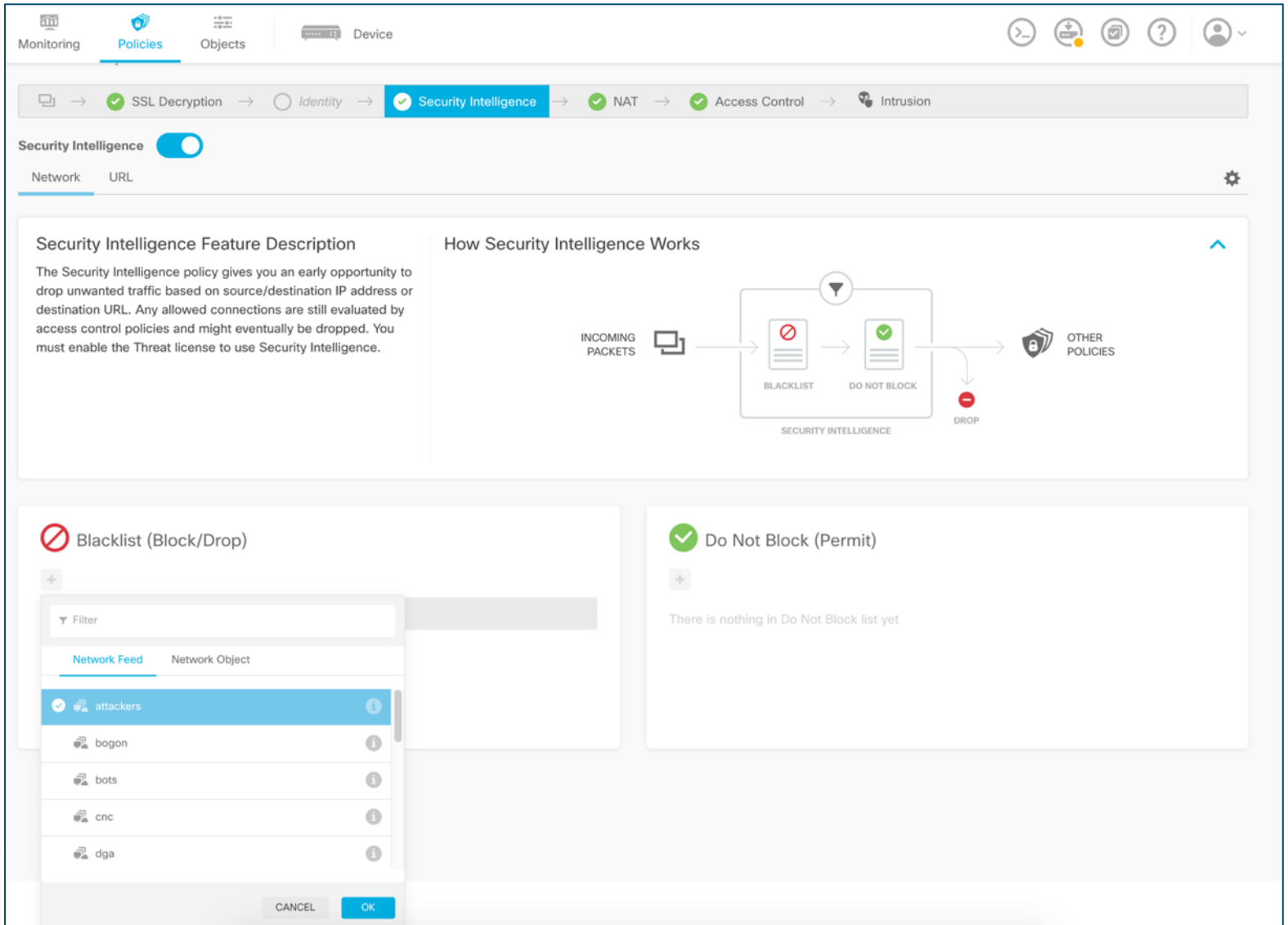
Простая безопасность

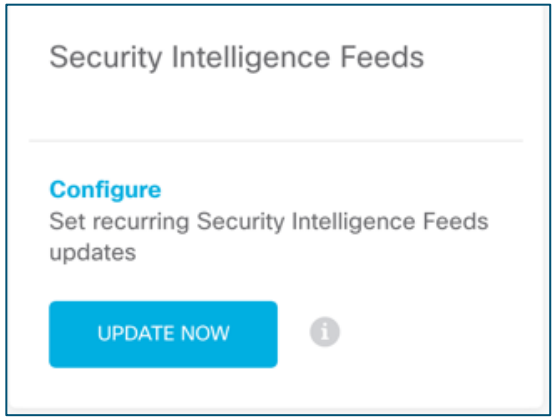
- Снижение количества ложных срабатываний
- Первая линия обороны с Cisco Security Intelligence
- Расширенная инспекция шифрованного трафика с SSL Decryption
- Простая миграция ASA→FTD с Flexconfig/SmartCLI
- Упрощение troubleshooting с CLI Console
- Управление NGFWv на VMware и KVM с FDM
- API для автоматизации/оркестрации

Настройка IPS сигнатур



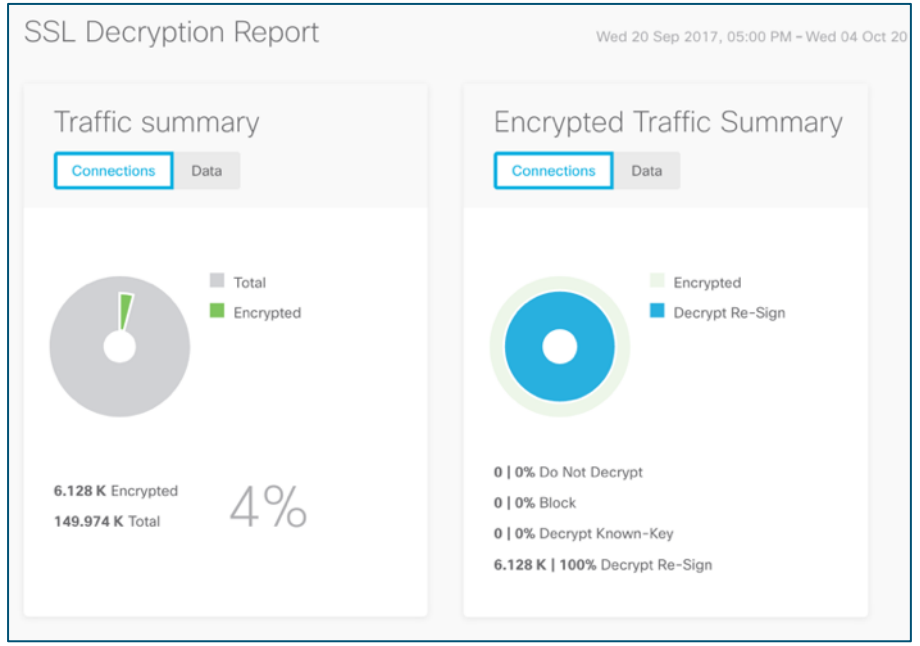
Поддержка Security Intelligence Feeds

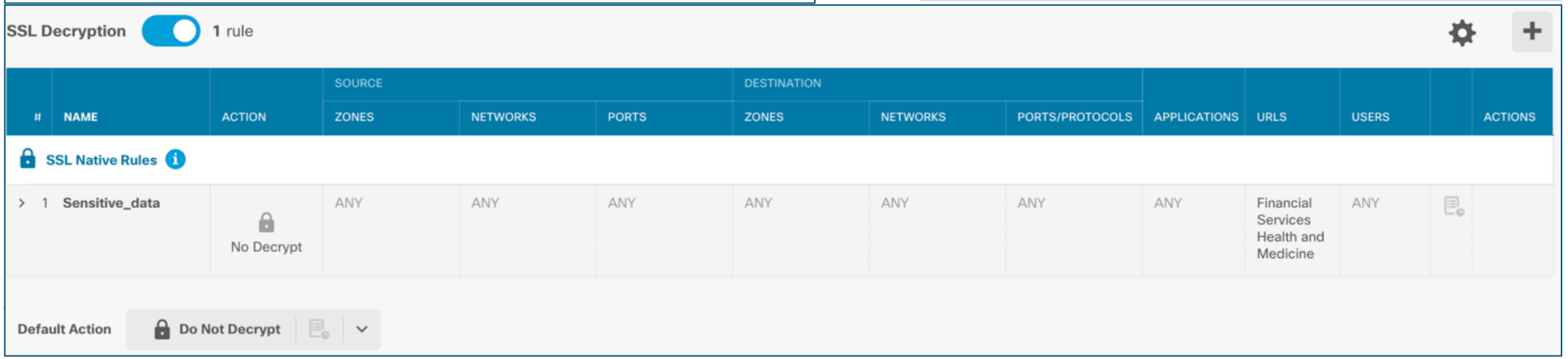




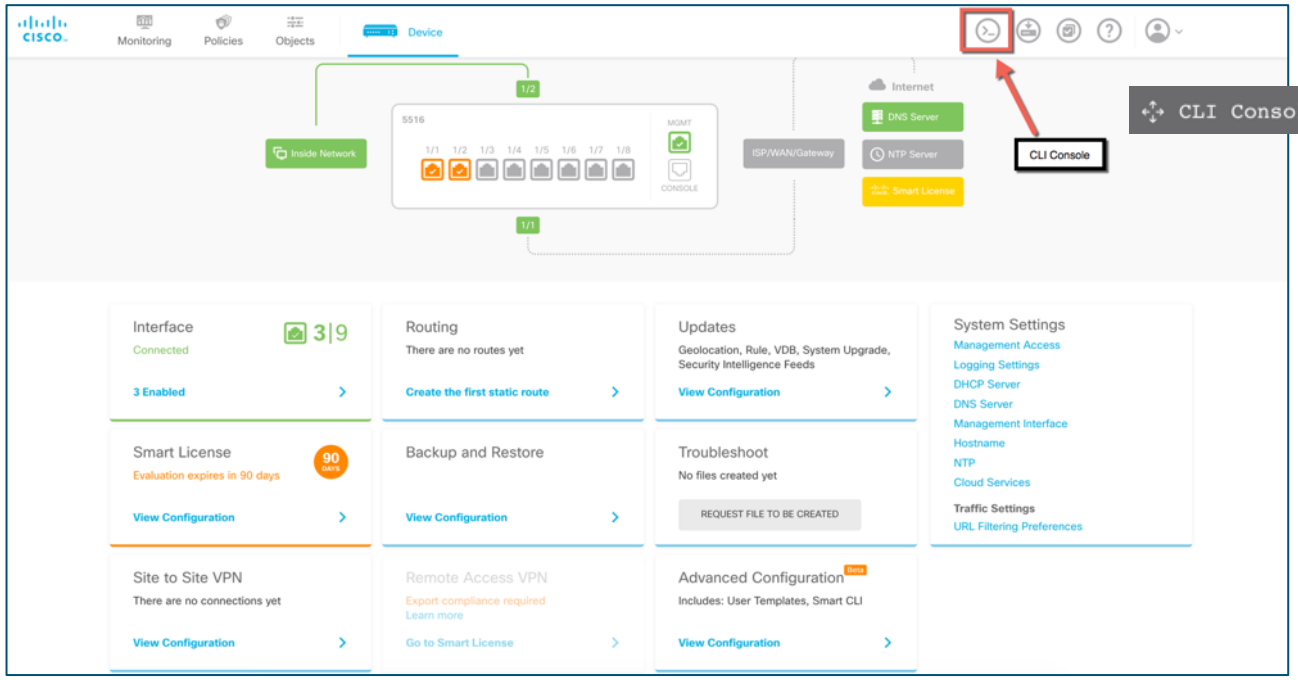
- Поддержка Cisco SI Feeds
- Включение whitelist/Blacklist

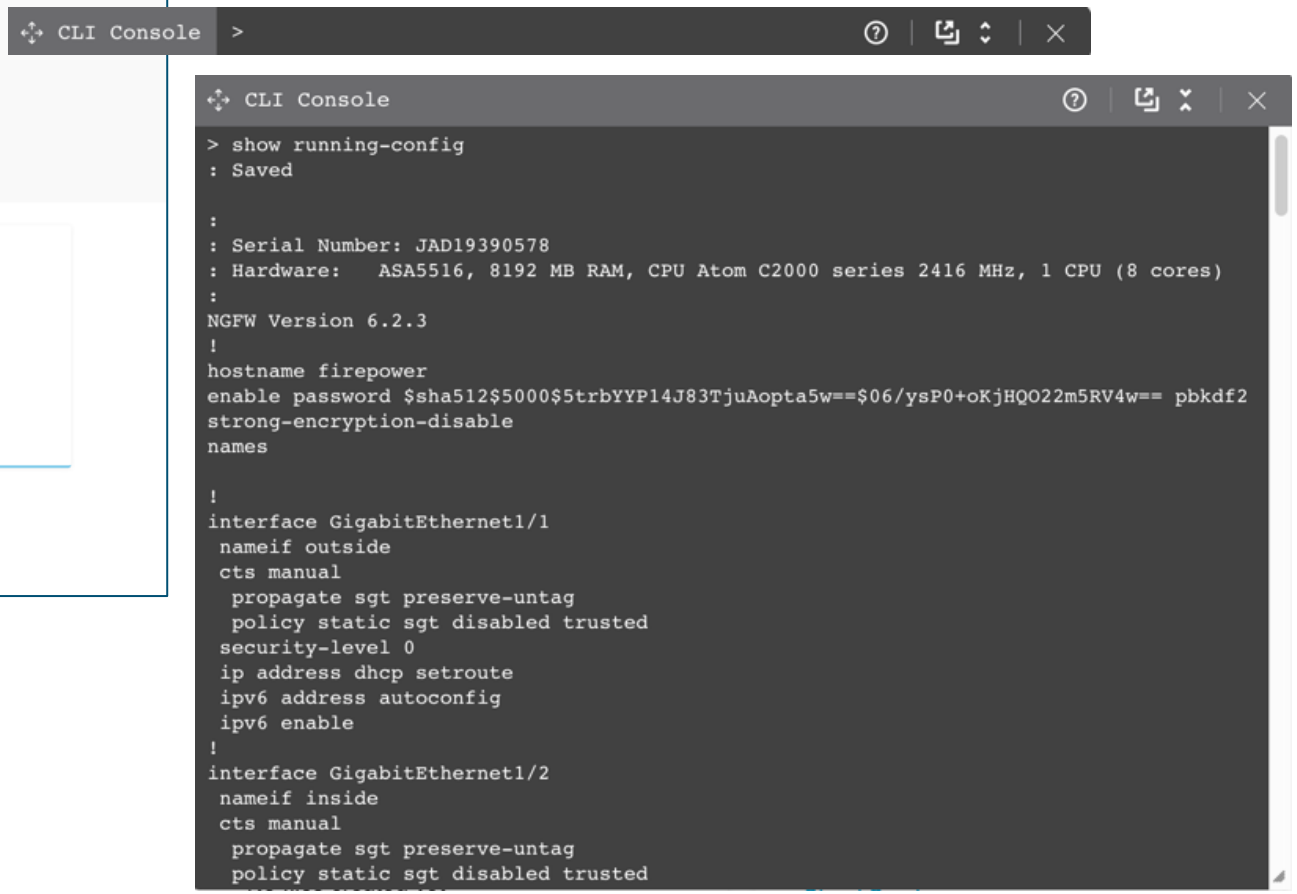
Расширенная инспекция трафика с помощью SSL Decryption





Простой Troubleshooting

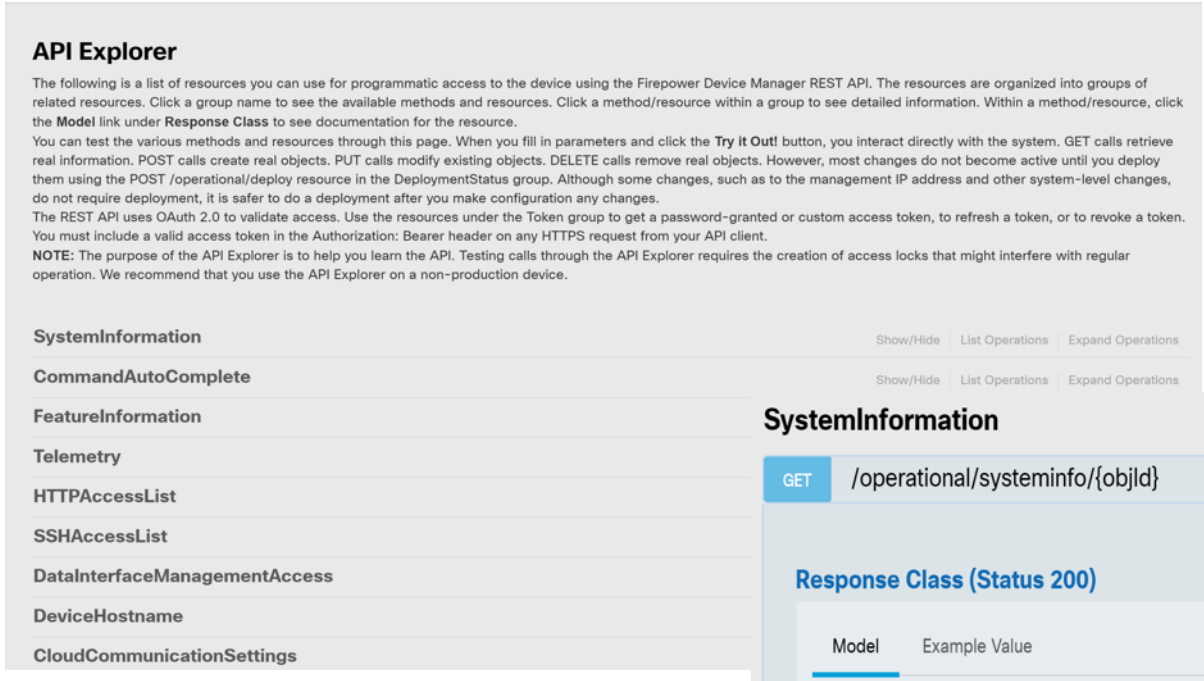




- Быстрый доступ к CLI командам
  - show, ping, traceroute, packet tracer

Автоматизация/оркестрация

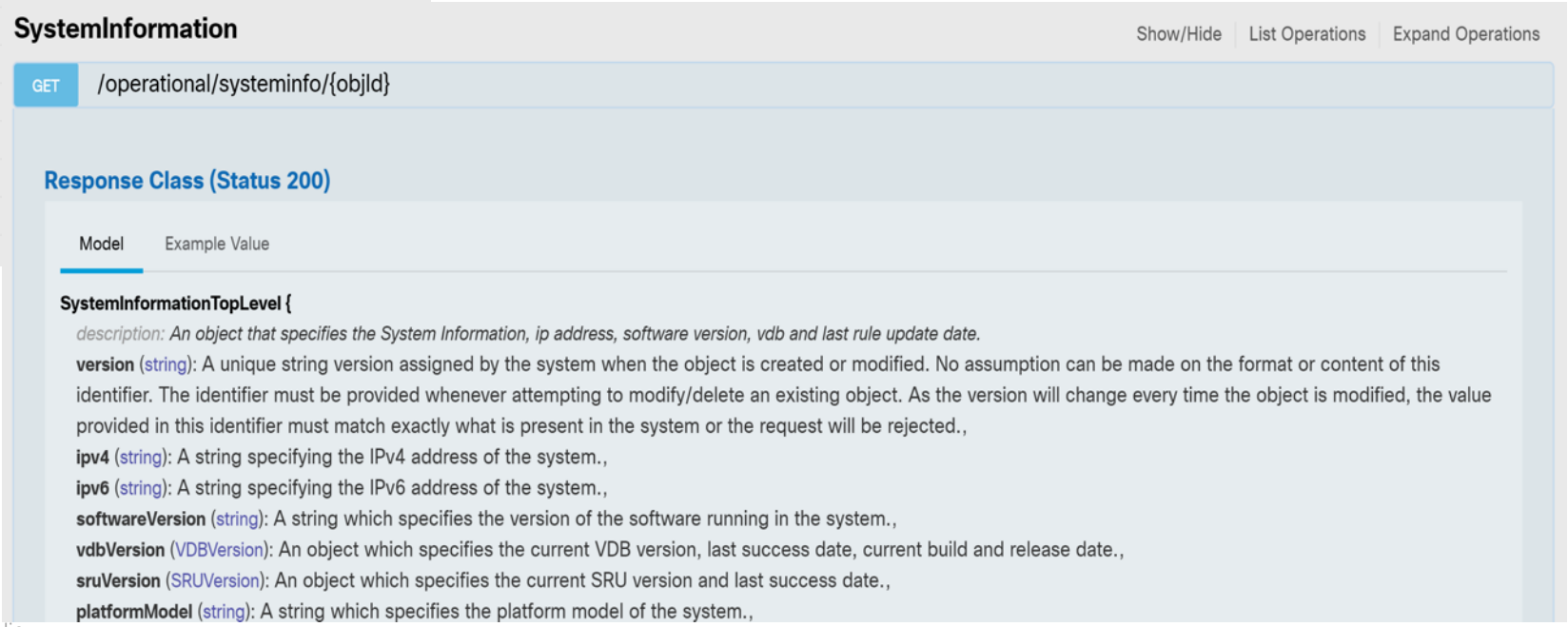
Новый API



Фаза 1

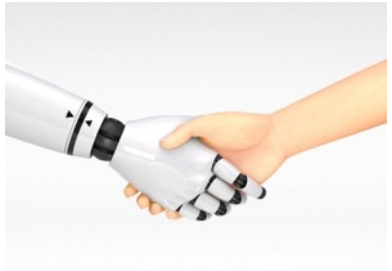
- Автоматизация прямо на устройстве
- Не нужен FMC
- Весь поддерживаемый функционал GUI
- https://<hostname>/#/api-explorer

- Направление на оркестрацию
- Позволяет легко автоматизировать процессы



Новый API FMC

- Выгоды
  - Быстрая и тесная интеграция с инструментами 3-х компаний
  - Ускоряет процесс настройки
  - Миграция ASA→FTD



EtherChannel/PortChannel Interface	CRUD
Redundant Interface	CRUD
NAT Policies, NAT Rules	CRUD, Bulk Post for Manual & Auto NAT
Interface Groups	CRUD
Security Zones	R
Ipv4 and Ipv6 Static Routing	CRUD, Bulk Post
FTD HA	CRUD (except Monitoring Intf, MAC Addr)

Улучшения использования

FDM

- Новая система мониторинга
- Новый Dashboard Web Application
- Отслеживание IP/пользователей

FMC

- Быстрое создание HA
- Аудит изменений, Просмотр CLI после развертывания
- Увеличенное окно политик
- Возможность создавать групповые объекты в правиле
- Copy/Paste конфигурации

Meraki MX

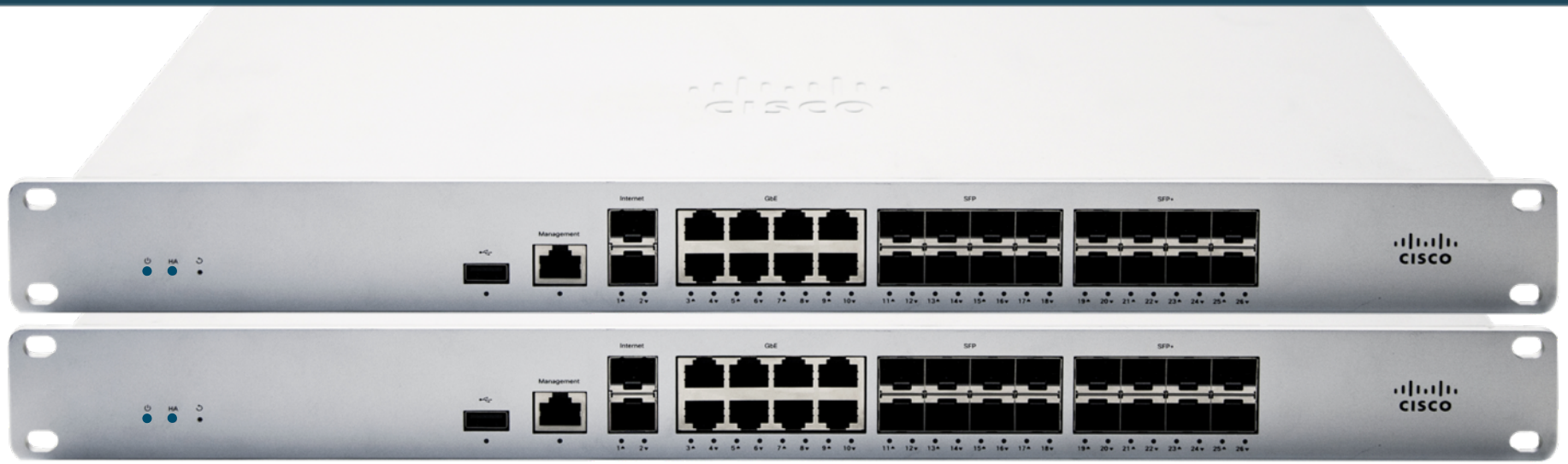
Новые устройства MX250 & MX450

Расширение портофолио MX новыми высокопроизводительными моделями

High Throughput

Flexible Interface types

Modular redundant power



Новые устройства MX250 & MX450

	MX250	MX450
		
Интерфейсы		
WAN	2 x 10G SFP+	2 x 10G SFP+
LAN	8 x 1G RJ45 8 x 1G SFP 8 x 10G SFP+	8 x 1G RJ45 8 x 1G SFP 8 x 10G SFP+
Пропускная способность	4 Gbps	6 Gbps
Количество клиентов	2,000	10,000
VPN производительность	1 Gbps	2 Gbps

Спецификация не окончательная

Представляем vMX100 для Azure

Virtual MX доступен для Microsoft Azure

- 500 Mbps VPN
- Доступен в Azure Marketplace
- Полные возможности SD-WAN
- Та же модель лицензировани

MX портофолио – осень 2017

Teleworker

Z1

~5 users

802.11ac Wireless & PoE

FW throughput: 50-100 Mbps

New

Z3

Small Branch

MX64

MX65

~50 users

802.11ac wireless & PoE

FW throughput: 250 Mbps

Medium Branch

MX84

~200 users

FW throughput: 500 Mbps

MX100

~500 users

FW throughput: 750 Mbps

Large Branch, Campus or Concentrator

New

MX250

~2,000 users

FW throughput: 4 Gbps

MX400

~2,000 users

FW throughput: 1 Gbps

New

MX450

~10,000 users

FW throughput: 6 Gbps

MX600

~10,000 users

FW throughput: 1 Gbps

Virtual

New

vMX

vMX100 for AWS & Azure

FW throughput: 750 Mbps

VPN & SD-WAN features

Новый MX Firmware – Функции безопасности

MX 13.24 ()

- Threat Grid
- Правила firewall FQDN/hostname
- Syslog экспорт для событий AMP
- DNS-based Google safesearch и Youtube ограничения
- URL фильтрация по списку для HTTPS запросов на основе запроса сертификатов

Облачная безопасность

Cisco Umbrella и CloudLock

Обзор решений

- Umbrella – безопасный доступ к Internet для любого пользователя в любой сети с любого устройства через DNS

  Функционал SIG, обновление категорий, отчетность, мобильные и роуминг клиенты.

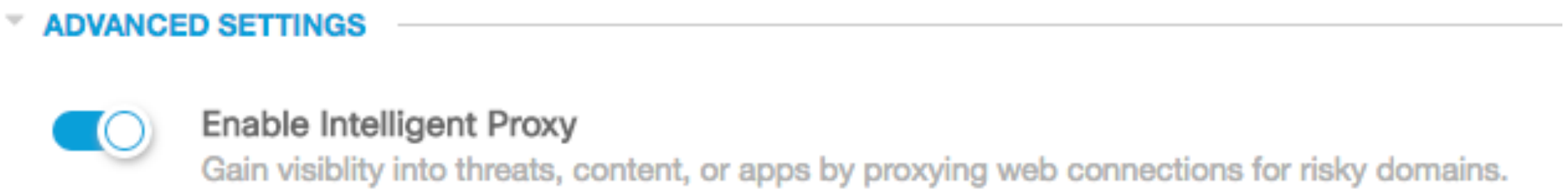
- Cloudlock – безопасность санционированных SaaS приложений

  Обновления Office 365, ServiceNow, App Discovery, и Cisco Spark.

- Полная видимость и защита в облаке

Cisco Umbrella

«Разумный» прокси (вышел)



Клиенты могут увидеть риски и угрозы с помощью проксирования трафика на порты 80/443.

- По умолчанию включен для новых политик
- Трафик проксируется если он в ”Grey List” Umbrella. Серый список – это набор доменов, которые являются «подозрительными», но не блокируются. Это управляется командой Umbrella.
- Трафик автоматически проксируется через нашу инфраструктуру если это включено в политике.

Инспекция файлов с помощью AMP и AV

Inspect Files

Selectively inspect files for malicious content using antivirus signatures and Cisco Advanced Malware Protection.

- Автоматически инспектирует файлы через прокси
- Инспекция с более чем ~200 расширениями
- Использование как AMP, так и AV для блокирования файлов
- Файл будет заблокирован при позитивном срабатывании

Блокирование URL

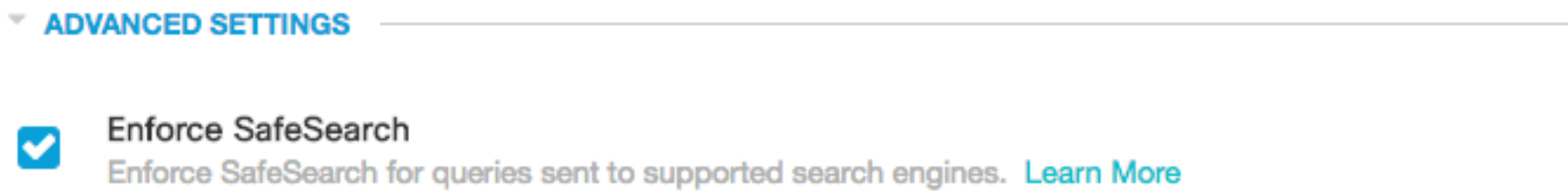
Позволяет заблокировать определенные URL путем перенаправления на прокси

- Клиенты могут блокировать любые URL, запрещенные в организации
- Добавление URL также блокирует любые «дочерние» URL, если они есть

SafeSearch (через DNS)

Позволяет организациям, которые хотят заблокировать контент к нежзелательному контенту заблокировать его в результатах поиска

- Google
- Bing
- YouTube



Коннекторы

AnyConnect

- Интеграция с Anyconnect на Windows и Mac
  - Защищает Anyconnect пользователей вне корпоративной сети

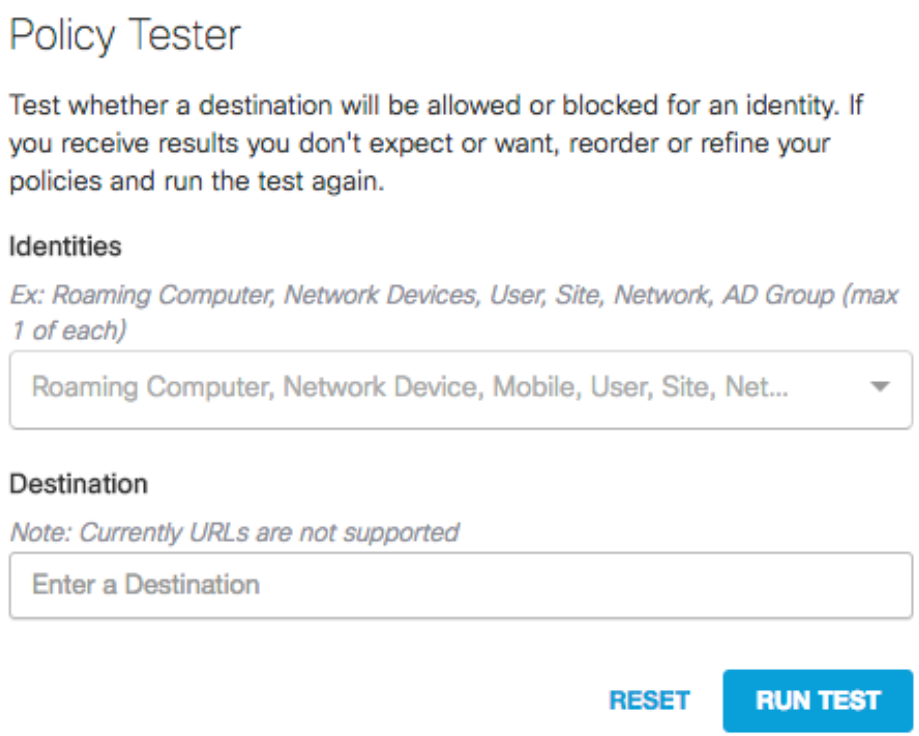
Роуминг-клиент

- Клиенты имеют возможность проксировать и защищать на IP ehjdyt yf Windows и MacCustomer ability to proxy and enforce at the IP Layer with the Windows and Mac Roaming Client (Released)
- Поддержка Active Directory (в работе)

Policy Tester (Released)

Enables administrators to understand whether or not a particular identity is blocked or allowed to go to a particular domain.

Administrators can now test the end state across all the policies they have configured to ensure their policies are working



Поддержка IPv6

Планируемая полная поддержка IPv6 в Umbrella

- Сейчас работает резолвинг адресов IPv6, но не политики

Блокирование приложений с помощью DNS

Возможность для Umbrella блокировать приложения с помощью DNS

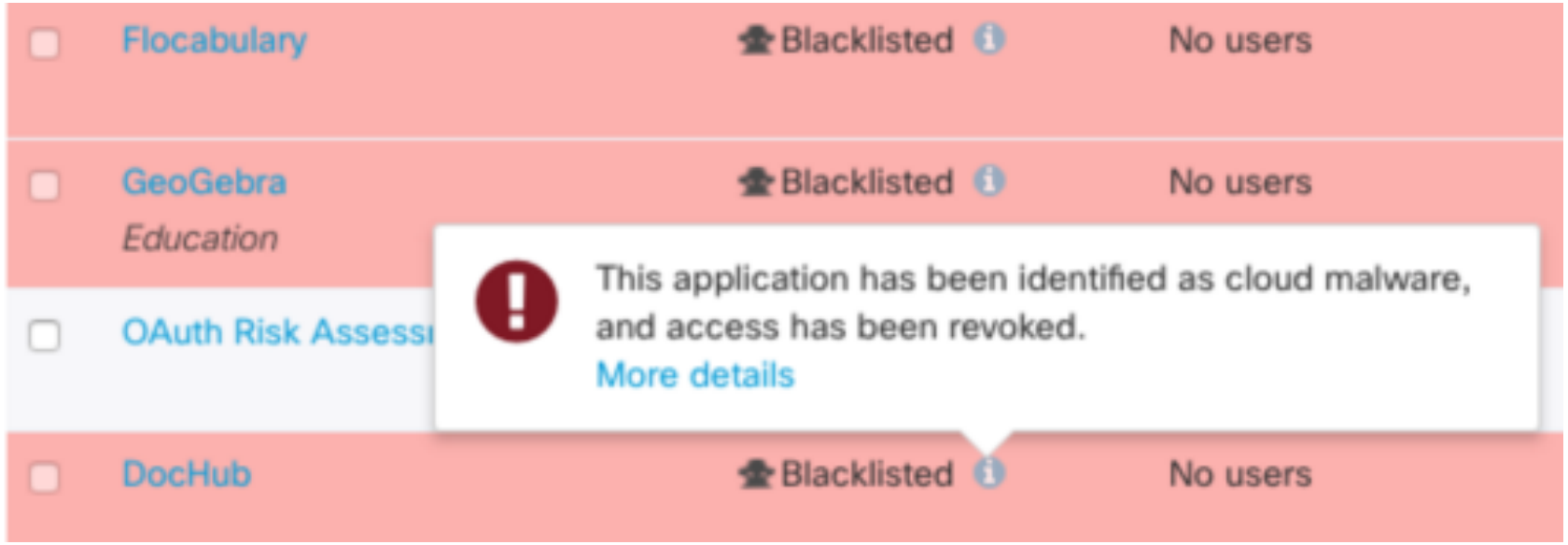
- Позволит организациям заблокировать определенные приложений через DNS
- Блокирование на основе политик
- Организации не надо будет знать все потенциальные домены для приложения. Umbrella использует свою базу данных для ассоциации доменов

Cisco Cloudlock

Cloudlock Apps Firewall

Последние улучшения

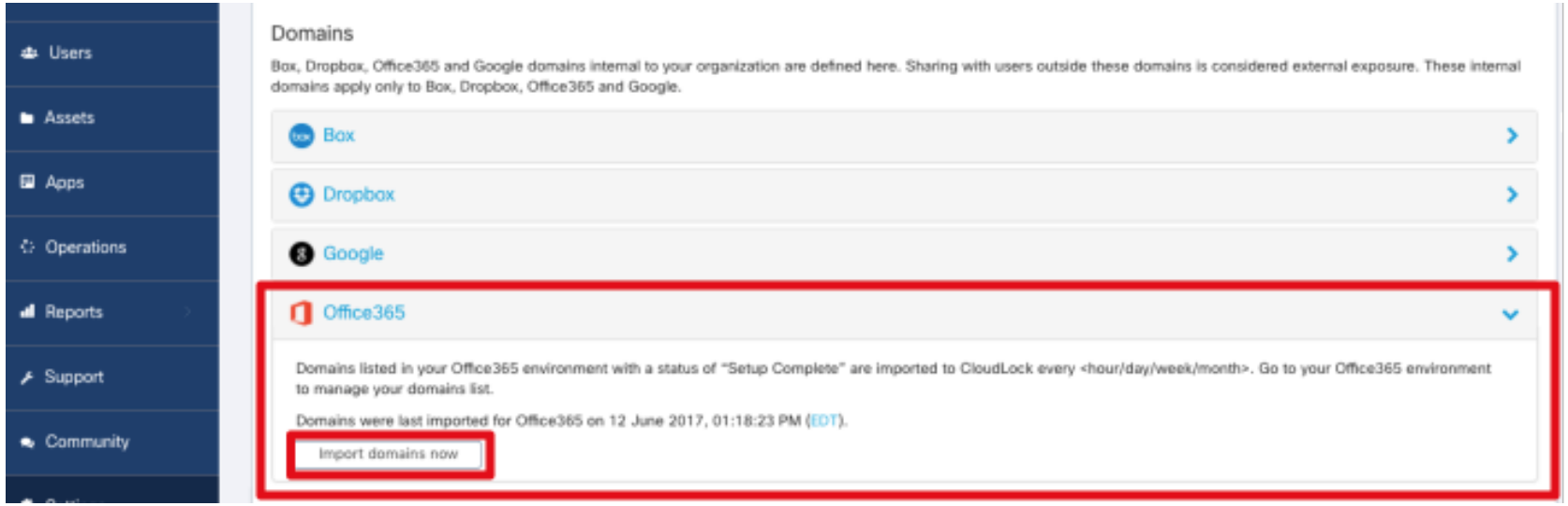
- Улучшили время обнаружения
- Черный список приложений



Cloudlock для Office 365

Последние улучшения

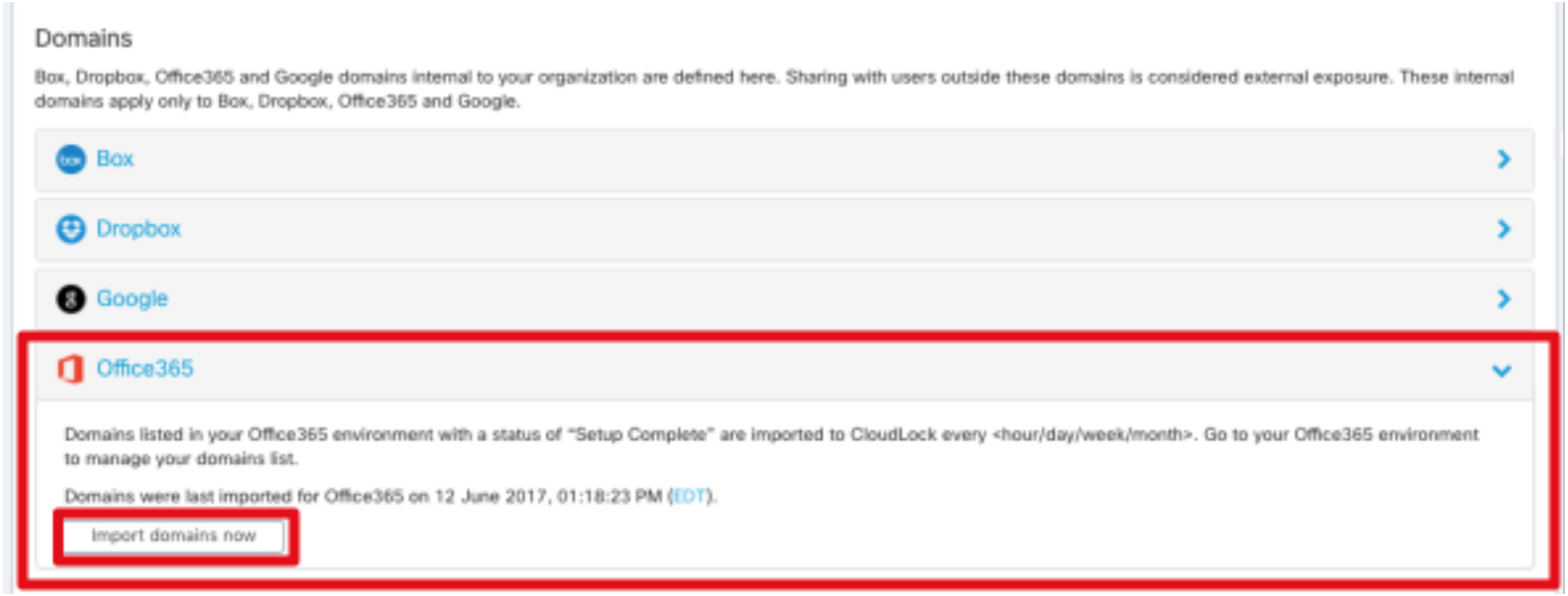
- Улучшенный процесс авторизации, больше не требуются права глобального админа для получения доступа к OneDrive и Sharepoint Online
- Возможность мониторинга или исключения определенных пользователей и групп



Cloudlock for Office 365 Improvements

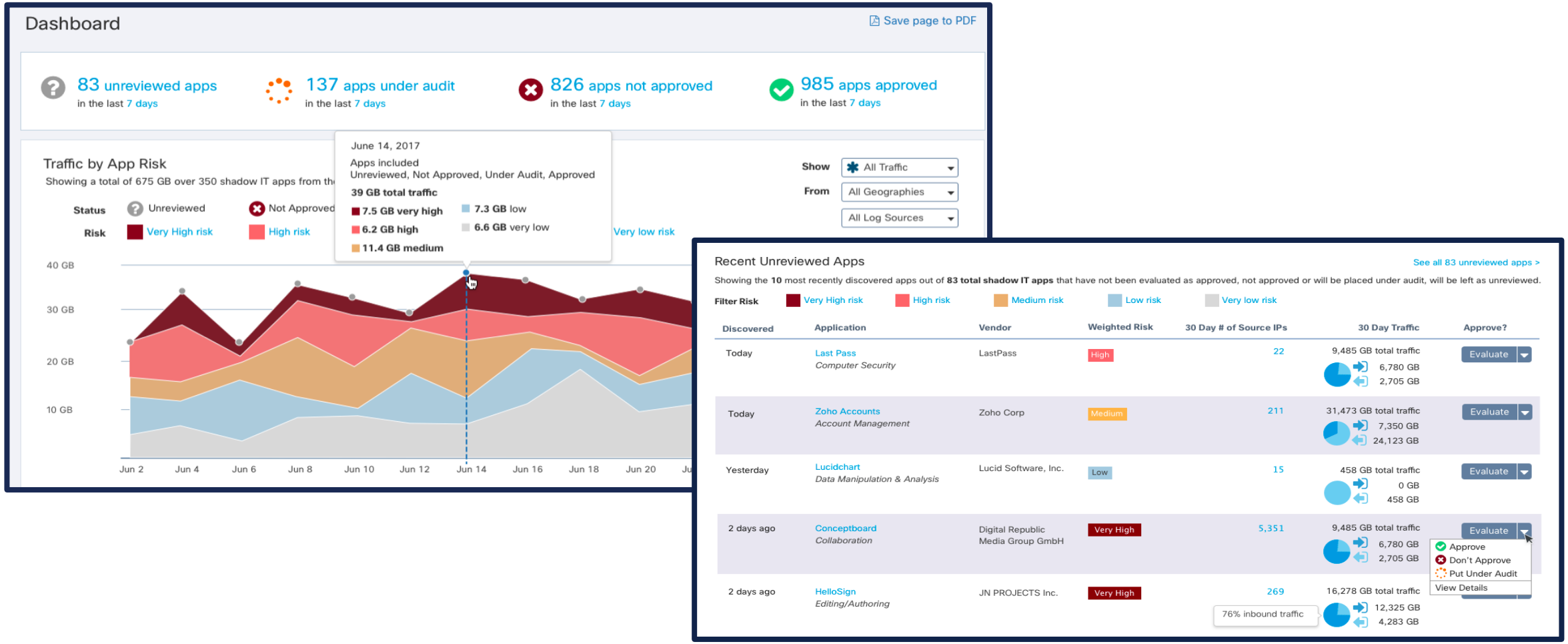
Recent Improvements

- Available domains automatically listed in platform configuration



Cloudlock App Discovery (Shadow IT)

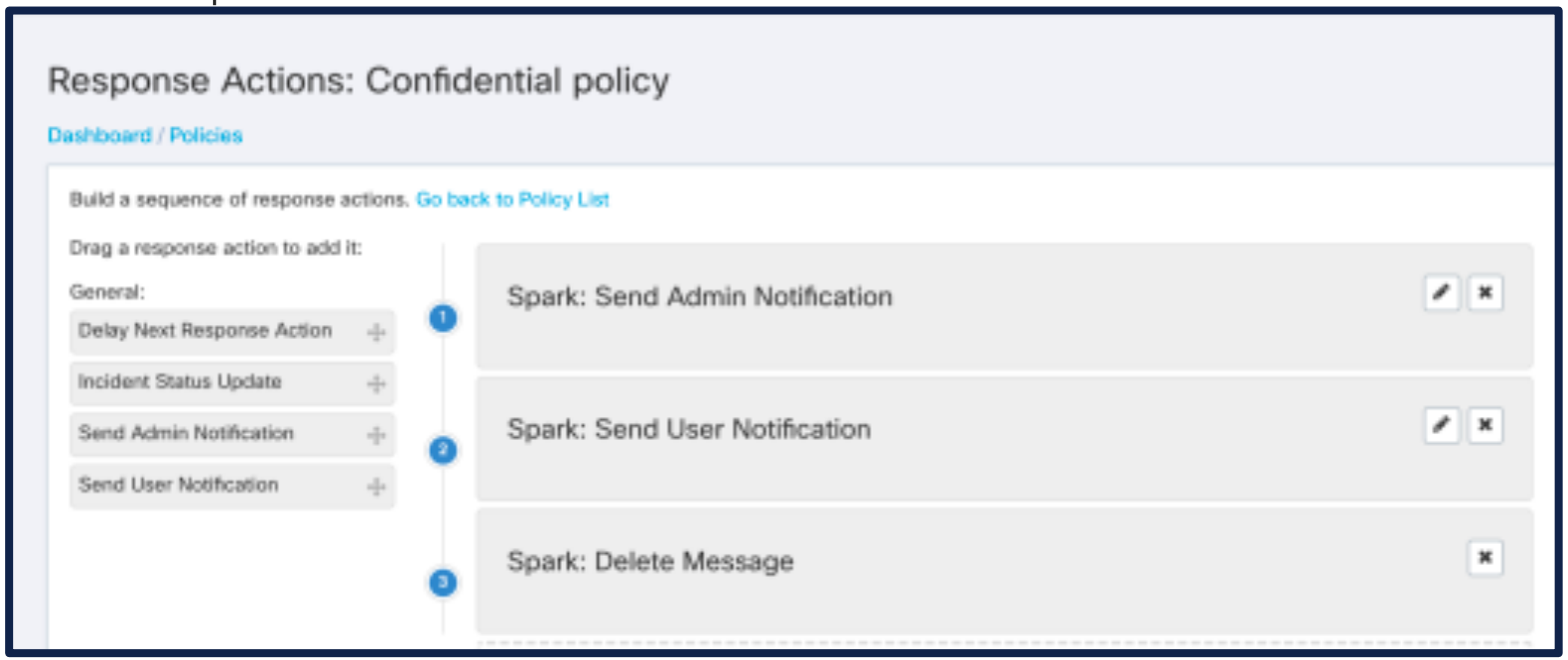
Сейчас в BETA



Cloudlock для Cisco Spark

Сейчас в BETA

- Идентификация чувствительной информации, которая существует в Spark spaces и загруженных файлах
- Нотификация о нарушениях политик на Spark
- Удаление сообщений и файлов



Email Security

- Email Security 11.0 и дальше

Email Security: ключевые фазы развития

Улучшение безопасности

- Улучшенная эффективность анти- спам, фишинг, спуфинг
- Интеграция
- Advanced Threat Detection

Гибкость платформы

- Образы для приватных и публичных облаков
- Поддержка большого количества физических и виртуальных платформ

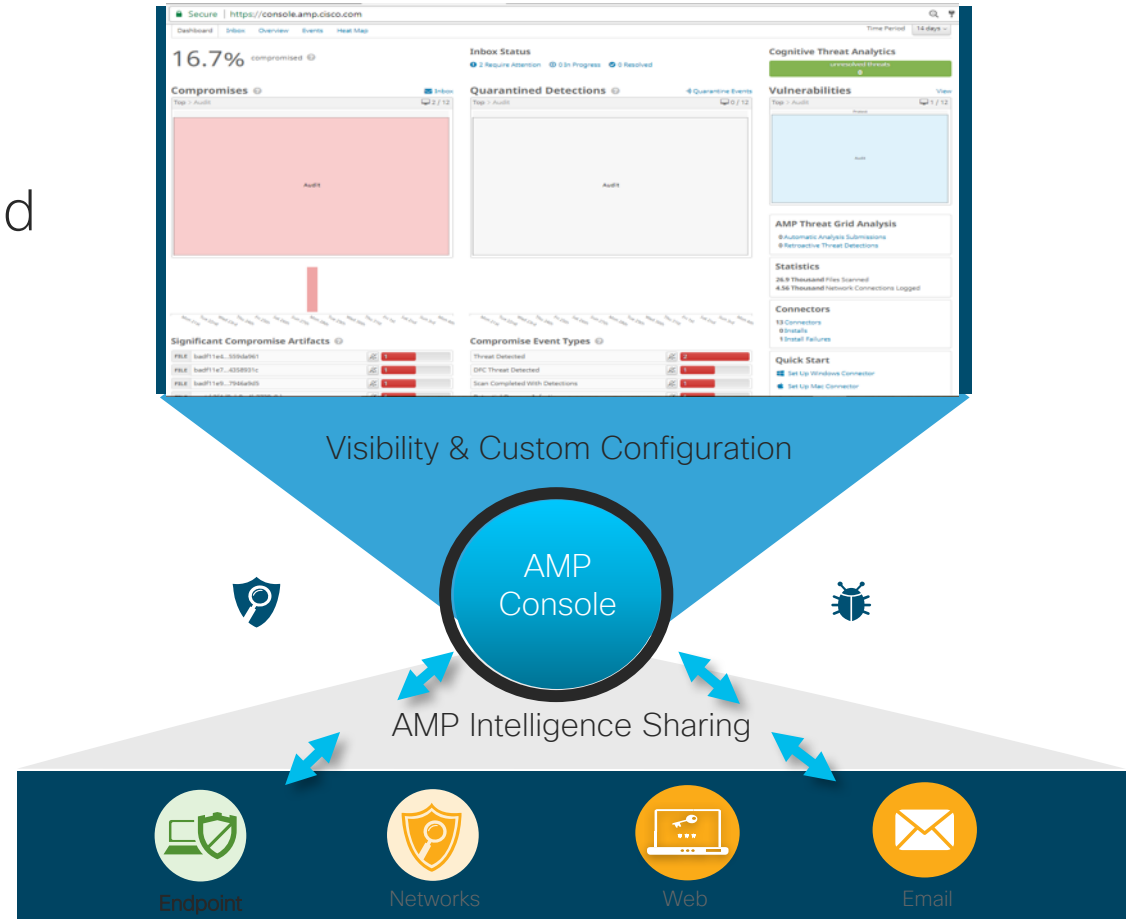
Улучшение UE

- Фокус на предоставлении улучшенных данных и инструментов для администраторов и аналитиков
- Выравние функционала CLI и GUI
- Соответствие с остальным портофолио Cisco

Email Gateway интегрируется в AMP консоль

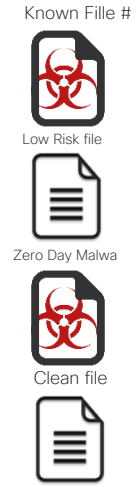
Видимость и контроль вредоносных файлов

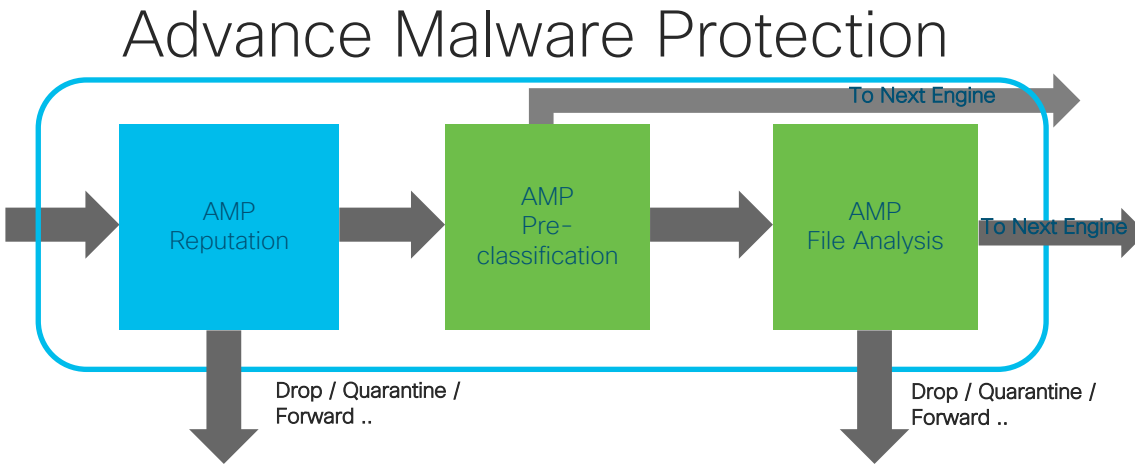
- Indicators of Compromise (IoC), File Trajectory
- несколько устройств (Email Gateways, End Points, Firewalls) и общая политика
- Whitelist, blacklist файловых хешей SHA через устройства



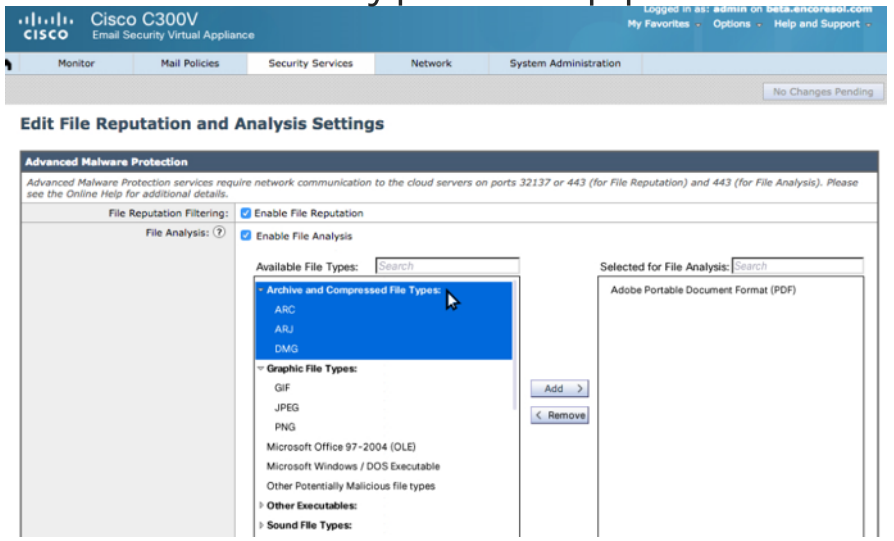
Улучшенные возможности AMP
Больше типов файлов и возможнстей

1. Расширение механизма классификации для детектирования файлов
2. Дополнение списка действий для подозрительных файлов
3. Поддержка всех типов файлов в AMP/TG
4. Возможность заблокировать ретро-предупреждения для файлов не в почтовом ящике пользователя





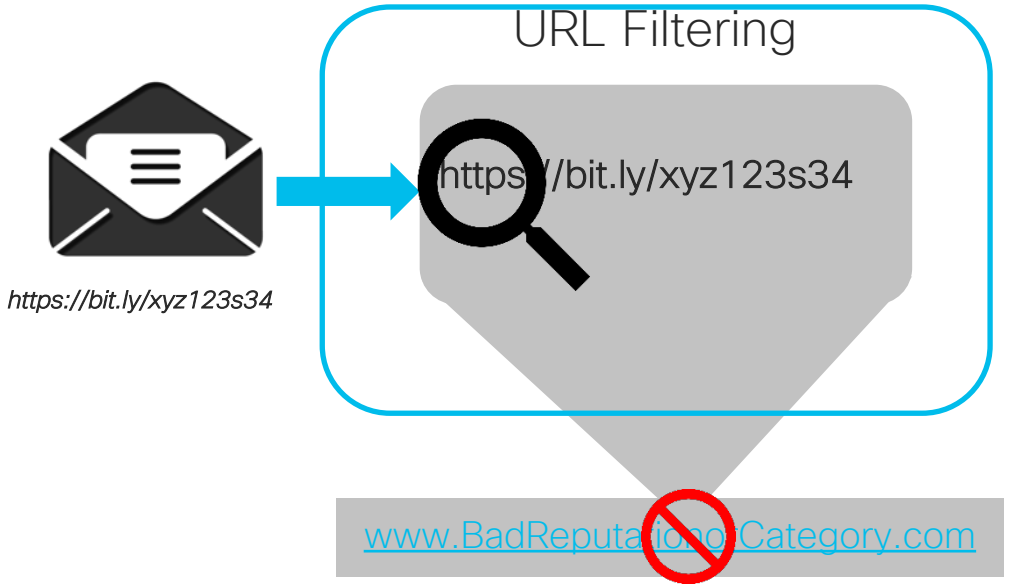
More File types supported

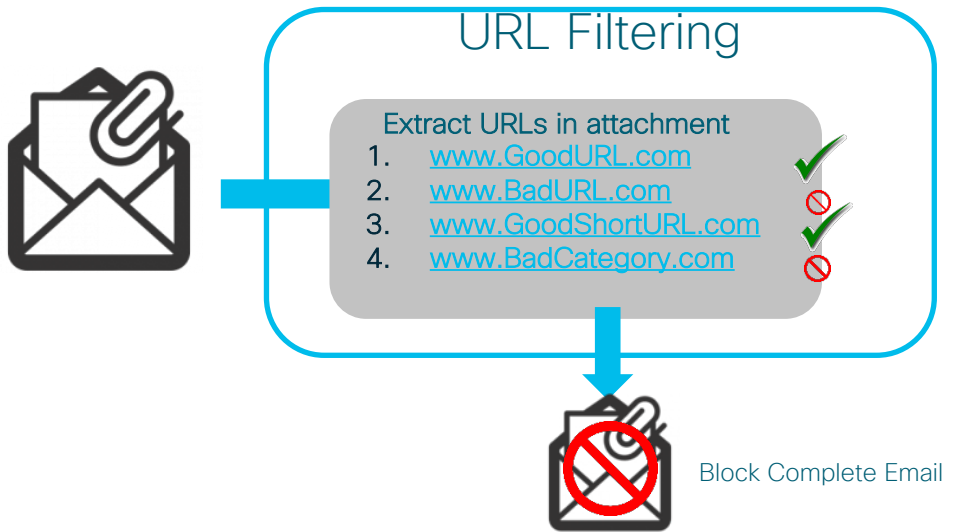


Augmented in 11.1

Улучшенная фильтрация URL
Защита от обфусцированных URL

- Обнаружение актуальных URL за сокращенными ссылками
- Обнаружение URL в присоединенных файлах

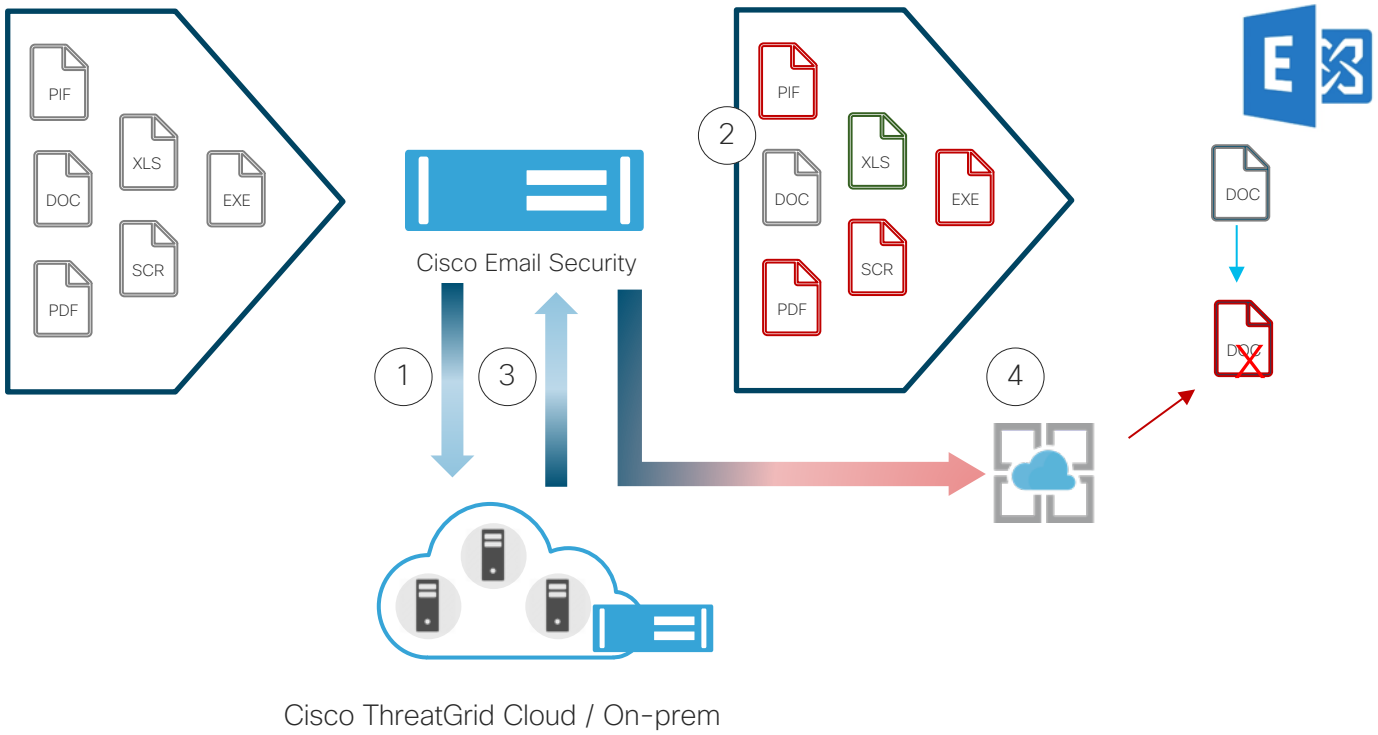




Mailbox Auto Remediation – MS Exchange

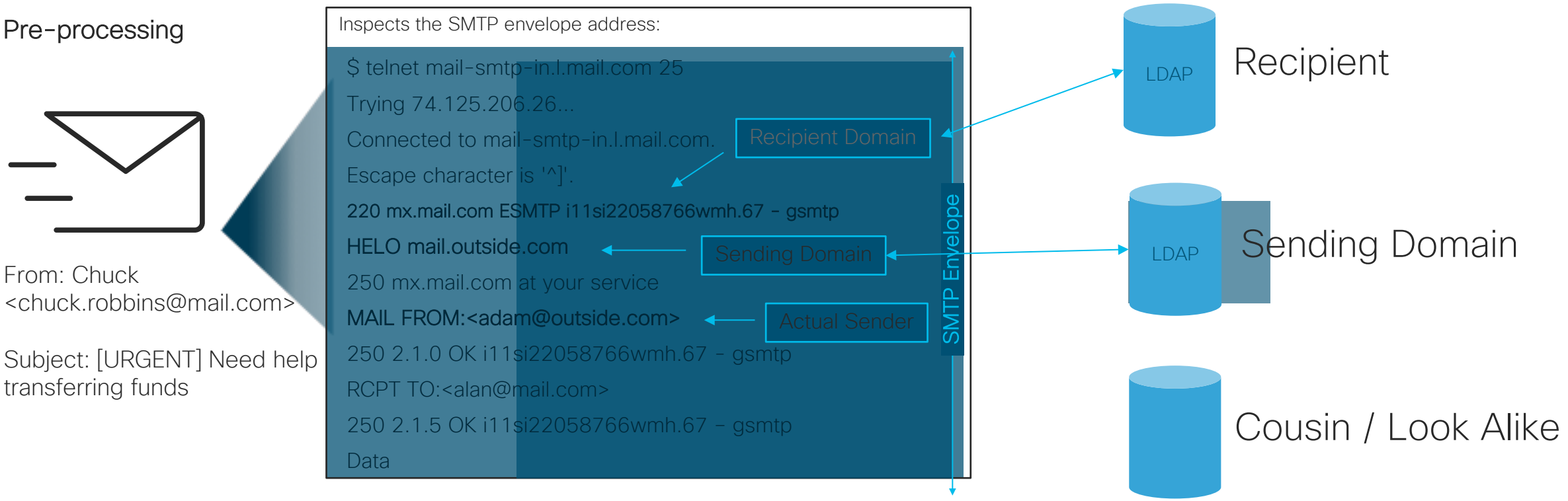
Уменьшайте время на реагирование

1. Аттач проанализирован
2. Аттач имеет неизвестное состояние и отправлен пользователю
3. Случилось ретроспективное событие и аттач оказался вредоносным
4. Автоматизированный вызов API позволяет удалить письмо из ящика пользователя



Forged Email Detection V2

Защита от спуфинг-атак / Business Email Compromise (BEC)

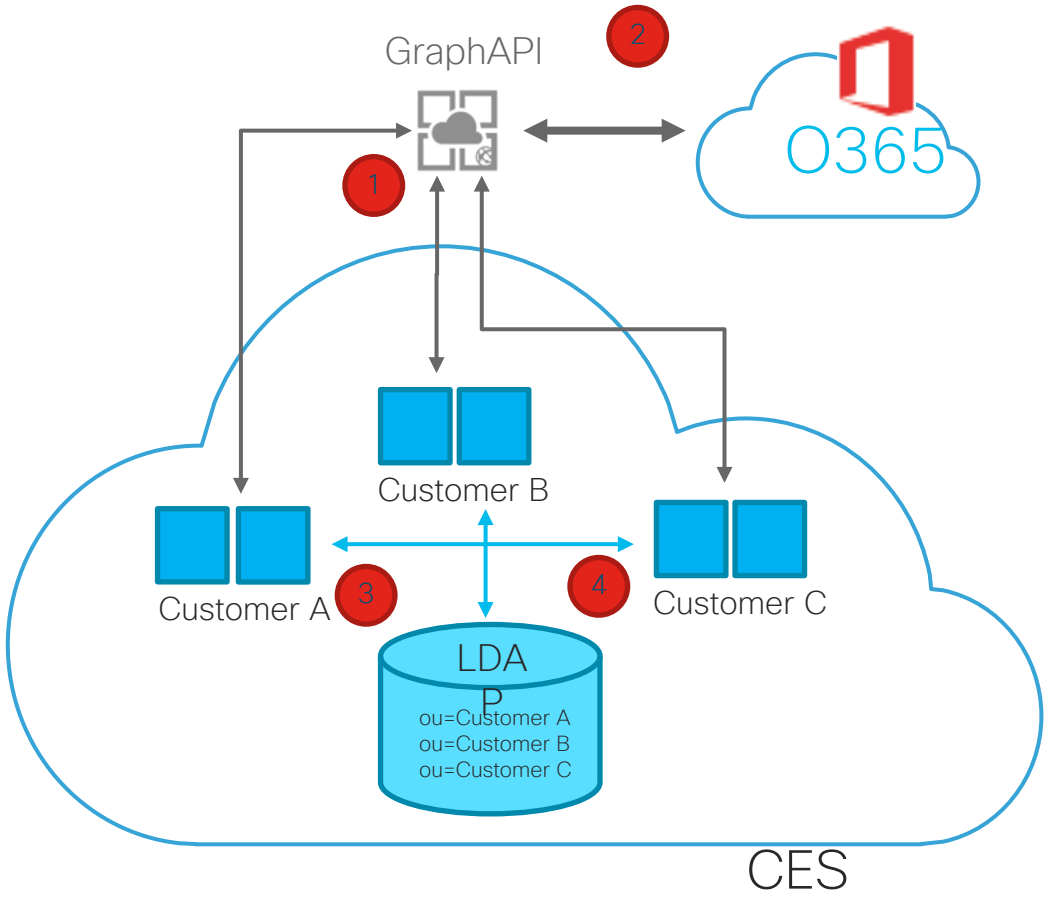


Inspect SMTP envelope for *True* sender address

Match sender address against company directory

O365 Connector

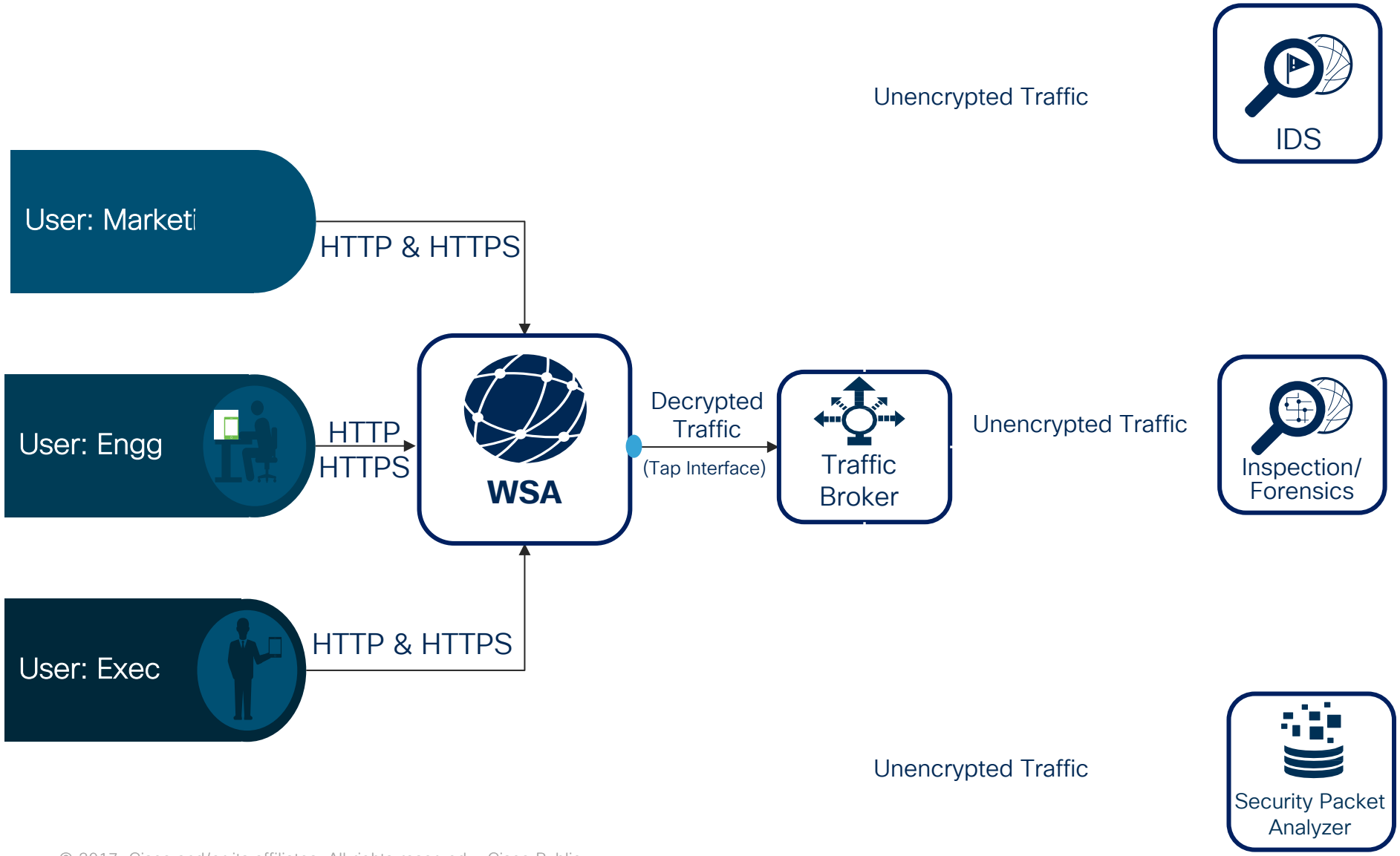
- Native LDAP and Mailbox Access functionality in CES with Azure
- Sync recipient and group information inside Azure AD with CES LDAP server
- Read-only access to the directory to review and verify records



Web Security Appliance

Web Traffic Tap

11.5

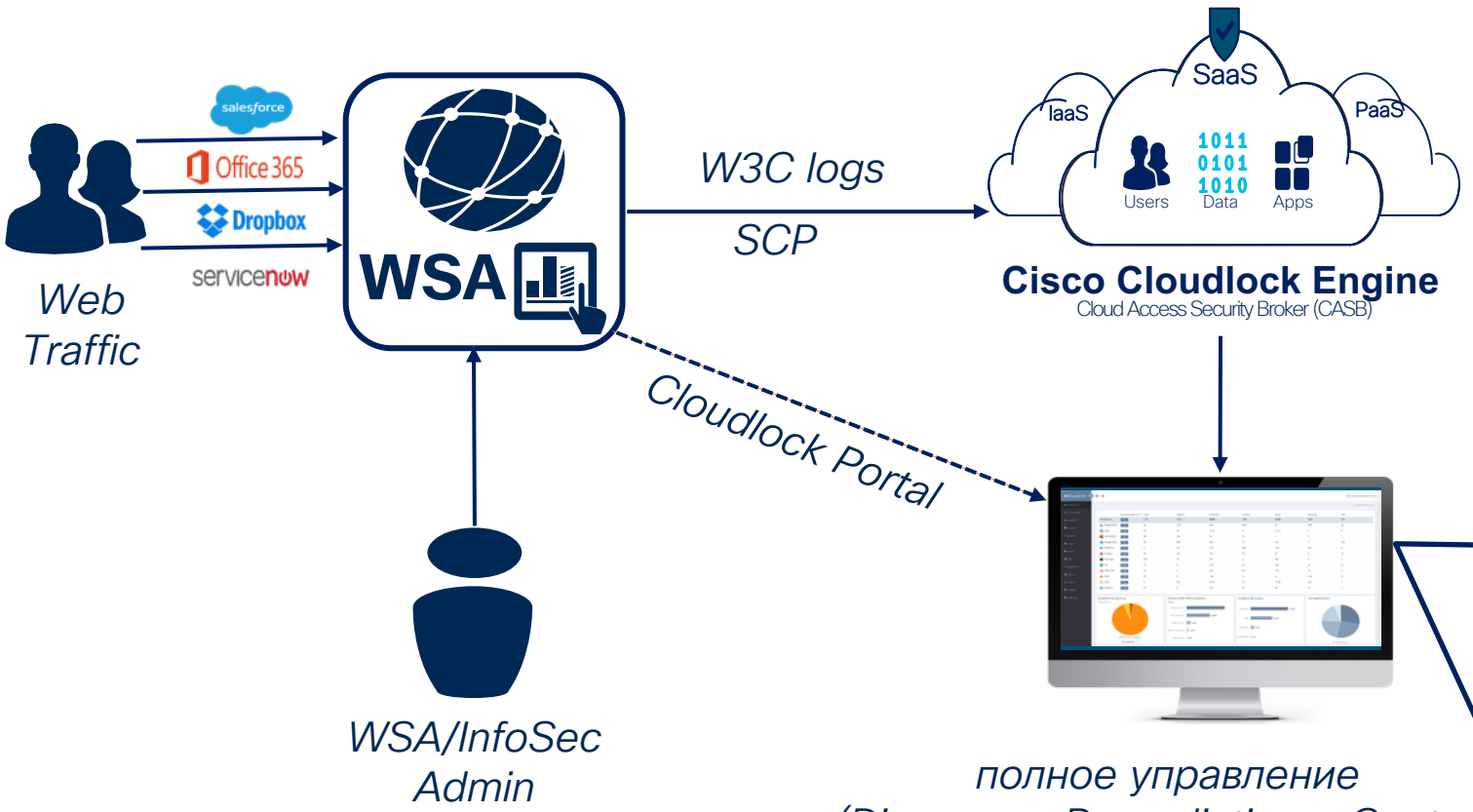


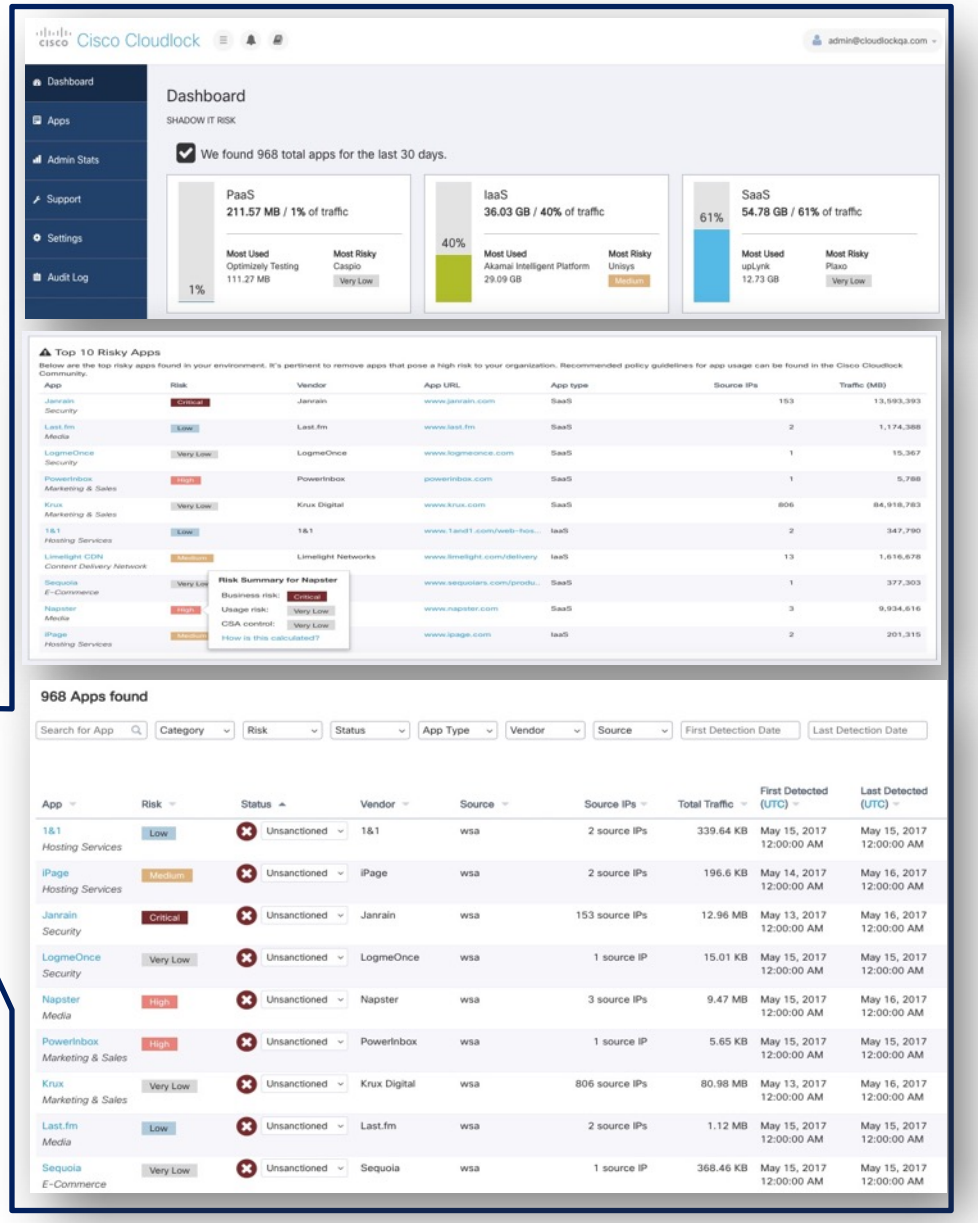
- High Performance SSL Decryption
- SSL Decryption only once for Network
- No Dedicated SSL Appliance Required
- Malware protection on SSL Traffic

Cisco Cloudlock интеграция

11.5

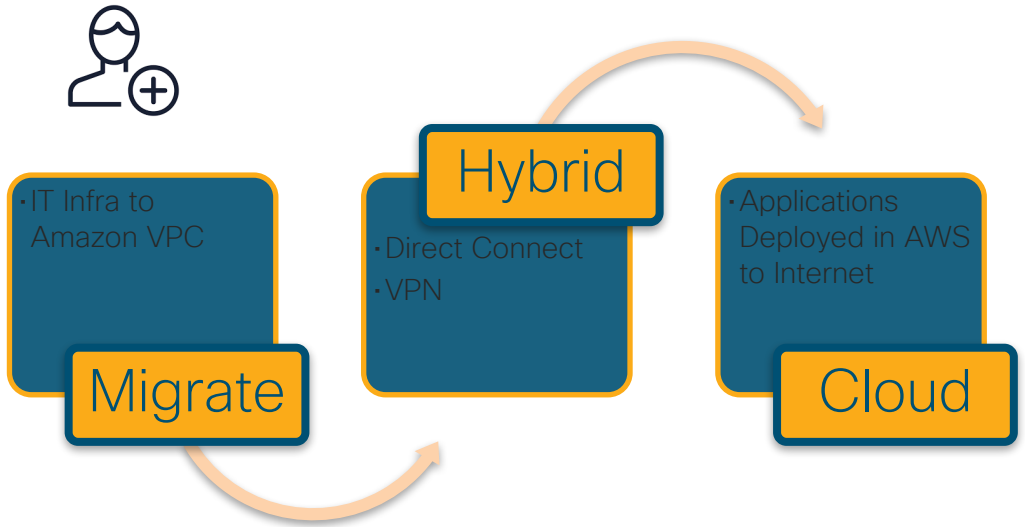
App Discovery



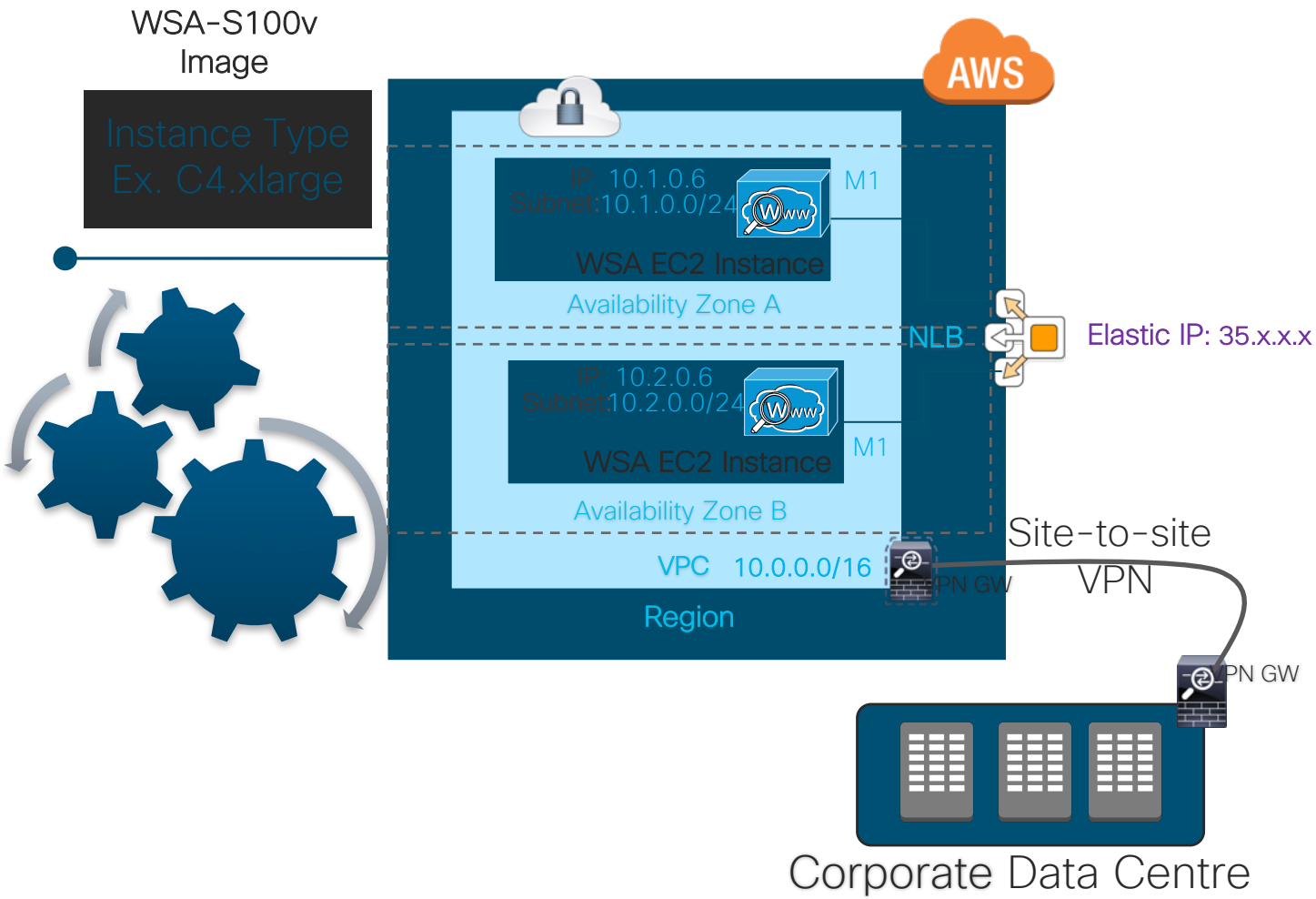


WSAv на Amazon Web Services

11.5

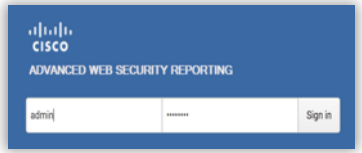


Virtual Image	AWS Instance Type
s100v	C4-xlarge
s300v	C4-2xlarge
s600v	C4-4xlarge

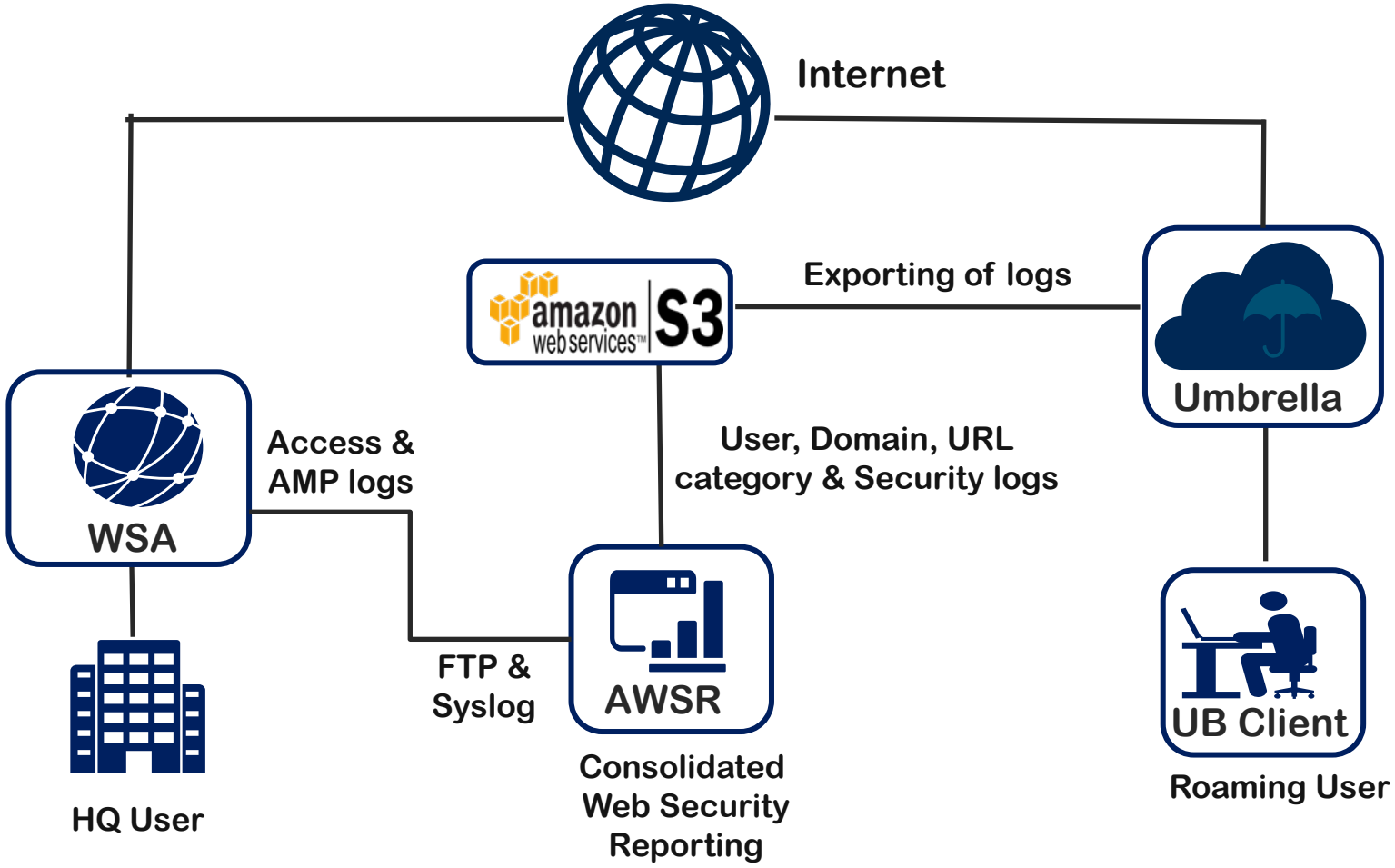


Ключевые возможности интеграции WSA

Advance Web Security Reporting v6.2



- Один механизм просмотра Web Security
- Настраиваемые отчеты
- Сохранение логов для расследований
- Групповые отчеты



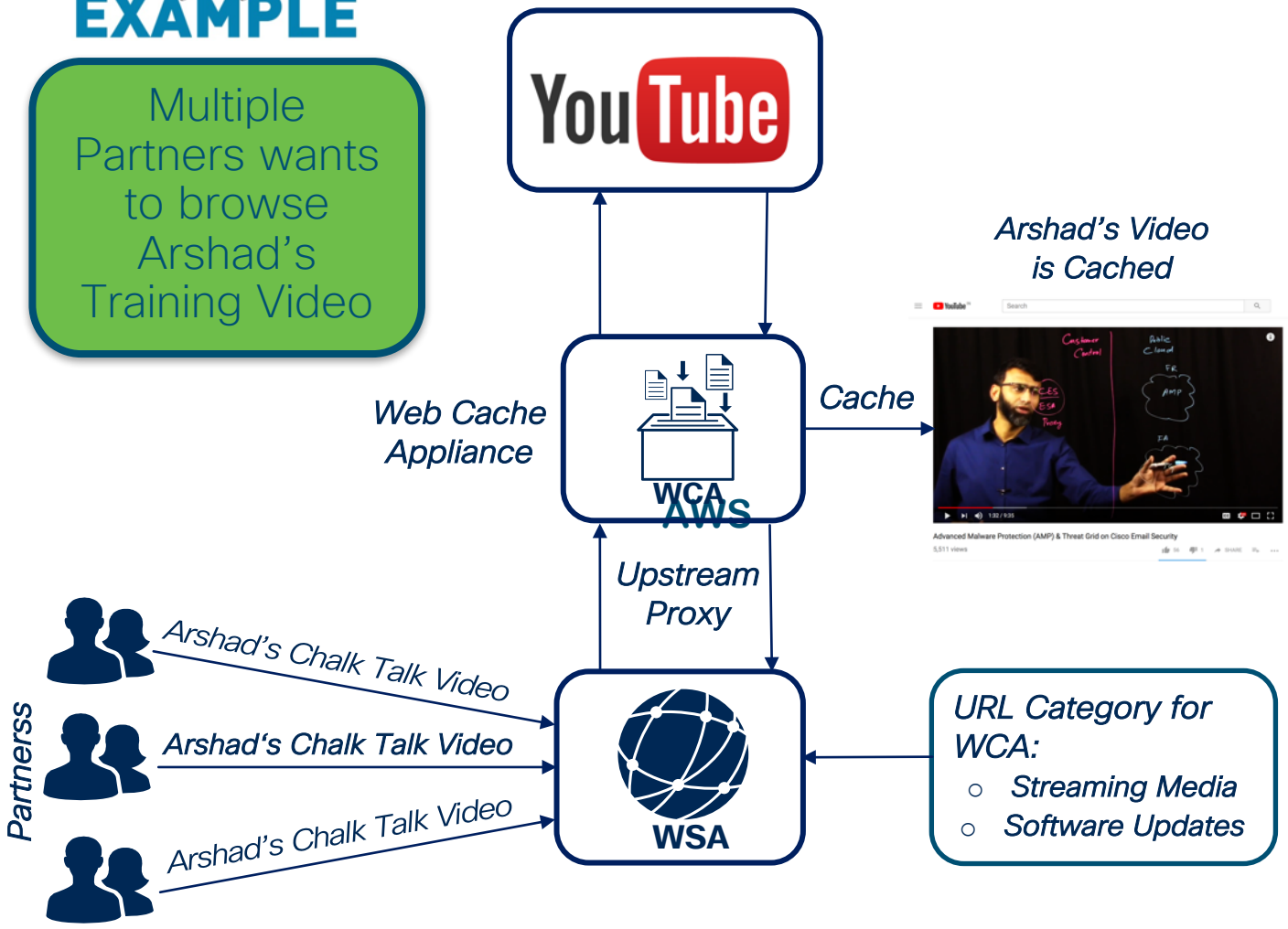
Video Caching Solution

Internet the way you want it.
Unveil Technology

- Saving Bandwidth
- Caching Video & Software Updates
- Blocking Adult Video content
- Video Resolution locker

Let me give you an
EXAMPLE

Multiple Partners wants to browse Arshad's Training Video

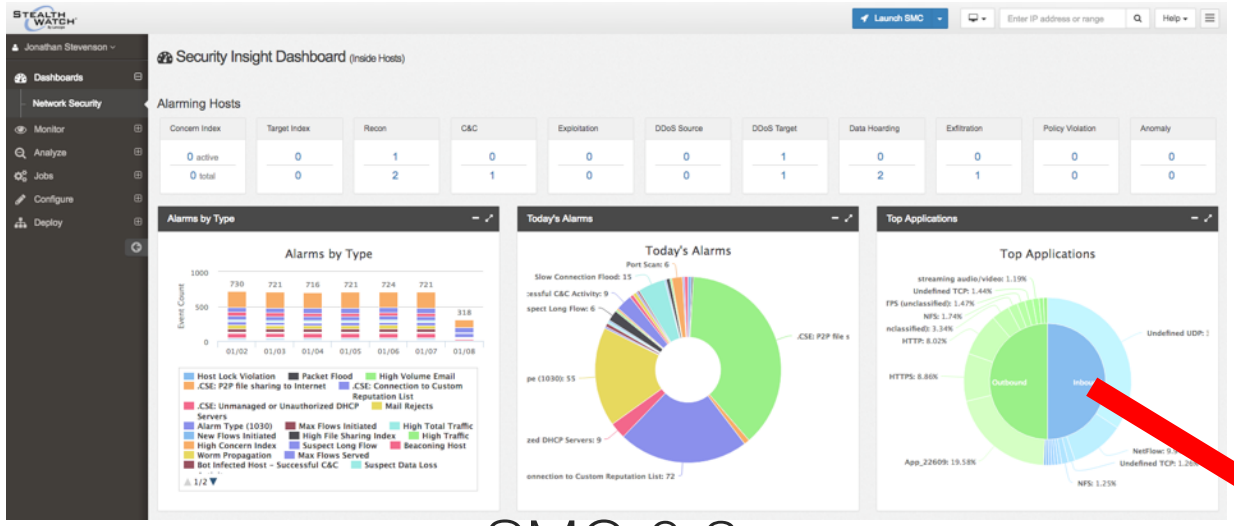


Stealthwatch

Аналитика безопасности для цифрового бизнеса

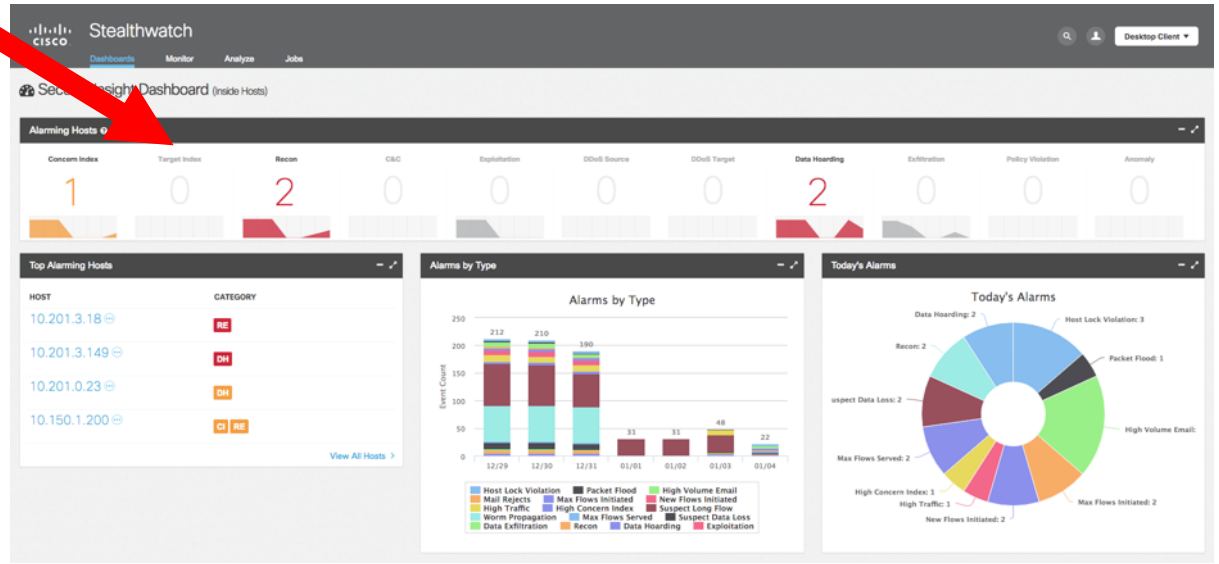
Новое в StealthWatch 6.9!

Существенные улучшения Web UI

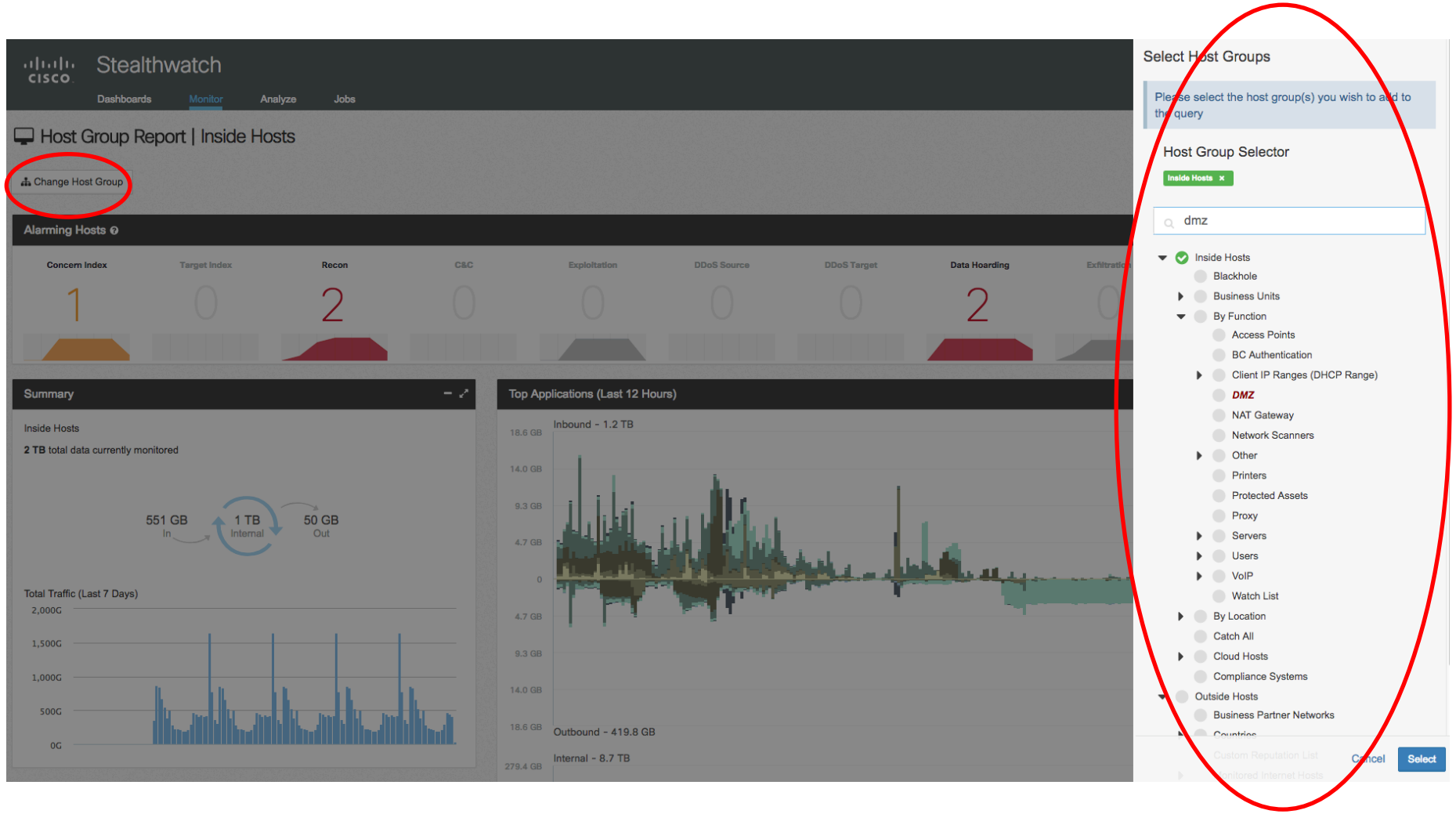


SMC 6.8

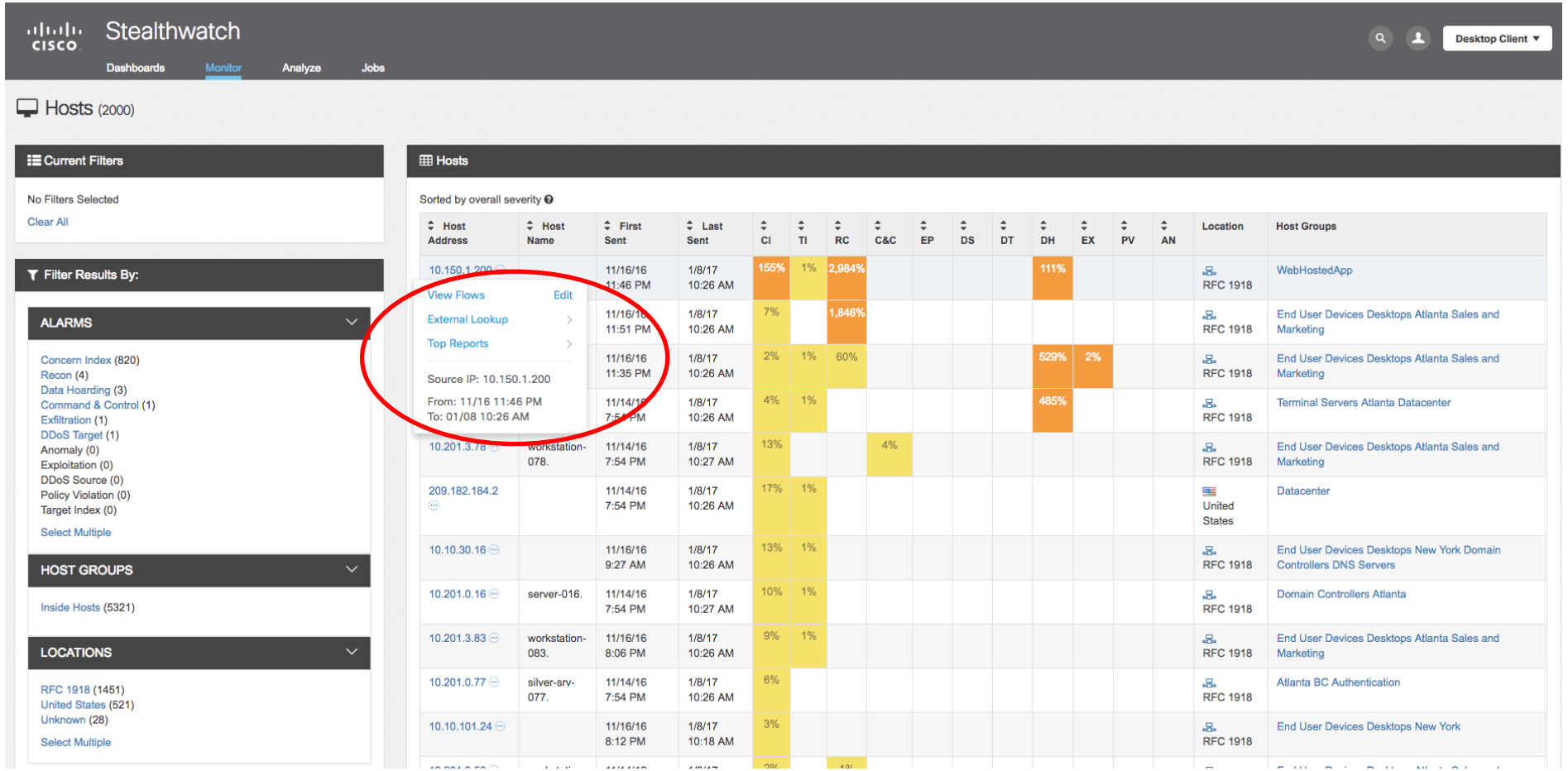
SMC 6.9



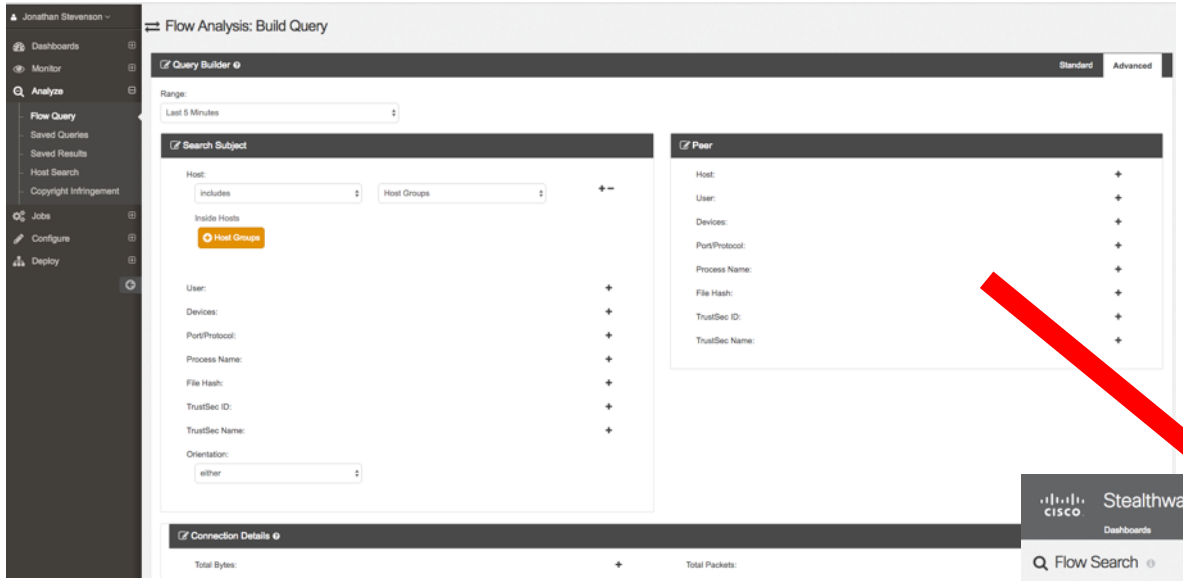
Host Group Reports



Поиск в ассоциированных потоках

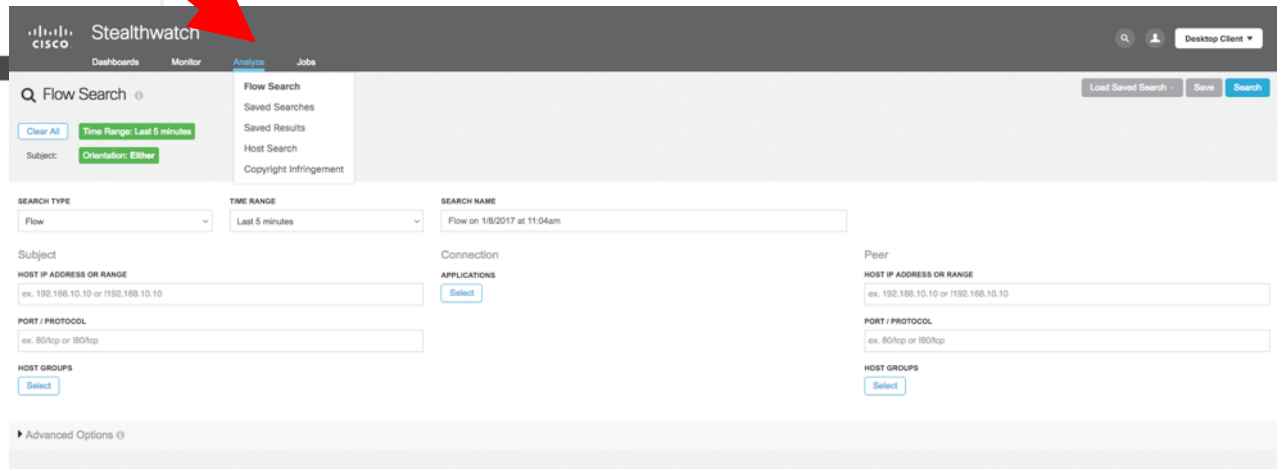


Расширенный поиск в потоках

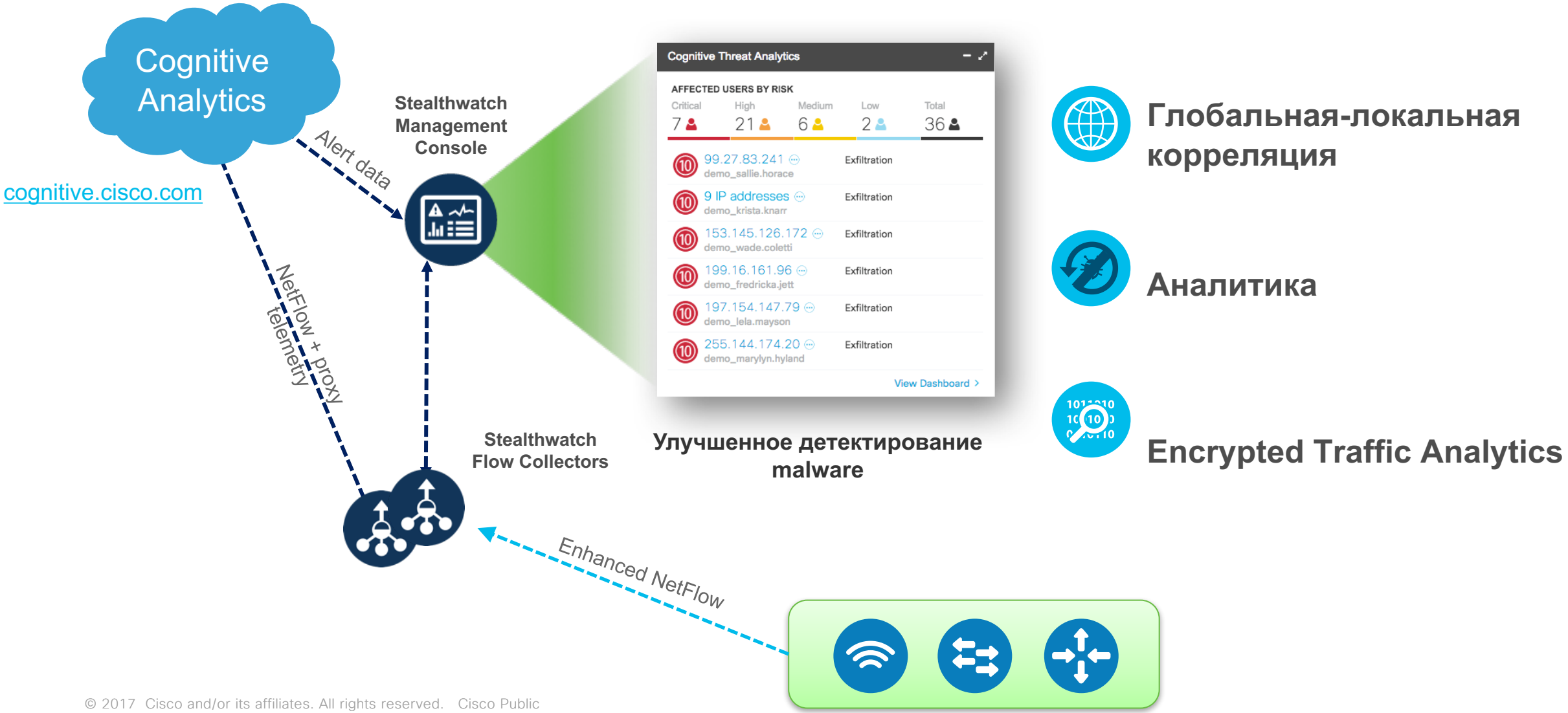


SMC 6.8

SMC 6.9

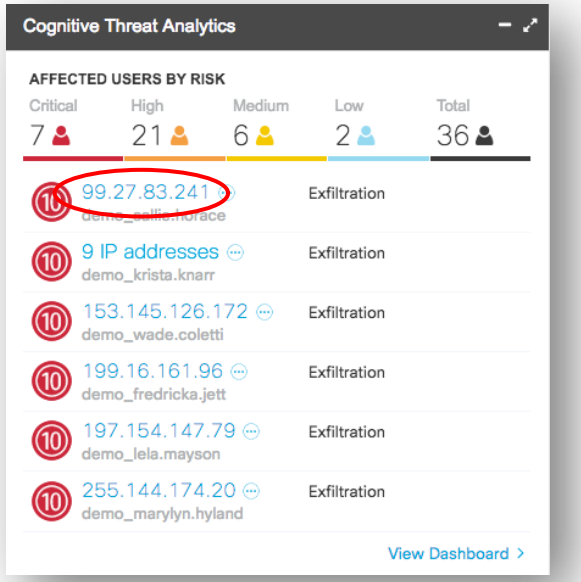


Stealthwatch и Cognitive Analytics



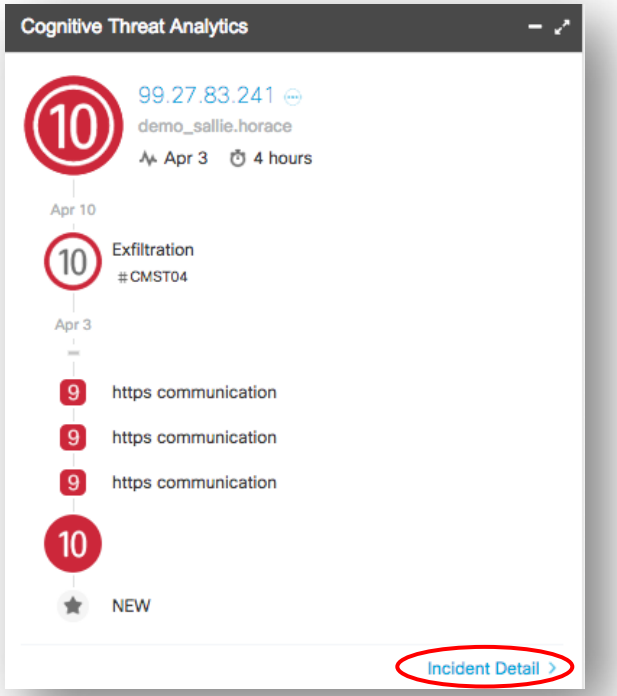
Stealthwatch ➤ Cognitive – User Flows

CTA виджет в SW



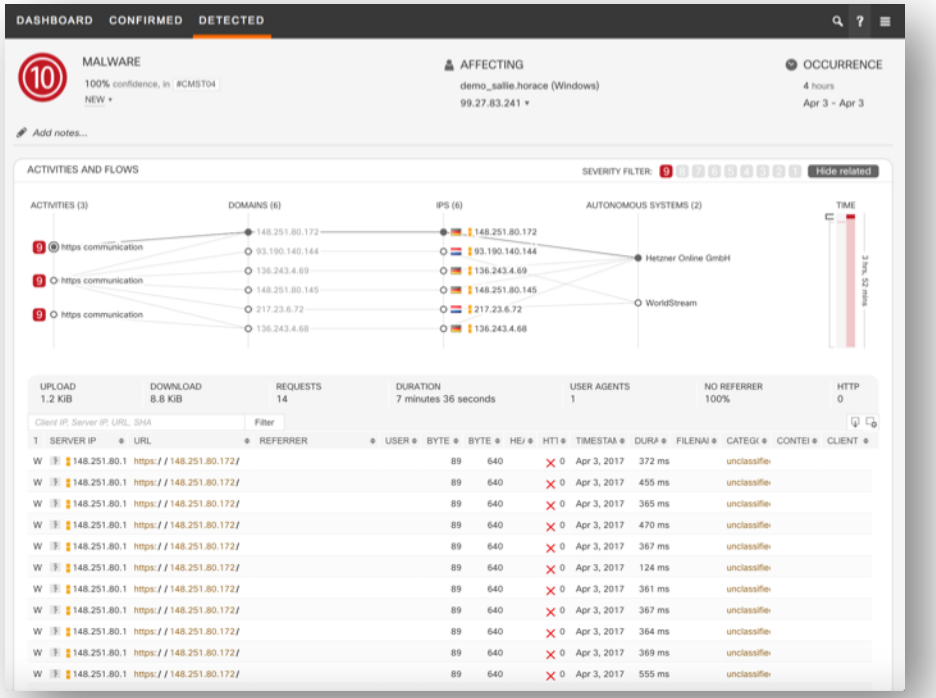
Выберите IP

CTA инцидент на консоли SW



Выберите детали

CTA в отдельном окне



CTA Dashboard на отдельной странице

Stealthwatch 6.10

Stealthwatch 6.10 – кратко

Расширения Web UI

- Расширенный поиск
  - Параметры запросов и результаты
  - Ограничение результатов запроса
  - Загрузка результатов запроса
  - Фильтрация результатов
- Расширенные группы событий
  - Host Report Security
  - Детали события безопасности
- Упрощение интерфейса

Отчеты о сети

- Статус и утилизация интерфейсов
- Host Group Traffic Widget

KVM Hypervisor support

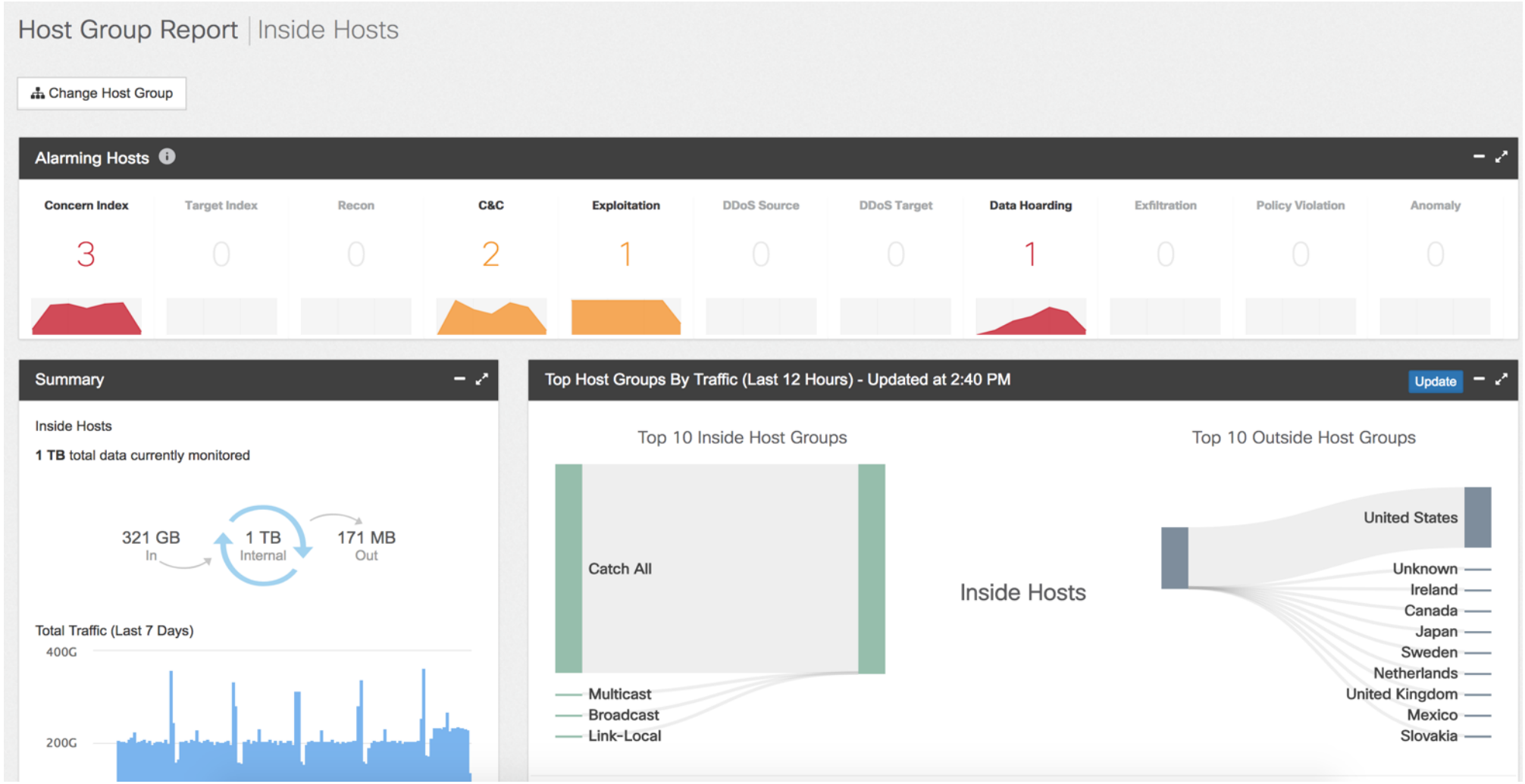
FIPS 140-2 Compliance

API enhancements

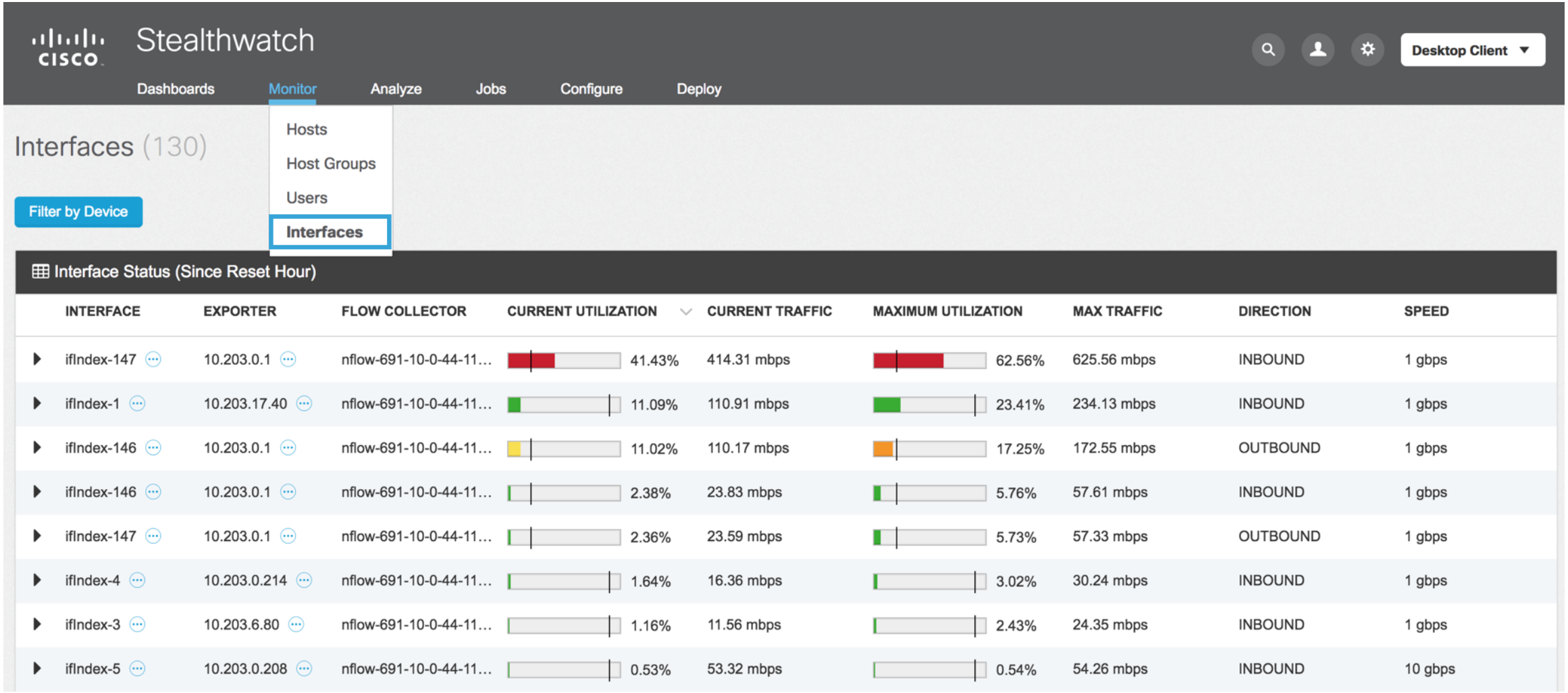
- Top reports
- Security events
- Network ops.

Расширения системы обновлений

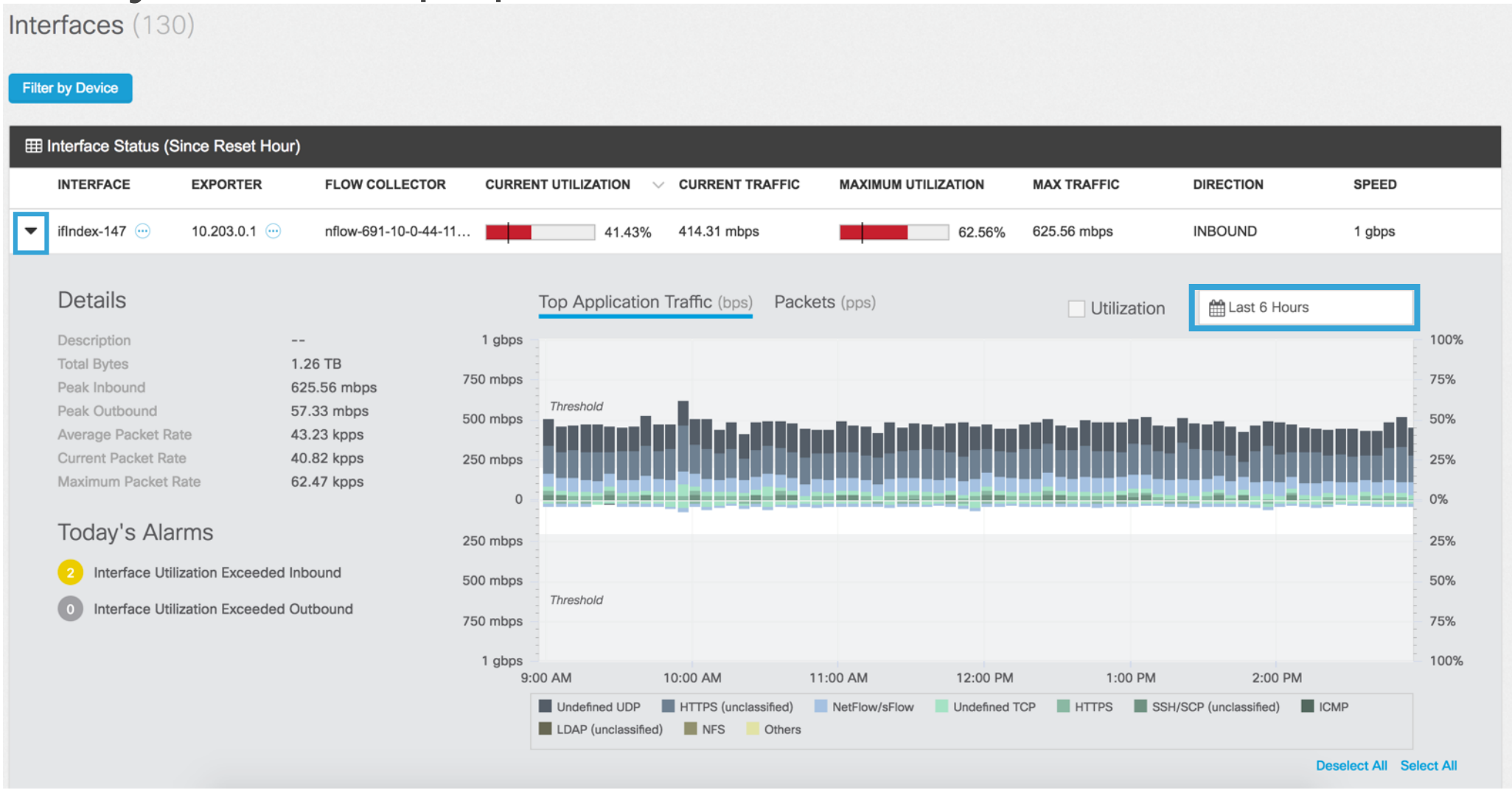
Host Group Dashboard Traffic Widget



Статус интерфейсов



Статус интерфейсов



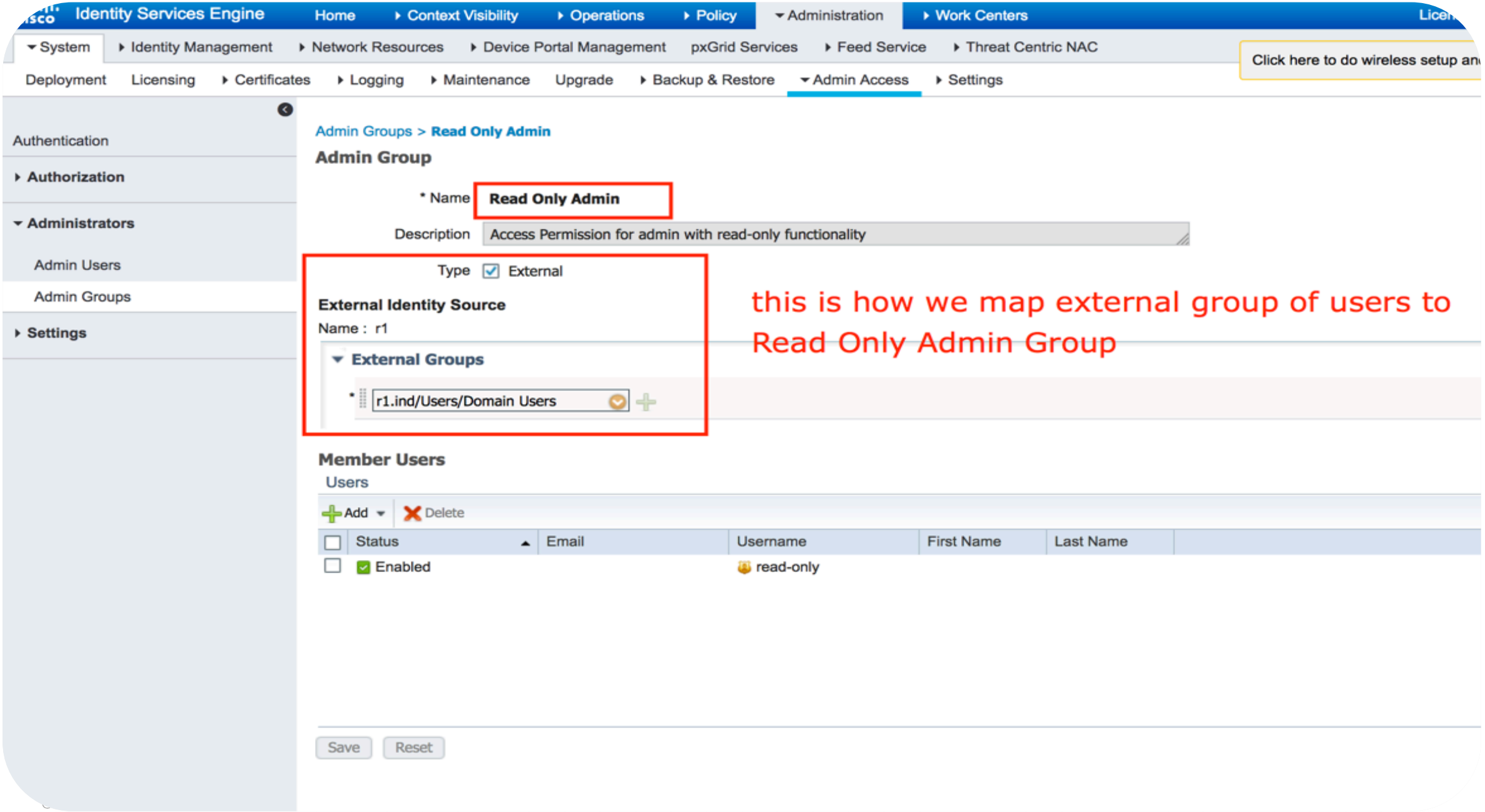
Обновления ISE

Он становится еще лучше!

ISE 2.3

Что вошло в релиз

- За сценой – не функциональные улучшения
- Администратор на чтение
- Логин используя Социальную сеть
- Коннектор Групповых политик
- Улучшения в Оценке состояния
- Изменения движка политик


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings
Click here to do wireless setup an
Authentication
Authorization
Administrators
Admin Users
Admin Groups
Settings
Admin Groups > Read Only Admin
Admin Group
* Name
Read Only Admin
Description
Access Permission for admin with read-only functionality
Type
External
External Identity Source
Name : r1
External Groups
r1.ind/Users/Domain Users
this is how we map external group of users to Read Only Admin Group
Member Users
Users
Add
Delete
Status
Email
Username
First Name
Last Name
Enabled
read-only
Save
Reset

Posture Issues Tackled by ISE 2.4

Customer Challenges

- Need to gracefully deal with end-user posture issues
- Need more flexibility with checks and remediation
- Need to see faster value from an ISE PoV

Seller Challenges

- Need to be able to tackle Forescount in their “agentless” story

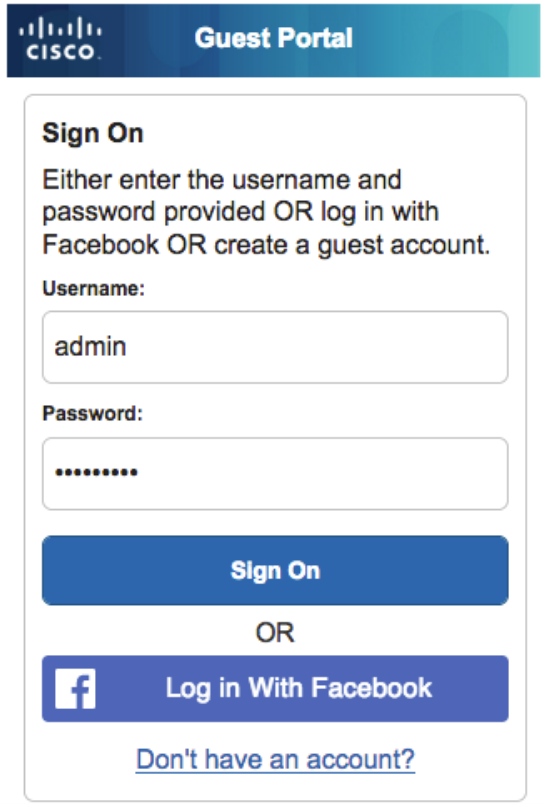
Логин через социальную сеть для гостей

Facebook логин для гостей (фаза 1)

Login using local ISE account

Create local ISE account

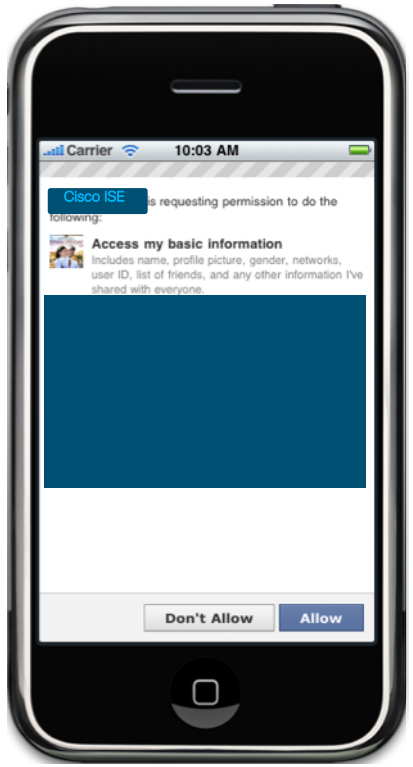
Login with social account



Phase 1 will include Facebook ONLY!!!

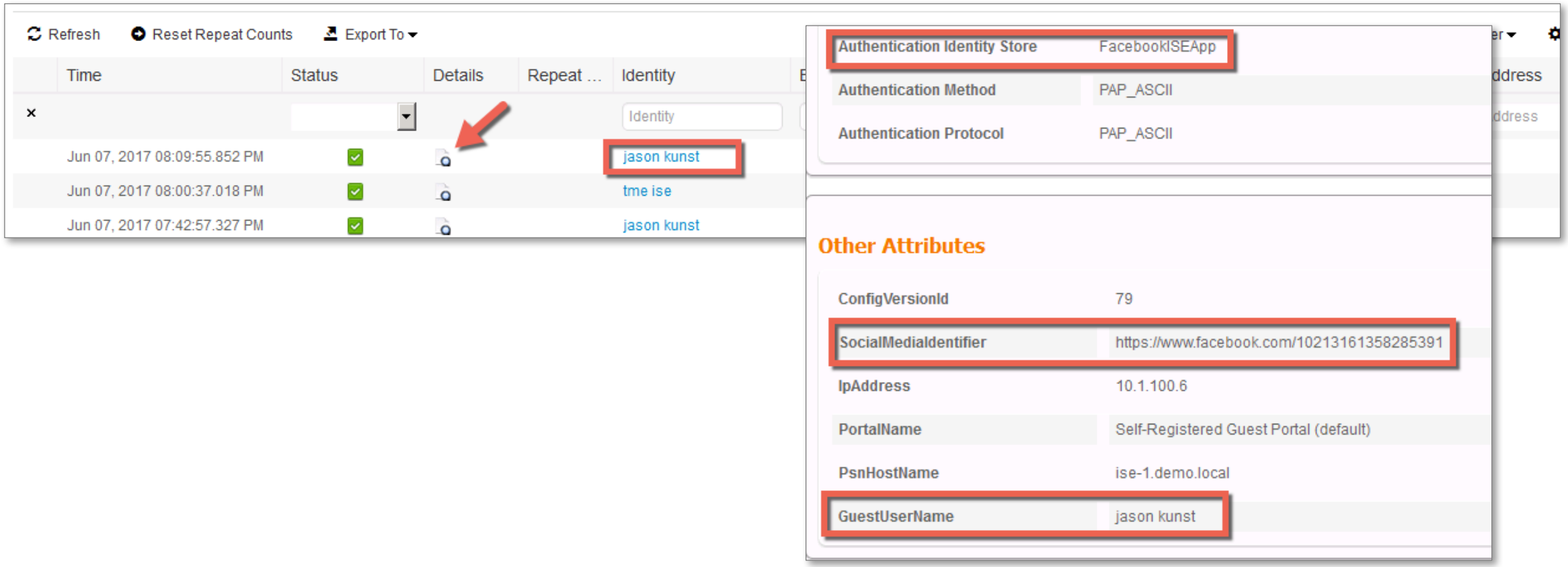
Доступ в первый раз

При первом заходе пользователь должен разрешить ISE получать базовые данные из Facebook



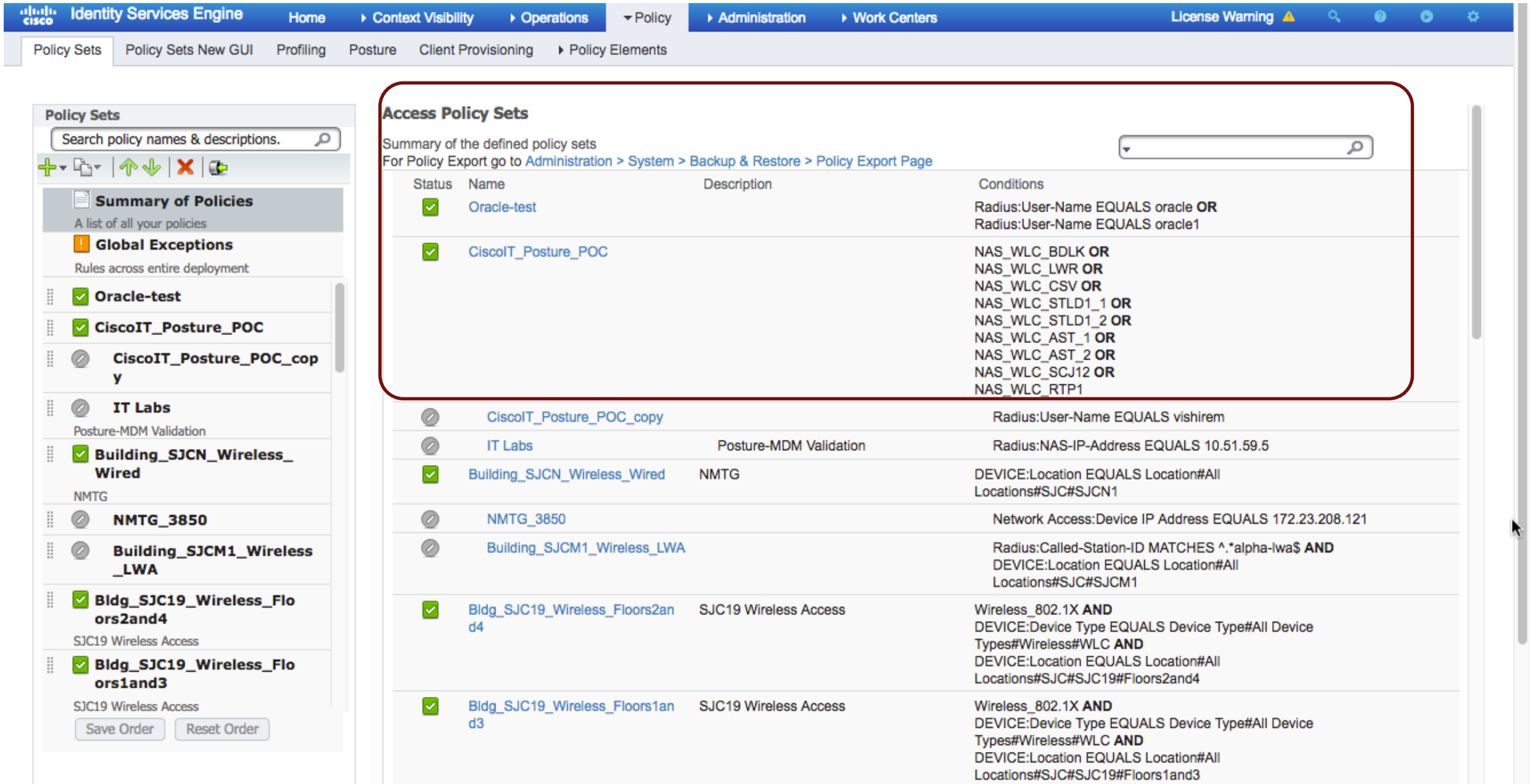
Информация в логах

Facebook Имя и идентификатор в Социальной сети

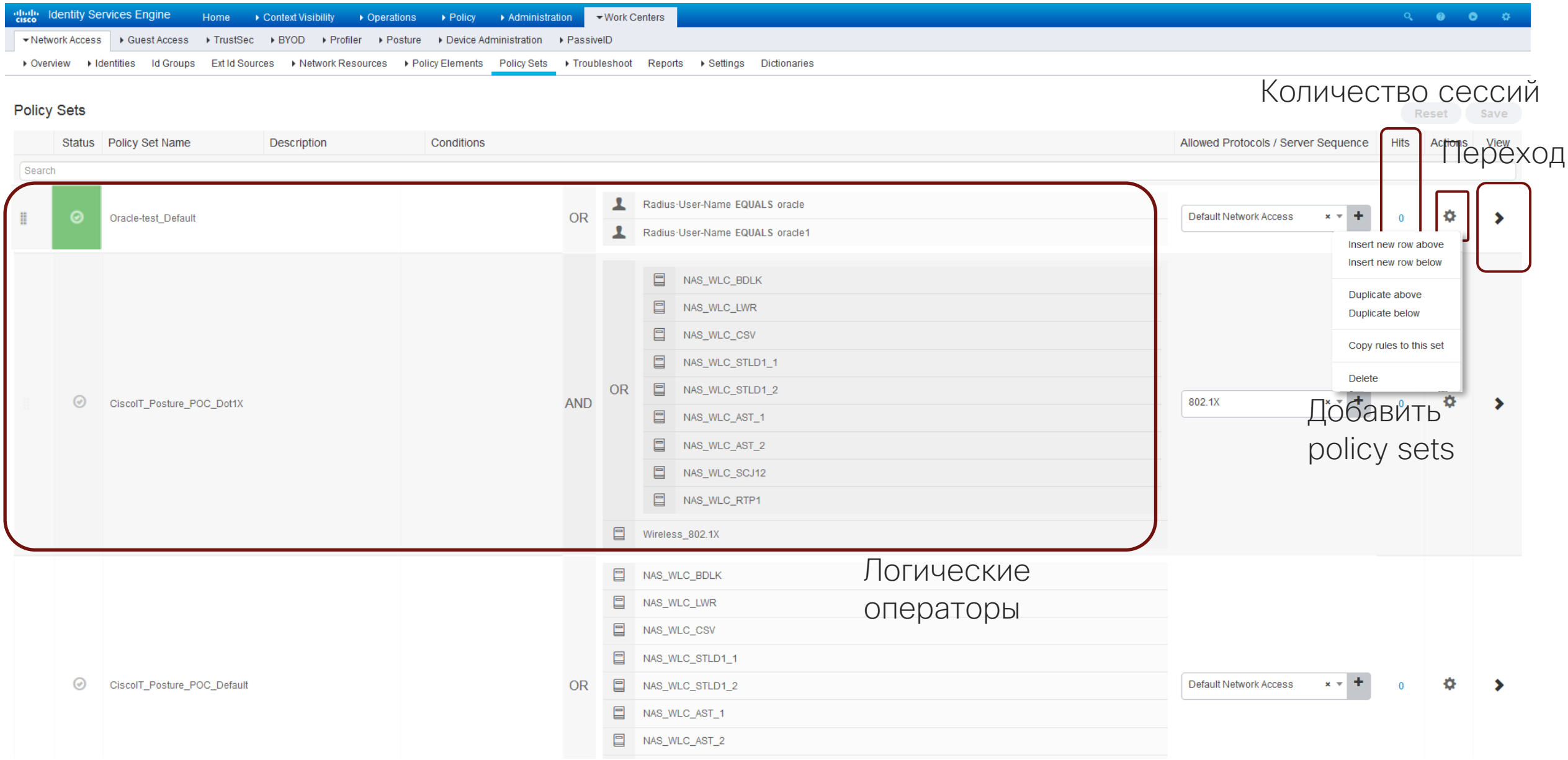


Улучшения в Policy UI

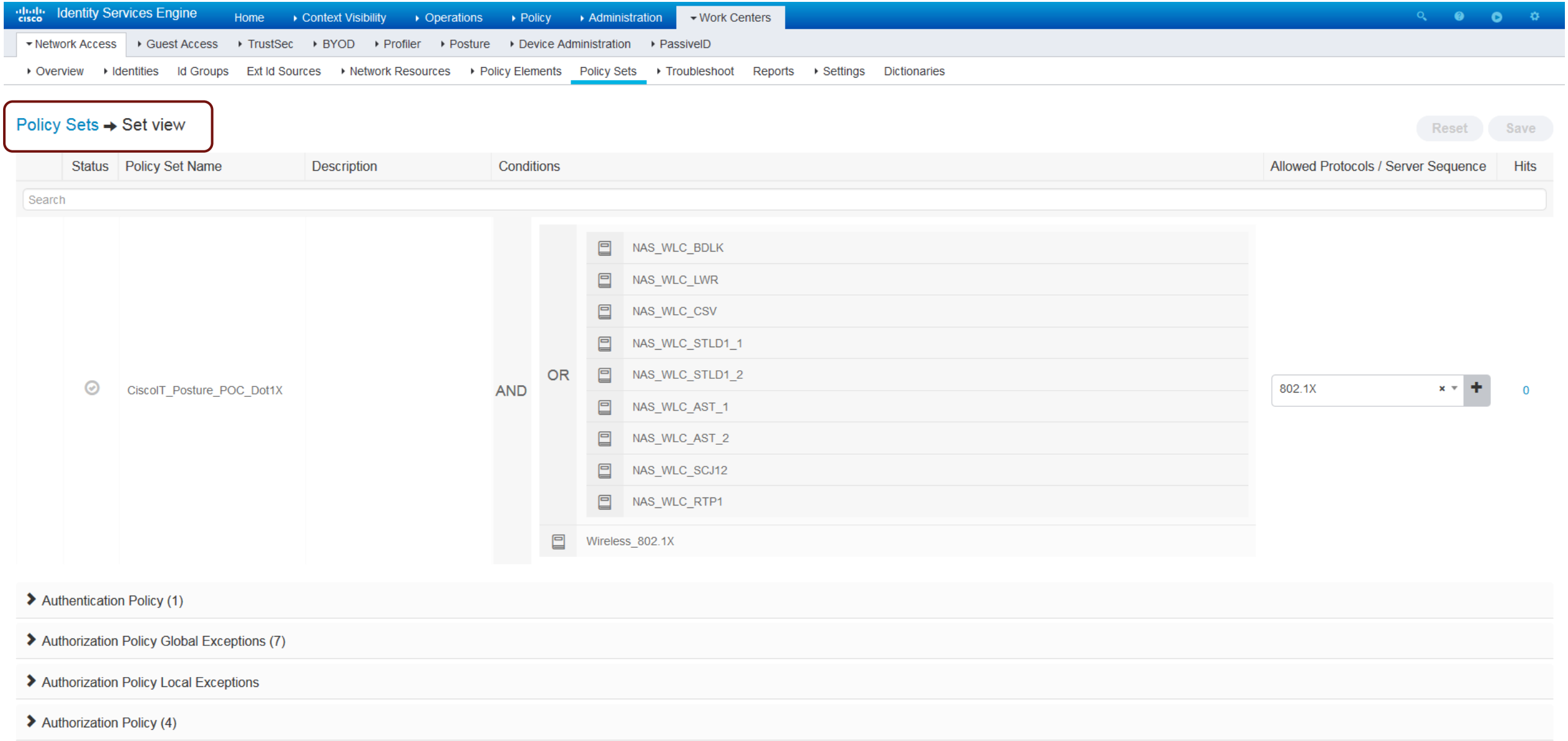
Пример групп политик – ISE 2.2



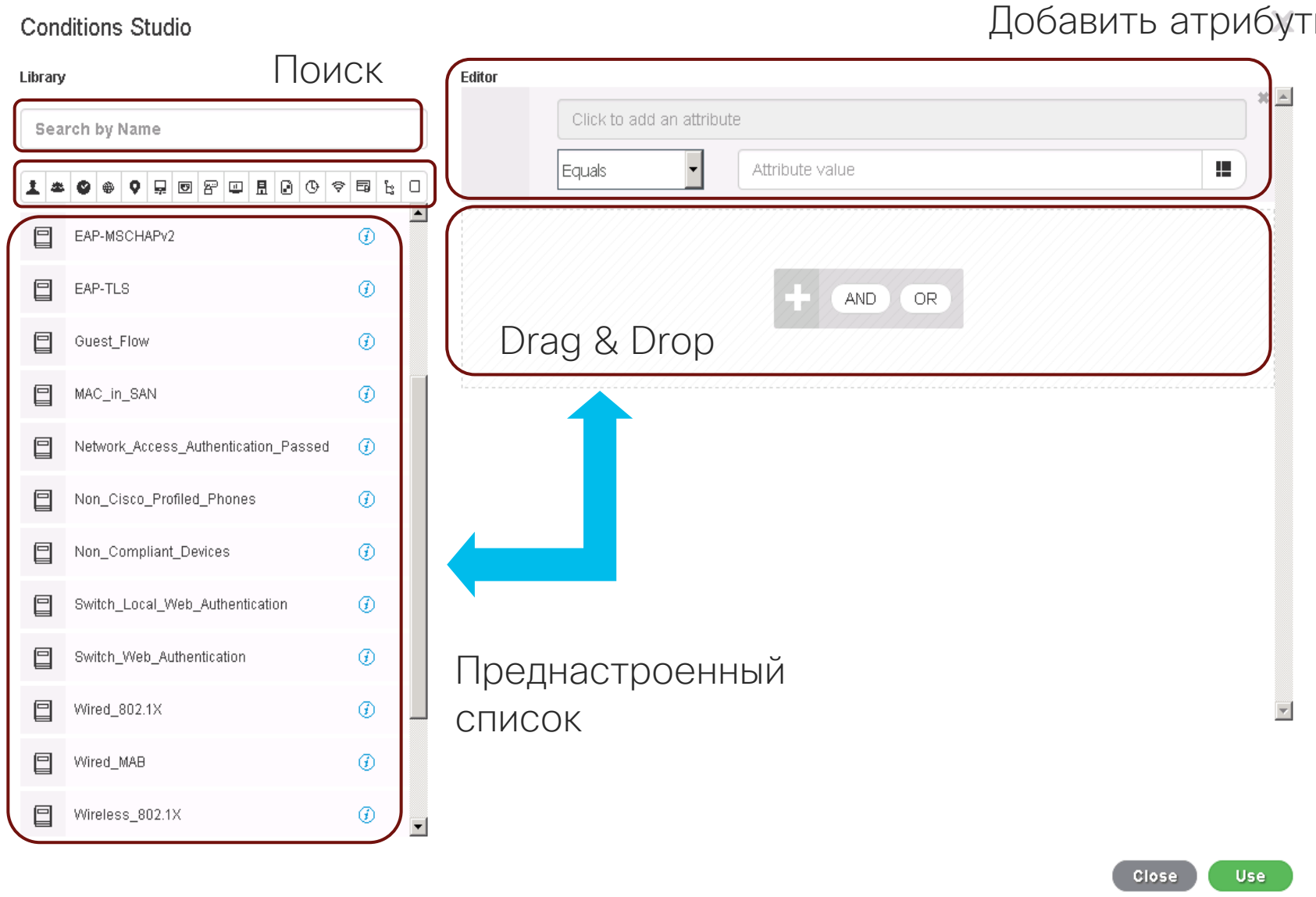
Улучшенный вид – Пример групп политик – ISE 2.3



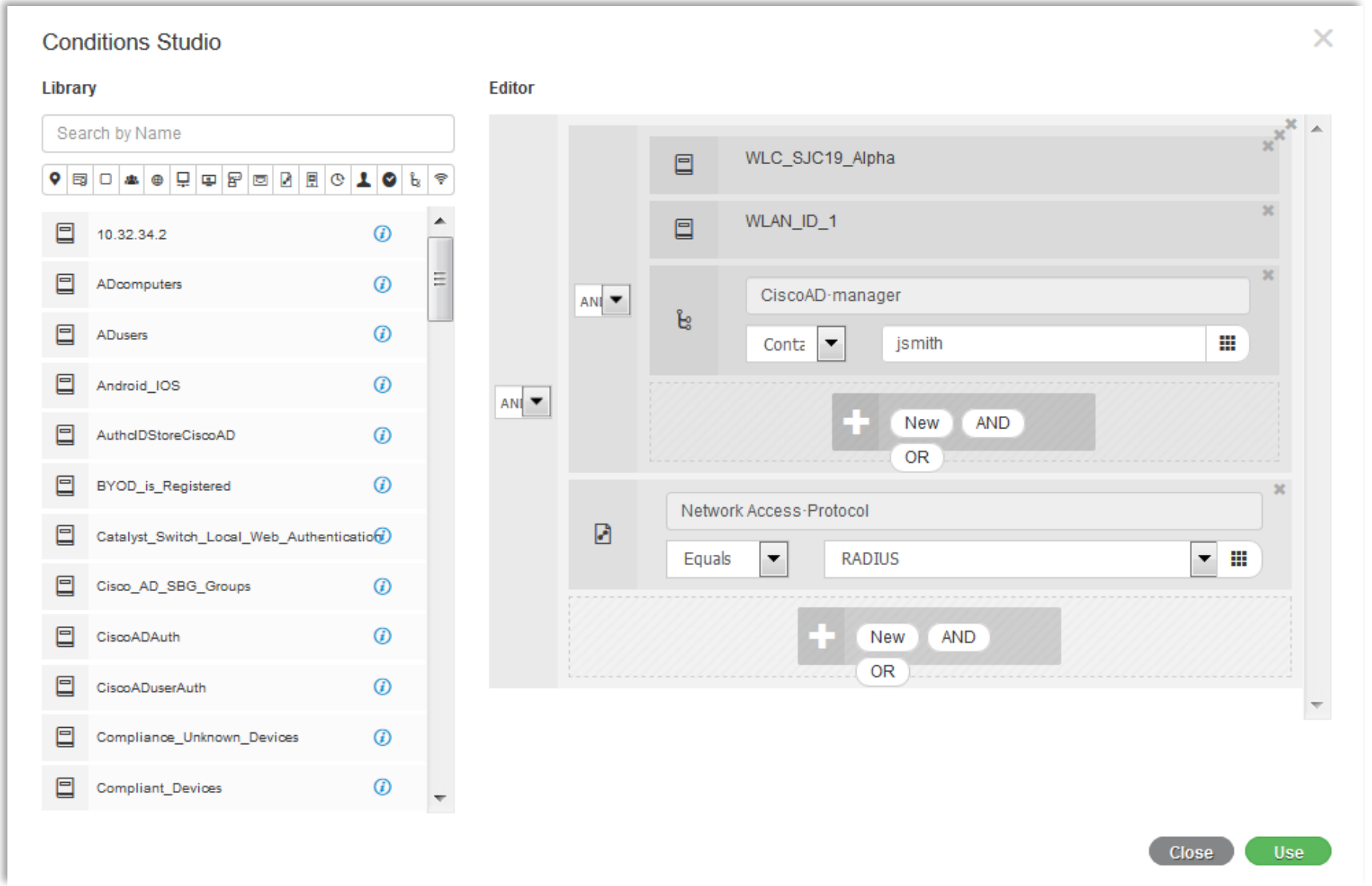
Обзор Групп Политик



Студия формирования условий



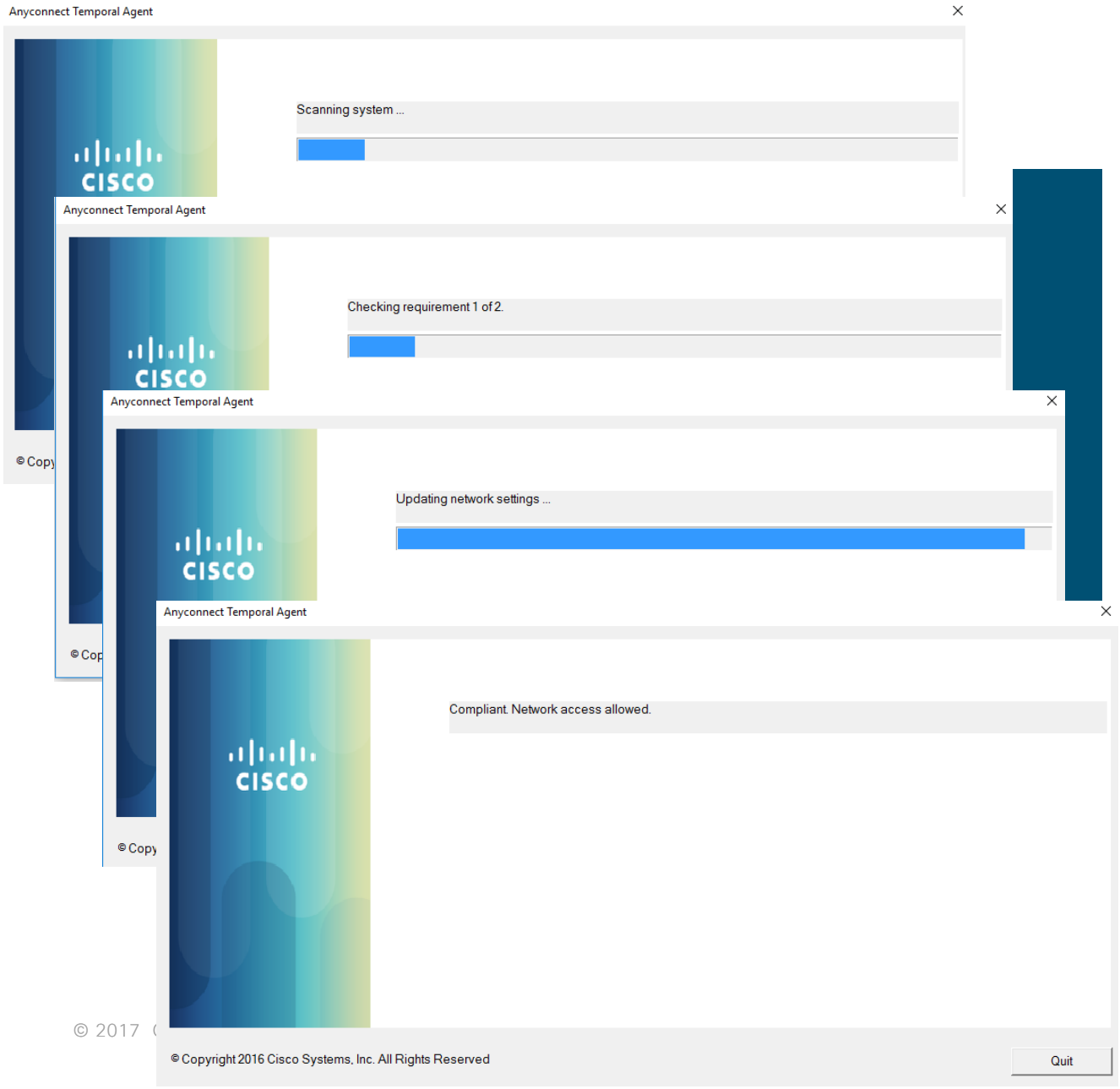
Составление условий политики



1. Добавление атрибутов
2. Создание условий с операторами (AND или OR)
3. Создание условий по необходимости с комбинациями AND/ OR.

Улучшения в оценке состояния

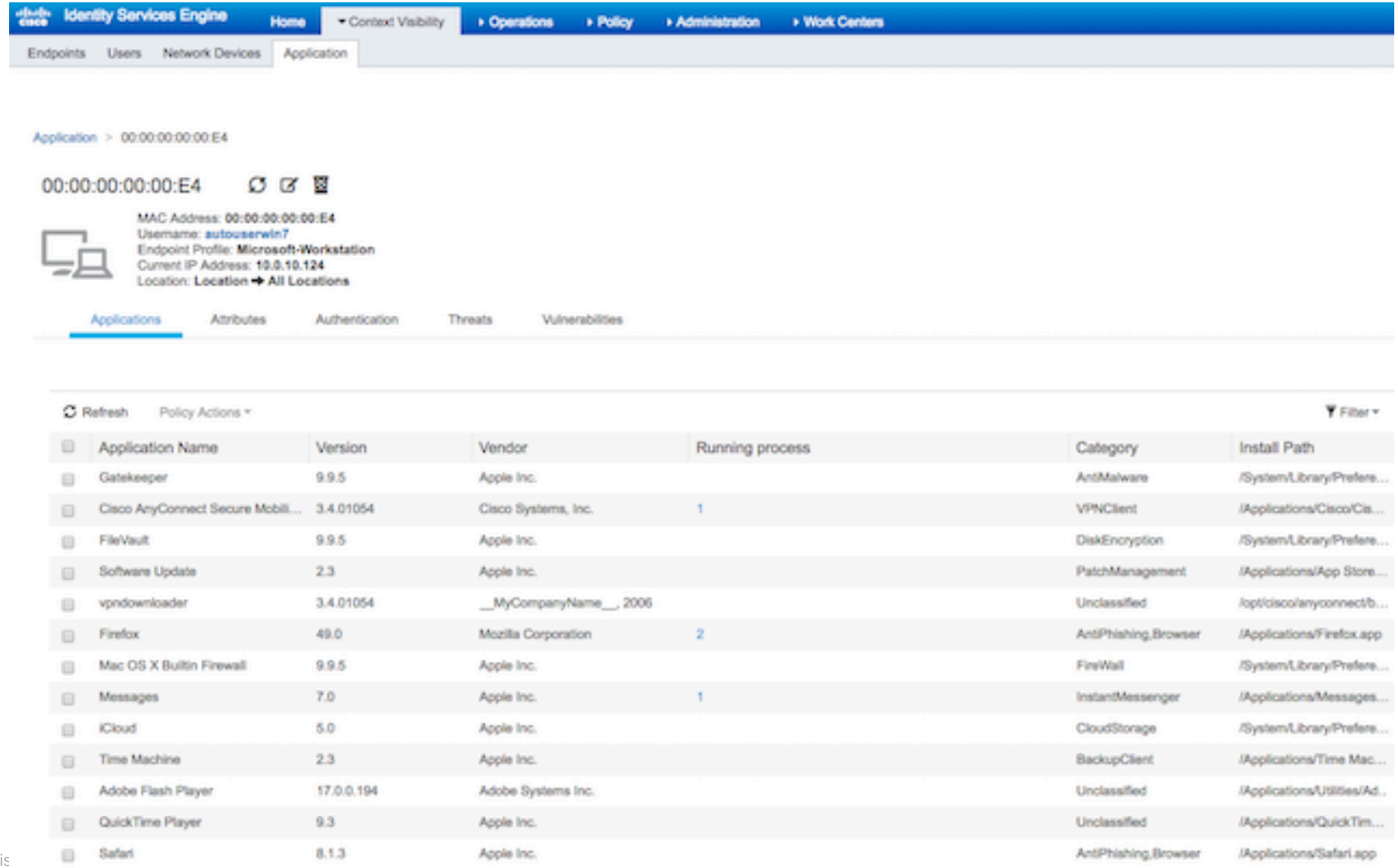
Temporal Agent (ISE 2.3)



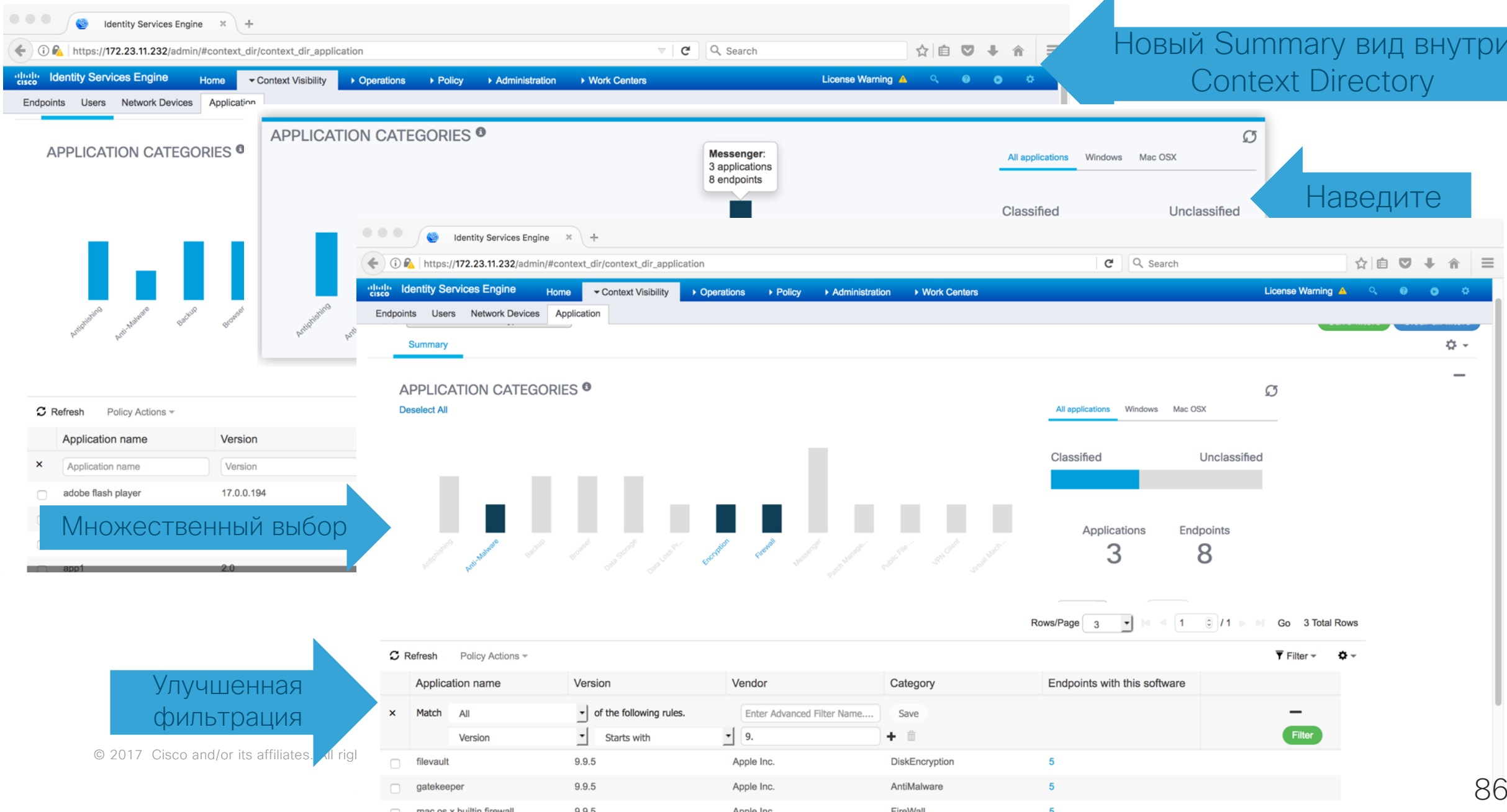
Детали

- Замена NAC Web Agent (только Windows) на временный Windows/exe и Mac OS/dmg
- Запускается один раз и удаляется
- Не требует административных привилегий
- Такой же богатый набор проверок что и AnyConnect (также с инвентаризацией ПО, но однократно)
- Только ручное исправление состояния
- Загружается с портала через URL перенаправление, возможно интегрировать с Guest, BYOD, CWA, etc.

Видимость установленных приложений



Новая инвентаризация приложений в ISE 2.3



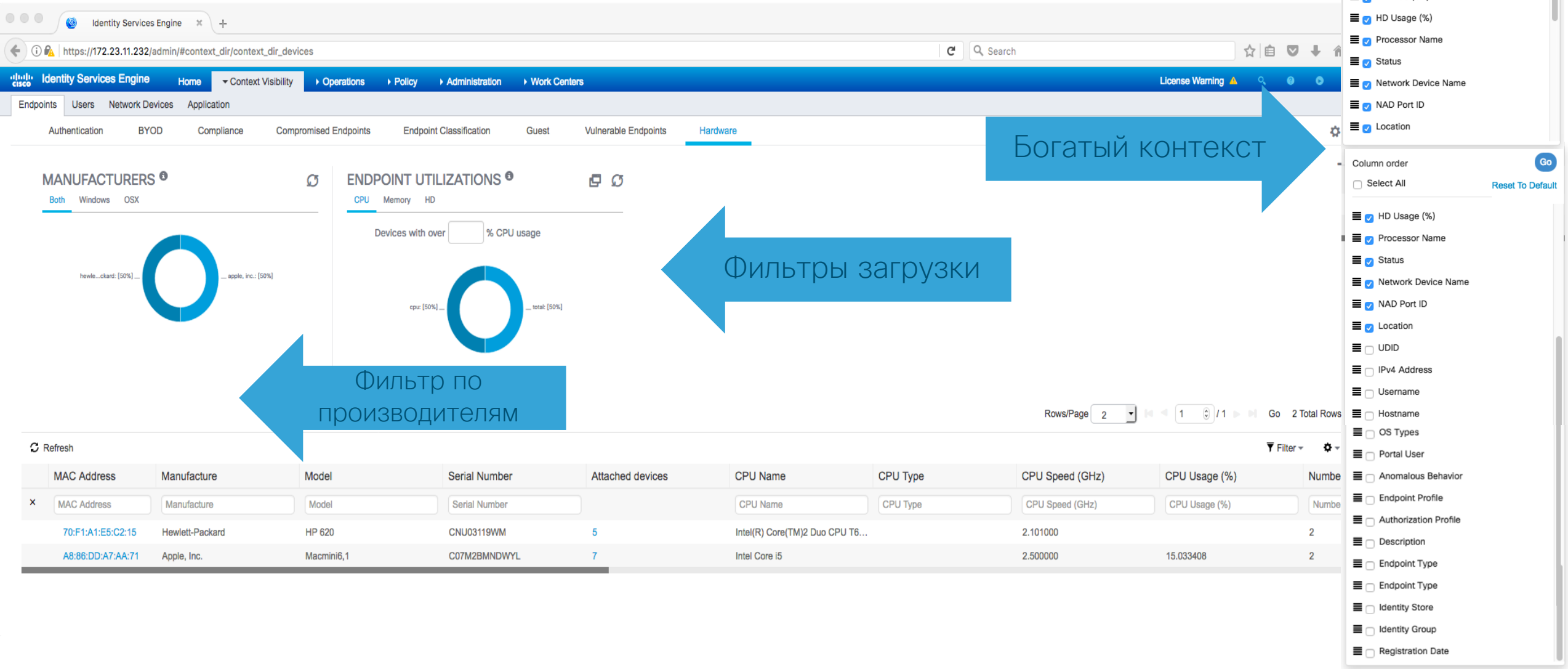
Новый Summary вид внутри Context Directory

Наведите

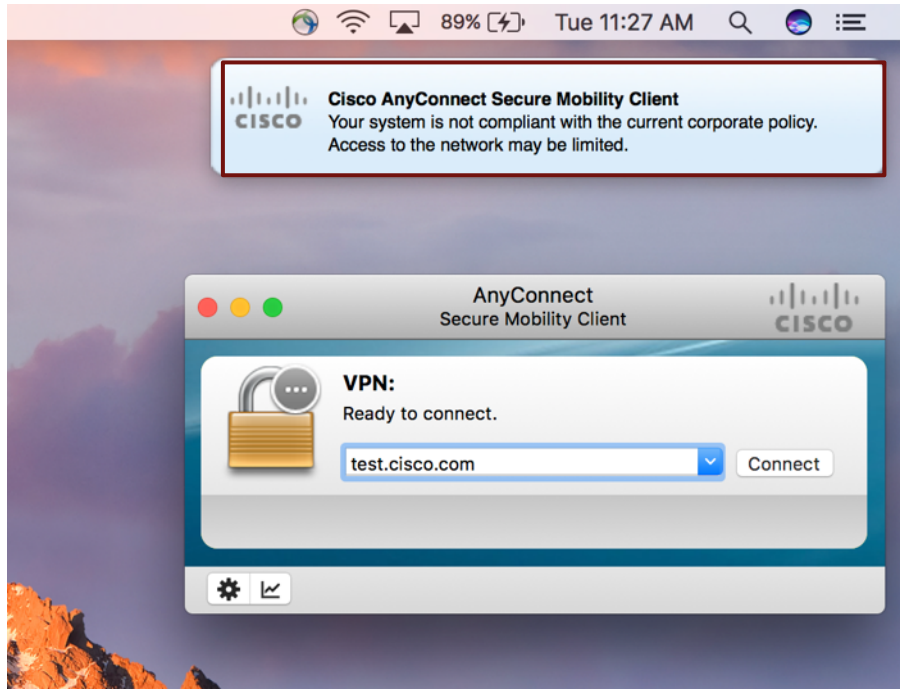
Множественный выбор

Улучшенная фильтрация

Новая аппаратная инвентаризация в ISE 2.3



Гибкие настройки уведомлений



Детали

- ✓ Использование системных уведомлений Windows и Mac OS
- ✓ Фокус на проблемах политик и ошибках связи
- ✓ Режимы агента (Full, Stealth, Stealth with Notification)

Agent Behavior

Parameter	Value	Notes
Enable debug log	No	
Operate on non-802.1X wireless	No	
Enable signature check	No	OSX: N/A
Log file size	5 MB	
Remediation timer	4 mins	The defau the global setting is
Agent Mode	Full	

Advanced Threat

AMP – вышло в 2017

- Command line capture
- Переделанный Dashboard
- Поддержка SAML
- Advanced Custom Detections для Mac и Linux Connectors
- Расширение поддержки Linux
- Поддержка инкрементальных обновлений сигнатур
- PCI compliance

Вышло в 2017 – Threat Grid

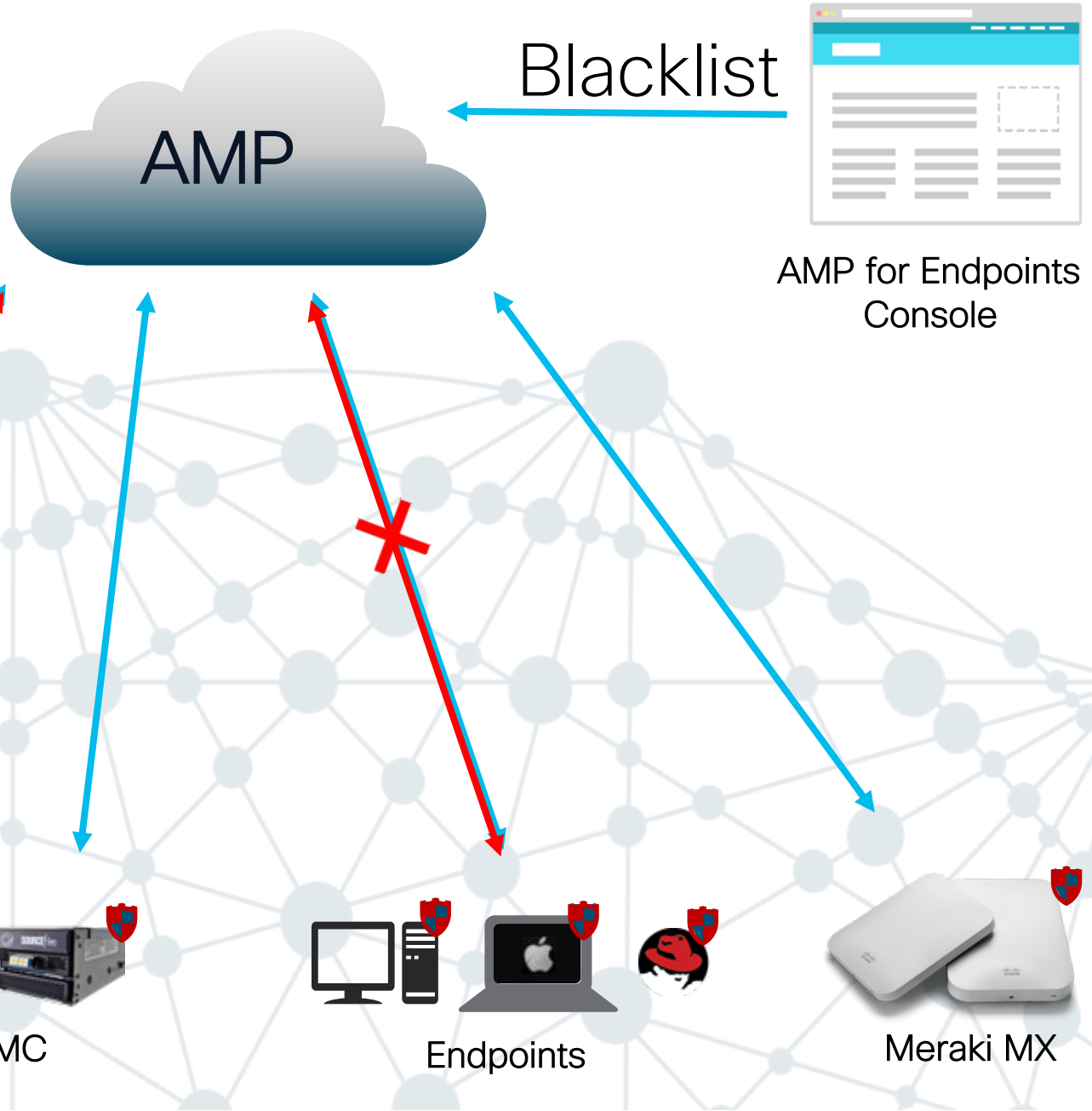
- Windows 10 поддержка
- Meraki MX интеграция
- Single Sign-on – AMP / TG
- Отслеживание источника отправки
- Sample packs

AMP

Расширенные возможности обнаружения

- Новый механизм эвристики
  - Детектирование и блокирование IOC на Endpoints в режиме реального времени
  - Windows Connector 6.0.x
- Защита от эксплоитов
  - Windows Connector 6.0.x
- Бета доступна для всех пользователей (в том числе и POV)

AMP Everywhere
AMP Unity




CISCO