СИСТЕМА ВИЗУАЛИЗАЦИИ И АНАЛИЗА РИСКОВ СЕТЕВОЙ БЕЗОПАСНОСТИ REDSEAL

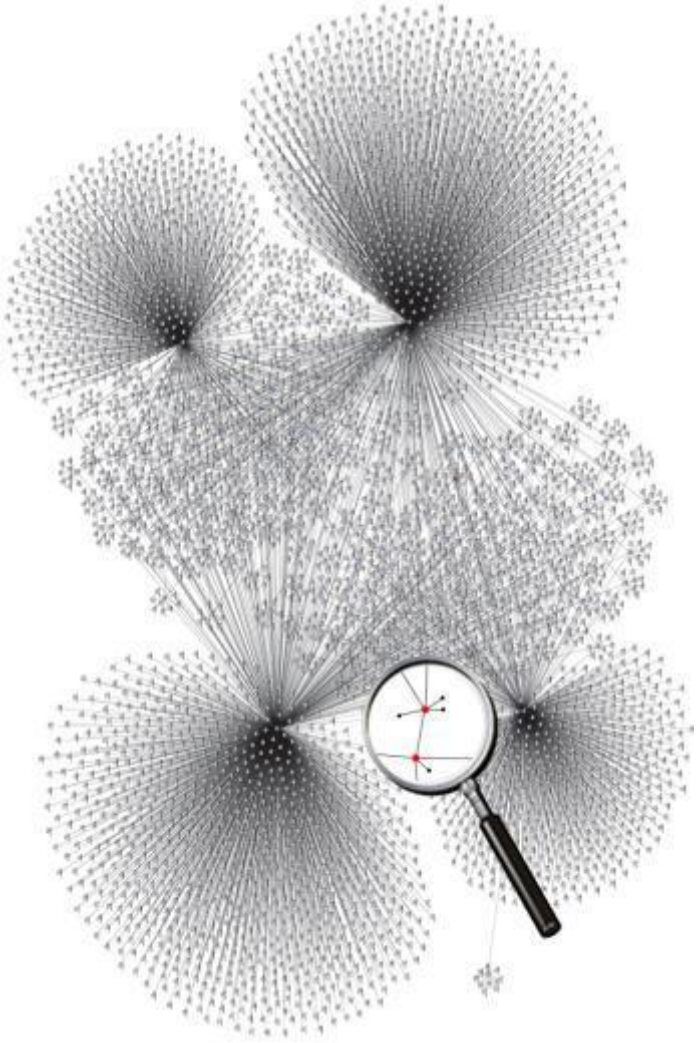
Роман Ванерке
Руководитель отдела технических решений
ЗАО «ДиалогНаука»

ДиалогНаука

Содержание

- Обзор системы визуализации и анализа рисков RedSeal
- Практическая демонстрация системы:
  - Демонстрация построения карты сети на примере распределенной сети
  - Демонстрация анализа рисков
- Заключение

Актуальные вопросы



Получение актуальной топологии сетевой инфраструктуры

Сложность в выявлении уязвимостей, связанных с архитектурой сети

Сложность приоритезации выявленных уязвимостей без привязки к топологии сети и значимости информационных активов

Отсутствие автоматизированного аудита конфигураций межсетевых экранов

Сложность в расследовании инцидентов информационной безопасности

ОБЕСПЕЧЕНИЕ СЕТЕВОЙ БЕЗОПАСНОСТИ В 2014

Сетевая безопасность

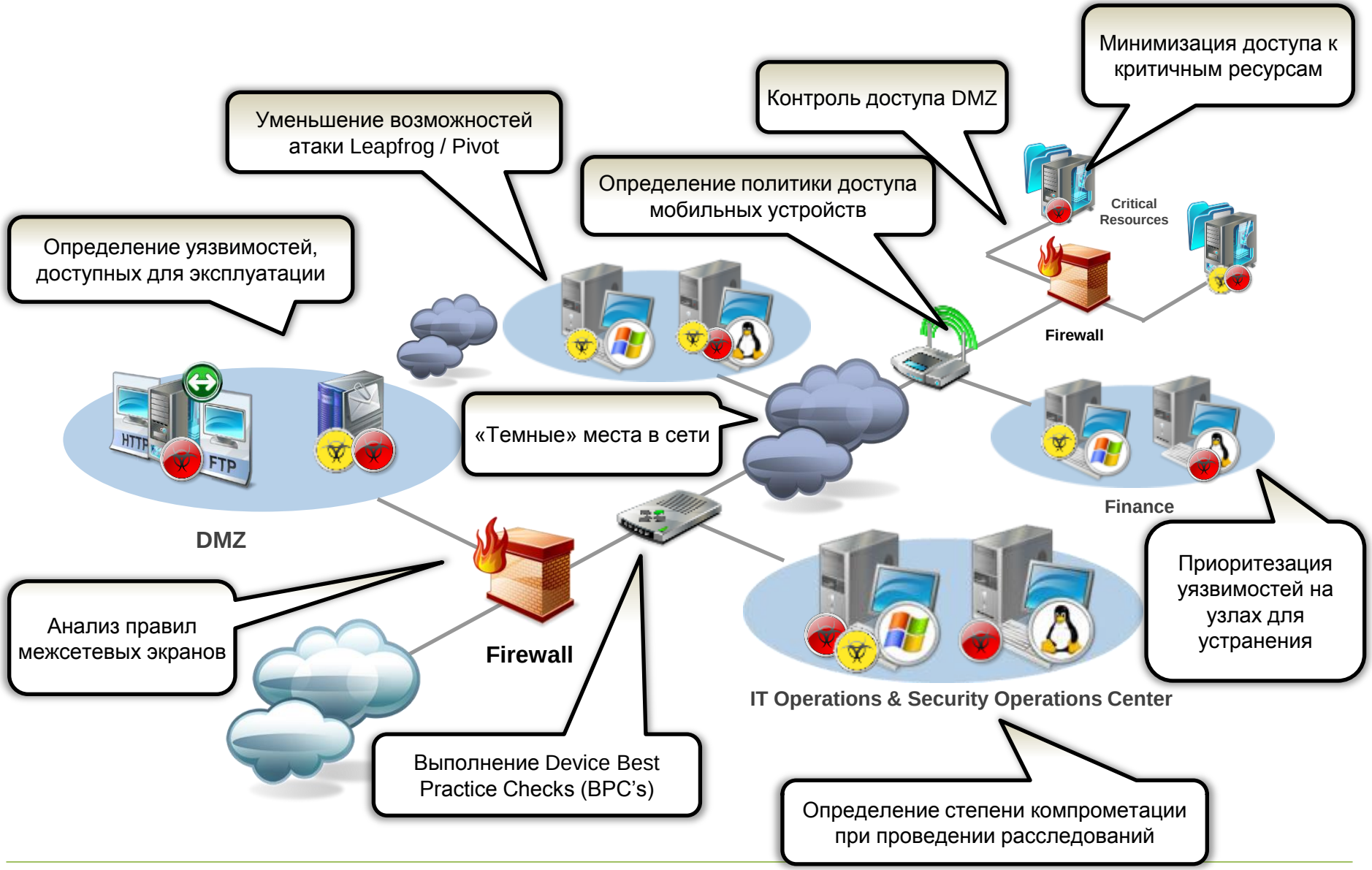
Сетевая безопасность 2014

Сетевая безопасность 2014

Сетевая безопасность 2014

We help large enterprises and government agencies master their network security risk

Возможности RedSeal



Как это работает

1. Выполняется сбор конфигураций МЭ, роутеров, коммутаторов и балансировщиков, развернутых в сети, как непосредственно с устройства, так и через CMDB

2. Используя проприетарные алгоритмы выполняется анализ конфигурационных файлов для построения виртуальной модели сети

3. Выполняются проверки Best Practice Checks (BPC) к конфигурациям для выявления эксплуатационных уязвимостей

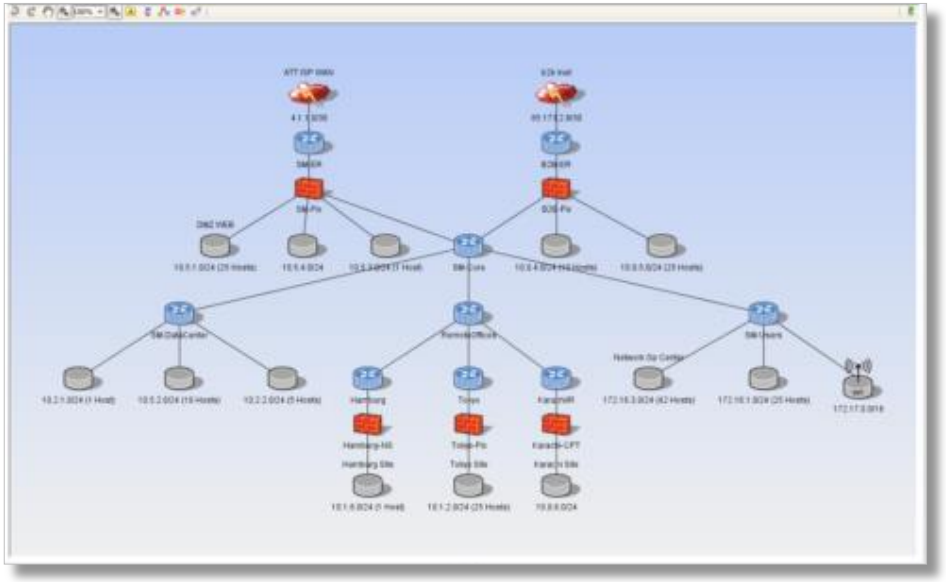
4. Также может быть загружена в систему информация об уязвимостях узлов сети, определение уязвимостей, эксплуатация которых возможна как непосредственно из недоверенной сети, так и требующих компрометацию промежуточных узлов

5. Симуляция атаки позволяет оценить, какие уязвимости могут быть про эксплуатированы при открытии доступа, позволяет администраторам приоритезировать задачи

Архитектура RedSeal

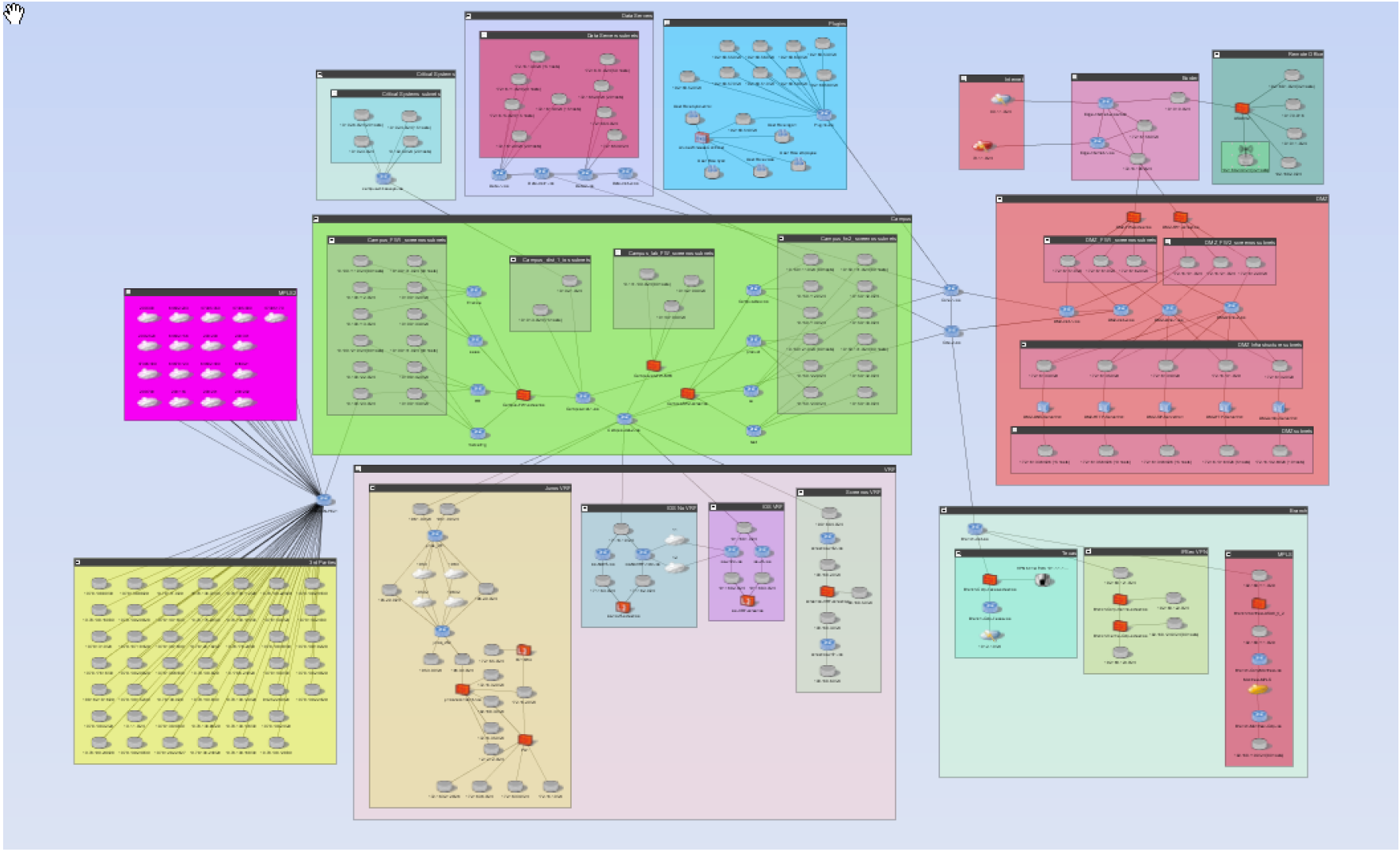
Архитектура RedSeal

Построение модели сети

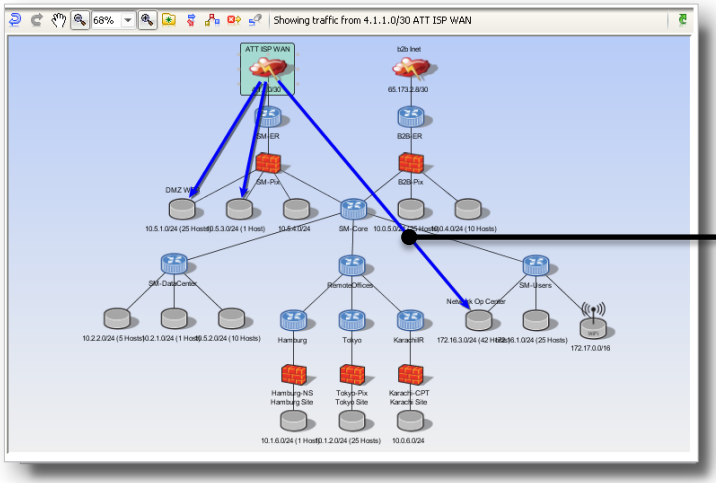


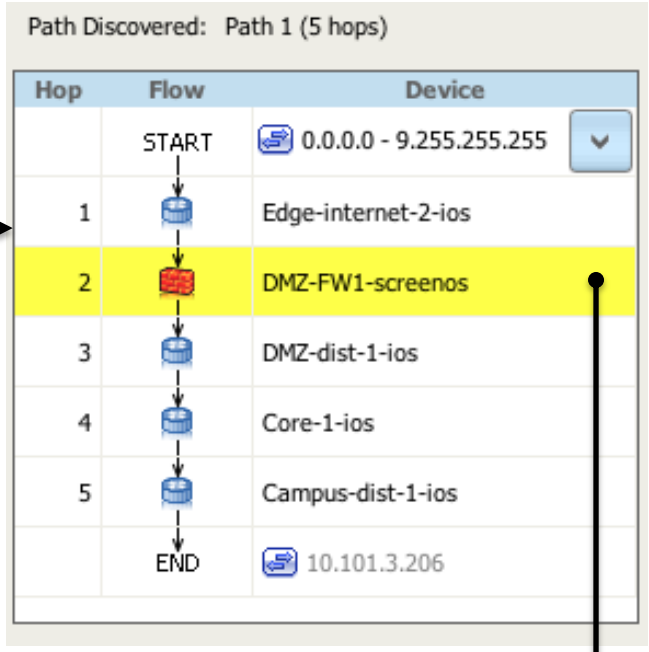
- Построение топологии сети путем считывания конфигураций устройств
- Считывание конфигураций из файлов или путем подключения к устройствам по сети
- Выявление «невидимых» ранее сегментов корпоративной сети
- Возможность экспорта карты сети в Visio и другие форматы

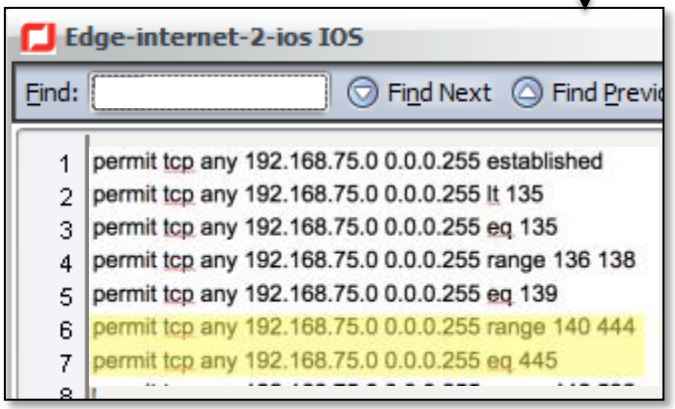
Пример модели сети



Контроль доступа на уровне сети







- Определение доступности узлов
  - «К чему можно получить доступ из сети Интернет?»
  - «Кто может получить доступ к АБС?»

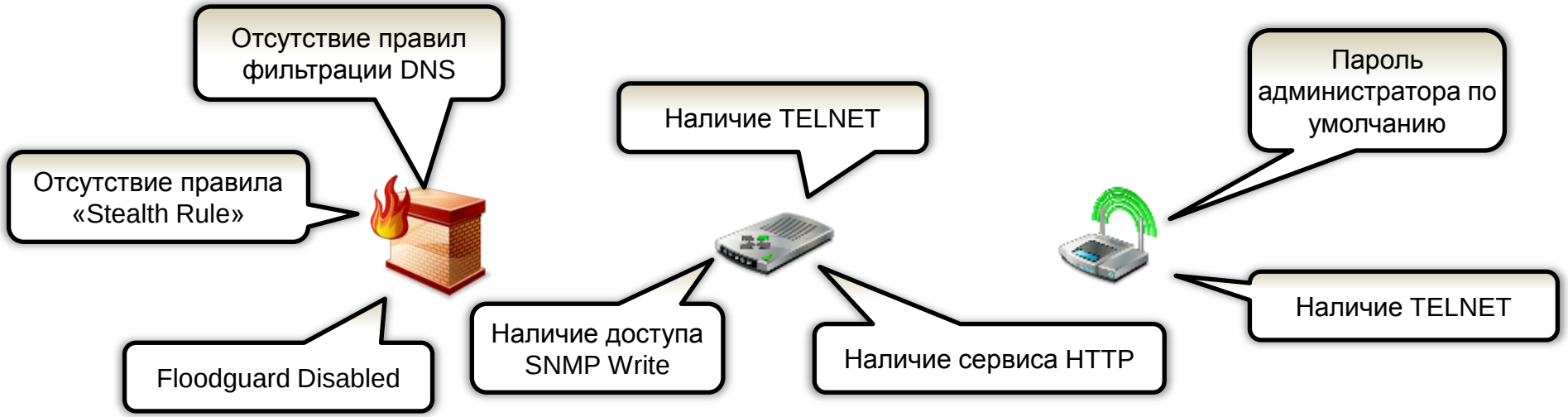
- Проверка корректности разграничения доступа
  - “Можно ли из недоверенной сети получить доступ к сегменту с критичными серверами?”

Анализ конфигурационных файлов

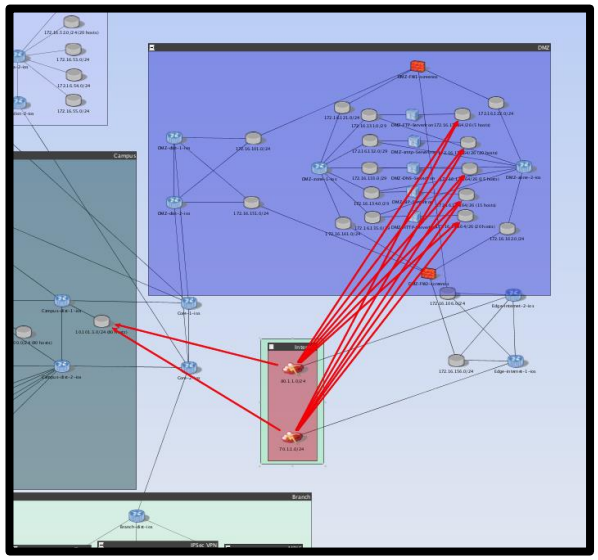
- Более 120+ проверок конфигураций устройств с целью выявления уязвимостей
- Возможность создания собственных проверок

Анализ правил фильтрации МЭ:

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

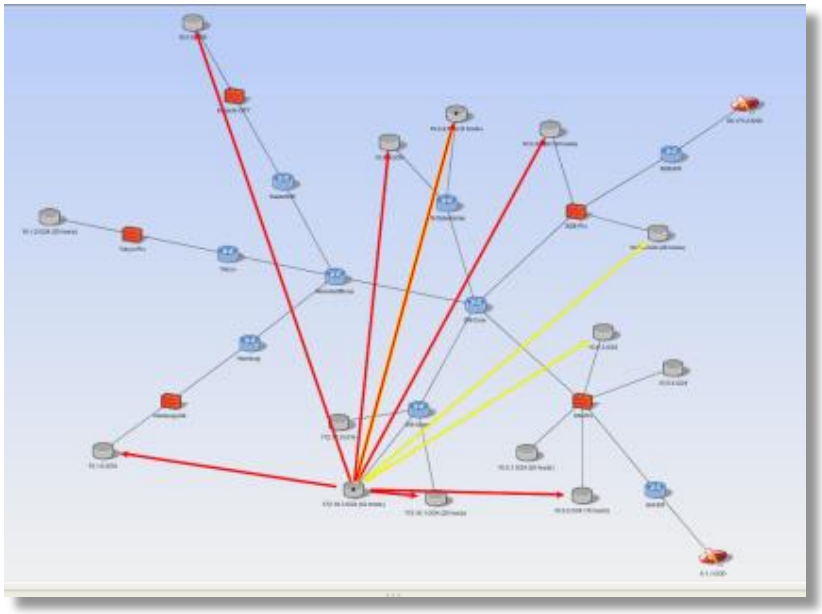


Визуализация возможных векторов атаки



Моделирование возможных векторов атаки на основе данных об уязвимостях и топологии сети

Определение многошаговых угроз, для реализации которых требуется компрометация промежуточных узлов сети



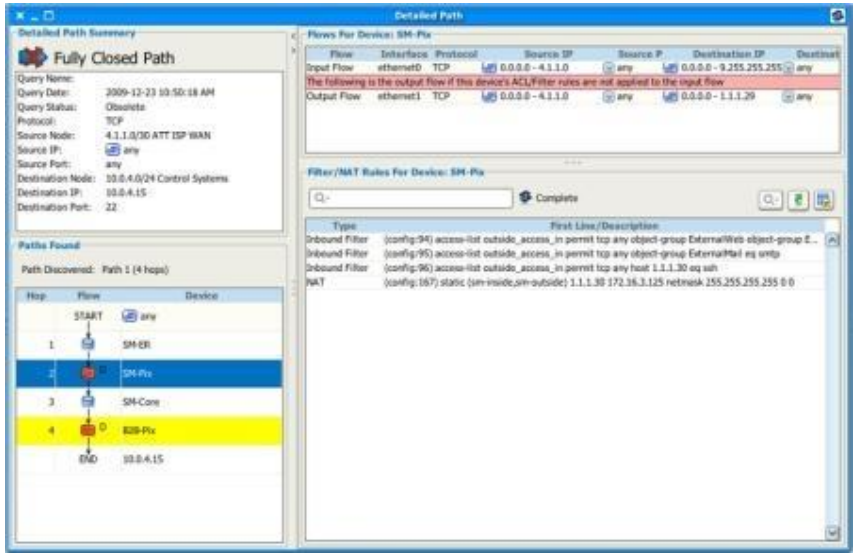
Приоритезация уязвимостей

- Ранжирование уязвимостей исходя из их достижимости для потенциального злоумышленника
- Приоритезация на основе значимости ИТ-активов
- Возможность импорта результатов сканирования
  - MaxPatrol (Xspider), Symantec, eEye, McAfee VME, Nessus, Rapid 7, Qualys, NMAP

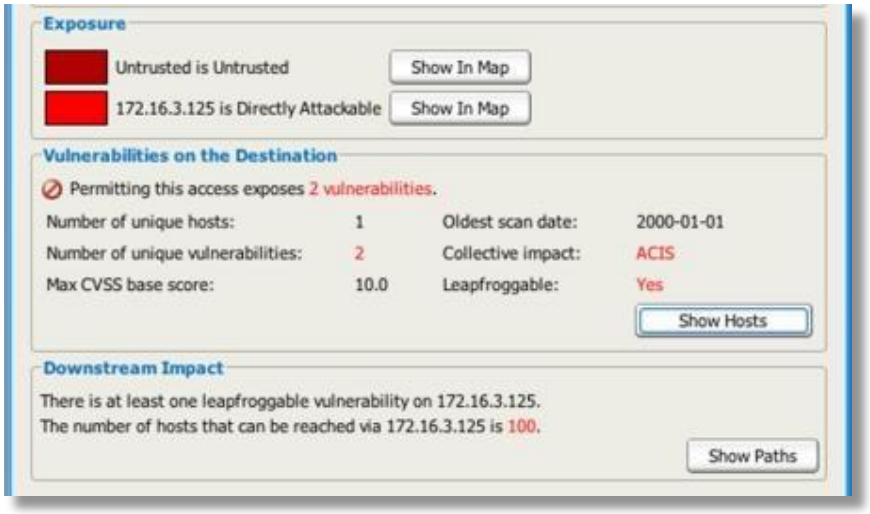
Контроль соответствия заданным политикам

- Мониторинг политик разграничения доступа в сети
- Наличие встроенных проверок для выполнения требований PCI DSS
- Развитые средств для определения собственных политик (например, разграничение доступа между филиалом и головным офисом)
- Реагирование на факты нарушения заданных политик:
  - Визуализация
  - Оповещения по email
  - Отчеты
  - Отправка событий в SIEM

Моделирование изменений в сети



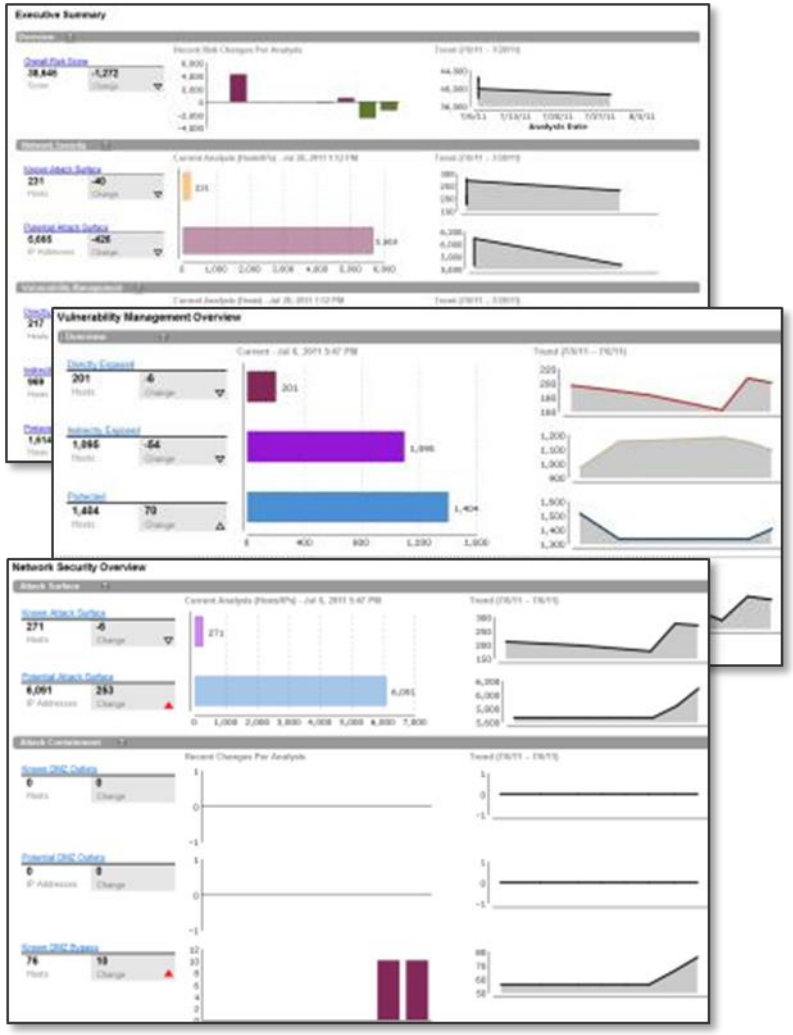
- Автоматическое определение изменений, которые необходимо внести в конфигурацию сети для предоставления/блокирования доступа к сегментам сети
  - Все устройства в пути доступа
  - Устройства,блокирующие/разреша ющие доступ
  - Правила/ACL, блокирующие /разрешающие доступ



- Оценка рисков, связанных с вносимыми изменениями в конфигурацию сети
- Информация о появляющихся уязвимостях
- Отображение возможных векторов атак

Построение отчетов

- 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

- 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

Особенности поставки и эксплуатации

- Возможна поставка в виде программного обеспечения, либо образа виртуальной машины VMware
- Комплекс работает в пассивном режиме не влияя на работоспособность сети
- Масштабируемость решения

Клиенты компании

Технологические компании	Ритейл	Финансовые организации	Правительственные организации	Телекоммуникации
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, 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

Ключевые возможности

- 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

Вопросы?

117105, г. Москва, ул. Нагатинская, д.1, стр.1

Телефон: +7 (495) 980-67-76 доб. 162
Факс: +7 (495) 980-67-75

http://www.DialogNauka.ru
e-mail: rv@DialogNauka.ru