NVisionGroup
ЭНВИЖН ГРУП
Динамичный интегратор

СРАВНЕНИЕ РЕШЕНИЙ ПО УПРАВЛЕНИЮ УСТРОЙСТВАМИ ОБЕСПЕЧЕНИЯ ИБ

TUFIN, ALGOSEC, FIREMON, SKYBOX, ~~REDSEAL NETWORKS~~

Кузеев Пётр

Ведущий эксперт ДИБ

NVisionGroup
ЭНВИЖН ГРУП

Кратко о вендорах

Вендор	Продукты	API	*Списки устройств	Дистрибутор в РФ
Tufin	Secure change, Secure Track, Secure App	Да (До)	Да (20+)	RRC
AlgoSec	Firewall Analyzer, Fireflow, Business Flow	Да	Да (20+)	NGS
SkyBox	Firewall Assurance, Change Management, Network Assurance, Risk control, Threat manager	Да(После)	Да (70+)	IITD
FireMon	Security Manager, Policy Planner, Risk Analyzer	Да	Да (30+)	SafeLine
~~RedSeal Networks~~	~~Security Risk Management, Continuous Monitoring and Audit, Predictive Threat Modeling~~	~~Нет~~	~~Нет~~	~~Нет~~

* полный список устройств по каждому вендору в приложении 1 (слайд №18)

NVisionGroup
ЭНВИЖН ГРУП

Tufin – SecureChange Workflow

SecureChange Workflow
Управление изменениями сетевой политики безопасности
Глубоко настраиваемые рабочие процессы
Надежное управление задачами
Отслеживание уровней обслуживания
Советник по изменению политик защиты
Упреждающий анализ рисков и автоматизированный контроль
Интеграция с системами обработки заявок
Полнофункциональный аудит безопасности

NVisionGroup
ЭНВИЖН ГРУП

Tufin – SecureTrack

Контроль

Анализ

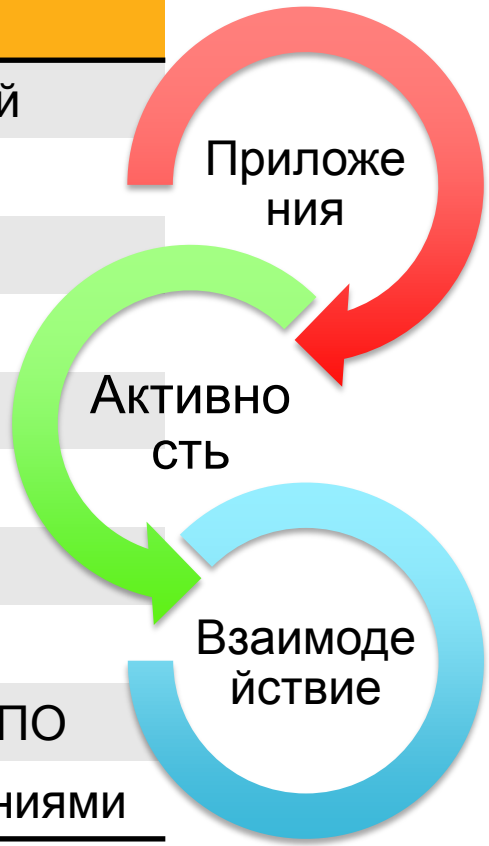
Схема

SecureTrack
Визуальный анализ для широкого класса устройств
Контроль и анализ изменений
Мониторинг операционной системы МСЭ
Оптимизация инфраструктуры безопасности
Анализ рисков
Корпоративный аудит и соответствие требованиям
Схема сетевой топологии
Сертификация правил
Автоматизированная генерация правил для МСЭ
Масштабируемость и возможность подстройки

NVisionGroup
ЭНВИЖН ГРУП

Tufin - SecureApp

Tufin – SecureApp
Управление политикой безопасности на основе приложений
Определение всех сетевых соединений для приложения
Отслеживание правильной работы приложений в сети
Упрощение процесса создания правил для приложений
Аудит работы приложений в сети
Улучшения взаимодействия между подразделениями
Управление зависимостями приложений
Постоянный контроль соответствия требованиям
Автоматический поиск возможностей оптимизации работы ПО
Удаление правил, связанных с неиспользуемыми приложениями



NVisionGroup
ЭНВИЖН ГРУП

AlgoSec – Firewall Analyzer

Firewall Analyzer

Управление конфигурациями брандмауэров

Аудит и проверка на соответствие стандартам

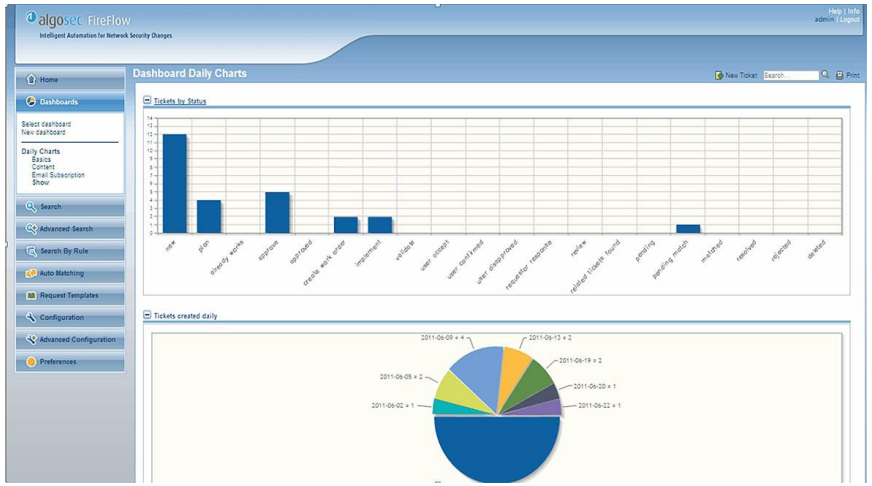
Анализ рисков

Оптимизация политик безопасности

Упрощение процедуры управления брандмауэрами

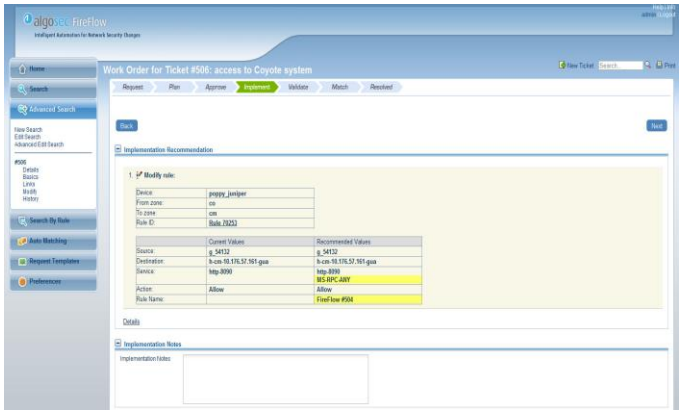
Проверки на соответствие минимальным требованиям ИБ

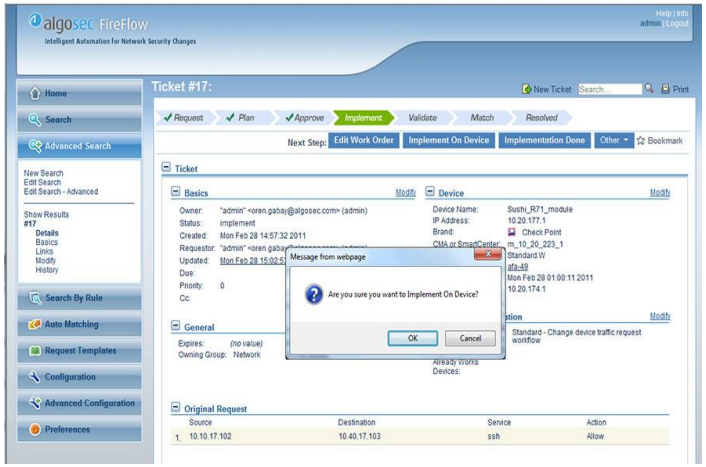
Управление конфигурациями роутеров



NVisionGroup
ЭНВИЖН ГРУП

AlgoSec - Fireflow





Fireflow

- Автоматизация процессов внесения и согласования изменений
- Проверка вносимых изменения на соответствия требования стандартов
- Анализ топологии
- Автоматизированное применение политики
- Отчёты по аудитам
- Автоматизированные проверки корректности работы применённых правил
- Интеграция с существующими системами контроля изменений
- Система согласований изменений для шлюзов веб фильтрации
- Отслеживание SLA

NVisionGroup
ЭНВИЖН ГРУП

AlgoSec – Business Flow

Business Flow

Автоматизированное создание правил под требования пользователя

Оценка влияние изменений на производительность системы

Удаление избыточных разрешений

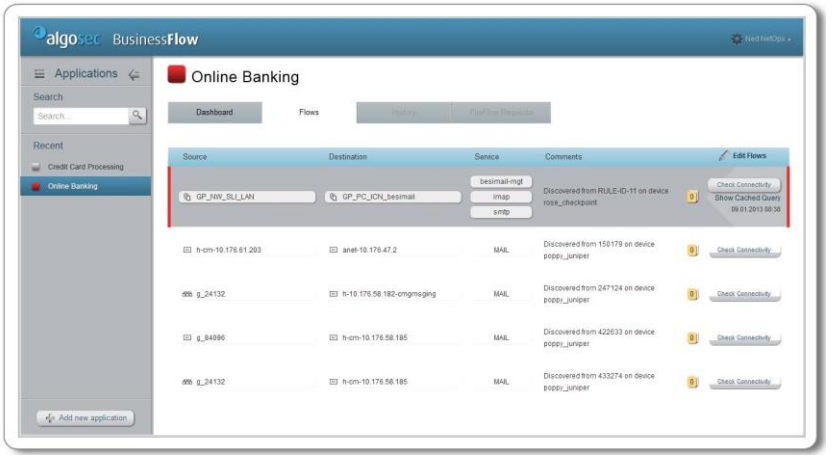
Портал-конструктор для создания правил и запросов

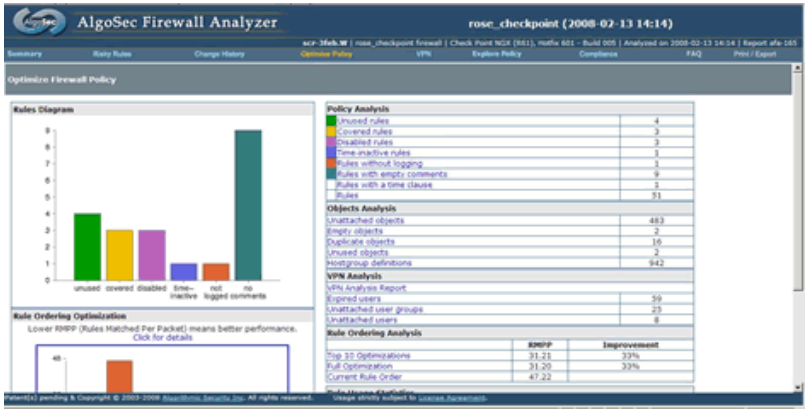
Настройка правильной работы приложения

Полный аудит всех изменений

Полная интеграция со всеми компонентами AlgoSec

Интеграция с CMDB – базой данных управления конфигурациями





NVisionGroup
ЭНВИЖН ГРУП

Skybox – Firewall Assurance

Firewall Assurance
Анализ конфигураций
Отчёты по аудиту
Контроль изменений
Применение политик, рекомендуемых стандартами
Поддержка систем IPS
Предварительная проверка вносимых изменений
Моделирование топологии
Интеграция со Skybox Change Manager

NVisionGroup
ЭНВИЖН ГРУП

Skybox – Change Manager

Change Manager

Система контроля изменений с веб интерфейсом

Полноценная система заявок

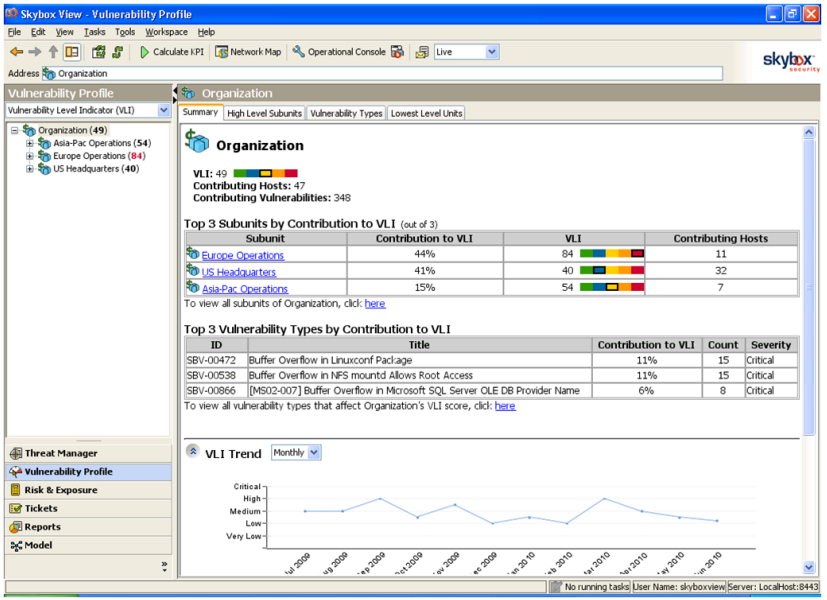
Поиск брандмауэров по заданным типам изменений

Проверяет актуальность соединений

Контроль соответствия политики

Автоматизированные оповещения по e-mail

Интеграция с системами обработки заявок сторонних производителей

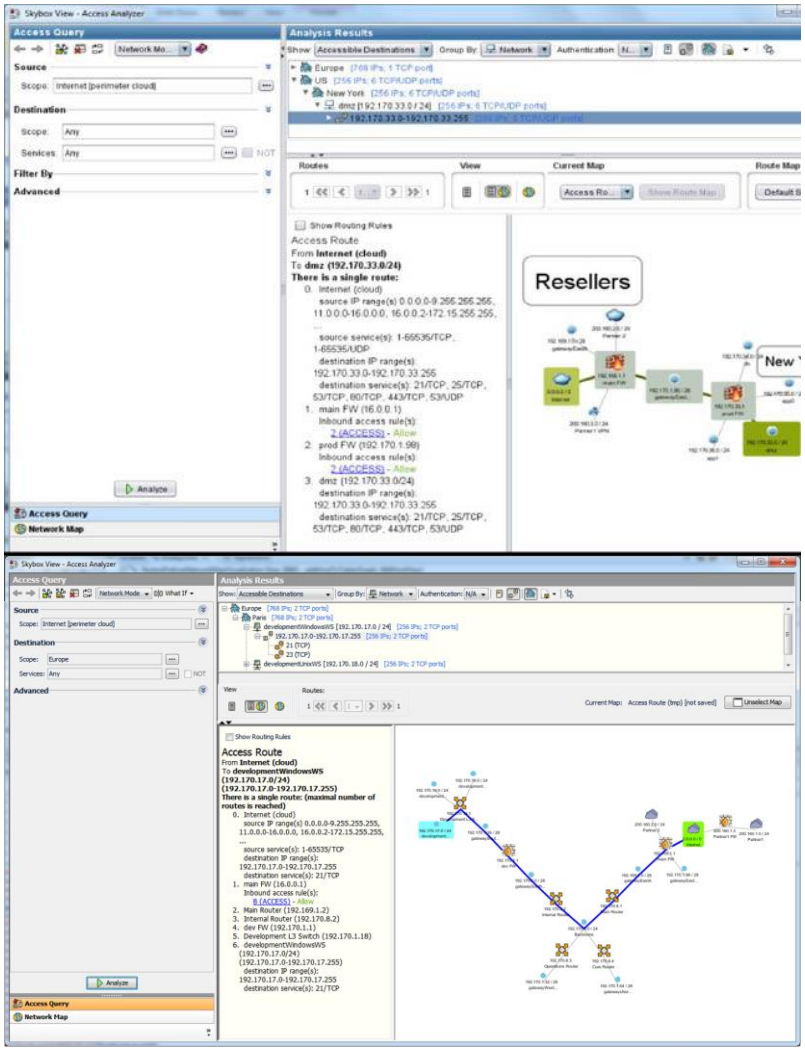


NVisionGroup
ЭНВИЖН ГРУП

Skybox – Network Assurance

Network Assurance

- Проверки соответствия сетевых устройств политикам ИБ
- Формирование топологии сети
- Применение политик, рекомендуемых стандартами
- Отчёты по соответствию стандартам ИБ
- Управление конфигурациями сетевых устройств
- Управление политикой доступа к сети
- Анализ проблем доступа
- Симуляция всей сети



NVisionGroup
ЭНВИЖН ГРУП

Skybox – Risk Control

Risk Control
Отчёты по уязвимостям и угрозам
Автоматическое создание и обновление виртуальной модели ИТ инфраструктуры
Настраиваемые варианты отчётов по запросу аудиторов
Встроенная система заявок
Улучшенный дизайн дашбордов
Оценки рисков воздействия на тот или иной узел
Автоматизированная приоритезация рисков
Автоматизированное приведение систем к соответствию политике ИБ

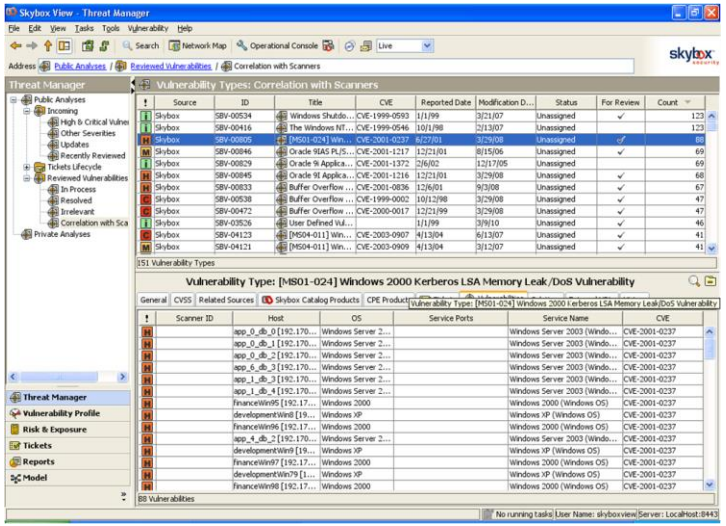
skybox security

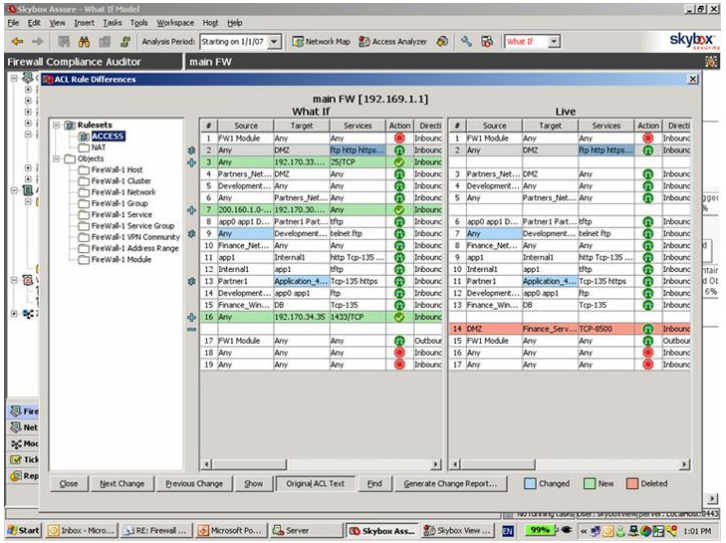
NVisionGroup
ЭНВИЖН ГРУП

Skybox – Threat Manager

Threat Manager

- Централизованное оповещение об угрозах с использованием репозитория уязвимостей
- Гибкая приоритезация угроз
- Рекомендации по устранению угроз
- Встроенная система заявок
- Отчеты по действиям и событиям
- Настройки параметров для SLA
- Прогнозирование последствий возможной реализации угроз
- Использование сторонних репозиториев
- Агрегация данных по всей компании



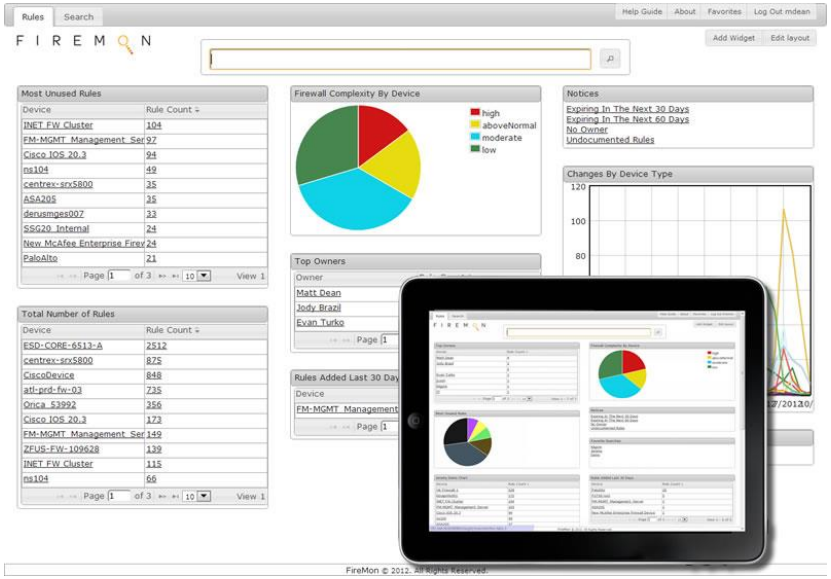


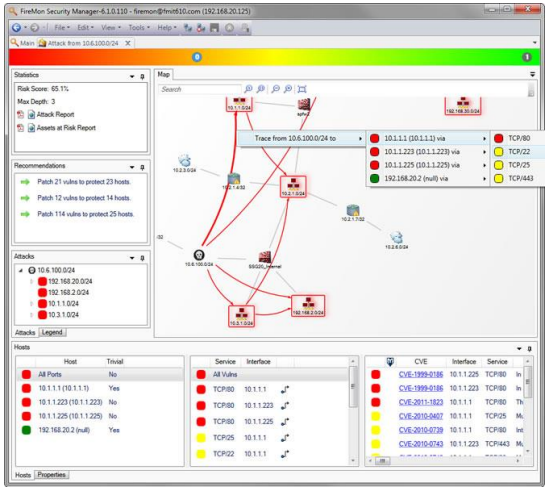
NVisionGroup
ЭНВИЖН ГРУП

FireMon – Security Manager & Policy Planner

Security Manager & Policy Planner

- Контроль каналов доступа
- Идентификация каналов атак
- Аудит
- Отчёты и уведомления о изменениях
- Настраиваемый анализ
- Отслеживание неиспользуемых правил
- Глубокий анализ топологии
- Оценка состояния брандмауэра
- Оптимизация политик брандмауэра
- Выявление скрытых правил
- Контроль отказоустойчивости
- Предварительный анализ изменений
- Анализ трафика



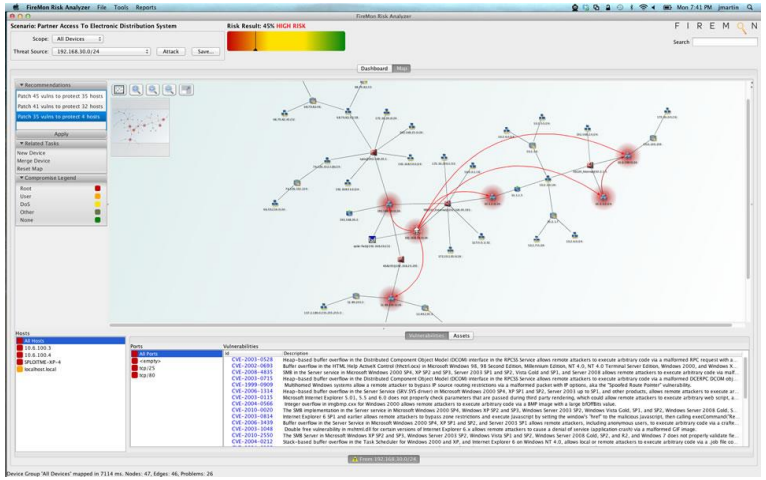


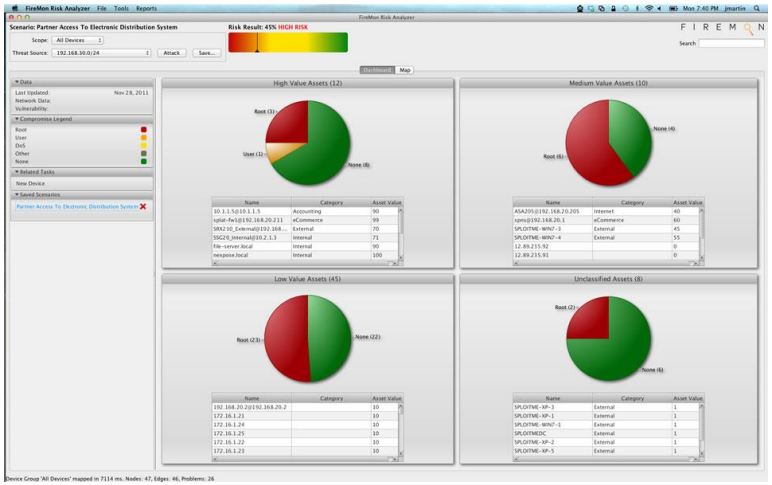
NVisionGroup
ЭНВИЖН ГРУП

FireMon – Risk Analyzer

Risk Analyzer

- Обзор рисков
- Рекомендации по устранению
- Приоритезация рисков
- Карта каналов атак
- Виртуальный патчинг
- Оценка рисков
- Определение возможных сценариев угроз





NVisionGroup
ЭНВИЖН ГРУП

Варианты поставки решений

Вендор	До 150	До 1000	До 2000
AlgoSec	1020/1021	1080/1081	1160
Tufin	T-500	T-1000 / XL	
FireMon	SPX310-ES/305-DC	SPX610-ES/605-DC	*
Skybox		SK 5000	
			**

* в определённых вариантах поставки может превышать это количество

** для всех вендоров существуют поставки в виде софта или виртуальной системы

Спасибо за внимание! Ваши вопросы?

Кузеев Пётр

Ведущий эксперт ДИБ

тел.: +7 (495) 641-1212 моб.: +7 (985) 9994824

e-mail: pkuzeev@nvg.ru, Skype: pkuzeev

NVisionGroup
ЭНВИЖН ГРУП
Динамичный интегратор

NVisionGroup
ЭНВИЖН ГРУП

Приложение 1 – Списки поддерживаемых устройств*

Cisco PIX
Cisco VPN3000
Citrix NetScaler
Enterasys routers
Extreme Networks Black Diamond
F5 BigIP
Fortinet Fortigate (FortiOS)
Gauntlet firewall
GTA GB firewall
HP TippingPoint
IBM Security Network Intrustion Prevention System (formerly IBM Proventia NIPS)
Juniper JunOS based devices (J-series, SRX) & Syslog
Juniper Netscreen ScreenOS based devices (ISG, SSG devices)

* для просмотра полного списка по всем вендорам нажмите на таблицу

NVisionGroup
ЭНВИЖН ГРУП

Приложение 2 – Ссылки, замечания по теме, комментарии

Информация
Tufin - http://www.tufin.com/ - техническая поддержка на русском языке
AlgoSec - http://www.algosec.com/ - акцент на бизнес процессах
FireMon* - http://www.firemon.com/ - поддержка экзотики (например, Secui NXG)
SkyBox* - http://www.skyboxsecurity.com/ - лидер по количеству устройств
RedSeal Networks - http://www.redsealnetworks.com/ - не работает в РФ

* у данных вендоров присутствует элемент для контроля и устранения уязвимостей на ендпойнтах, единственное кардинальное отличие (кроме списка поддерживаемых из коробки вендоров), которое можно учитывать перед пилотным тестированием