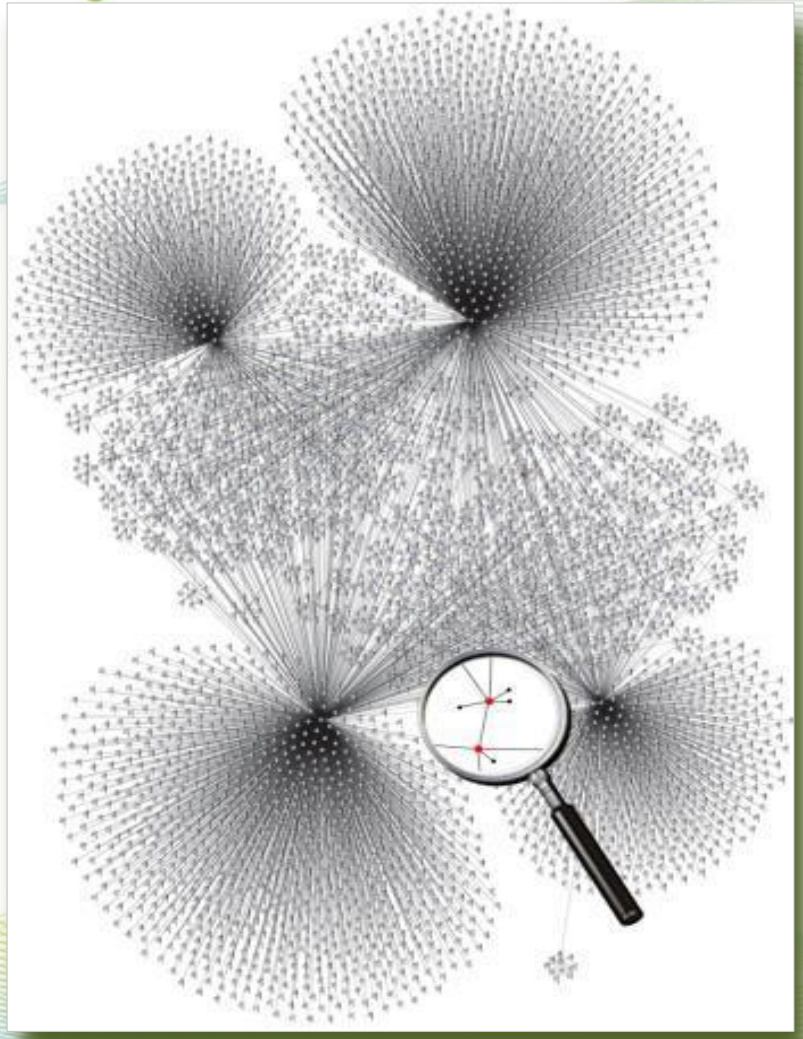
IT Guard

СИСТЕМА ВИЗУАЛИЗАЦИИ И АНАЛИЗА РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ

СУЩЕСТВУЮЩИЕ ПРОБЛЕМЫ ИБ

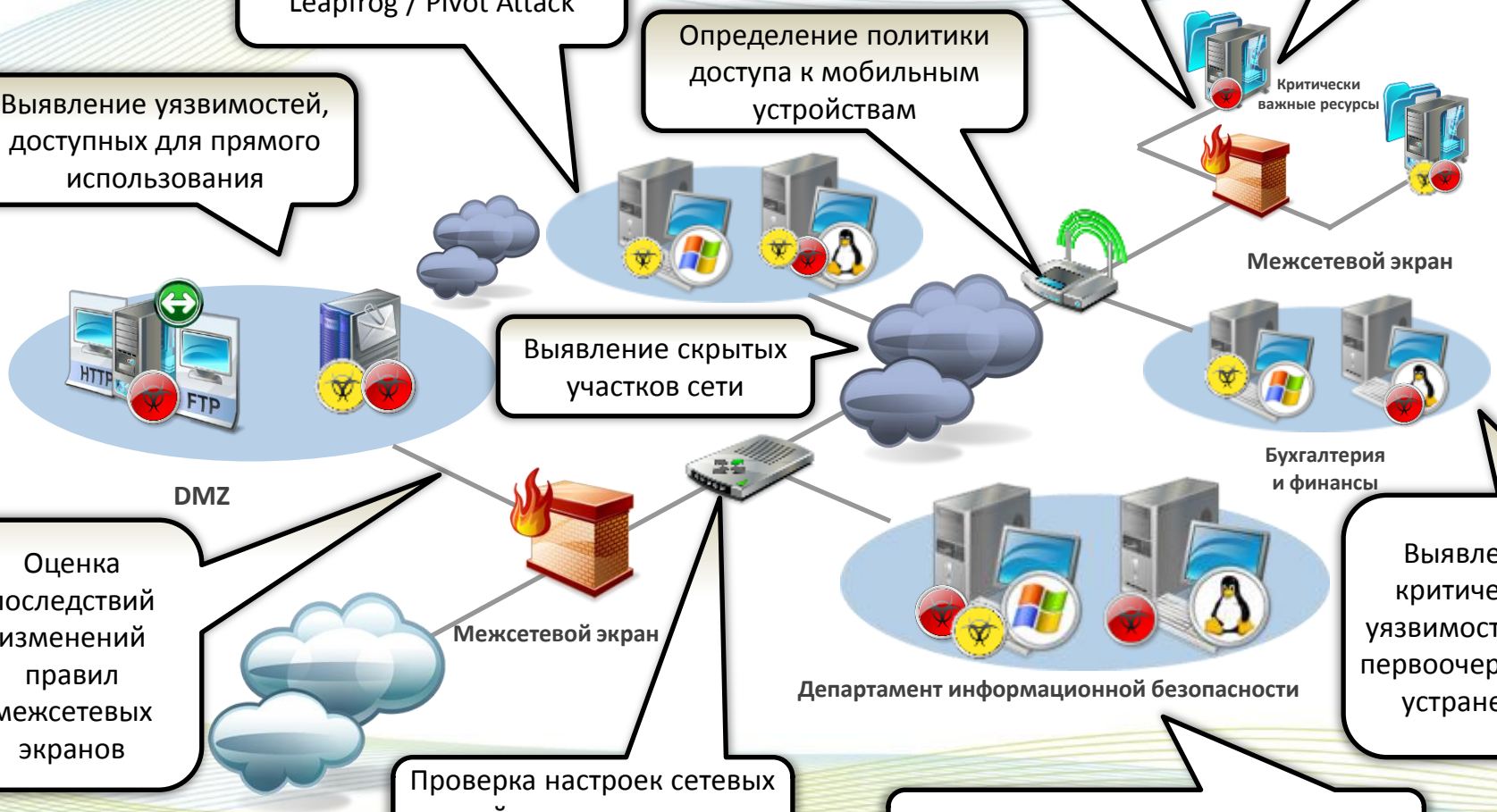
IT Guard



- **Получение актуальной топологии сетевой инфраструктуры**
- **Сложность в выявлении уязвимостей, связанных с архитектурой сети**
- **Отсутствие автоматизированного аудита конфигураций межсетевых экранов**
- **Сложность приоритезации выявленных уязвимостей без привязки к топологии сети и значимости информационных активов**
- **Сложность в расследовании инцидентов информационной безопасности**

REDSEAL РЕШАЕТ МНОГО ПРОБЛЕМ

IT Guard



АРХИТЕКТУРА REDSEAL

IT Guard

Отчеты

Отправка событий об инцидентах в SIEM

Оповещения

Платформа RedSeal

Сетевые устройства (маршрутизаторы, межсетевые экраны, балансировщики)

Juniper NETWORKS

CISCO

Check Point SOFTWARE TECHNOLOGIES LTD.

CITRIX

f5

BROCADE

Системы управления

CISCO

hp

solarwinds

tripwire

Сканеры безопасности

RAPID 7

McAfee

QUALYS

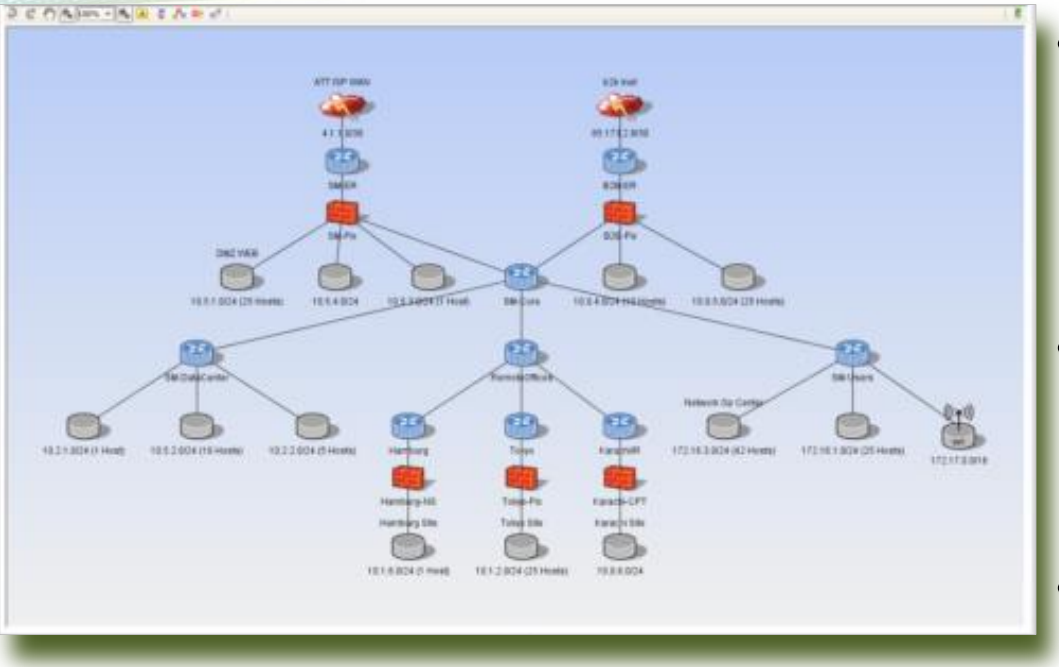
nCircle

TENABLE Network Security

Nessus

MAXPATROL

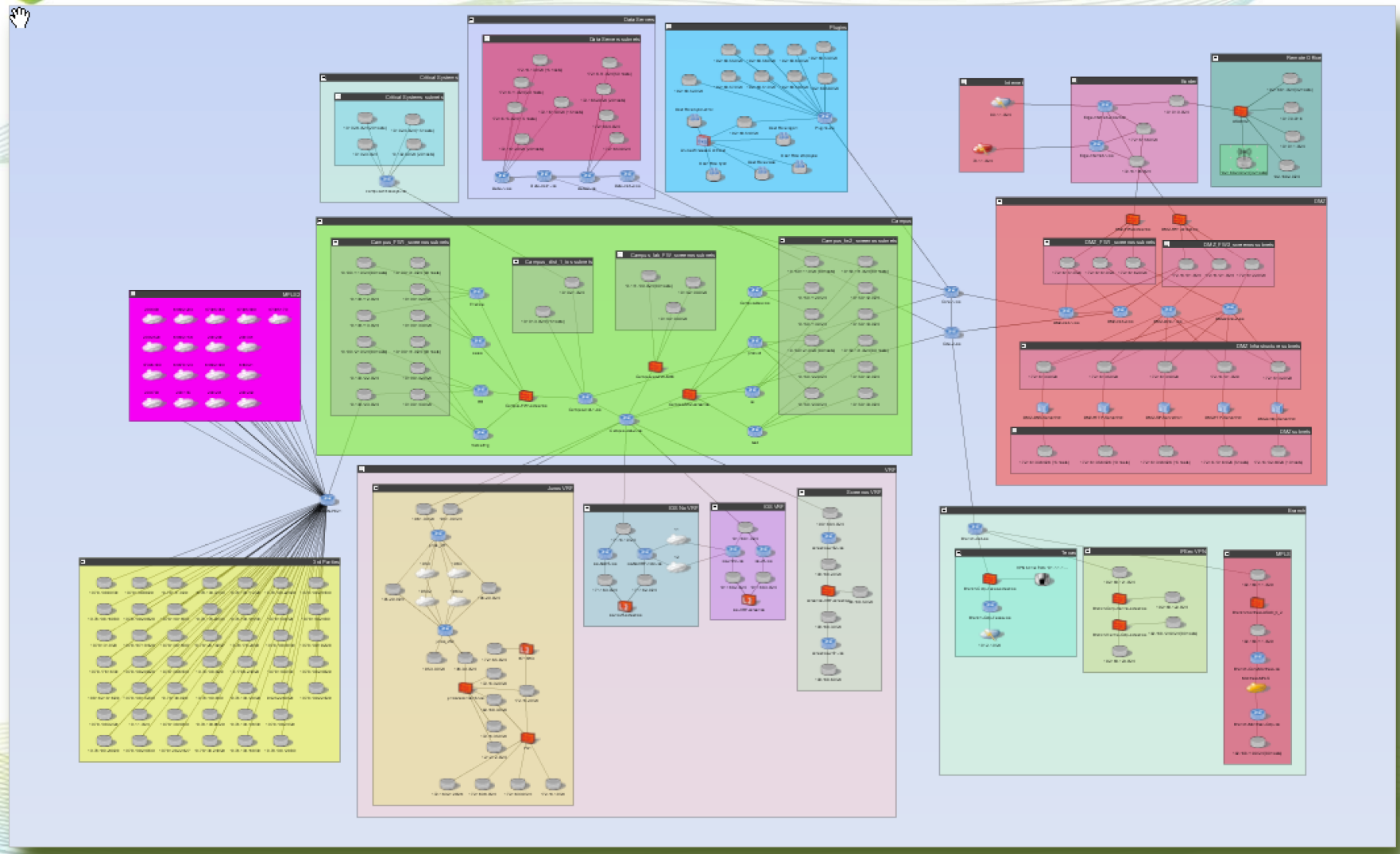
ПОСТРОЕНИЕ МОДЕЛИ СЕТИ



- **Построение топологии сети путем считывания конфигураций устройств**
- **Считывание конфигураций из файлов или путем подключения к устройствам по сети**
- **Выявление «невидимых» ранее сегментов корпоративной сети**
- **Возможность экспорта карты сети в Visio и другие форматы**

ПРИМЕР МОДЕЛИ СЕТИ

IT Guard



АНАЛИЗ КОНФИГУРАЦИОННЫХ ФАЙЛОВ

IT Guard

- **Более 130+ проверок конфигураций устройств с целью выявления уязвимостей**

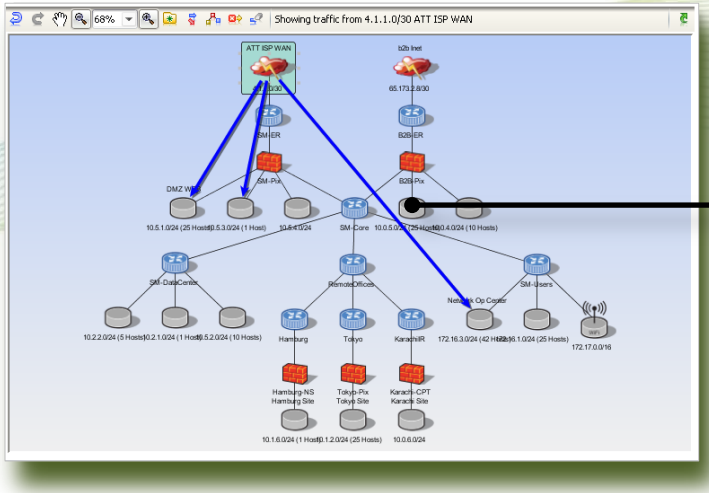
- **Возможность создания собственных проверок**

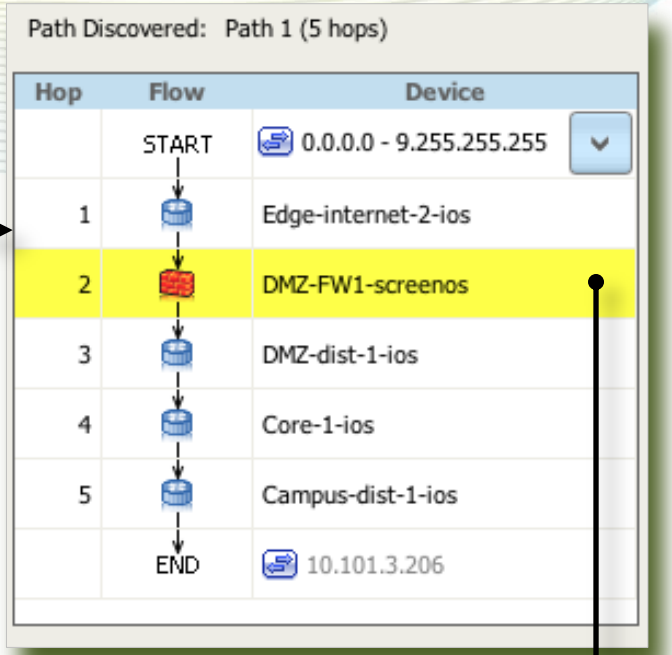
Анализ правил фильтрации МЭ:

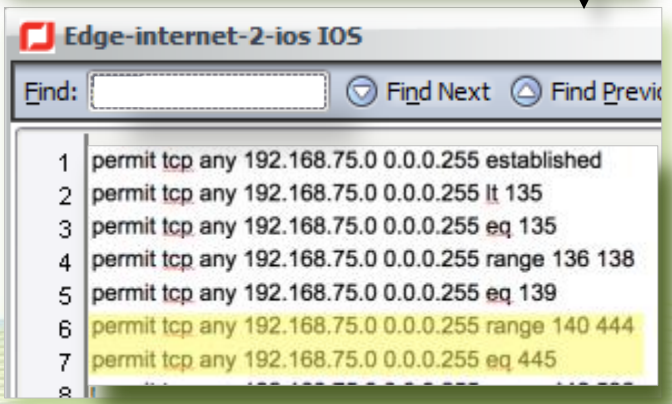
- **Выявление ненужных правил**
  - **Избыточные**
  - **Неработоспособные**
  - **Неактивные**
- **Выявление неиспользуемых правил**
  - **Анализ времени последнего применения**
  - **Анализ частоты использования**

КОНТРОЛЬ ДОСТУПА НА УРОВНЕ СЕТИ

IT Guard

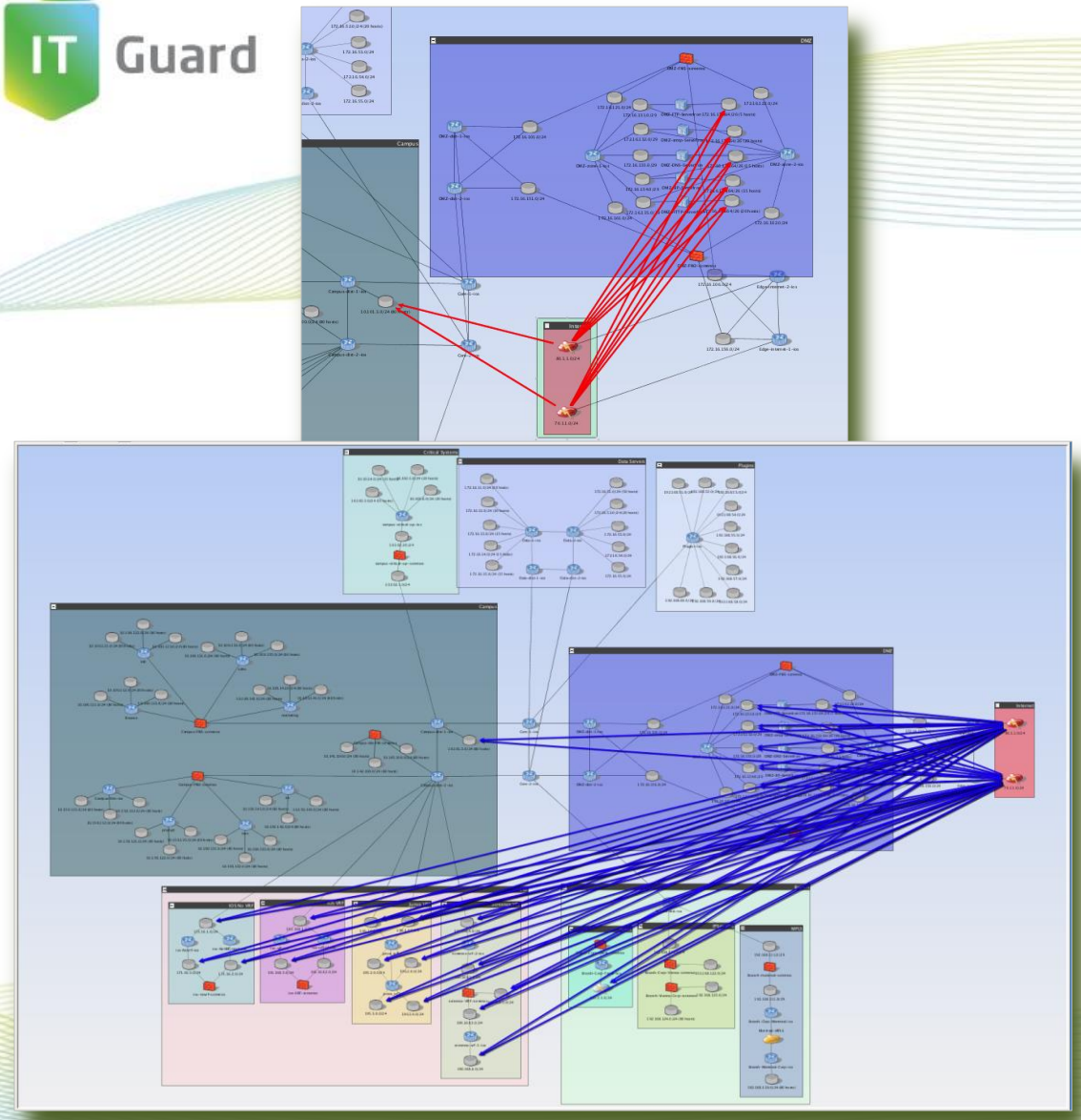






- Определение доступности узлов
  - “К чему можно получить доступ из сети Интернет?”
- Проверка корректности разграничения доступа
  - “Можно ли из не доверенной сети получить доступ к сегменту с финансовыми серверами?”

ВИЗУАЛИЗАЦИЯ ВОЗМОЖНЫХ ВЕКТОРОВ АТАКИ



- **Моделирование возможных векторов атаки на основе данных об уязвимостях и топологии сети**
- **Определение многошаговых угроз, для реализации которых требуется компрометация промежуточных узлов сети**

ПРИОРИТЕЗАЦИЯ УЯЗВИМОСТЕЙ

IT Guard

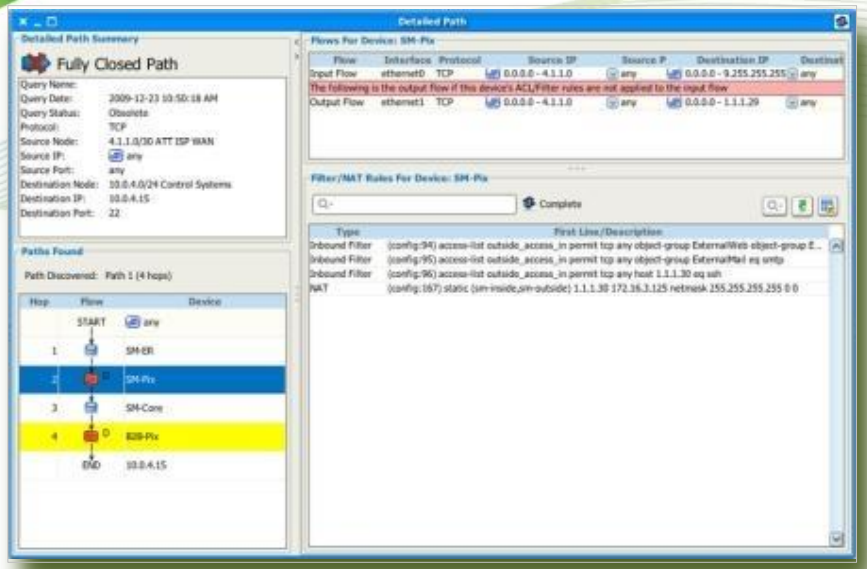
- **Ранжирование уязвимостей исходя из их достижимости для потенциального злоумышленника**
- **Приоритезация на основе значимости ИТ-активов**
- **Возможность импорта результатов сканирования**

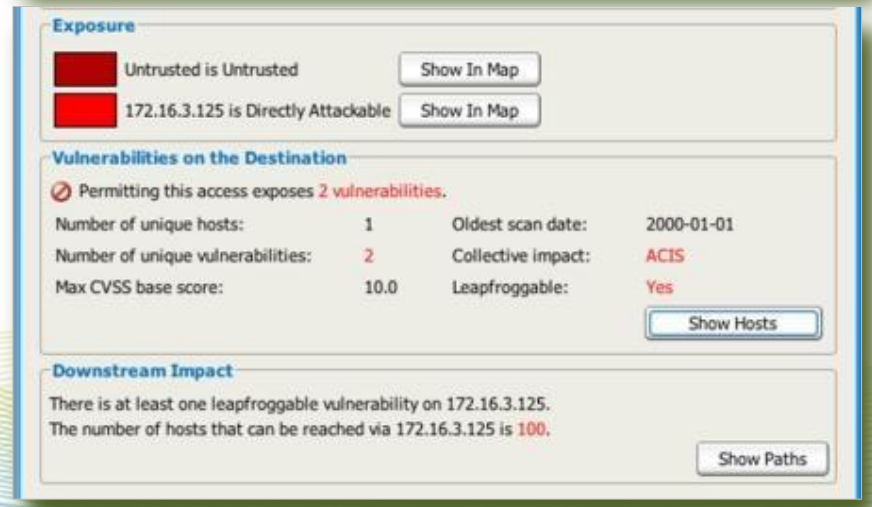
КОНТРОЛЬ СООТВЕТСТВИЯ ЗАДАННЫМ ПОЛИТИКАМ

- Мониторинг политик разграничения доступа в сети
- Наличие встроенных проверок для выполнения требований PCI DSS
- Развитые средств для определения собственных политик
- Реагирование на факты нарушения заданных политик:
  - Визуализация
  - Оповещения по email
  - Отчеты
  - Отправка событий в SIEM

МОДЕЛИРОВАНИЕ ИЗМЕНЕНИЙ В СЕТИ

IT Guard



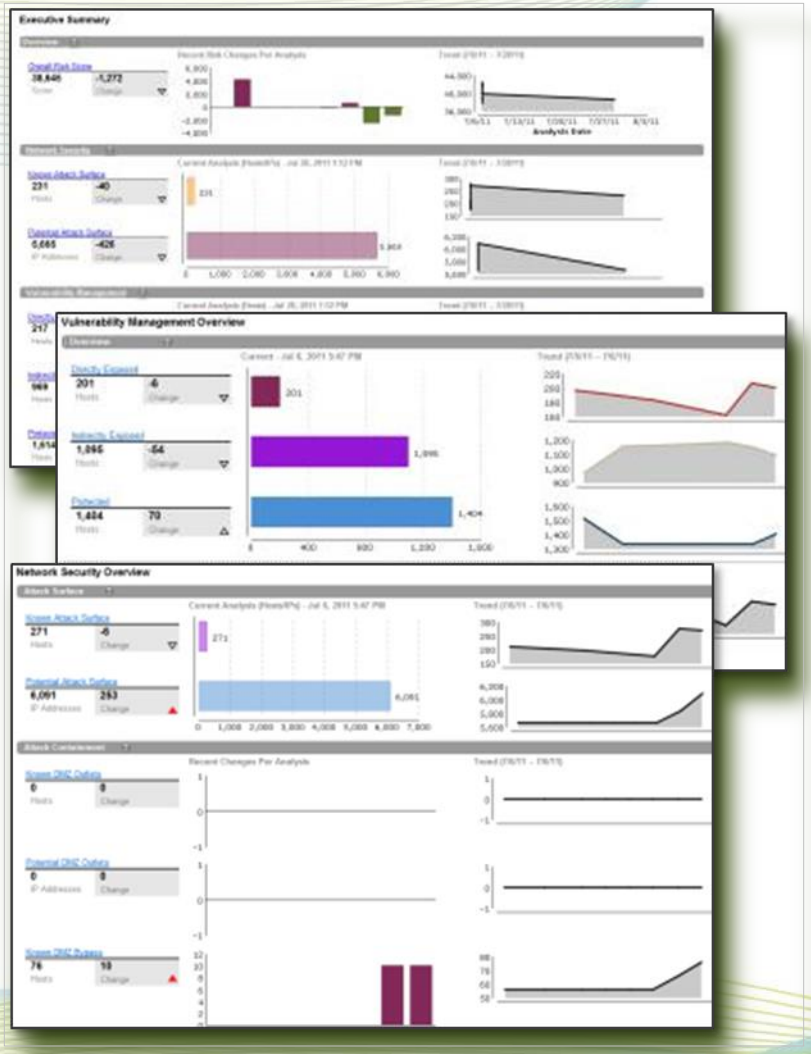


- **Автоматическое определение изменений, которые необходимо внести в конфигурацию сети для предоставления/блокирования доступа к сегментам сети**
  - **Все устройства в пути доступа**
  - **Устройства, блокирующие/разрешающие доступ**
  - **Правила/ACL, блокирующие /разрешающие доступ**
- **Оценка рисков, связанных с вносимыми изменениями в конфигурацию сети**
  - **Информация о появляющихся уязвимостях**
  - **Отображение возможных векторов атак**

ПОСТРОЕНИЕ ОТЧЕТОВ

IT Guard

- **Общие отчеты и показатели**
  - **Результаты работы системы**
  - **Выявление имеющихся нарушений политик безопасности**
  - **Ключевые риски сетевой безопасности**
- **Отчеты для управления рисками ИБ**
  - **Контроль доступа и оценка соответствия**
  - **Управление уязвимостями**
  - **Конфигурации по лучшим практикам**
- **Управление отчетами**
  - **Экспорт в PDF и другие форматы**
  - **Возможность создания собственных отчетов**



ИНТЕГРАЦИЯ С SIEM-СИСТЕМАМИ

IT Guard

- **Возможность автоматической отправки в систему мониторинга (SIEM) информации о выявленных инцидентах безопасности:**
  - **Нарушение политики разграничения доступа**
  - **Несанкционированные изменения в конфигурации сетевого оборудования и межсетевых экранов**
  - **Выявление уязвимостей в настройках сетевых устройств**
- **Интеграциями с решениями HP ArcSight, Symantec, McAfee SIEM и Cisco Security Manager**

КЛИЕНТЫ КОМПАНИИ

Технологические компании	Ритейл	Финансовые организации	Правительственные организации	Телекоммуни-кации
RIM, NVIDIA, CBS Interactive, NetApp, Apple, ORACLE, CISCO, McAfee, YAHOO!, Autodesk, AVNET, STROZ FRIEDBERG DIGITAL RISK MANAGEMENT & INVESTIGATIONS	TARGET, SAFEWAY, GAP, The Pampered Chef, Disney, Coinstar, WILLIAMS-SONOMA, CARLSON, TOYOTA, WAL★MART, PETSMART, StubHub!, LOWE'S, Publix, TSC TRACTOR SUPPLY CO, Stein Mart, meredith, Allison Transmission	SVB, Morgan Stanley, UBS, ally, element payment services, PAYCHEX, AMERICAN EXPRESS, CapitalOne, Liberty Mutual, TransUnion, First Data, CyberSource the power of payment, SallieMae, Century 21	DEPARTMENT OF DEFENSE, NATIONAL SECURITY AGENCY, FEDERAL AVIATION ADMINISTRATION, DEPARTMENT OF EDUCATION, IQT IN·Q·TEL, NAVY FEDERAL CREDIT UNION, EDD Employment Development Department State of California, fisa, UNITED STATES POSTAL SERVICE, CMS.gov Centers for Medicare & Medicaid Services, GENERAL DYNAMICS Information Technology	T-Mobile, TIME WARNER CABLE, comcast, CABLEVISION, Vonage, Westinghouse, TATA COMMUNICATIONS, PACIFICORP, PG&E, New York Power Authority

СПЕЦИФИЦИРОВАНИЕ

= Лицензия * “N” - L3

“N” = 50 min … add min 10

Первичная закупка: лицензия на минимальное количество 50 устройств (+ шаг в 10 устройств L3).

Апгрейд: дозакупка возможна минимум на 10 устройств L3.

Поддержка = 20% от Лицензии*“N” - L3 + %18 НДС

1-2-3 Года: 1=20%; 2=(20%+19%); 3=(20%+19%+18%)

- Поддержка и обслуживание Premium 24 x 7 для продуктов RedSeal: 24x7x365.
- Поддержка и обслуживание: по телефону, по электронной почте, через веб-портал = время реакции 4 часа.
- Включает все обновления, модернизации и исправления программного обеспечения.

КЛЮЧЕВЫЕ ВОЗМОЖНОСТИ

IT Guard

- **Автоматическое построение модели сети (сетевой топологии)**
- **Оценка настроек сетевых устройств и межсетевых экранов с точки зрения соответствия лучшим практикам и стандартам информационной безопасности**
- **Оценка эффективности используемых правил фильтрации межсетевых экранов (выявление неиспользуемых, избыточных или ошибочных правил)**
- **Автоматическое построение векторов возможных атак на основе текущей сетевой топологии, имеющихся сетевых средств защиты и актуальных уязвимостях**
- **Автоматическое выделение наиболее приоритетных уязвимостей, устранение которых приведёт к устранению наиболее опасных векторов атак**
- **Отслеживания изменений в настройках сетевого оборудования и сетевых средств защиты**
- **Выявление нарушений политики разграничения доступа на уровне сети**

НАШИ КОНТАКТЫ

IT Guard

Компания IT Guard - дистрибьютор, специализирующийся на продаже продуктов в области информационной безопасности через сеть партнеров на территории России и стран СНГ. Эффективная логистика и наличие складской инфраструктуры гарантируют партнерам своевременную поставку.

Компания IT Guard обладает высокой компетенцией: имеет в штате сертифицированных инженеров, оказывает всестороннюю поддержку партнерам, занимается организацией консультационных и обучающих мероприятий для партнеров и их клиентов.

REDSEAL NETWORKS. STONESOFT A McAfee Group Company EnCase DELPHIX

CYBERARK hp agileSI applied ERP security invincea Cyberoam Securing You

115093, г. Москва, Партийный пер., д. 1, к. 46

Телефон: +7 (495) 767-16-19

http://itgrd.ru

e-mail: info@itgrd.ru