Автоматизация оценки безопасности сети

Алексей Лукацкий

Бизнес-консультант Cisco

Рассматриваемые темы

- Традиционный подход
- Новые возможности: автоматизация
- Пример внедрения: моделирование сети
  - Глобальная инфраструктура Cisco
- Пример внедрения: защита важных активов
  - Изоляция инфраструктуры открытых ключей (PKI)
- Пример внедрения: защита зоны
  - Очистка граничных точек присутствия (PoP)
- Пример внедрения: автоматизация оценки периметра
  - Пассивное тестирование глобального предприятия на проникновение угроз извне
- Пример внедрения: ежедневное управление изменениями

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

– это не только разработчик

- ~94,000 сотрудников и контрактников
- ~300 офисов в 90 странах
- ~400 зданий
- 4 центра обработки данных

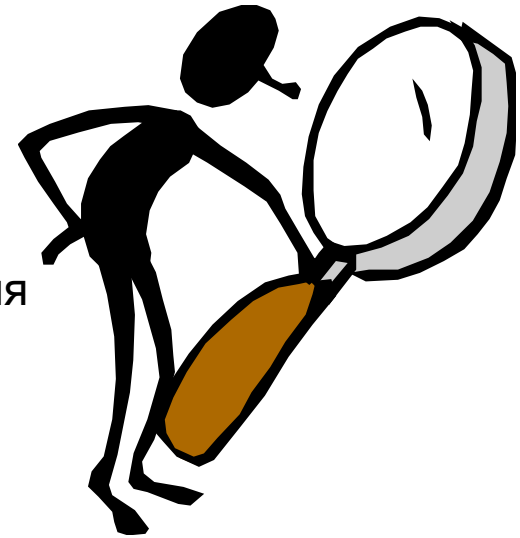
- ~24,000 смартфонов с мобильной почтой и мобильными приложениями
  - RIM BlackBerry,
  - iPhone
  - Windows Mobile Smartphone,
  - Nokia Symbian,
  - Palm OS
- 129 операторов связи
- 80,000+ управляемых лэптопов/ПК
  - Windows, Mac, Linux

Более 180,000 людей по всему миру в большой «семье» Cisco

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Современный аудит безопасности сети

- Как правило, аудит на уровне сети рассматривается, а его результаты обрабатываются отдельно от аудита на уровне узлов
- Сеть:
  - Приложенные усилия и пристальное внимание
    - Сбор конфигураций; печать конфигураций; чтение конфигураций
    - Процесс аналогичен проверке телефонной книги
- Узлы:
  - Уровень 1: администраторы применяют исправления
    - Проблема: надежда — это не стратегия
  - Уровень 2: проверка на наличие систем, где не установлены исправления
    - Проблема: количество данных превышает объем, который можно обработать
  - Уровень 3: очистка на основе рисков
    - Проблема: расстановка приоритетов — легче сказать, чем сделать



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Области, требующие изменений

- Стандартные группы:
  - Эксперты по атакам на узлы
    - Работа без понимания контекста сети или бизнеса
    - Недостаточно сетевых специалистов
    - Важные знания в головах нескольких специалистов
- Однообразные действия по проверке
  - Аналогично ситуации, в которой количество авиакомпаний превышает число бригад по обслуживанию самолетов
- Потребности:
  - Выполнение каждой проверки за меньшее время
  - Повышение точности
  - Запись правил для следующей проверки
  - Объединение знаний специалистов — проблемы должны рассматриваться в контексте

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Отличия оценки сети

Обратите внимание, что ворота ЗАПЕРТЫ!

Вы не сможете найти маршрут обхода межсетевого экрана при анализе правил межсетевого экрана

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Пример внедрения: «проект «Атлас»

- Цель:

  отображение всей глобальной среды Cisco

  обзор основных взаимодействий

  аудит доступа к важным областям

- Ресурсы:

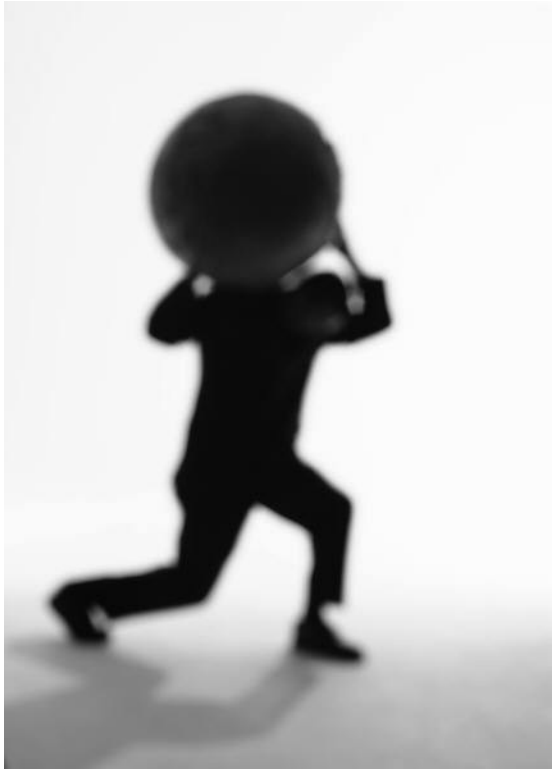
  Установленное ПО по моделированию сети

  Срок - две недели

  27 000 файлов конфигураций с 27000 маршрутизаторов и коммутаторов

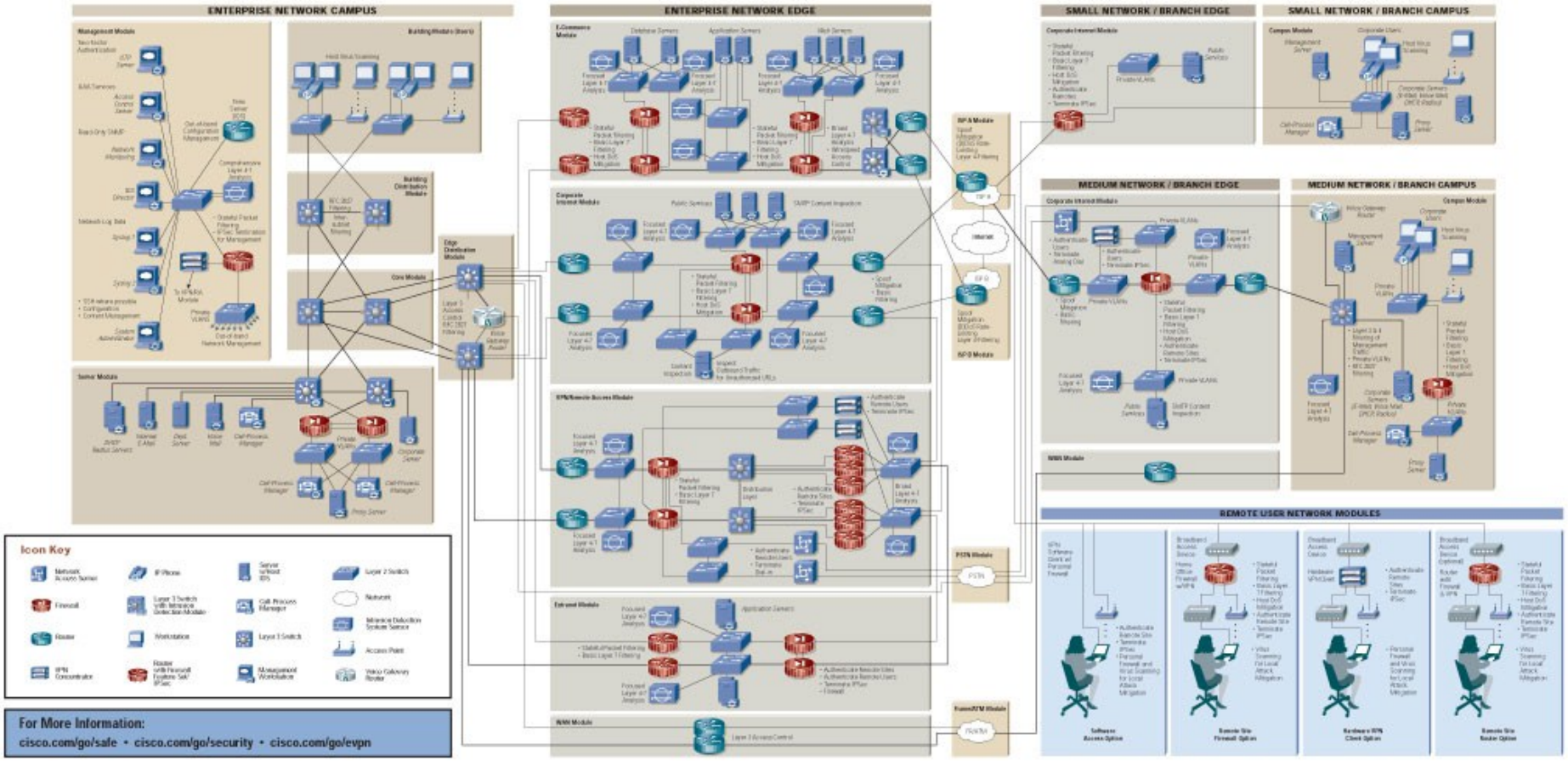
  Изначально использовался сервер стоимостью около 5 000 долларов США (четыре ядра, 32 Гбайт ОЗУ)

  Теперь работает на базе Cisco UCS — повышенное быстродействие!



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

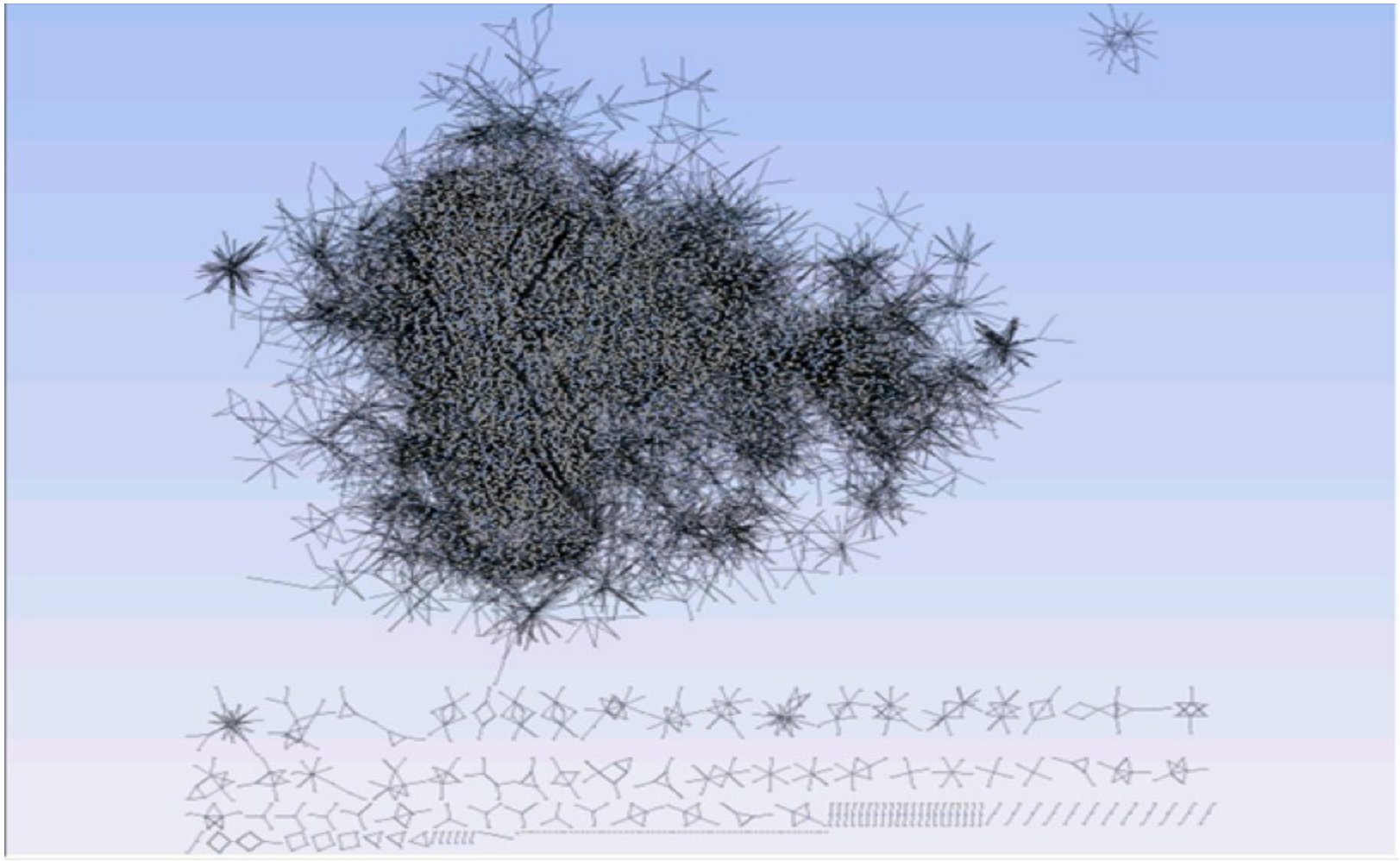
Как обычно рисуют корпоративную сеть?



Урок 1. Высокоуровневый взгляд всегда поверхностен

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

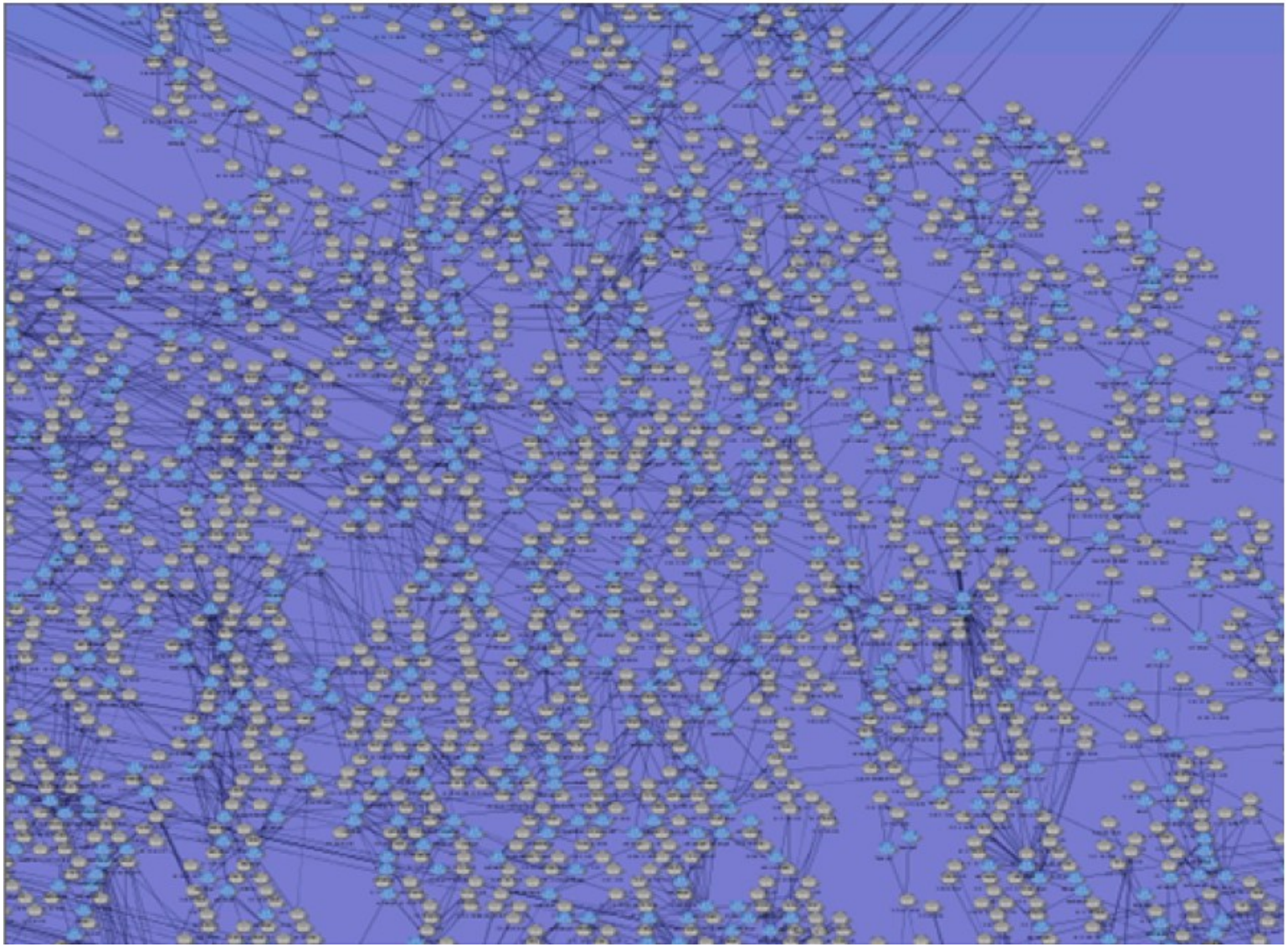
Как выглядит корпоративная сеть на самом деле?



Урок 2. Требуется репозиторий конфигураций и понимание сети, а не только ИБ

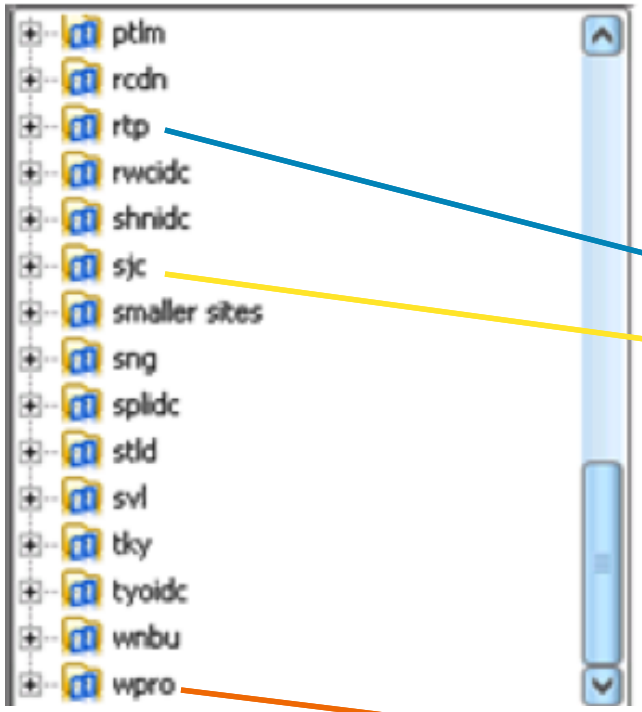
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

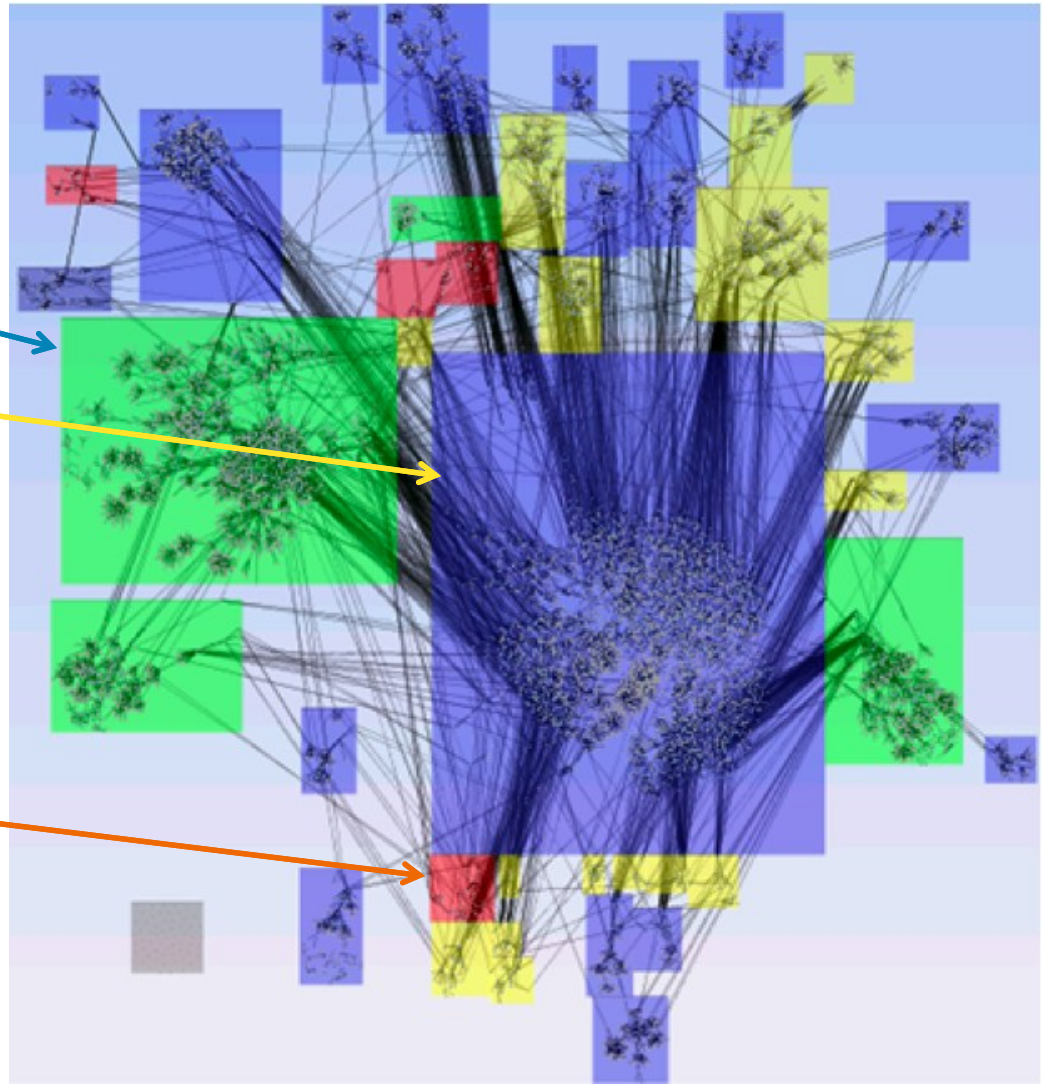
В глубине выглядит не лучше



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Организация глобальной сети Cisco



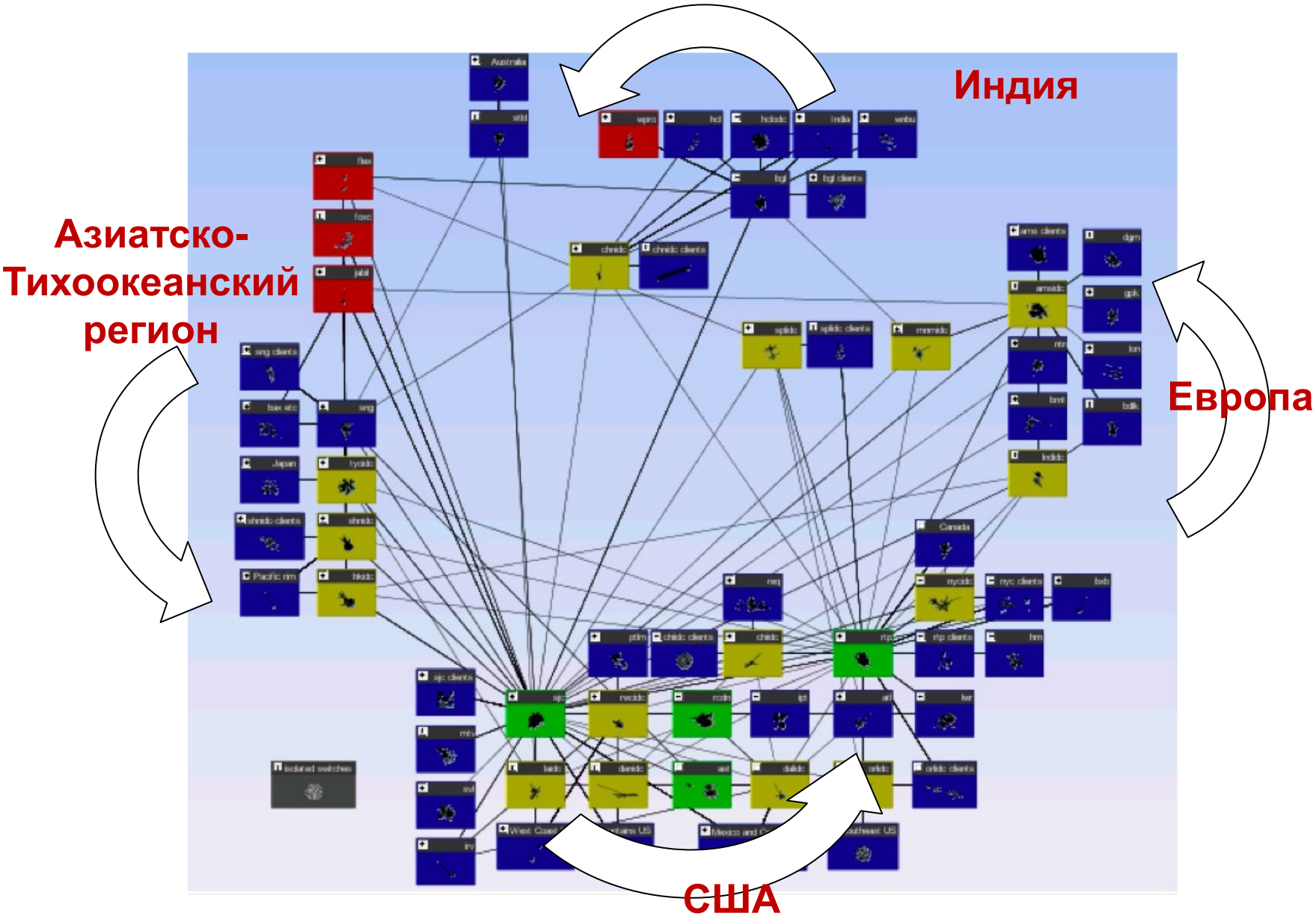


- Зонирование ежедневно меняющихся 56000 сетей (30 миллионов IP-адресов)

Урок 3. Принятые условные обозначения – вам в помощь

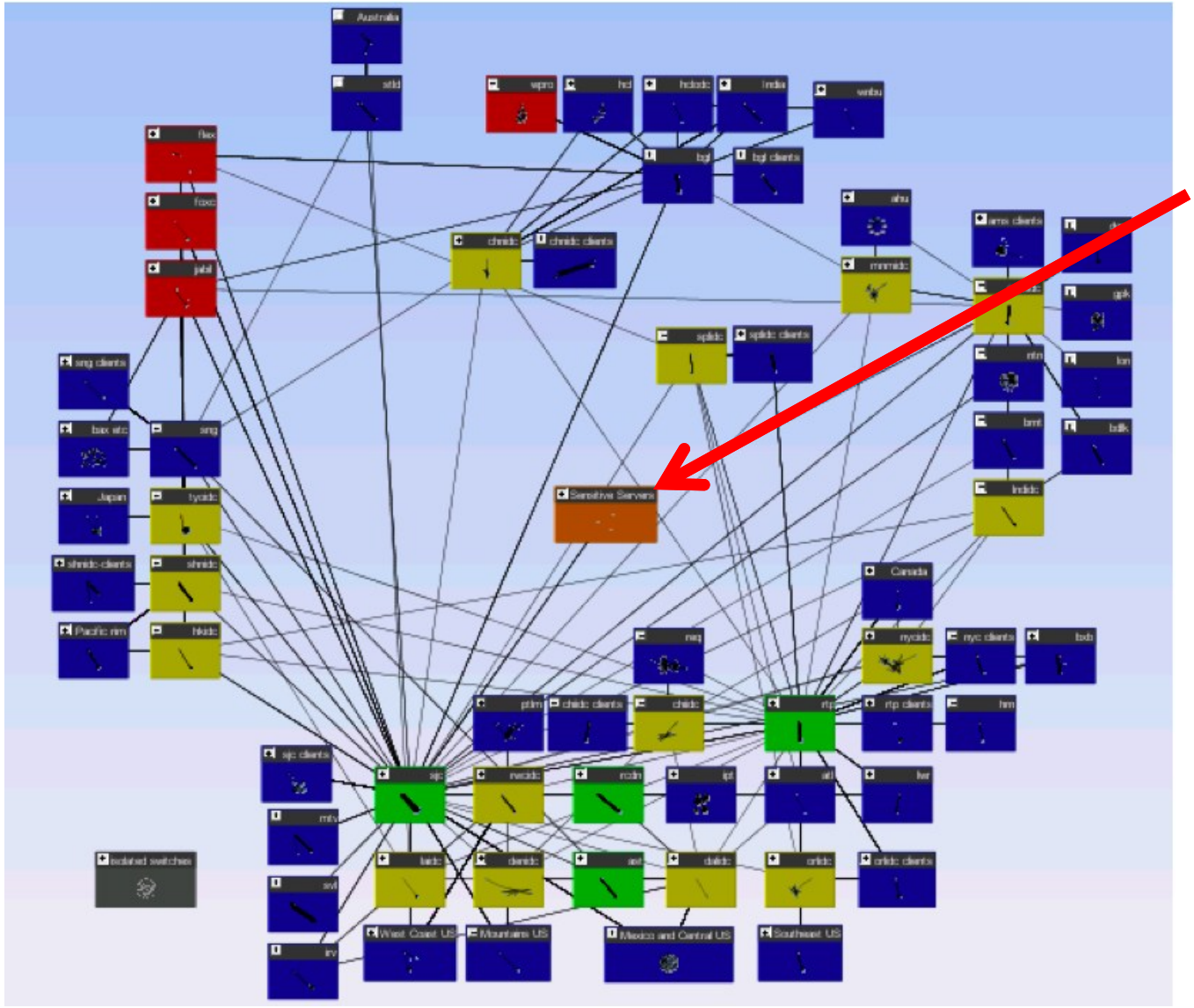
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Окончательное зонирование



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Выделение ключевых серверов

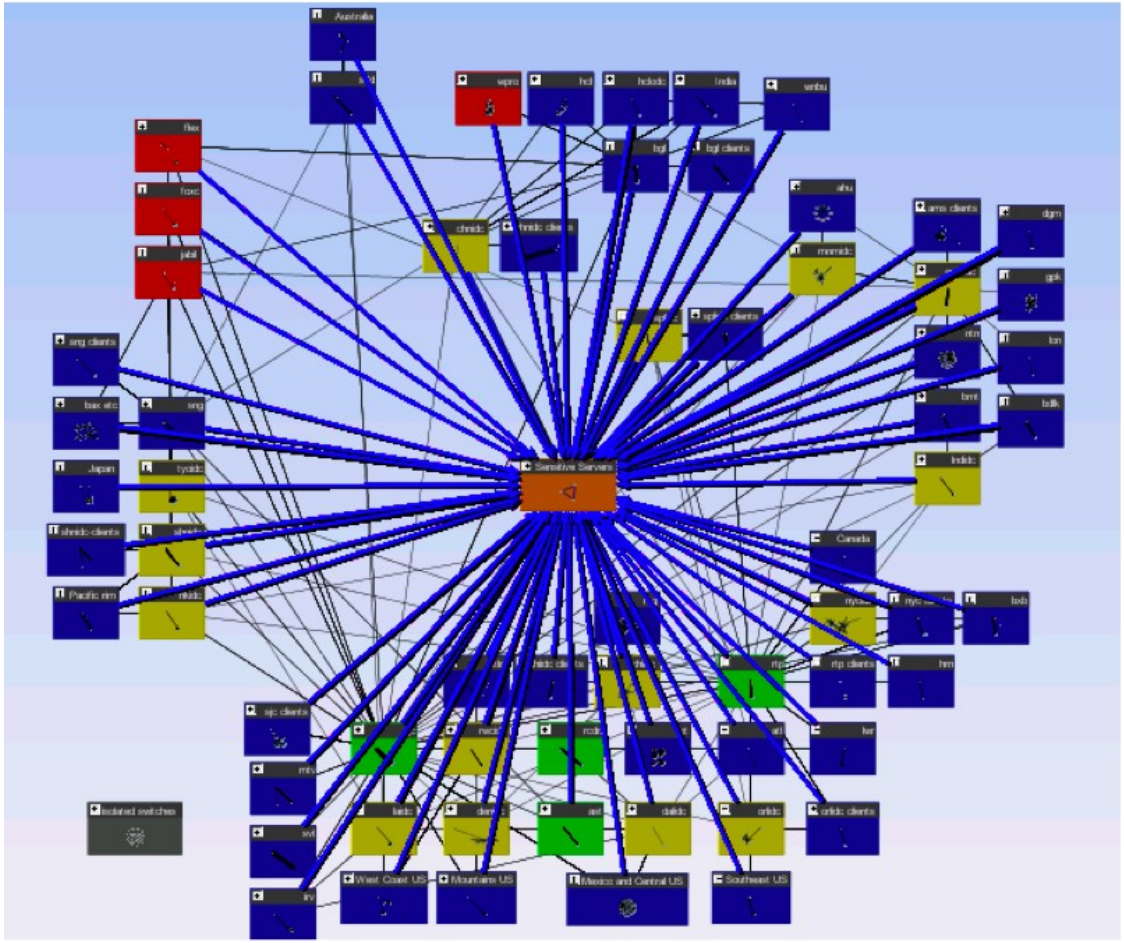


Сервера с важными данными

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Автоматический расчет подключений

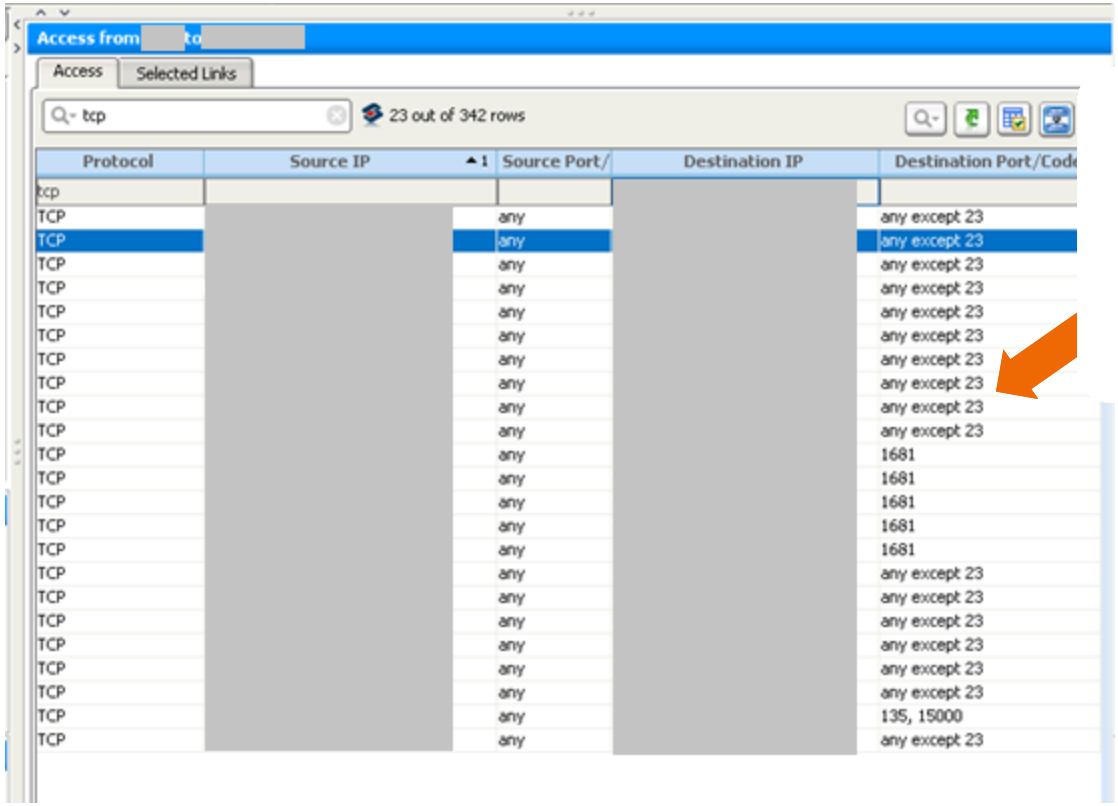
- Синие линии означают пути доступа к важным серверам
- Четко видна потребность в сегментации



Урок 4. С помощью рисунков можно легко объяснить сложные понятия, а система моделирования сети помогает понять информационные потоки

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Автоматизация анализа каждого потока



Источник	Порт назначения
любой	любой, кроме 23
любой	любой, кроме 23
любой	любой, кроме 23
	…

- Подробный анализ каждой синей линии
- По крайней мере мы заблокировали интерфейс Telnet

  (По понятным причинам некоторые особенности скрыты)

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Промежуточные результаты: до и после

- До:
  - Отсутствие способа наглядного представления глобальной инфраструктуры
- После:
  - Карта записи в «атласе»
  - Сформирована рабочая платформа для будущих проектов
  - Использование графических элементов для объяснения проблем безопасности неспециалистам

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Идем дальше: защита важных активов

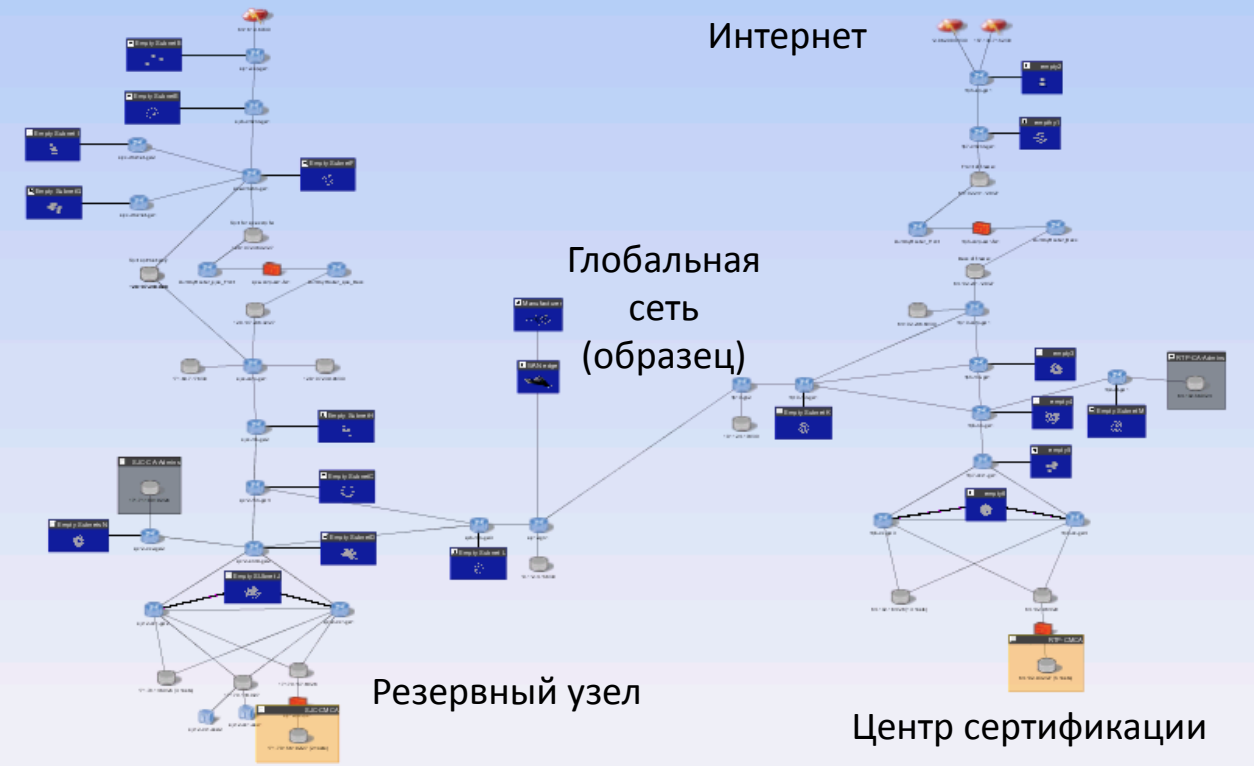
- Проверки PoP снаружи
  - Широкий диапазон охвата, поиск основных брешей системы безопасности
  - Проблема: большое количество проверяемых попыток доступа
  - Не удается быстро записывать все правила для входящего доступа
  - Некоторые активы требуют особого внимания
- Для критически важных активов необходима работа изнутри
  - Начать действия следует с известной цели
  - Нужно ограничить область охвата, усилить акцент
  - Постоянная повторная оценка

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Распределенная инфраструктура открытых ключей

- Основной узел + резервный узел

  Создание координатной схемы не представляло труда — был взят пример из атласа

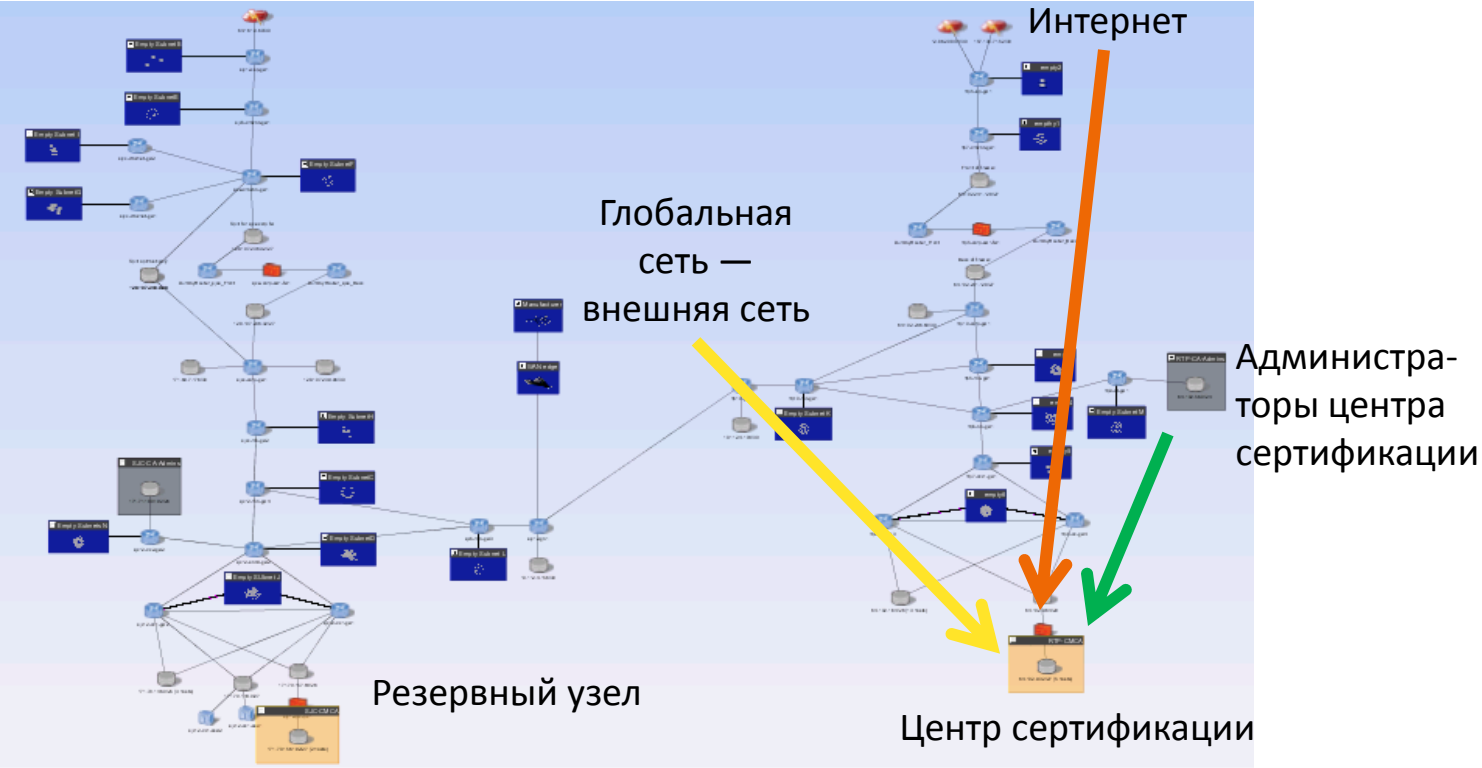


Урок 5. Справочный атлас — полезное средство для последующей работы

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Распределенная инфраструктура открытых ключей

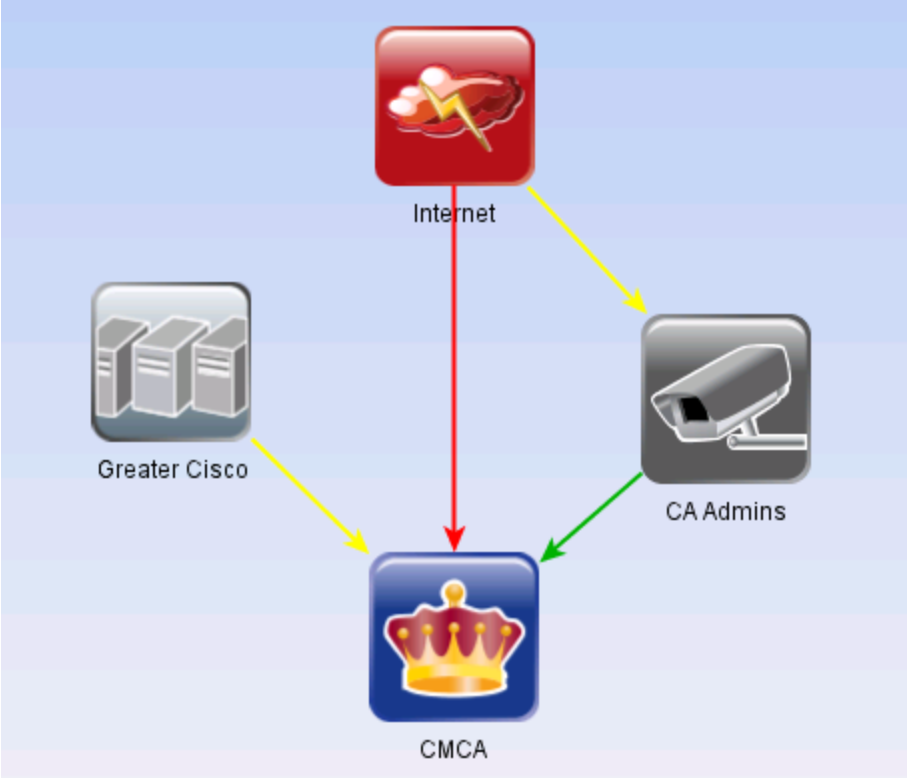
- Доступ строго контролируется
  - Ненадежные сторонние производители осуществляют доступ по сертификатам
  - Общий доступ должны иметь только администраторы центра сертификации



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Автоматизация создания высокоуровневой политики доступа

- Запись отношений основных зон
- Стрелками показаны направления нежелательного доступа по их критичности

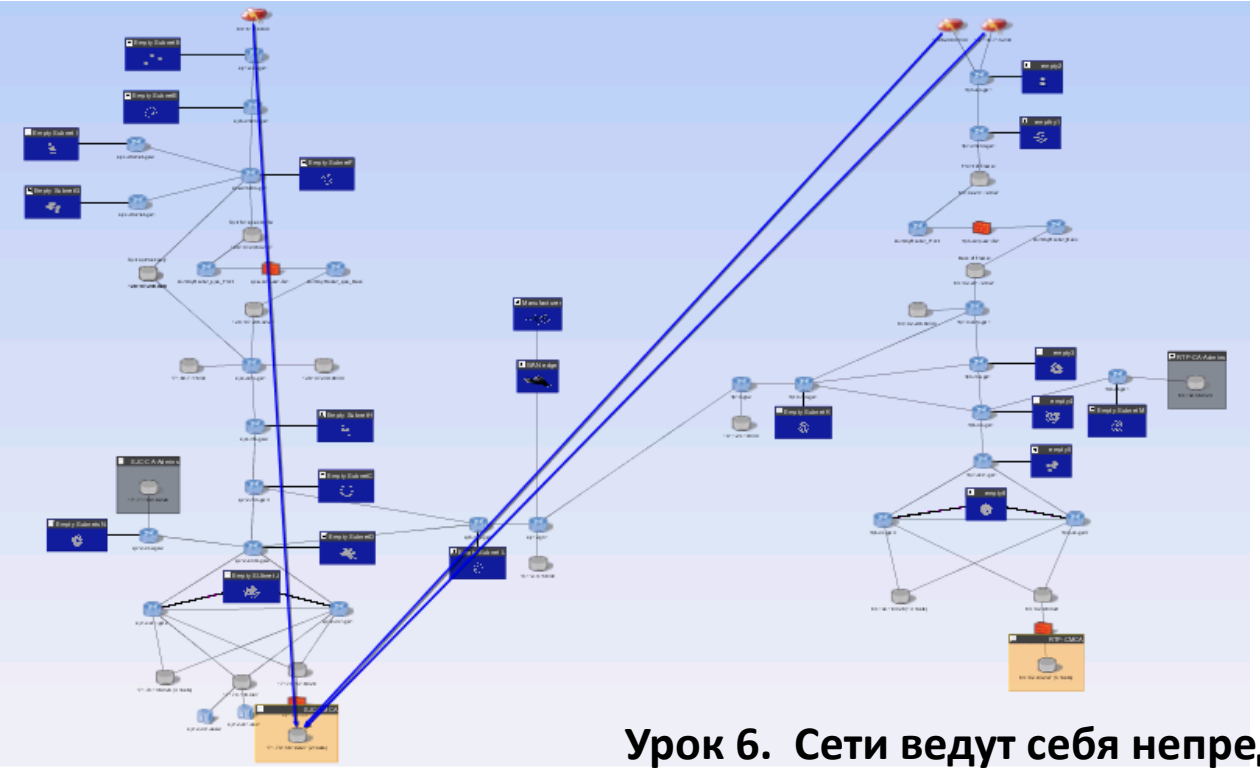


© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Изучение неожидаемого доступа

- Поток на основной центр сертификации отсутствует
- Неожидаемый доступ в Интернет был только на резервном сайте

  И даже этот неожидаемый доступ был предоставлен ограниченному количеству источников



Урок 6. Сети ведут себя непредсказуемо

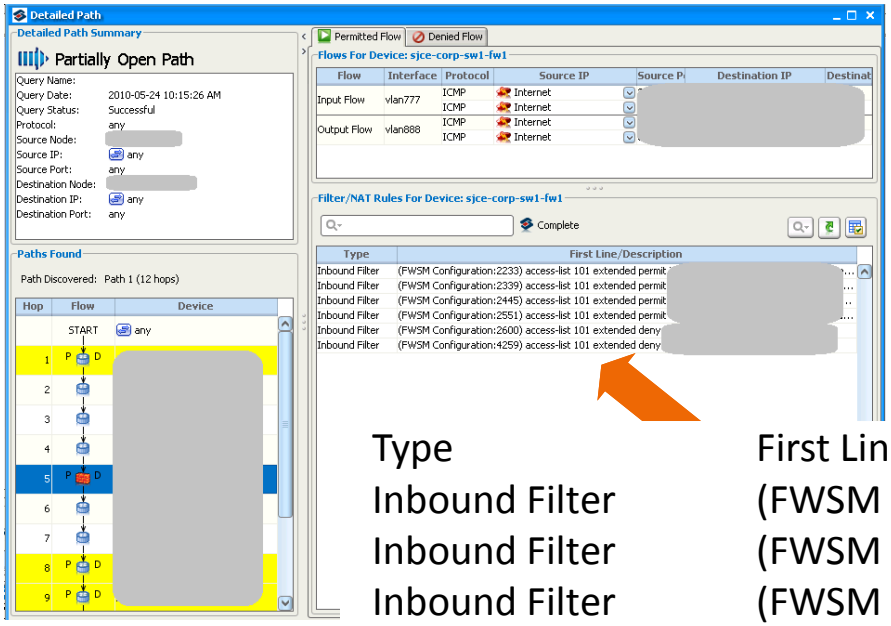
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Устранение нежелательного доступа

- Найдите подробный путь неожидаемого доступа
- Определите точную причину

  В этом случае причиной является необновленная группа объектов на межсетевом экране

Доступ найден



Пройдите через один прыжок

Отображение пути на «карте метро»

Type	First Line/Description
Inbound Filter	(FWSM Configuration:2233)
Inbound Filter	(FWSM Configuration:2339)
Inbound Filter	(FWSM Configuration:2445)
Inbound Filter	(FWSM Configuration:2551)
Inbound Filter	(FWSM Configuration:2600)
Inbound Filter	(FWSM Configuration:4259)

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Промежуточные результаты: до и после

- До:
  - Важные сведения затеряны в крупных и сложных сетях
- После:
  - Специальный набор правил для проверки функций защиты
  - Создание за два дня
  - Ежедневная повторная оценка по мере возникновения и распространения изменений сети
  - Автоматическая отправка сообщений с итоговым состоянием

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Идем дальше: защита зон

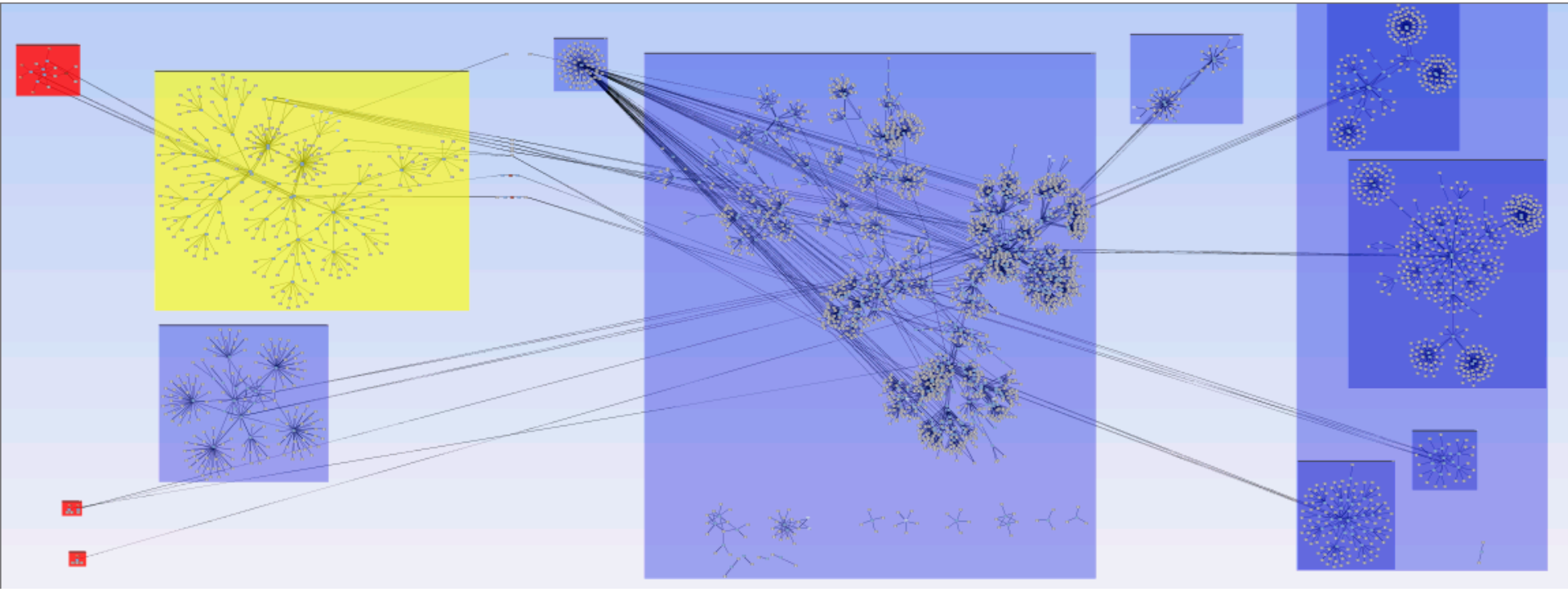
- Cisco располагает 15 основными точками контроля (PoP) для внешних подключений
- Обычное время оценки вручную: 90 дней для каждой PoP
- Конечный результат:
  1. Создание карты
  2. Запись основных зон:

     Интернет, DMZ, внутренняя сеть, лаборатории и т.д.
  3. Анализ нарушений практических рекомендаций
  4. Добавление уязвимостей узлов, выявленных после проверок
  5. Выполнение теста на проникновение

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Карта сети комплекса заданий в Сан-Хосе

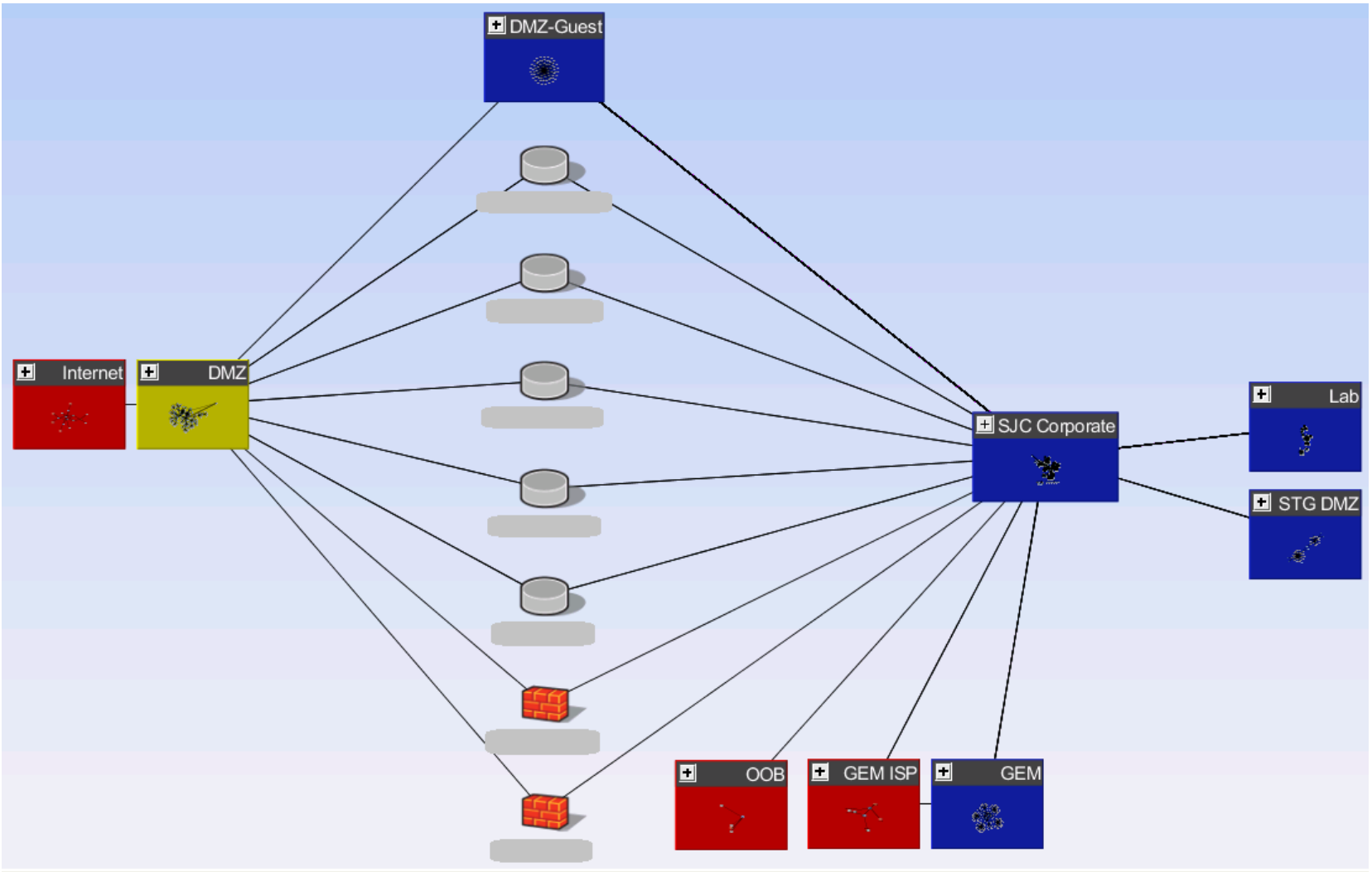
- Карта одной точки присутствия
- Зонирование произведено полуавтоматически



Интернет Демилитаризованная зона (DMZ) Основной сайт Лаборатории

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Карта сети комплекса заданий в Сан-Хосе



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Пример проверок соответствий лучшим практикам

- Автоматическая проверка более 100 правил
- Ненадежные или отсутствующие пароли, избыточные правила и т. д.

Check ID	Title	Severity
RS-16	Unencrypted Passwords	HIGH
RS-25	Default Enable Password	HIGH
RS-26	Default Password	HIGH
RS-29	No Password for User	HIGH
RS-38	Weakly Encrypted Password	HIGH
RS-41	Superfluous Enable Password	HIGH
RS-55	No Password on Console	HIGH

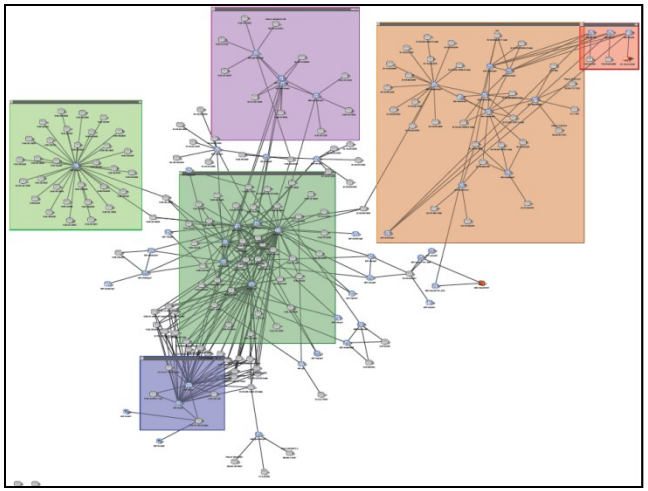
- Катящийся камень мхом не обрастает? В изменяющихся сетях все по-другому…

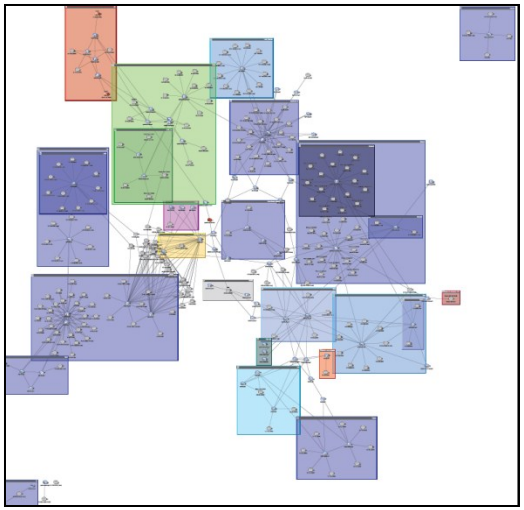
Урок 7. Лучшие практики получили свое название не просто так

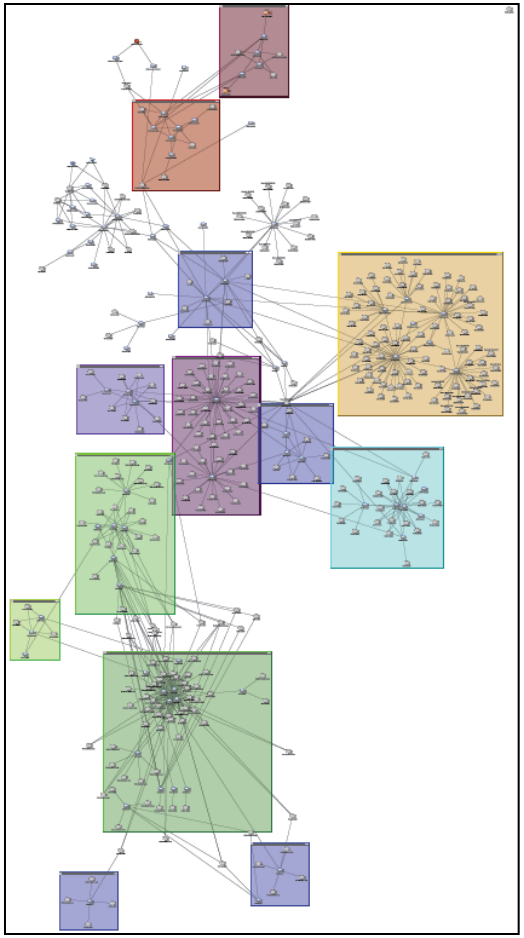
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Дополнительные образцы карт

- Карты 9 PoP, созданные и зонированные за одно утро
- Экспорт в форматы Visio и PDF





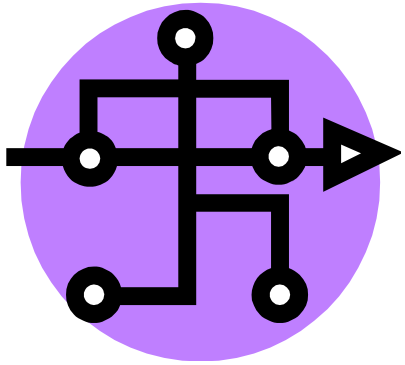


Урок 8. Это могут сделать обычные пользователи.

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

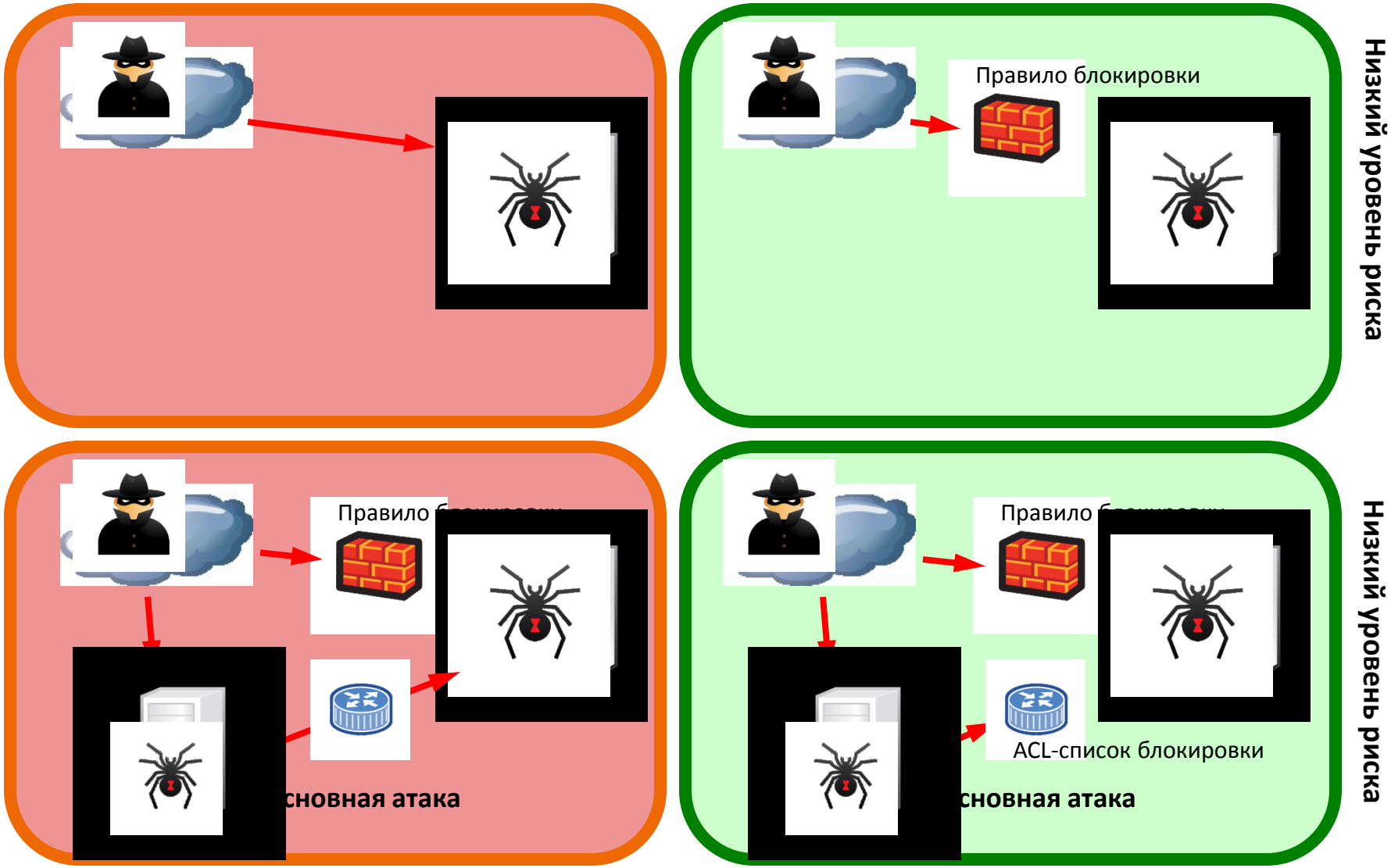
Проверка на проникновение в режиме оффлайн

- Следующим уровнем анализа является проверка на проникновение
- Использование карты сети совместно с проверками узлов
- Добавление расчетов доступа
- Программное обеспечение автоматически оценивает направления атак
- Определение слабых сторон с высоким уровнем риска



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

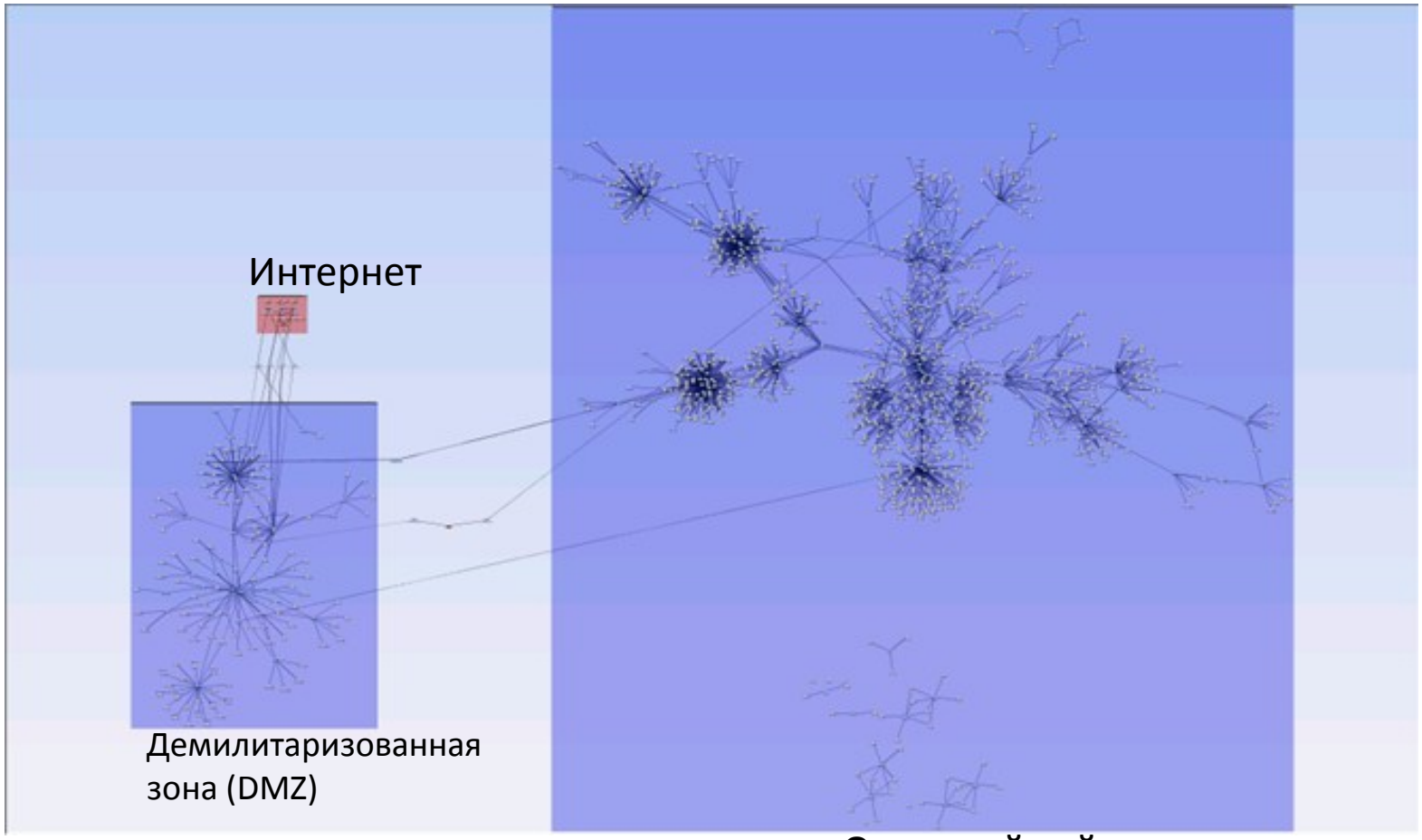
Риск от сетевых атак



28

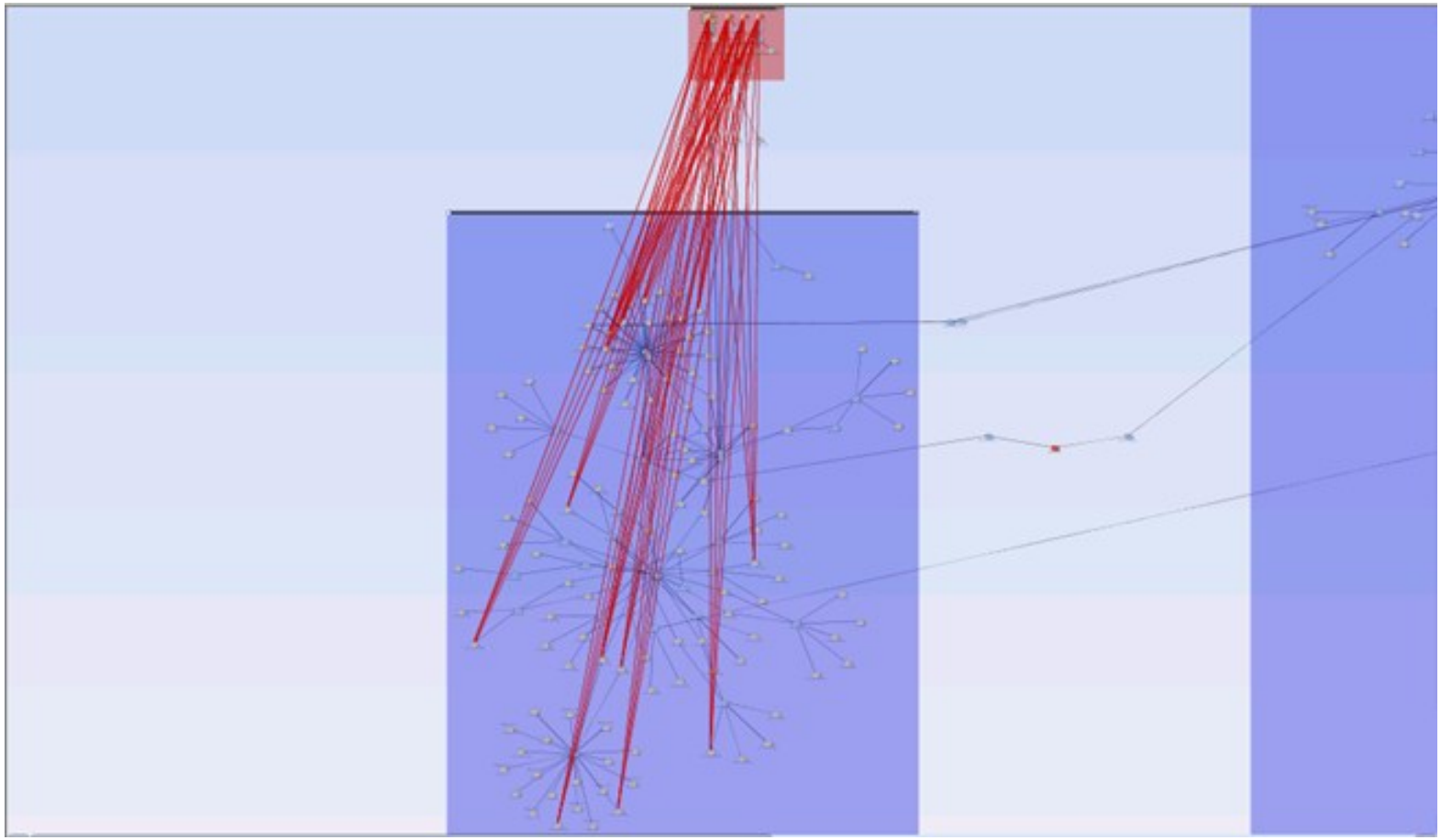
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Пример цепочки атак: ДО



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

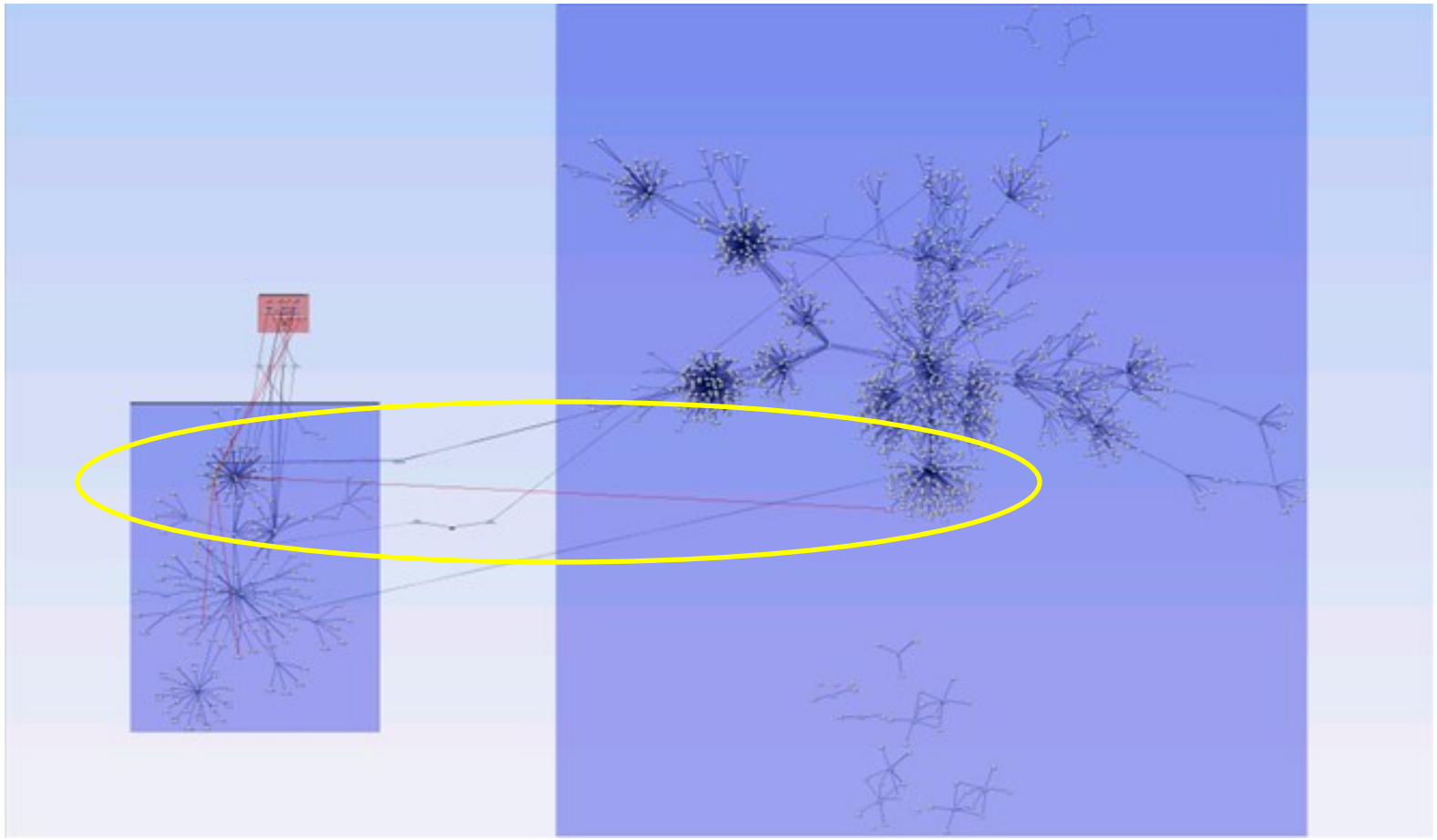
Этап 1. Уязвимые объекты в DMZ



- Злоумышленники могут захватить эти интернет-серверы

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

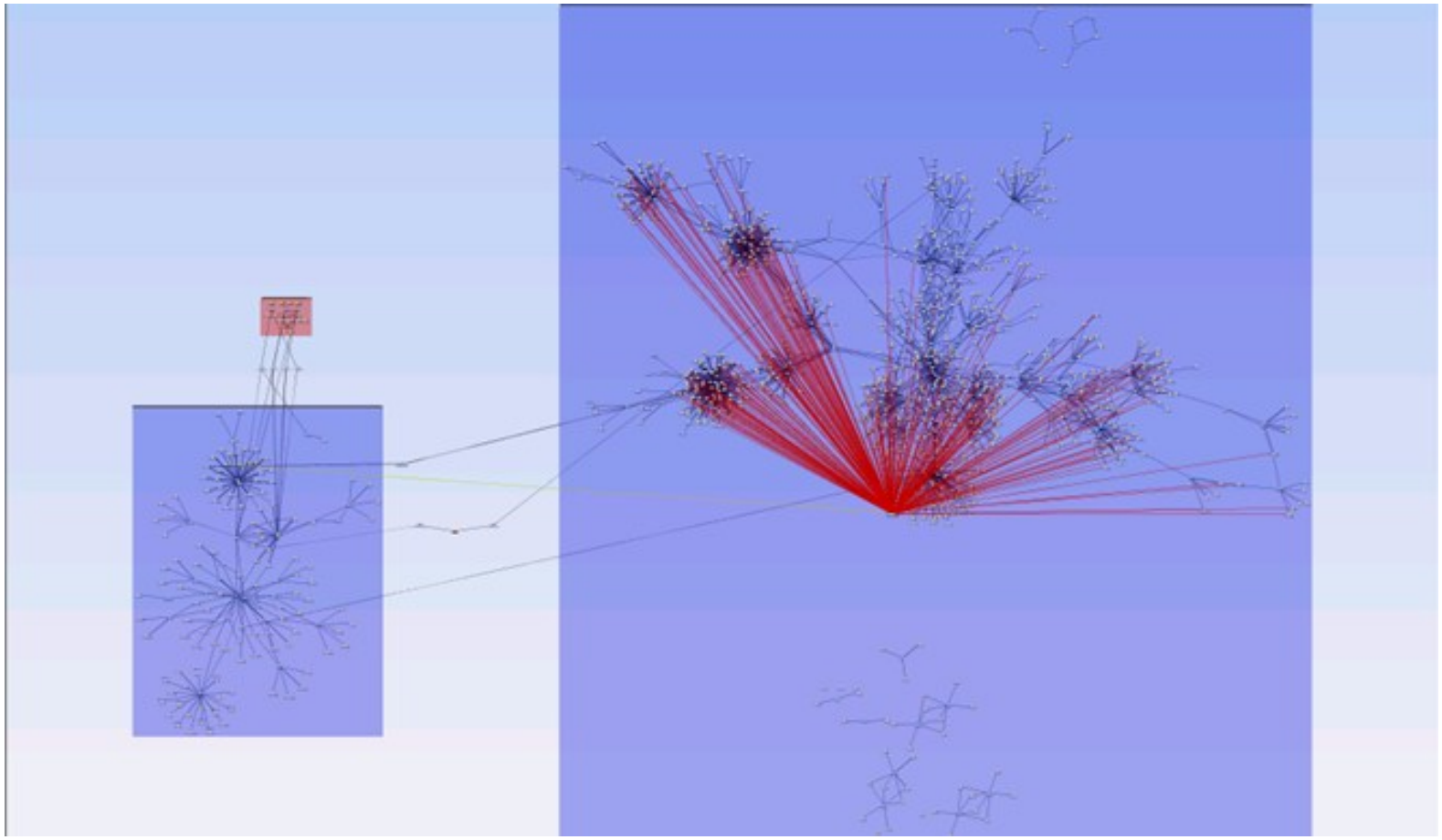
Этап 2. Проникновение некоторых атак



- Возможно действие лишь некоторых основных атак

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Этап 3. Веерное развертывание атаки

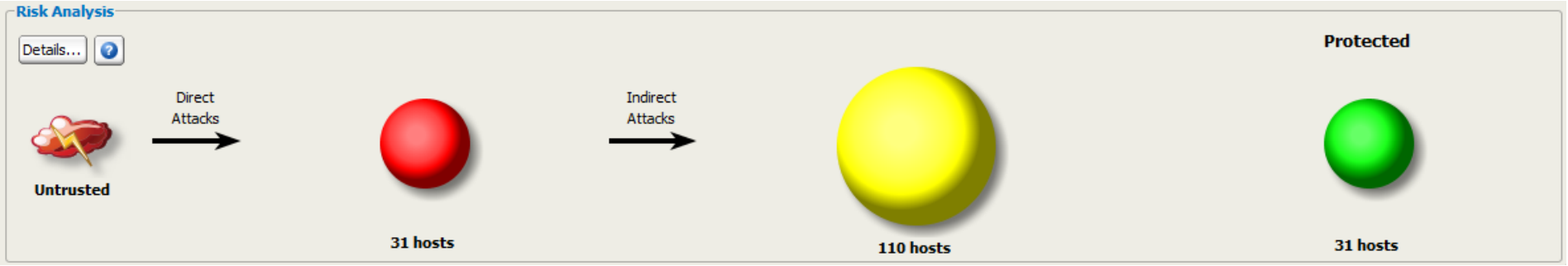


- Злоумышленник может проникнуть в случае, если он найдет брешь, которую вы еще не устранили

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Результаты теста на проникновение

- Пример результата



Злоумышленники извне могут захватить красные узлы

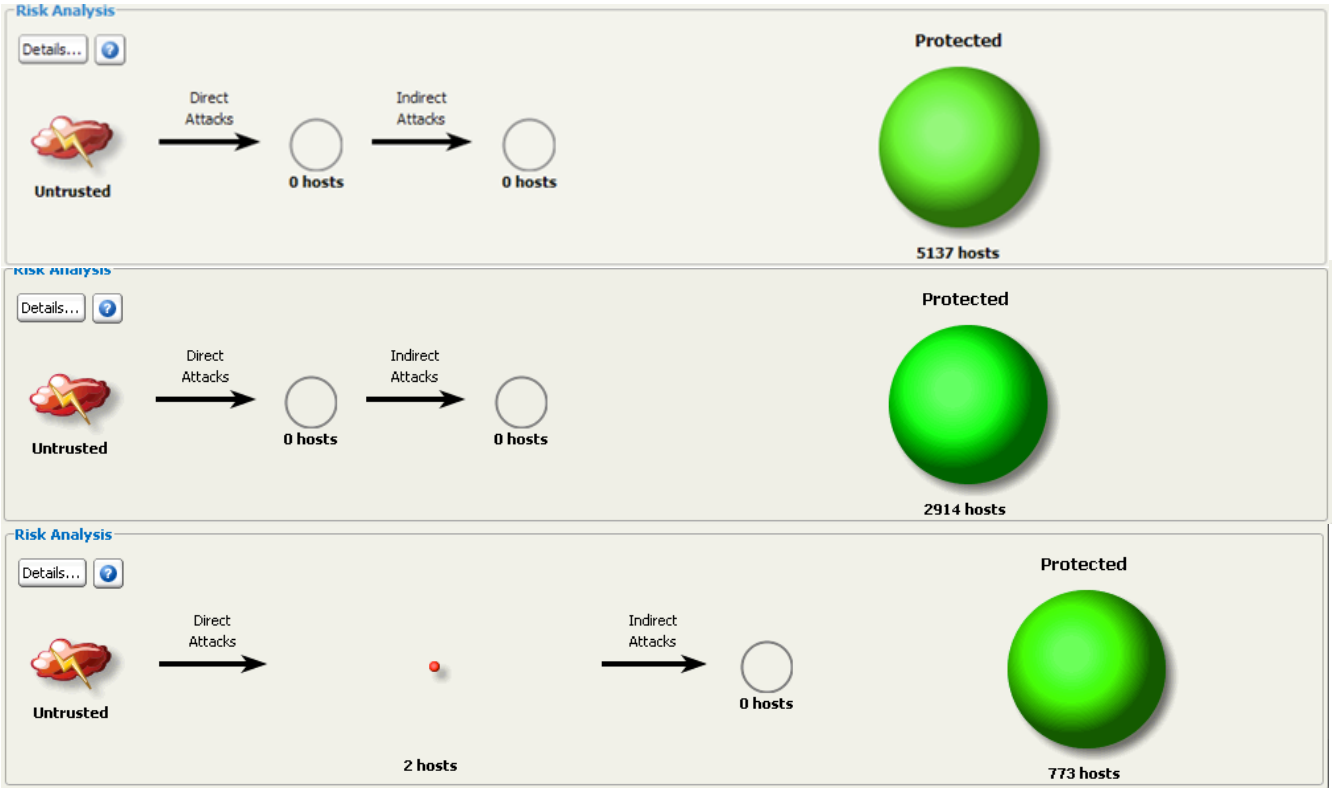
Затем идет атака желтых узлов

Однако зеленые узлы не подверглись воздействию никаких атак

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Результаты недавнего анализа точек присутствия

- Проанализировано три точки из девяти
- Они чисты — небольшая площадь соприкосновения



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Промежуточные результаты: до и после

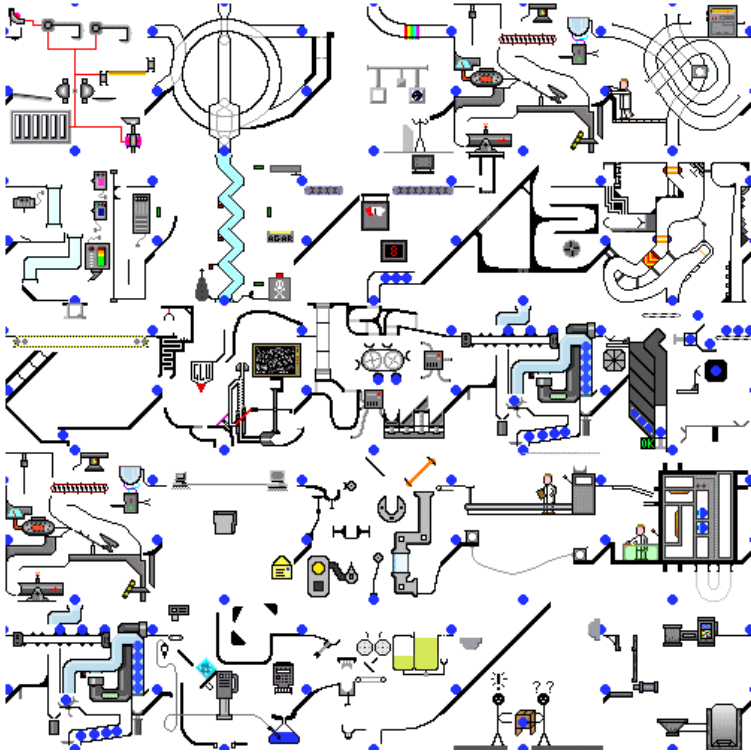
- До:
  - Проверка каждой PoP занимала 90 дней
  - Данные об уязвимости узлов не учитывались
- После:
  - Группа выполняет 9 проверок PoP за один день
  - Интегрированная оценка
    - Анализ конфигурации сети
    - Зонированная карта
    - Уязвимости узлов
    - Анализ пути распространения атаки
  - Дополнительное преимущество: карту и результаты можно использовать повторно во время следующего посещения

Урок 9. Данные о сети + данные об уязвимостях + направление атаки = GOLD (общая онлайн-диагностика)

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Идем дальше: автоматизированная оценка периметра

- Ежедневно проверяется 9 PoP? Как насчет проверки всех 15 каждую ночь?
  - Со временем данные устаревают
  - Актуальные данные имеют преимущество
  - Единственное решение — автоматизация



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

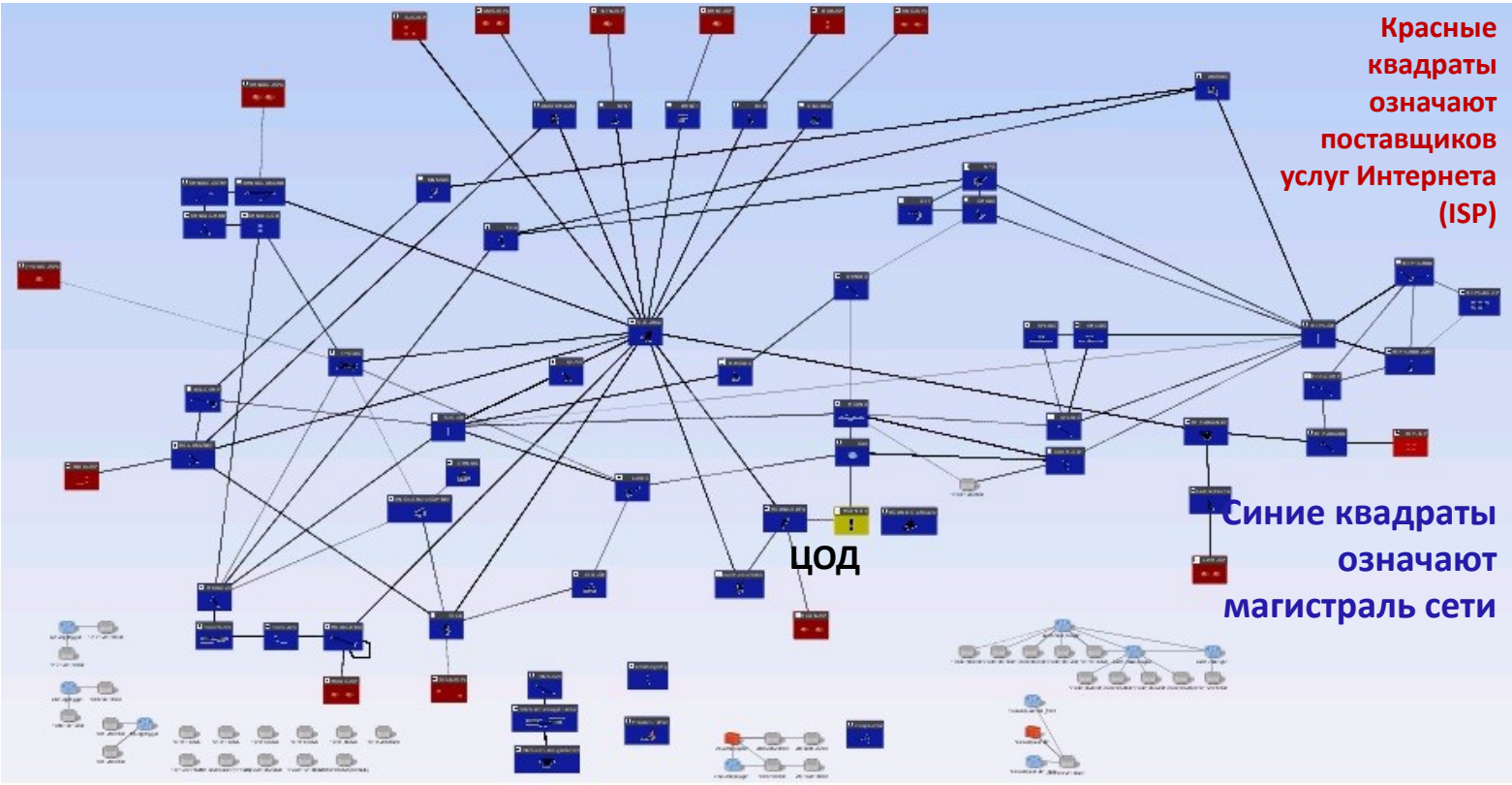
Объектная модель оценки риска (проект REOM)

[Также называемая «всевидящее око Мордора»]

- Проект по пассивной проверке на проникновение для всех точек присутствия Cisco
  - ПО для моделирования сети получает данные конфигурации сети и интегрирует их с данными сканера уязвимости
- Глобальное представление
  - Cisco ISP — сгруппированы для оценки всех 15 PoP
  - Всей магистральной сети и всех DMZ
  - ЦОД в Ричардсоне (т.е. объект для атаки)
- Цель
  - Автоматизация всех процессов, минимальное участие человека
  - Отчеты об уязвимых объектах и направлениях
  - Анализ тенденций

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

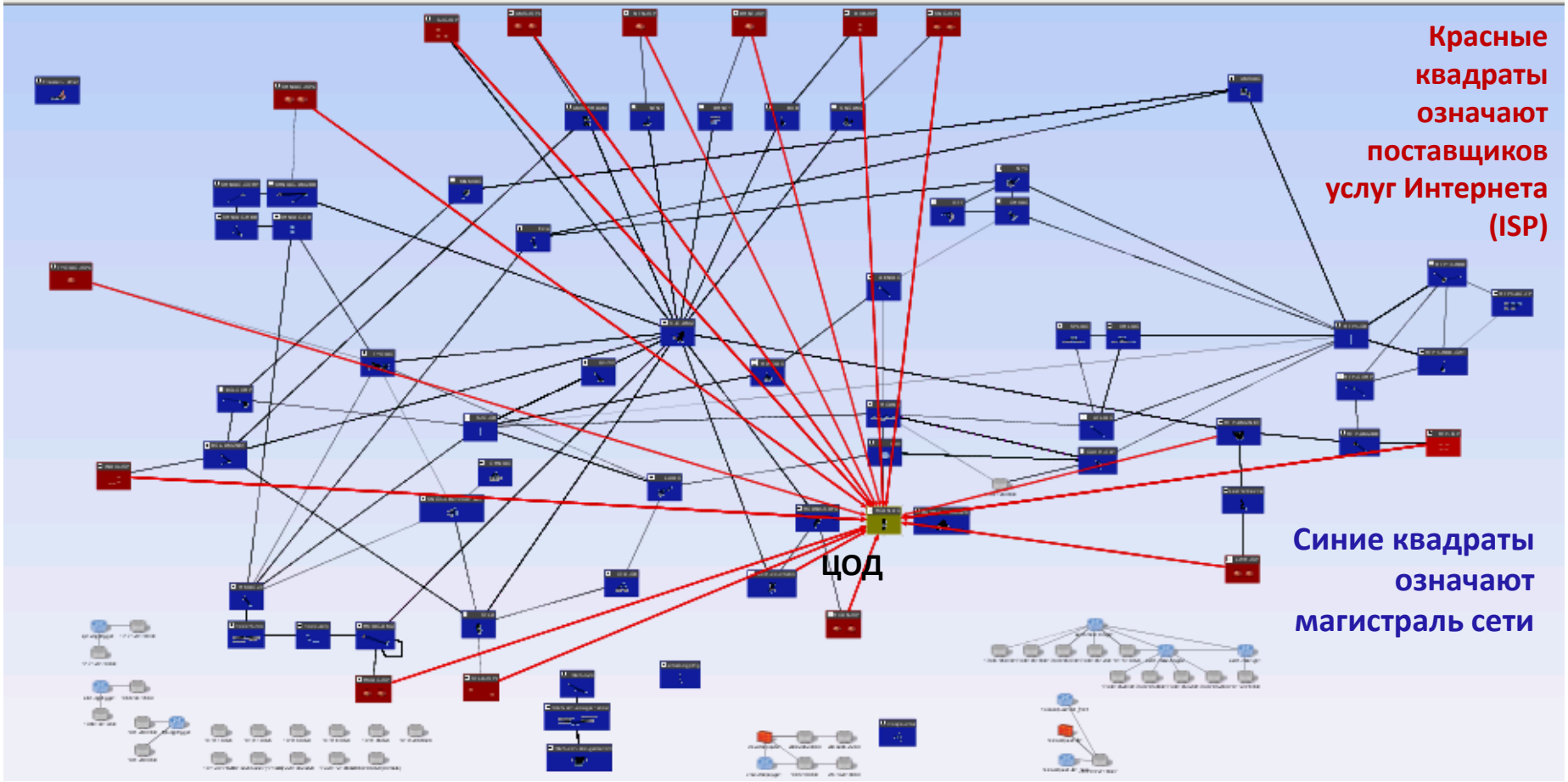
Объектная модель оценки риска



- Модель содержит все данные о магистральной сети, DMZ, ЦОД и уязвимостях.
  - ~750 конфигураций сети; ~ 9 000 узлов с уязвимостями; конфигурации обновляются ежедневно; проверка уязвимостей занимает от 3 до 5 дней; отчеты предоставляются еженедельно
- Полная автоматизация

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

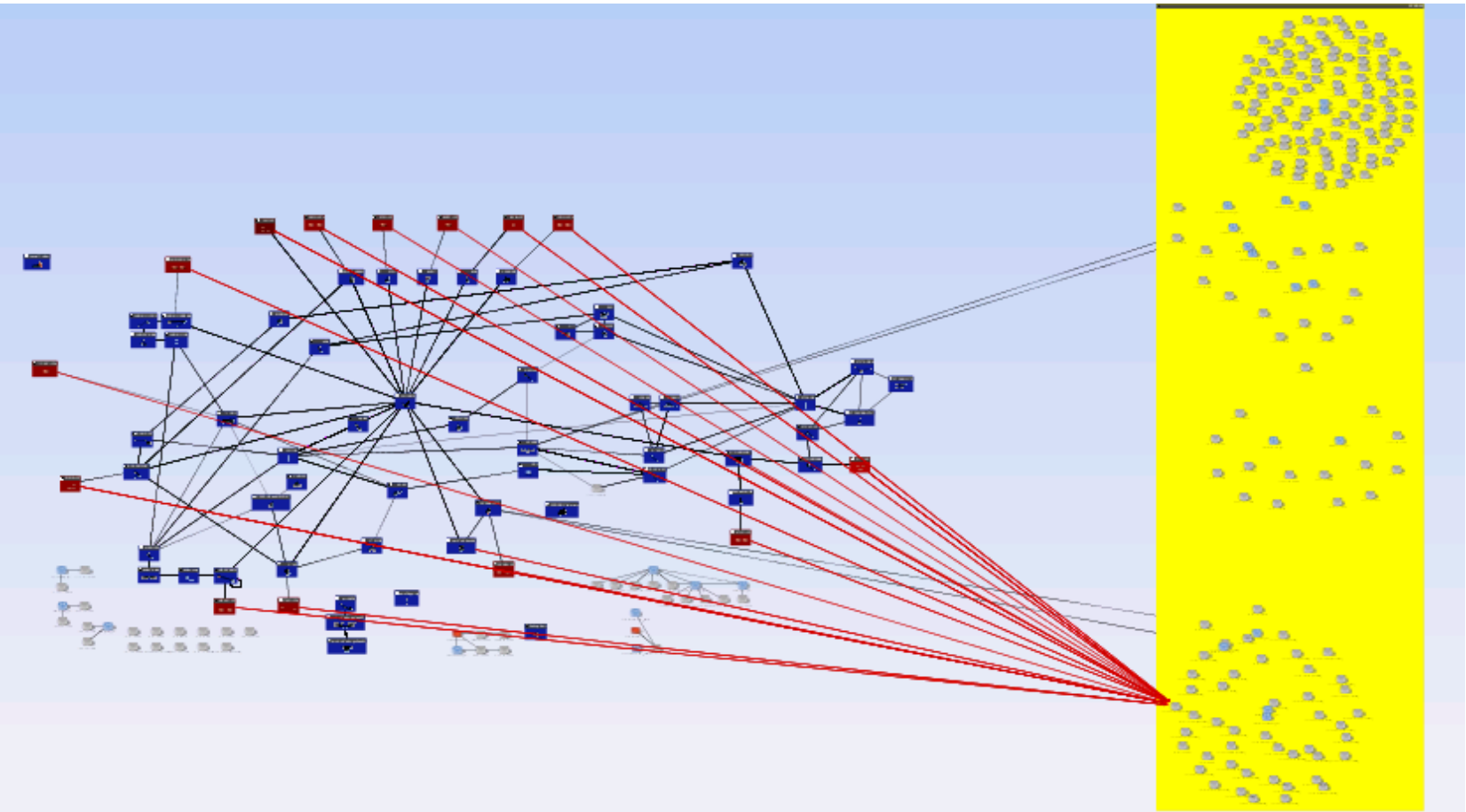
REOM с путями атак



- Автоматическое вычисление пути атак на основе данных подключений и сведений об уязвимостях

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Более подробное представление ЦОД

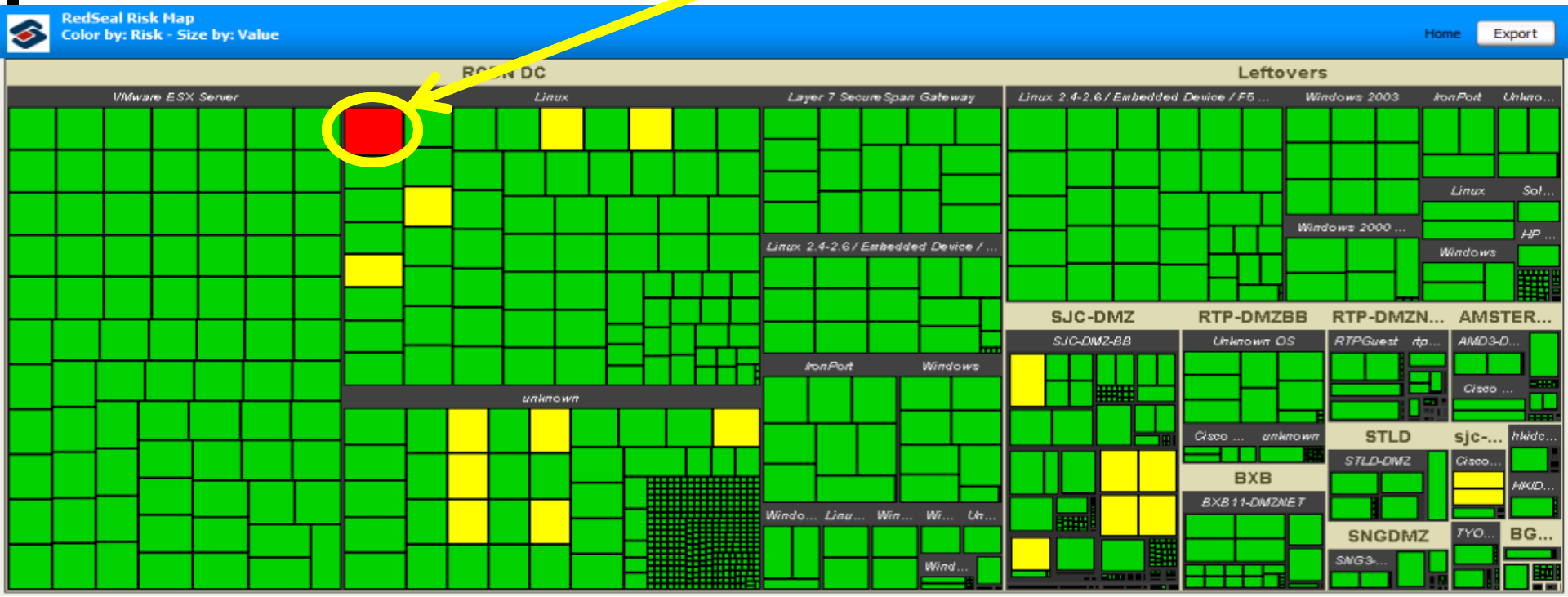


- Атаки попадают в одну подсеть (как ни странно, это хорошая новость)
- Обратили внимание на сегментацию сети в ЦОД?

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Какие объекты подвержены действию атак и предположительно являются уязвимыми?

Причина здесь!

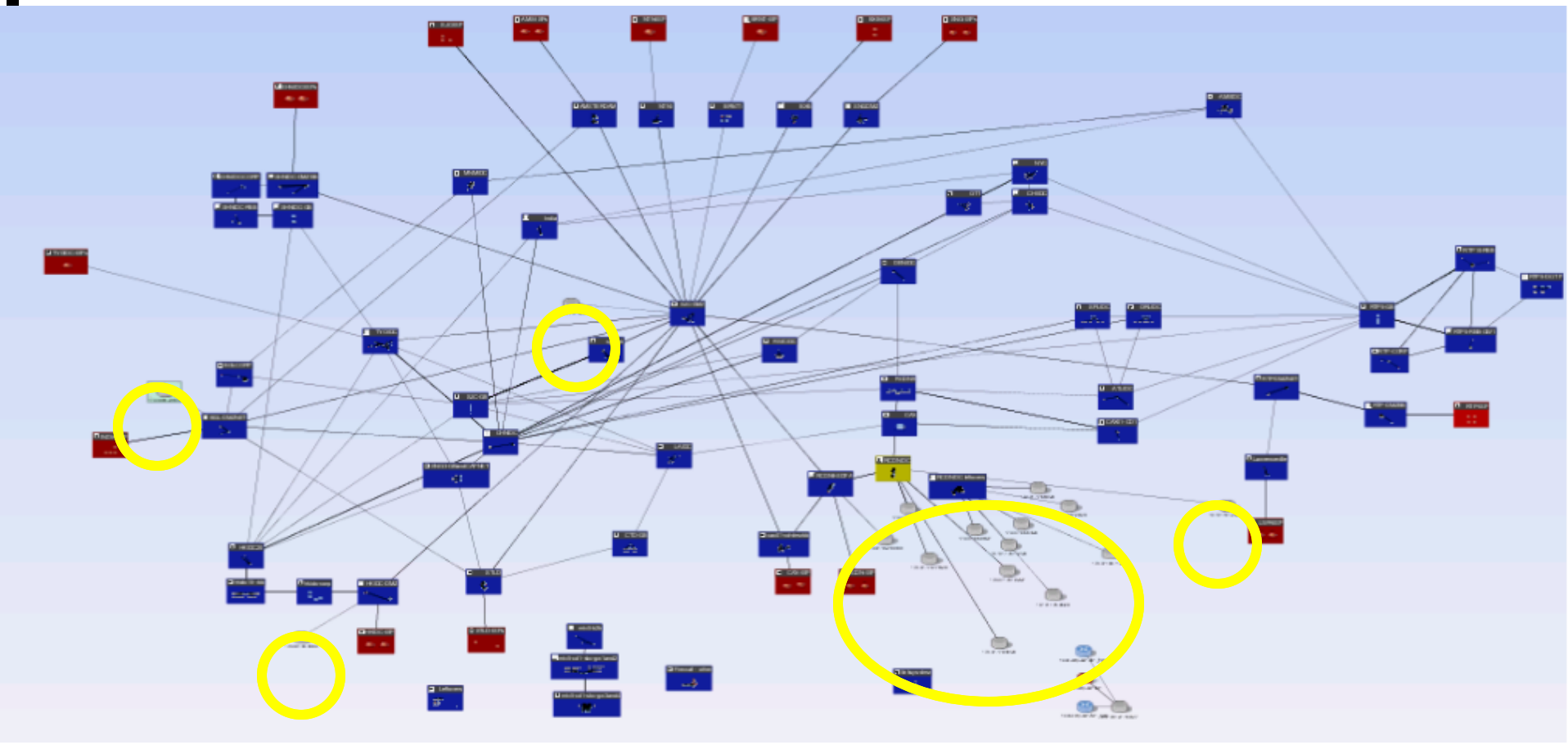


- Несколько представлений узлов, сервисов и топологии
- Выделение высокоприоритетных возможностей восстановления

Redseal Systems, Inc. Все права защищены.

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Ежедневное изменение — новые подсети



- Подсети формируются ежедневно
- При добавлении подсетей узлы и уязвимости автоматически интегрируются в модель

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Проверки соответствия лучшим практикам

Non-contiguous Wildcard — Severity: low — Check ID: RS-21

Description: A wildcard in the configuration references a set of non-contiguous IP addresses. This is frequently done by mistake—0.0.0.240, which addresses 16 non-contiguous hosts, might easily get set instead of the intended 0.0.0.15 wildcard. (If the ***redundant-security-rule*** test has also failed for the same block of addresses, fix the non-contiguous problem first. It may be producing a false-positive ***redundant-rule*** warning.)

Remediation: If not intentional, the wildcard should be replaced with a contiguous wildcard.

Primary Capability > Router — 1 of 5 network devices have at least 1 issue

Device ▾	Summary	Violation ID
	Non-contiguous wildcard found Line 2673 permit tcp any [redacted] 0.0.0.32 eq www	119
	Non-contiguous wildcard found Line 2790 permit ip any [redacted] 0.0.0.128	124
	Non-contiguous wildcard found Line 2827 permit ip any [redacted] 0.0.0.128	126

Inverted Mask in Access List — Severity: medium — Check ID: RS-92

Description: An inverted subnet mask was found in an access list rule. An inverted mask can inflate a range of 255 addresses to as many as 16.7 million, causing severe performance degradation of the RedSeal analysis engine. RedSeal ignores rules containing inverted masks, since they are almost certainly configuration errors.

A common mistake when configuring access lists is to specify the mask using ***do care*** bits when the platform expects ***don't care*** bits. That is, for example, to match hosts of the form 172.16.1.*, the correct form for IOS and Foundry is 172.16.1.0 0.0.0.255. An operator may sometimes enter 172.16.1.0 255.255.255.0 by mistake. Since the mask uses ***don't care*** bits, this actually matches hosts of the form *.*.*.0. Also note that the router can remove any values covered by ***don't care*** bits, so the incorrect entry will show up as 0.0.0.0 255.255.255.0 instead of what the operator typed originally. Permitting every address that ends in zero is almost certainly not the intended filter, since *.*.*.0 specifies 16.7 million distinct permissible addresses.

Remediation: Verify the original intent of this line and replace with the correct host and mask.

Урок 10. Компьютеры справляются с чтением телефонных справочников лучше вас. Смиритесь с этим.

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Проверки соответствия лучшим практикам

- Перекрывающиеся подсети

Violation ID: 16,653

Title: Overlapping Subnets

Check: RS-84

Summary: Overlapping subnets found and 2 other subnets), Interface on device defines subnet and 3 other devices agree, Interface on device defines subnet and 6 other devices agree, Interface on device defines subnet and 2 other devices agree.

Description: Overlapping subnets have been detected. This can indicate a serious network misconfiguration, causing hosts in either subnet to be unreachable from some parts of the network. If intentional (two isolated parts of the network legitimately using similar address space), you should limit the configurations loaded into to a subset of the network that excludes overlaps in internal addressing.

Remediation: Renumber one or more of the subnets so they use non-overlapping address space.

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

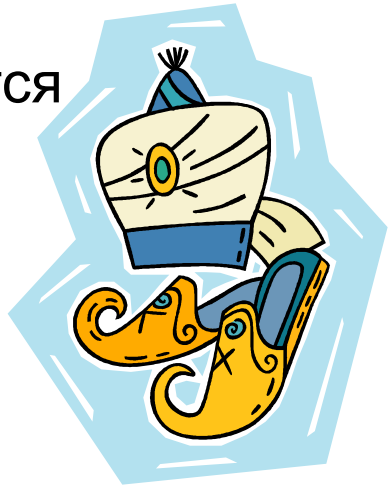
Объектная модель оценки риска. Краткое резюме

- Множество других преимуществ (приобретение, внешняя сеть, лаборатории, CSIRT, планирование архитектуры и т. д.)
- Получаемые преимущества:
  - Полный тест на проникновение для всех 15 PoP каждую ночь
  - Модель «комплексное решение Cisco» для использования в качестве основы для других проектов
- Почему это важно:
  - Теперь мы знаем о возникновении и распространении атак и можем противостоять им
- Наши партнеры:
  - Global Network Operations (GNO владеет магистральной сетью и DMZ) и руководители проектов в группе восстановления GNO
- Постоянная работа с группами по устранению проблем

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Идем дальше: управление ежедневными изменениями

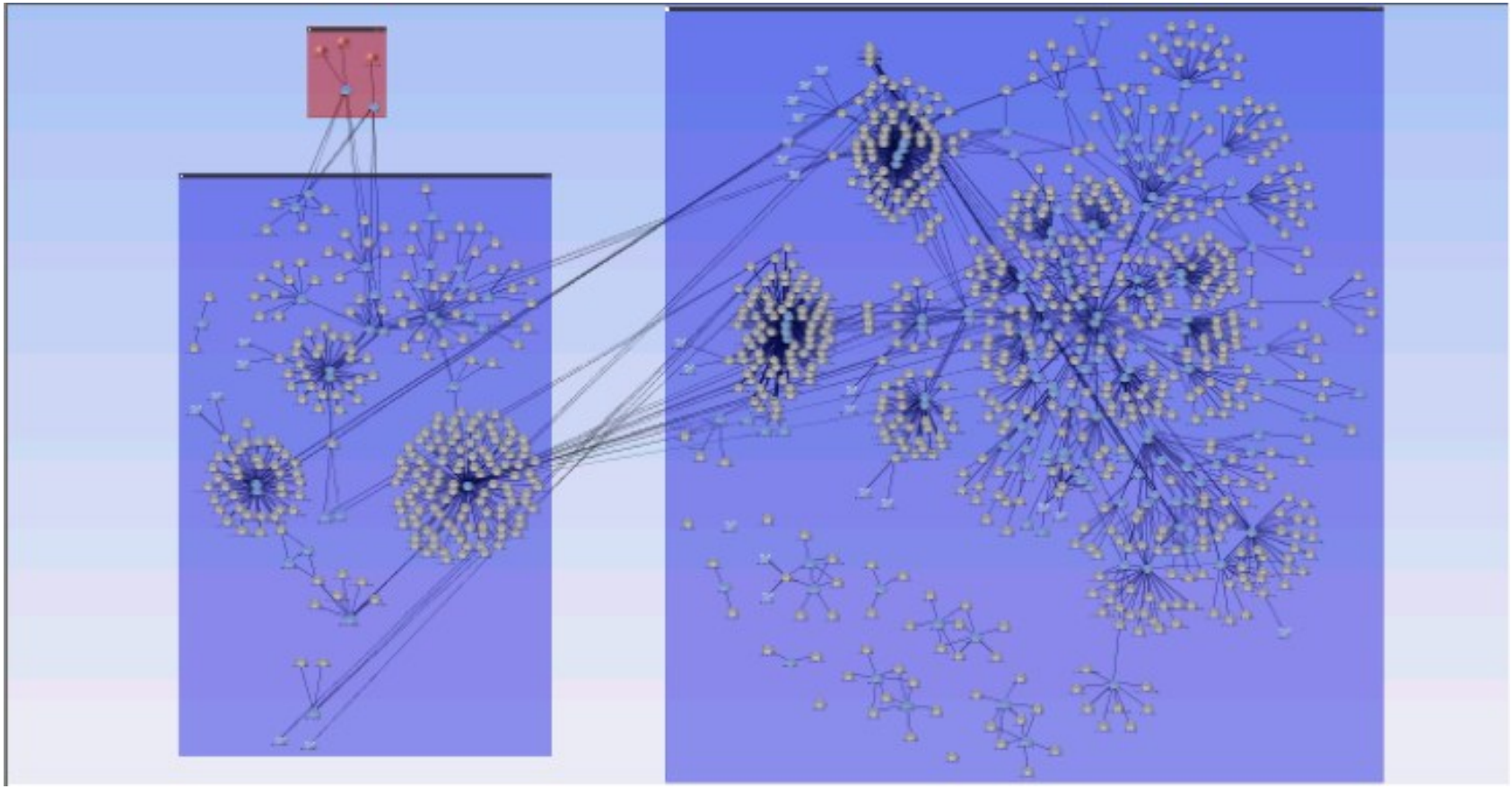
- Запросы на изменения доступа от бизнес-подразделений поступают в большом количестве и достаточно быстро
- Отделы обеспечения безопасности получают запросы на утверждение
- Стандартные основы для утверждения отсутствуют
- Отделам обеспечения безопасности не удается играть роль Джеймся Бонда
  - Требуются четкие и однозначные причины отклонения изменений



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Карта сети комплекса зданий RTP

Интернет



Демилитаризованная зона (DMZ)

Комплекс зданий Cisco

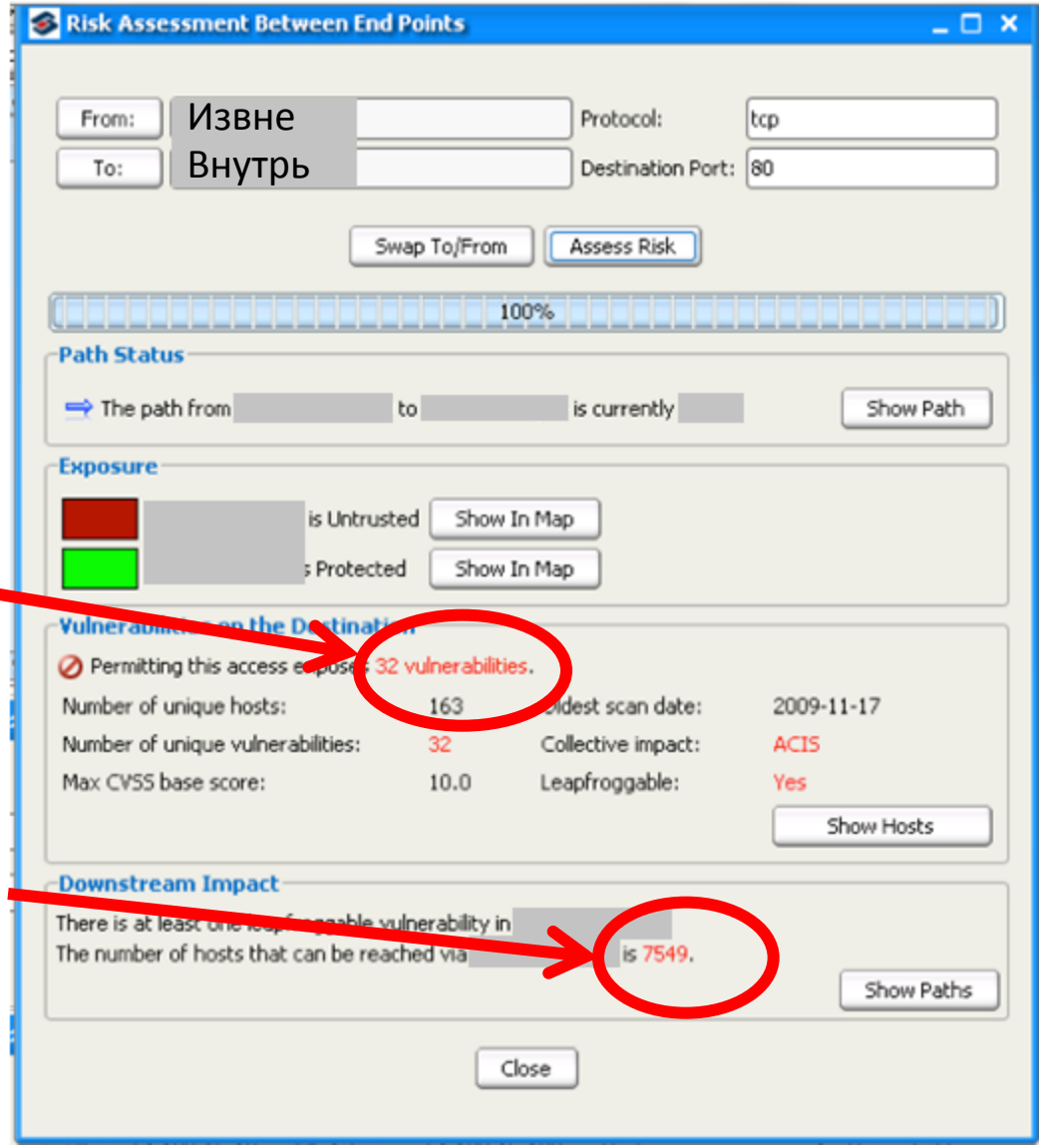
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Запрос на подключение клиента

- Создание модели сети
- Ввод данных об уязвимости
- Потребность бизнеса: открыть одну сеть класса C :80

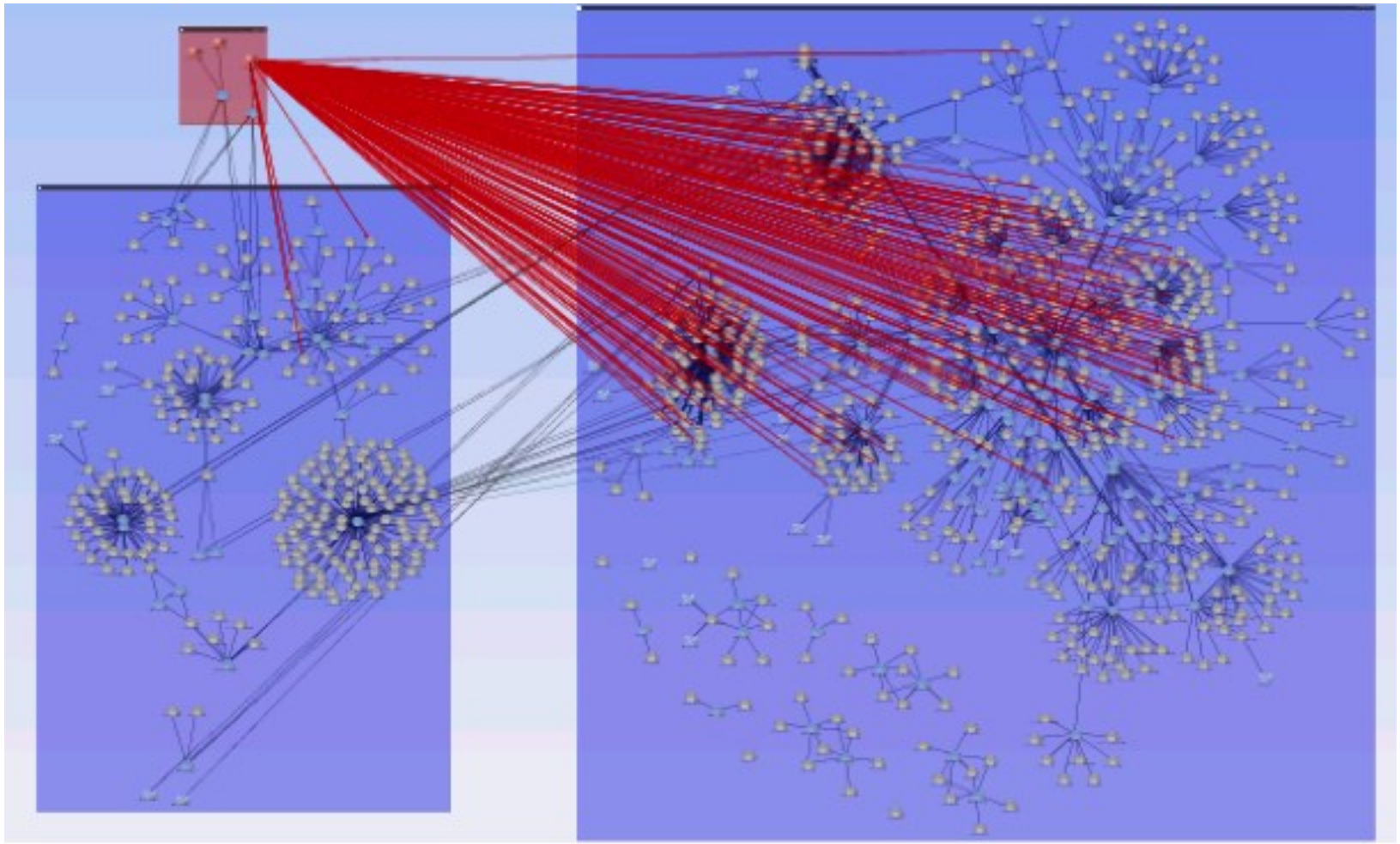
- Подключение выявляет 32 уязвимости

Нисходящий эффект?
Выявлено 7 549 уязвимостей



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Воздействие подключения клиента

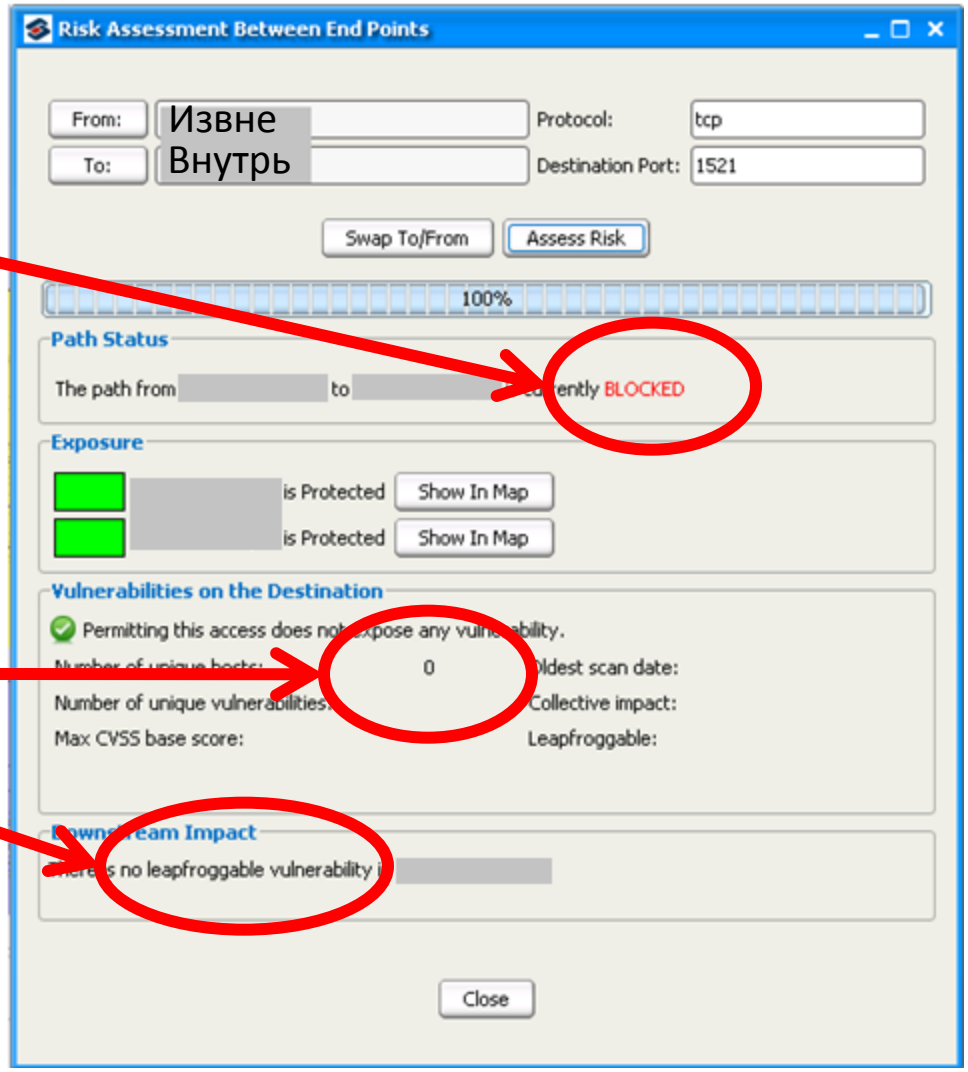


© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Приемлемая оценка риска

- Доступ ЗАБЛОКИРОВАН

- Отсутствуют уязвимые узлы, нет связанных уязвимостей



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Изоляция частично заблокированного пути доступа

Detailed Path

Detailed Path Summary

Partially Open Path

Query Name:	
Query Date:	2010-04-05 11:34:51 AM
Query Status:	Successful
Protocol:	any
Source Node:	
Source IP:	any
Source Port:	any
Destination Node:	
Destination IP:	any
Destination Port:	any

Paths Found

Path Discovered: Path 1 (14 hops)

Hop	Flow	Device
	START	any
1		sjc
2		sjc
3		sjc
4		sjcl
5		sjcl
6	P D	sjcl
7		sjcl
8		sjc

Permitted Flow | Denied Flow

Select a device in the Selected Detailed Path

Flow	Interface	Protocol	Source ...	Source Port	Destination IP	Destination

Select a device in the Selected Detailed Path

0 rows

Type	First Line/Description

Close | Help

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Определение правил межсетевого экрана

Detailed Path

Detailed Path Summary

Partially Open Path

Query Name:	
Query Date:	2010-04-05 11:34:51 AM
Query Status:	Successful
Protocol:	any
Source Node:	
Source IP:	any
Source Port:	any
Destination Node:	
Destination IP:	any
Destination Port:	any

Paths Found

Path Discovered: Path 1 (14 hops)

Hop	Flow	Device
	START	any
1		sjc
2		sjc
3		sjc
4		sjc
5		sjc
6	P D	sjc
7		sjc
8		sjc

Permitted Flow | Denied Flow

Flows For Device: sjc

Flow	Interface	Protocol	Source ...	Source Port	Destination IP	Destination
Input Flow	TenGigabitEthernet7/0	ICMP EIGRP				
Output Flow	TenGigabitEthernet8/0	Remaining columns are same as Input Flow				

Filter/NAT Rules For Device: sjc

Complete

Type	First Line/Description
Inbound Filter	(config:55) access-list OUTSIDE_ACCESS_IN extended permit eigrp any any
Inbound Filter	(config:56) access-list OUTSIDE_ACCESS_IN extended permit icmp any any echo-reply
Inbound Filter	(config:57) access-list OUTSIDE_ACCESS_IN extended permit icmp any any time-exceeded
Inbound Filter	(config:58) access-list OUTSIDE_ACCESS_IN extended permit icmp any any unreachable

Close | Help

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Изоляция правила блокировки

Detailed Path

Detailed Path Summary

Partially Open Path

Query Name:	
Query Date:	2010-04-05 11:34:51 AM
Query Status:	Successful
Protocol:	any
Source Node:	
Source IP:	any
Source Port:	any
Destination Node:	
Destination IP:	any
Destination Port:	any

Paths Found

Path Discovered: Path 1 (14 hops)

Hop	Flow	Device
	START	any
1		sjc
2		sjc
3		sjc
4		sjc
5		sjc
6	P D	sjc
7		sjc
8		sjc

Permitted Flow | Denied Flow

Flows For Device: sjc

Flow	Interface	Protocol	Source ...	Source Port	Destination IP	Destination
Input Flow	TenGigabitEthernet7/0	any ex... ICMP				
The following is the output flow if this device's ACL/Filter rules are not applied to the input flow						
Output Flow	TenGigabitEthernet8/0	Remaining columns are same as Input Flow				

Filter/NAT Rules For Device: sjc

Complete

Type	First Line/Description
Inbound Filter	(implicit) deny all

Close Help

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Результат: до и после

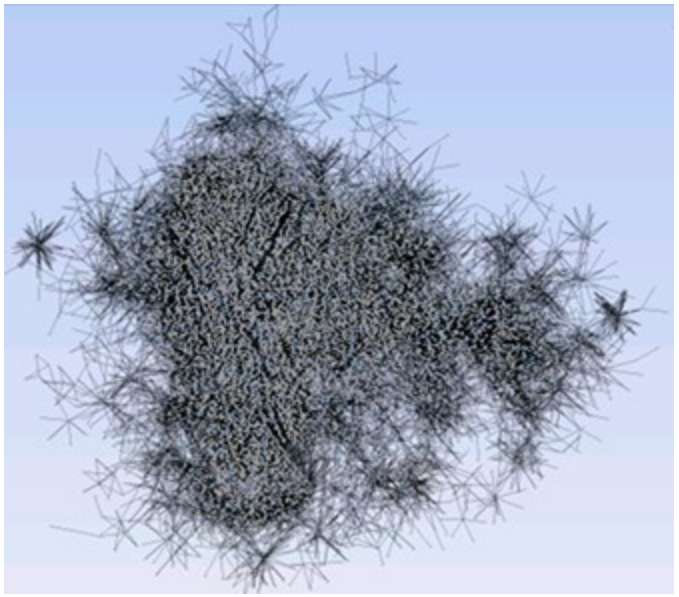
- До:
  - Соблюдение только основных лучших практик («проверка орфографии»)
  - Предоставление исключений на основе необходимости, без реальной оценки рисков
- После
  - Автоматическая оценка влияния изменений на безопасность
  - Визуализация для демонстрации природы воздействия атак
  - Автоматическое выделение правил, требующих изменений

Урок 11. Наконец-то мы можем вести логически последовательный разговор с бизнесом

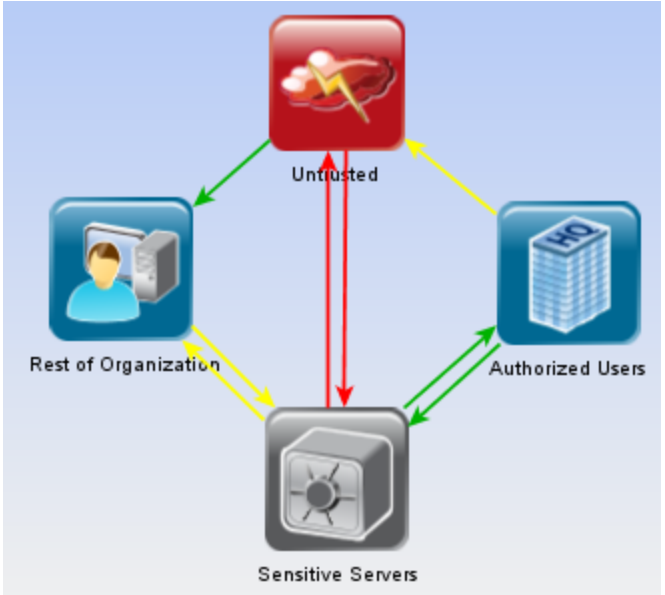
© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Автоматизация проверки сети

До:



После:



© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Рассмотренные вопросы

- Большая топология (Bug Splat) — очень полезна, но слишком велика для обработки
- Тактическая цель (PKI) — найти небольшую, но важную проблему и решить ее
- Оценка периметра с уязвимостями — девять точек контроля в день
- Пассивное тестирование периметра на проникновение угроз извне — автоматически, в любом месте, ежедневно
  - Объектная модель оценки риска
  - Все точки присутствия, сети и уязвимости
- Управление изменениями — ведение последовательного разговора с бизнесом

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

Полученные уроки

- Урок 1. Требуется репозиторий конфигураций
- Урок 2. Принятые условные обозначения – вам в помощь
- Урок 3. С помощью рисунков можно легко объяснить сложные понятия
- Урок 4. Справочный атлас — полезное средство
- Урок 5. Сети как накопители несобираемого мусора
- Урок 6. Практические рекомендации получили свое название не просто так
- Урок 7. Это могут сделать обычные пользователи
- Урок 8. Данные о сети + данные об уязвимостях + направление атаки = GOLD (общая онлайн-диагностика)
- Урок 9. Компьютеры справляются с чтением телефонных справочников лучше вас. Смиритесь с этим.
- Урок 10. Наконец-то мы можем вести логически последовательный разговор с бизнесом

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco

security-request@cisco.com

Благодарю вас за внимание

© Cisco и (или) дочерние компании, 2011 г. Все права защищены. Общедоступная информация Cisco