Чем решения Cisco по ИБ могут помочь в условиях кризиса?

Алексей Лукацкий

Бизнес-консультант по безопасности

О чем мы хотели говорить?

Cisco против операционных рисков

Руководство
Неполная картина рисков компании

Совет директоров
Необоснованные решения

Внутренний контроль
Неполный анализ рисков

ИТ и ИБ
Утечка данных & безопасность

Поставки
«Черный список» поставщиков

Финансы
Сложные международные требования соответствия и отчетности

Управление кадрами
Безопасность и охрана труда сотрудников

Сбыт
Высокий кредитный риск

ИТ и ИБ
Конфликты между отделами

Инфраструктура
Простои и отказы сети

Cisco SONA Framework

Приложения

- Коммерческие приложения
- Собственная разработка
- Software as a Service (SaaS)
- Композитные приложения/SOA

Общие ключевые сервисы

Коммуникации реального времени

Мобильность

Доставка приложения

Безопасность

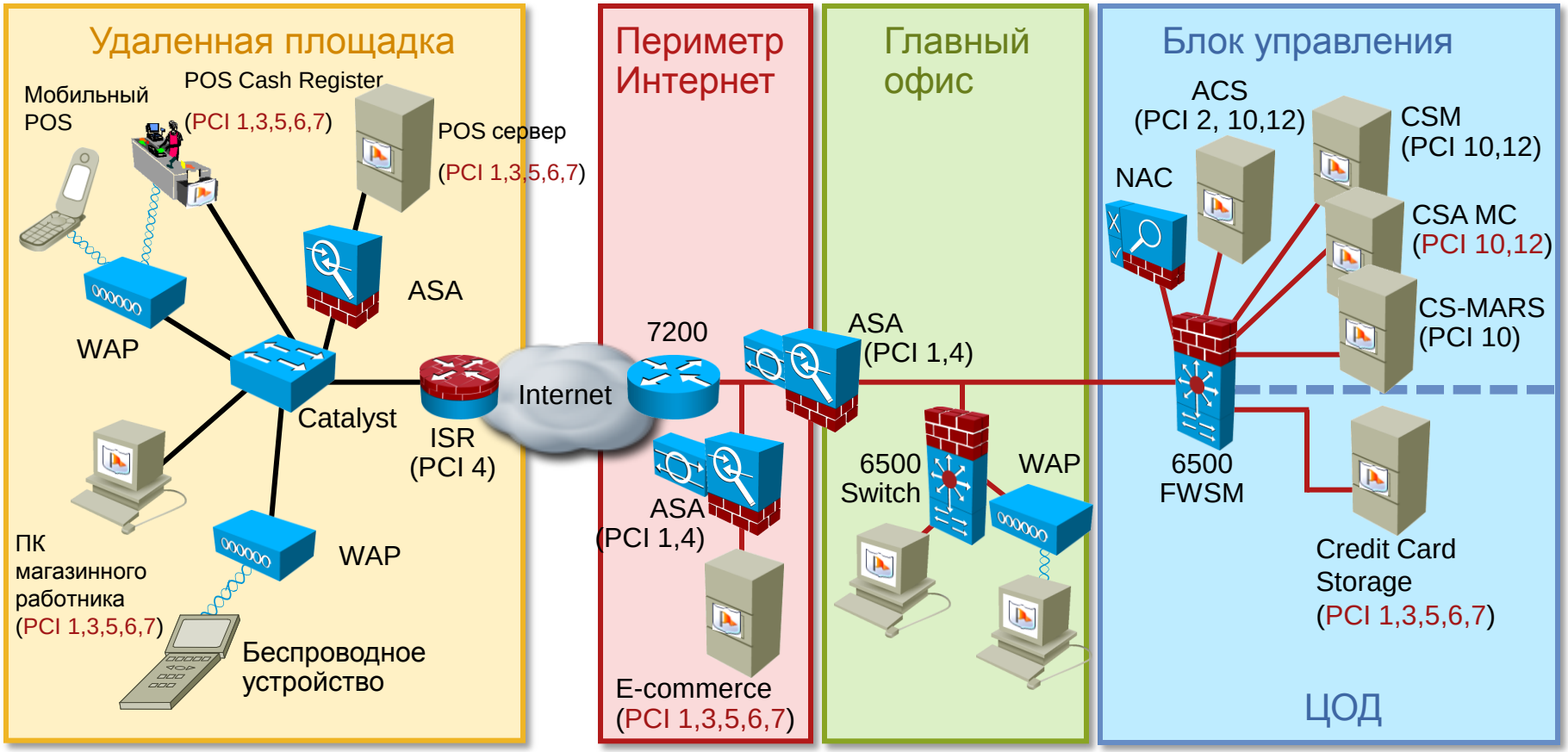
Управление

Виртуализация

Транспорт

Физическая инфраструктура

Cisco для PCI DSS



Примечание! Отображена реализация не всех требований

О чем мы будем говорить?

“Любой кризис – это новые возможности”

Уинстон Черчилль

Чем характеризуется нынешний кризис

- Нехватка финансовых ресурсов
- Замораживание проектов с неочевидной выгодой
- Финансирование проектов с быстрой отдачей
- Сокращение ИТ- и ИБ-персонала
- Просыпается интерес к аутсорсингу
- Экономия и снижение операционных и капитальных затрат

Осознание ситуации

- Проблемы, требующие решения

  В ИБ мы обычно осознаем только эту составляющую (и то, с точки зрения угроз/рисков), забывая про все остальные

- Цели, которые нужно достичь
- Потребности, которые необходимо удовлетворить
- Существование целей или потенциально утерянных возможностей

Службы ИБ, как никогда, должны демонстрировать понимание бизнеса, его проблем и способов их решения

Снижение операционных затрат

- Снижение арендной платы
  - За счет уменьшения занимаемой площади
  - За счет переезда в новые, более дешевые помещения
- Уменьшение числа командировок
- Сокращение персонала
  - За счет сотрудников филиалов, доп.офисов, удаленных площадок
  - За счет ИТ-, ИБ-персонала головного офиса
  - За счет передачи задач на аутсорсинг
- Сокращение затрат на Интернет-трафик

Другие задачи

- Рост продуктивности сотрудников
- Снижение капитальных затрат
  - За счет снижения затрат на лицензии на ПО
  - За счет отказа от приобретения ПО и «железа»
- Защита от «разворовывания» бизнеса

Снижение арендной платы
Сценарий 1

Снижение арендной платы

- Снижение арендной платы → уменьшение арендуемых площадей → перевод сотрудников на дом → решение Cisco по защищенному удаленному доступу
- Экономия на:
  - Аренда площадей
  - Питание сотрудников
  - Оплата проездных (если применимо)
  - Оплата канцтоваров
- Дополнительно
  - Улучшение психологического климата за счет работы дома
  - Рост продуктивности

Вопросы, на которые нужны ответы

- КТО получает доступ?
- КАК он получает доступ?
- КАКИЕ приложения он использует?
- Это ЧЕЛОВЕК или обезличенное УСТРОЙСТВО?
- ИМЕЕТ ли он право на такой доступ?
- ОТКУДА он получает доступ?
- Как ЗАЩИТИТЬ **обе** стороны?
- СООТВЕТСТВУЕТ ли узел доступа требованиям политики безопасности?
- Как УСТРАНИТЬ несоответствие?

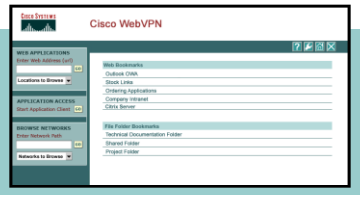
Сравнение технологий удаленного доступа

Существует 2 основные технологии удаленного доступа: IPSec и SSL. SSL – более новая технология; обычно более дешевая и обеспечивающая лучший доступ для партнеров и контрактников (по сравнению с IPSec). SSL обеспечивает более быструю связь, чем IPSec.

IPSec VPN

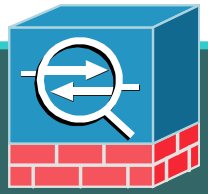
- Широко распространенная, отработанная технология
- Хорошо подходит для расширенного доступа сотрудников с корпоративнымы компьютерами

SSL VPN



- Расширяет защищенный доступ для «не-сотрудников», например, контрактников и временных служащих
- Облегченный доступ для партнеров
- Обеспечивает доступ “отовсюду”, включая недоверенные и неуправляемые ПК (Интернет-кафе)
- Снижает операционные затраты, связанные с клиентским ПО

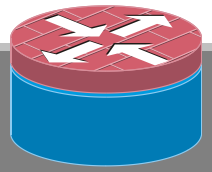
Cisco ISR или Cisco ASA как VPN?



Cisco ASA 5500

- Позиционируется как устройство защиты
- Содержит последние инновационные решения по предотвращению различных угроз и атак
- Множество функций организации защищенного удаленного доступа (VPN)
- Специальный функционал, обеспечивающий простое программное обновление

Cisco ISR Router



- Позиционируется как маршрутизатор
- Содержит последние сетевые решения, тесно интегрированные с инновационными решениями по безопасности
- Богатые функциональные возможности по построению межофисных VPN (site-to-site VPN)
- Максимально объединены сетевые возможности и функции защиты на одной платформе

Специализированные решения, работающие в любом сценарии внедрения

Cisco ASA 5500

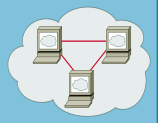
МСЭ / Защита приложений

- Многоуровневый анализ пакетов и трафика
- Расширенные службы проверки приложений и протоколов
- Контроль сетевых приложений
- Расширенная защита мультимедиа и голосовых приложений

IPS / Анти-вирусная защита

- Защита от сетевых червей и вирусов
- Обнаружение и фильтрация вредоносного кода
- Технология аккуратного предотвращения и упреждающее реагирование
- Корреляция событий и упреждающее реагирование

Контроль доступа и аутентификация



- Контроль на 4 и 3 уровне
- Контроль состояния
- Гибкость политик для пользователей, сетевых, приложений

Защита соединений

- Не требующие вмешательства автоматически обновляемый удаленный доступ по IPSec
- Гибкие и защищенные сервисы SSL VPN
- Поддержка QoS, маршрутизации в VPN
- Интегрированная защита от угроз для VPN

Интеллектуальные сетевые сервисы Cisco

- Малая задержка
- Различная топология
- Поддержка Multicast
- Виртуализация сервисов
- Сетевая сегментация
- Маршрутизация, распределение нагрузки

Сравнение VPN-клиентов

	Cisco VPN Client	Cisco SSL VPN Client	Cisco AnyConnect VPN Client
Протокол	IPsec	SSL (HTTPS)	DTLS, SSL (HTTPS) - Auto
Средний размер	10 МБ	400 КБ	1.2 МБ
Установка	Распределение	Автозагрузка Распределение	Автозагрузка Распределение
Права администратора	Да	Только для инсталляции (Stub installer доступен)	Только для инсталляции (MSI доступен – Windows)
Поддержка ОС	2K/XP/Vista 32-bit, Linux, Mac OS X, Solaris UltraSparc	2000/XP	2K/XP/Vista (32 & 64-bit), Linux, Mac OS X, Windows 2008 Server
Перезагрузка после установка	Нет	Да	Да
Head End	ASA/PIX/3K/IOS	ASA/3K/IOS	ASA/IOS

Защита IP-телефонии

- Поддержка SIP, SCCP, H.323, MGCP
- Защита от SIP-атак, включая Rate Limit SIP-запросов
- Контроль звонков (whitelist, blacklist, абоненты, SIP URI)
- Динамическое открытие нужных портов
- Звонки только для «зарегистрированных» телефонов
- Инспекция зашифрованных звонков, включая сигнализацию (SRTP/TLS)

Интеграция защитных функций

Прикладной МСЭ и контроль доступа
Контроль приложений
Контроль доступа по пользователям/группам
Обнаружение аномалий в протоколах
Фильтрация с контролем состояния

Отражение угроз
Обнаружение ВПО
Обнаружение червей
Обнаружение шпионских программ

Удаленный доступ по VPN

Всесторонняя защита ПК
Предварительная оценка
Отражение вредоносного ПО
Защита данных/сессий
Очистка памяти после сессии

Точное применение политик
Корреляционный анализ в режиме реального времени
Расчет рейтинга риска
Блокирование атак
Завершение опасных сессий

Усиливает эшелонированную оборону, блокируя червей, вирусы и т.п. … без дополнительных устройств и снижения производительности

Что такое контроль доступа к сети?

Использование сети для обеспечения выполнения требований политик по соответствию состояния подключающихся устройств их требованиям

Возможность доступа определяется соответствием состояния

Сначала установите политики доступа. Затем:

НЕТ СООТВЕТСТВИЯ = НЕТ ДОСТУПА К СЕТИ

Cisco NAC решает ключевые проблемы

Внедрить ролевой контроль доступа

Cisco NAC применяет политики доступа и соответствия на базе ролей

Управлять пользователями и активами

Cisco NAC аутентифицирует и контролирует гостей и неуправляемые активы/ресурсы

Обеспечить соответствие требованиям

Cisco NAC оценивает, помешает в карантин и устраняет несоответствие endpoints

Компоненты Cisco NAC

Уровень соответствия

NAC Manager

Централизованное управление, конфигурация, отчеты и хранение политик

NAC Agent или Web Agent

Бесплатный клиент для расширенного сканирования

802.1x Supplicant

802.1x supplicant через CSSC или встроенный supplicant Vista

Обновления правил

Плановые автоматические обновления для антивирусов, критические патчи и другие приложения

Уровень сервисов NAC

NAC Profiler

Аггрегирует данные от Collector для оценки ролей и привилегий

NAC Collector

Сбор данных из сети для определения типов устройств

NAC Guest

Сервер управления доступом гостей с всесторонними функциями

NAC Server

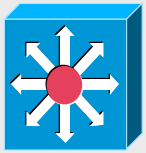
Оценка, соответствие и контроль

ACS

Система управления доступом по политикам для 802.1x

Уровень инфраструктуры

Устройства сетевого доступа



Cisco Security Agent 6.0

Всесторонняя защита ПК, серверов, лэптопов и POS-терминалов

- Интегрированный агент, единое управление
- Защита от известных и новых угроз
- Предотвращение утечек информации
- Обеспечение политик использования приложений
- Усиление защиты за счет интеграции с инфраструктурой сети
- Обеспечение соответствие корпоративным и национальным регулятивным требованиям

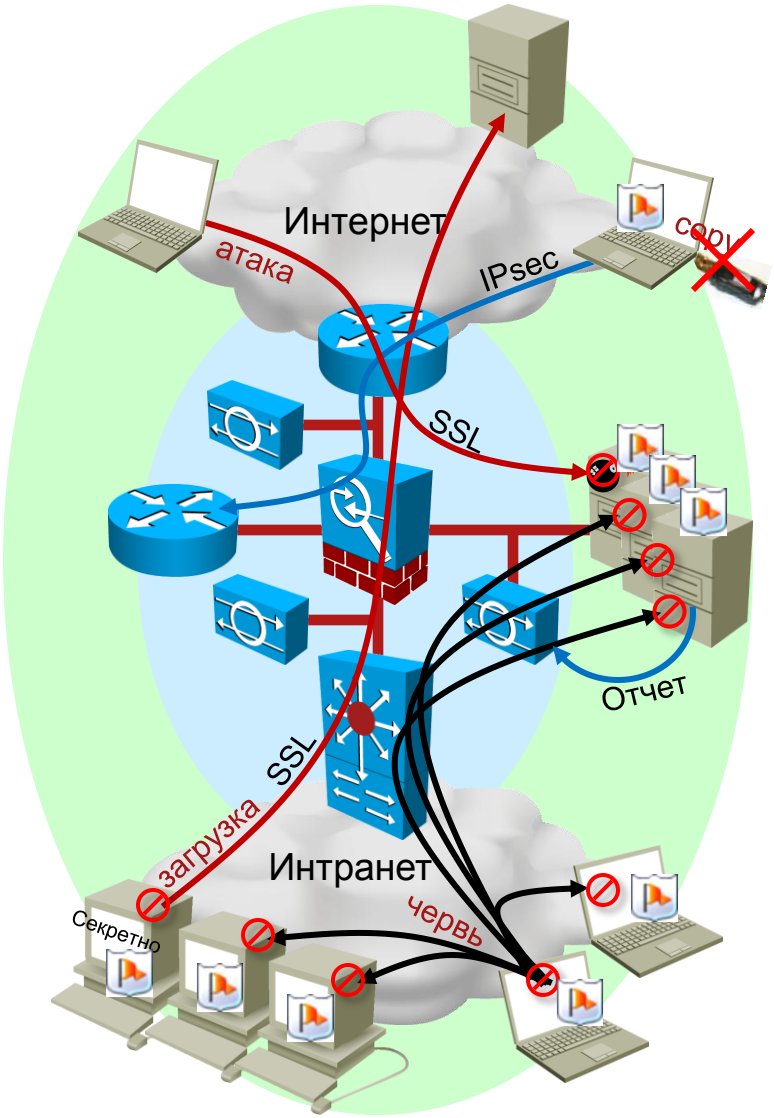
Преимущества для бизнеса:

- **Возможность для ИТ управлять рисками для бизнеса**
- **Внедрение политик и защита критических бизнес-активов**
- **Уменьшение бремени ИТ-управления**
- **Снижение затрат**

Расширенная безопасность ПК

с Cisco Security Agent

- Cisco Security Agent повышает защиту за счет:
  - **Защиты от 0-day-атак**, базируясь на поведении ОС и приложений
  - **Контроля содержимого** после расшифрования или до зашифрования (например, SSL, IPsec)
  - **Контроля доступа к устройствам ввода/вывода**, базируясь на процессе, местоположении в сети и содержимом файла
  - **Централизованного управления** и мониторинга событий
  - **Взаимодействие в рамкахSDN** с другими решениями, такими как NAC, IPS, QoS, MARS, VOIP и т.д.



Рост продуктивности сотрудников

Рост продуктивности сотрудников

- Рост продуктивности → снижение времени, потраченного на дорогу → перевод сотрудников на дом → решение Cisco по защищенному удаленному доступу
- Рост продуктивности – от 10% до 40%
- Дополнительно:

  Увеличение рабочего времени

  Экономия на аренде площадей

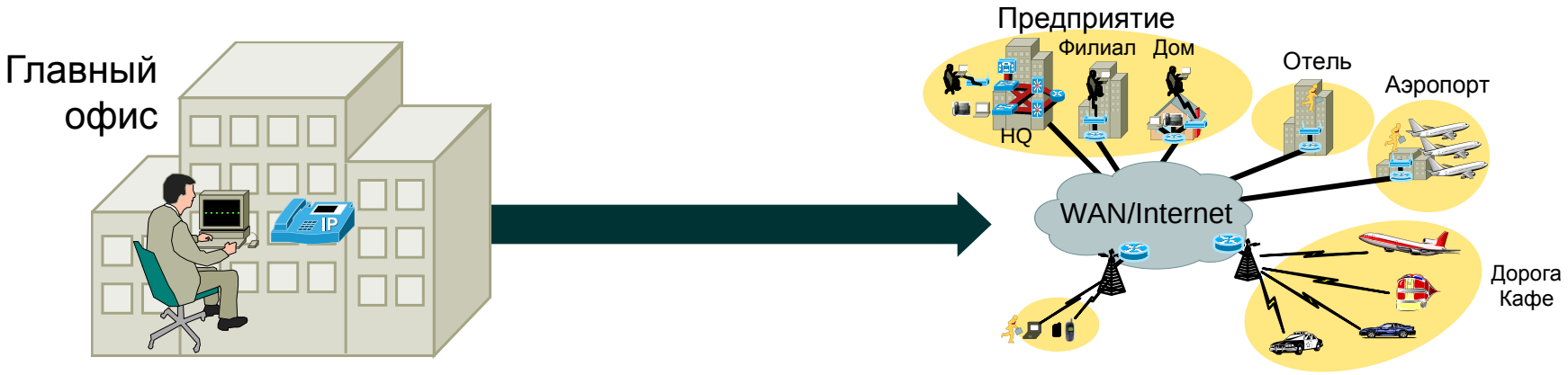
  Экономия на питании сотрудников

  Экономия на оплате проездных (если применимо)

  Экономия на оплате канцтоваров

  Улучшение психологического климата за счет работы дома

Рост продуктивности



Вчера: Люди “шли” на работу	Сегодня: Работа “идет” к людям

	100 сотрудников	500 сотрудников	1000 сотрудников
Зарплата ($25K в год)	**$2,5 млн.**	**$12,5 млн.**	**$25 млн.**
1 час потери продуктивности	**$1,200**	**$6,000**	**$12,000**
Потери в год от 1 часа в неделю	**$62,5K**	**$312,5K**	**$625K**

- Многие компании фокусируются на предоставлении сервиса на своей территории (зарплата, билеты, документооборот…)
- Сотрудник в среднем тратит только 30–40% времени в офисе

Снижение арендной платы
Сценарий 2

Снижение арендной платы

- Снижение арендной платы → переезд в новые, более дешевые помещения → отказ от СКС → развертывание Wi-Fi → решение Cisco по защищенному беспроводному доступу
- Экономия на:

  Аренде площадей

  Прокладке СКС

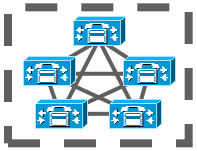
Уменьшение числа командировок

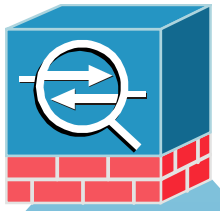
Уменьшение числа командировок

- Уменьшение числа командировок → внедрение видеоконференцсвязи/унифицированных коммуникаций/TelePresence → решение Cisco по защищенному удаленному доступу и защите унифицированных коммуникаций
- Экономия на:

  Командировочных затратах ($300-400 на авиабилет + $100 на гостиницу в сутки)

Cisco ASA и унифицированные коммуникации





Контроль звонков

- SIP, SCCP, MGCP, H.323
- Контроль и инспекция
- Понимание потока и заголовка звонка
- Защита от DoS-атак
- TLS Proxy для зашифрованной сигнализации
- NAT/PAT

Инфраструктура

- Предотвращение сервисов для UC
- Сигнатуры для атак на UC
- VPN для голоса/видео (V3PN)
- Предотвращение атак «переполнение буфера»

Endpoints

- Инспекция RTP/RTCP
- SIP и SCCP Video Endpoints – IP phones, VT Advantage, Cisco Unified Personal Communicator
- Политики - разрешить/запретить звонки с незарегистрированных телефонов, абонентов, whitelist, blacklist

Приложения

- Инспекция SIP/SCCP/CTIQBE/TAP/JTAPI
- Контроль доступа и инспекция для - Cisco Unity, Meetingplace, Presence, Cisco Telepresence, IM over SIP, Microsoft
- Таймауты для аудио/видео-соединений

Контроль доступа **Отражение угроз** **Сетевая политика** **Защита сервисов** **Шифрование видео & голоса**

Сокращение персонала

Сокращение персонала

- Сокращение ИТ\ИБ-персонала в центральном офисе → автоматизация «ручных» задач → решения Cisco по управлению ИБ
- Выгоды:

  Автоматизация и снижение числа ошибок

  Снижение затрат на персонал
- Если руководство не планирует никого увольнять, предлагать такое решение первым не стоит

Затраты на ИТ-специалиста

- Затраты на ИТ-специалиста

  Базовая зарплата ИТ-специалиста - $2500 в месяц ($30000 в год)

  Переменная зарплата – комиссионные

  Премиальные – премии по итогам квартала, года, разовые

  Выплаты по участию в прибылях, издержки на предоставление сотрудникам прав на приобретение акций

  Социальные выплаты – медицинское обслуживание, фонд государственного социального страхования, питание

  Налоги – пенсионный фонд, налог на ФОТ…

  Аренда помещения

  Оборудование – компьютер, мобильный телефон…

35-40 тысяч долларов в год

Cisco Security Management Suite
Мониторинг, анализ и отражение

Cisco Security Management Suite

CISCO SECURITY MANAGER

Облегчает управление политиками

Всесторонняя настройка

Анализ с точки зрения сети и устройства

CISCO SECURITY MARS

Быстрое обнаружение угроз и отражение

Анализ топологии

Анализ и корреляция данных

- Аудит с помощью Network Compliance Manager
- Интеграция с Cisco Secure Access Control Server
  - Ролевой контроль доступа
  - Регистрация действий

Cisco Security Manager

Управление политикой

Централизованное **управление политиками** для МСЭ, VPN и IPS

Хорошо **масштабируем**

Наследование политик позволяет эффективно распределять их по сети

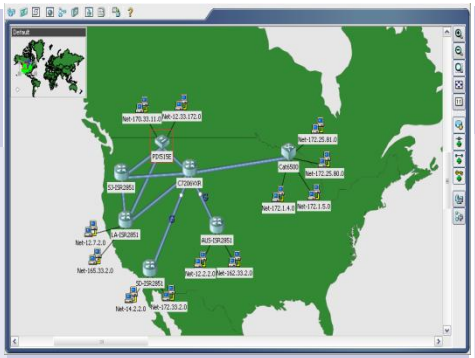
Мощное **группирование устройств**

Удобство использования

Визуальное управление политиками через таблицы или **карту сети**

Функция **Jumpstart**: удобный инструмент обучения

Эффективная **визуализация**:
- Policy-based
- Device-based
- Map-based
- VPN based



Управление МСЭ

Настройка политик для ASA, PIX, FW SM и IOS Firewall

Единая таблица правил для всех платформ

Анализ политик

«Умное» редактирование правил в таблице

Устранение избыточности и противоречивости

Управление VPN

VPN Wizard настраивает Site-to-Site, hub-spoke и full mesh VPN за несколько кликов мыши

Настройка VPN для удаленного доступа, DMVPN и устройств с Easy VPN

Управление IPS

Автоматическое обновление сенсоров IPS

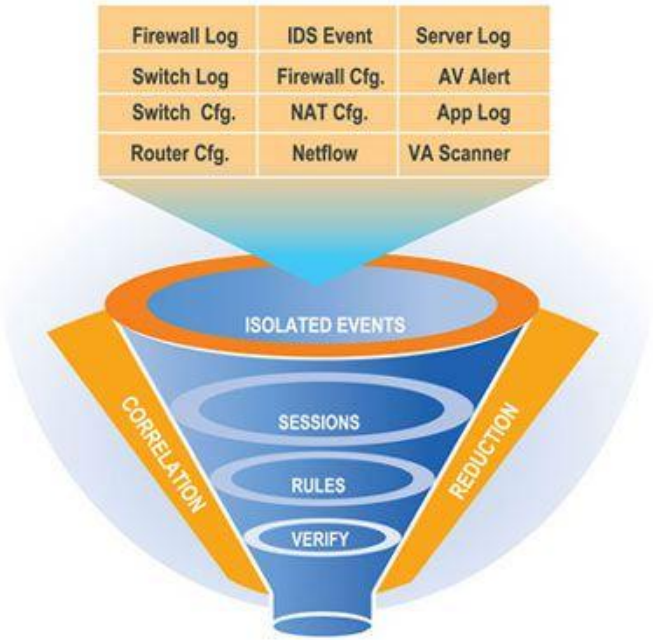
Поддержка **Outbreak Prevention Services**

Cisco Monitoring, Analysis and Response System

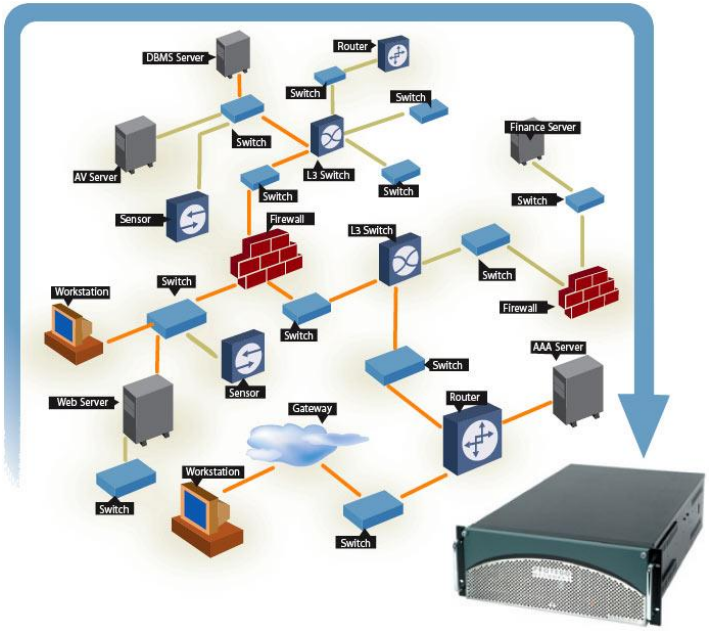
- Сбор, анализ и корреляция данных от разнородных источников и в разных форматах

  NIDS, MCЭ, маршрутизаторы и коммутаторы, CSA

  Syslog, SNMP, RDEP, SDEE, NetFlow, XML API, системные и пользовательские логи



- Локализация и отражение атак



- Ключевые отличия от других SIM

  Визуализация инцидентов и их отображение на карте сети

  Отражение на уровне 2 и 3

  Анализ SDEE и NetFlow

Cisco Network Compliance Manager

Определение политики, конфигурации

ИТ-, ИБ-персонал

Tools Manager

Network Architect

Network Manager

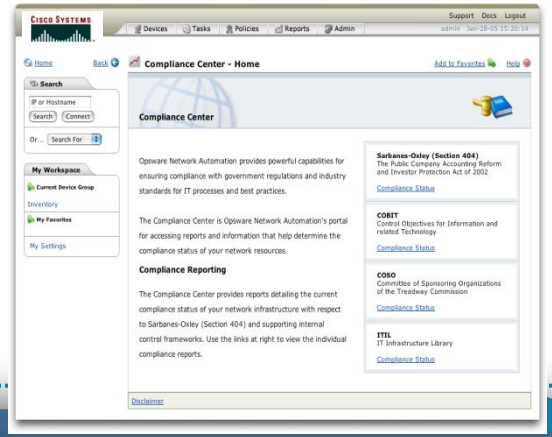
Security Engineers

Network Engineers

NOC Operators

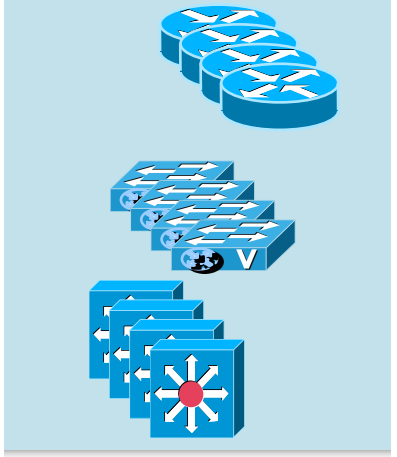
Аудитор
Менеджер
Директор

Средства управления сетью



Предотвращение ошибок & контроль процесса через единую точку контроля

Сеть



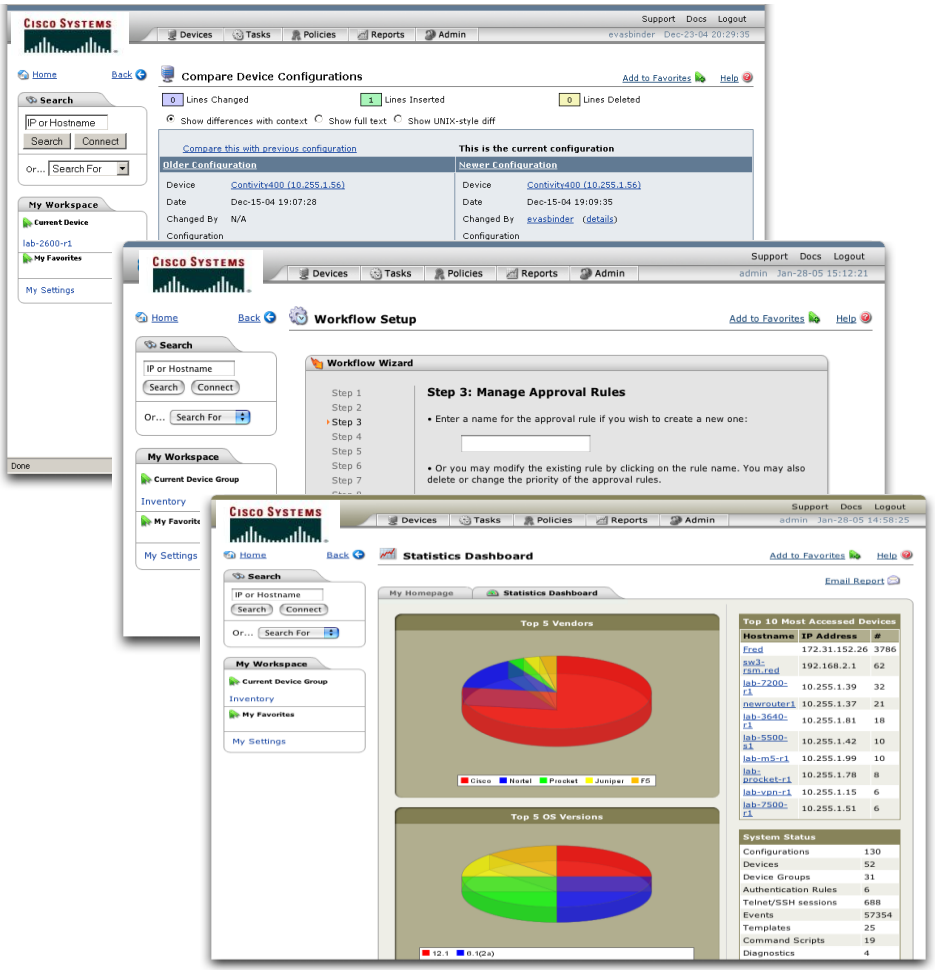
Контроль и стандартизация по всей инфраструктуре в центральном и защищенном месте

Автоматизация сложных сетевых задач управления через специализированный многозадачный инструмент

Цели NCM

Обзор Network Compliance Manager

Высоко масштабируемое, мультивендорное решение для централизованной проверки соответствия и управления изменениями



Контроль и управление конфигурацией и изменениями

- Контроль изменений в реальном времени
- Контроль непротиворечивости
- Применение политик
- Аутентификация через RADIUS, LDAP, Secure ID, TACACS или Active Directory

Аудит и проверка соответствия

- Создание собственных политик соответствия
- Генерация отчетов соответствия (SOX, VISA CISP, HIPAA, GLBA, ITIL, CobiT, COSO)

Расширенная генерация отчетов

- Статус сети
- Рекомендации по приведению в соответствие

Преимущества NCM

Ручной контроль	Автоматический контроль
MTTR из-за ошибки конфигурации: **150 минут**	MTTR из-за ошибки конфигурации: **15 минут**
Простои & инциденты из-за ошибок в «ручных» конфигурациях: **80%**	Простои & инциденты из-за ошибок в «ручных» конфигурациях: **20%**
Среднее время обнаружения уязвимости: **2 недель**	Среднее время обнаружения уязвимости: **Менее 2 минут**
Настройка нового устройства: **6 часов**	Настройка нового устройства: **20 минут**
Изменений в час: **20**	Изменений в час: **5,000**
Среднее число соответствующих узлов в сети: **3%**	Среднее число соответствующих узлов в сети: **100%**

Источник: 2005 EMA Survey и отзывы пользователей

Сокращение персонала

- Сокращение ИТ\ИБ-персонала в удаленных офисах → управление удаленными решениями по ИБ → решения Cisco по управлению ИБ
- Выгоды:

  Автоматизация и снижение числа ошибок

  Снижение затрат на персонал
- Если руководство не планирует никого увольнять, предлагать такое решение первым не стоит

Наследование и распределение политик
“Создали один раз – внедрили много раз”

Что это такое?

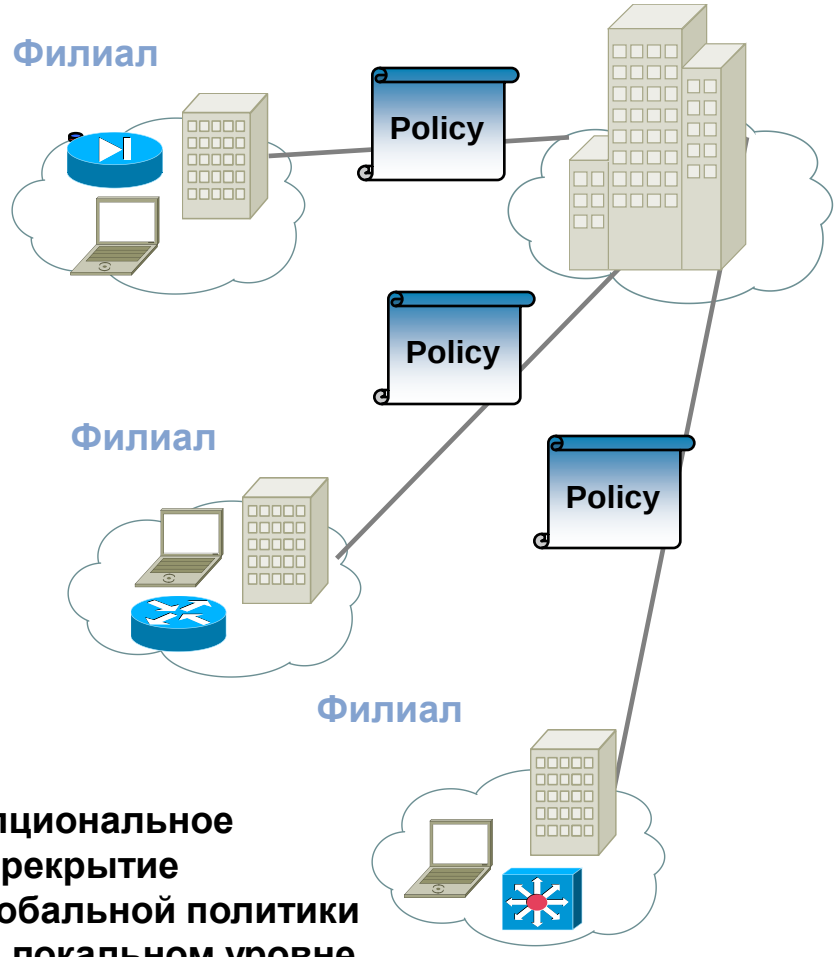
- Нарушение связи между устройством и политикой

Пример:

- Общие политики для групп устройств:
  - МСЭ в филиале
  - Site-to-site VPN
  - Управление устройством
- Обязательные политики:
  - Запрет IM и P2P
  - Разрешить SSH, SSL

Преимущества:

- Снижение сложности управления
- Не требует много ресурсов



Опциональное перекрытие глобальной политики на локальном уровне

Масштабное распределение

Что это такое?

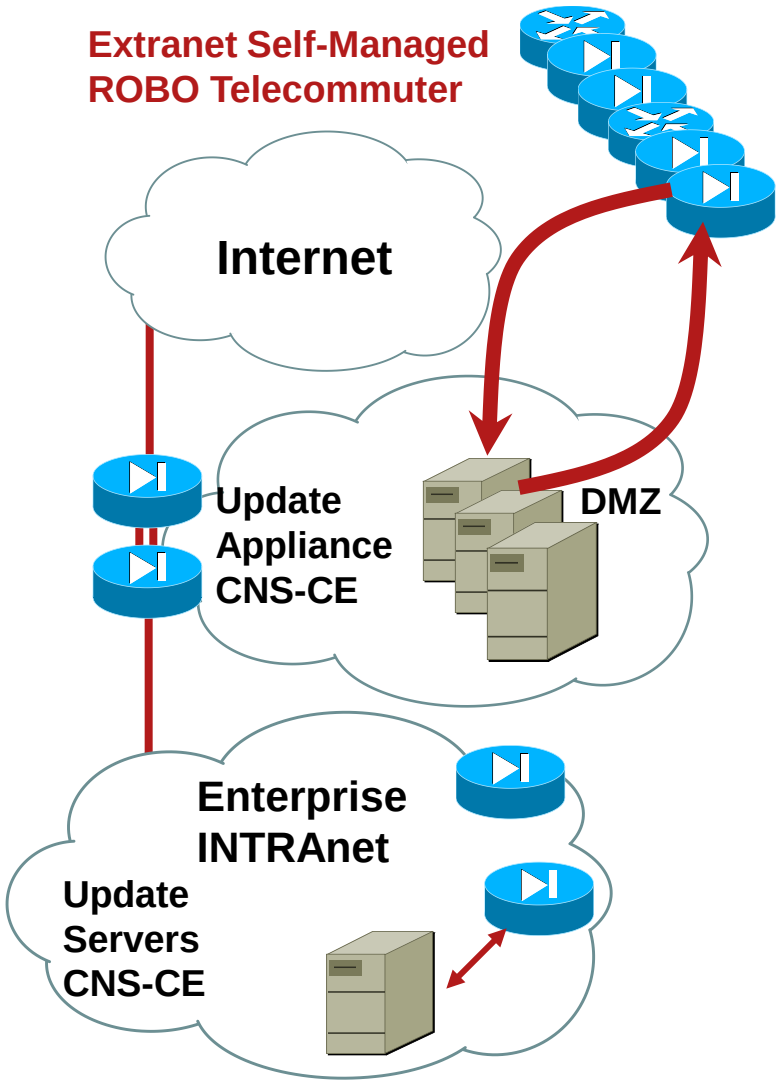
- Метод простого распределения политик и ПО на тысячи устройств

Пример

- Обновление большого числа удаленных МСЭ с динамической адресацией, нерегулярными линками или адресами за NAT
- Обновление конфигурации и ПО
- Обновление устройства, когда оно активно
- Масштабирование через Web-технологии

Преимущества

- Минимальные человеческие и временные затраты на построение защищенной сети



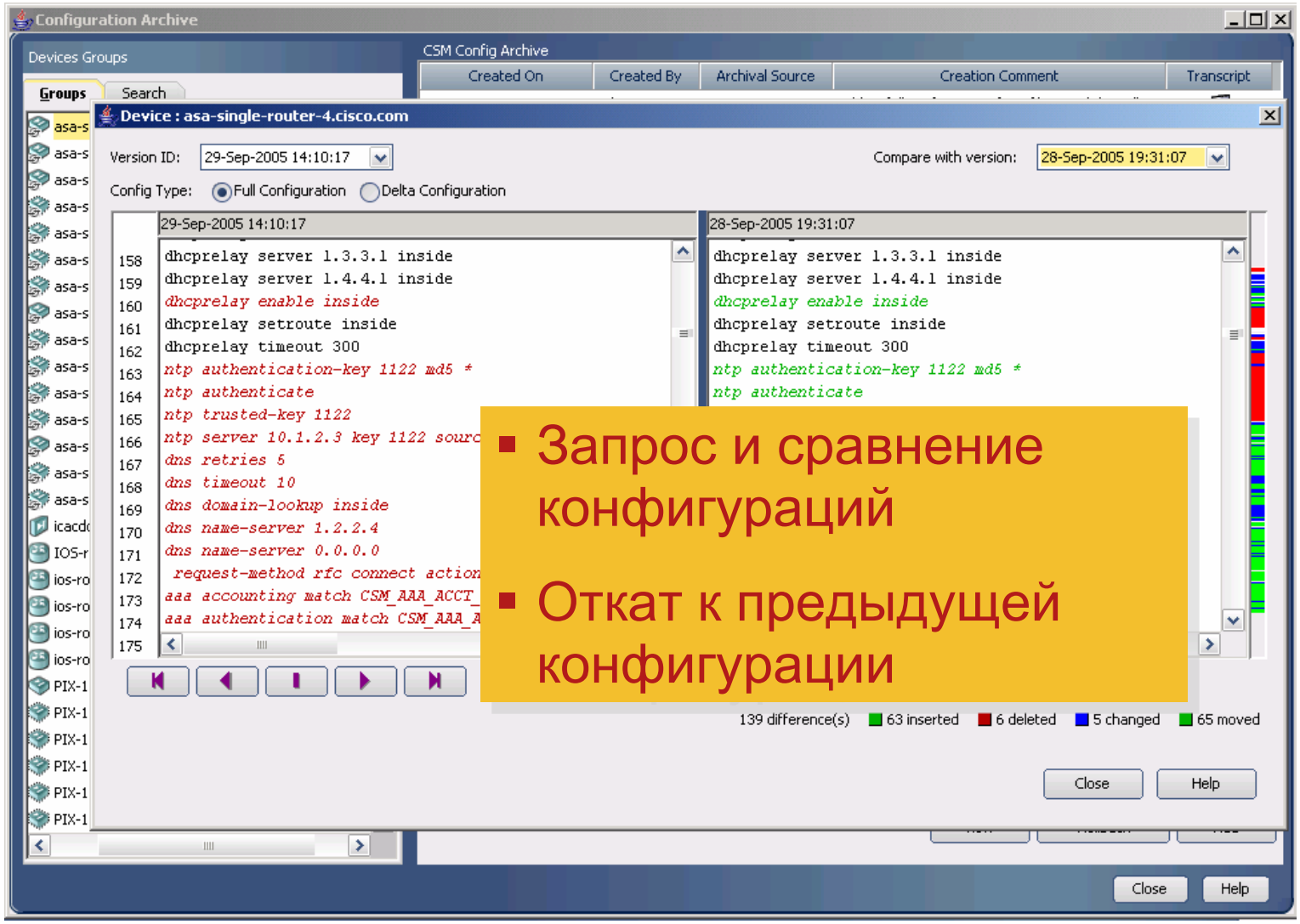
Сокращение персонала

- Сокращение ИТ\ИБ-персонала за счет аутсорсинга → контроль аутсорсера → решения Cisco по аудиту ИБ → NCM, CSM
- Выгоды:

  Контроль исполнения контрактных обязательства

  Снижение затрат на персонал
- Если руководство не планирует никого увольнять, предлагать такое решение первым не стоит

Power Tools: Config Archive, FlexConfig



- Запрос и сравнение конфигураций
- Откат к предыдущей конфигурации

Сокращение затрат на Интернет

Сокращение затрат на Интернет

- Контроль действий сотрудников в Интернет → блокирование загрузок постороннего ПО, музыки, видео и контроль посторонних сайтов → решение Cisco по контролю URL
- Экономия на:

  Интернет-трафике
- Дополнительно

  Рост продуктивности (может быть)

  Защита от вирусов и троянцев в загружаемом трафике

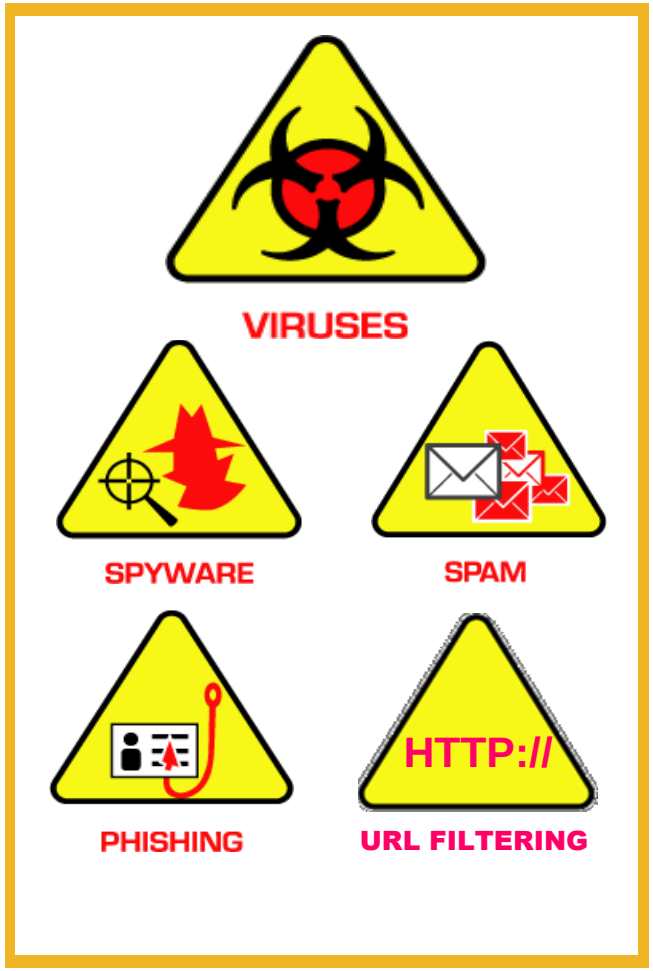
IronPort Web Security Appliance

IronPort Web Security Appliance

Одновременных TCP соединения	100,000 duplex	Легко справляется с пиковой загрузкой
Количество транзакций HTTP в час	10M unburdened, 5-7M burdened	Может обслуживать 10-25 тыс пользователей (в зависимости от профиля трафика)
Средняя задержка	5-15 milliseconds	Прозрачно для пользователя

Контроль содержимого (Anti-X) на шлюзе

- Anti-Virus: Обнаружение и лечение в реальном времени файловых вирусов и вредоносного кода для протоколов SMTP, HTTP и FTP
- Anti-Spam: Высокопроизводительный интеллектуальный антиспам модуль, использующий белый/черный список адресов и базу спамовых сигнатур
- Anti-Spyware: Всесторонняя защита от шпионского ПО, которое может привести к снижению производительности или утечки информации
- Anti-Phishing: Защита пользователей от мошенничества с помощью антифишинговых возможностей
- URL Blocking and Filtering: Слежение, регистрация и контроль доступа к Internet URL



Сравнение решений по контролю контента

	Cisco ASA 5500 CSC SSM	Cisco ASA 5500 CSC Embedded	IOS Content Filtering
Anti-Spam	Полная	NRS только (включает 10 пользователей)	Нет
URL Filtering	Полная	Полная	Полная
Anti-Virus	Полная	Полная	Нет
Signature Set	Полная	Подмножество	N/A
Pattern File Size	18 MB	15 MB	N/A

Защита бизнеса от «разворовывания»

Защита бизнеса от разворовывания

- Увольнение сотрудников → желание «урвать» → кража информации → решение Cisco по контролю утечек информации
- Выгоды:

  Защита от утечек интеллектуальной собственности, банковской и коммерческой тайны, персданных и т.п.
- Дополнительно

  Защита почты

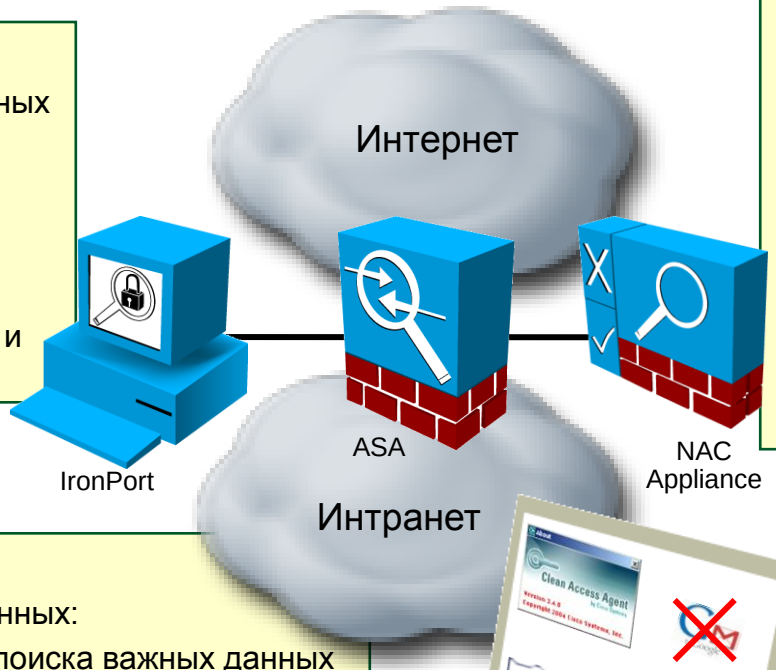
  Защита ПК, лэптопов от широкого спектра угроз

  Защита от преследования за нарушение обращения с защищаемой информацией

Комплексное решение по защите

IronPort

- Предотвращает утечку данных на периметре сети
- Сканирование многих протоколов
- Рост эффективности существующей инфраструктуры Anti-Spam и Anti-Spyware

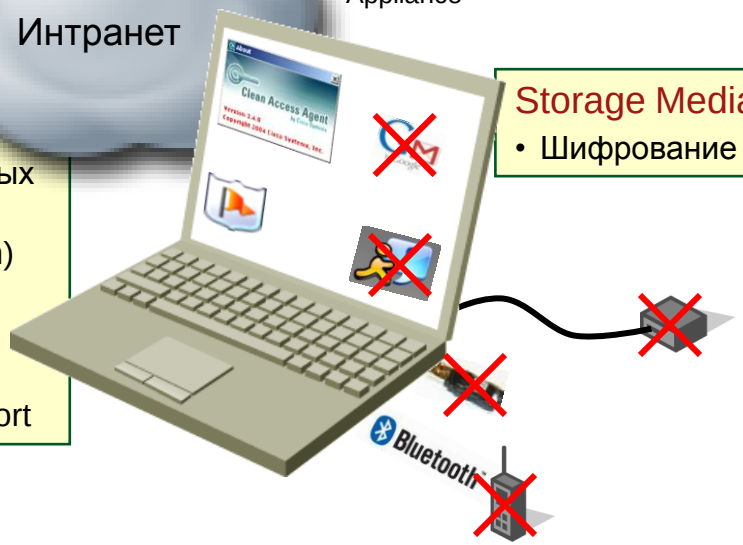


NAC Appliance

- Проверка версии и запуска CSA
- Проверка состояния системы (например, “insecure boot detected”) и наличия конфиденциальных данных
- Проверка привилегий пользователя, если CSA сообщает о наличии конфиденциальной информации

Cisco Security Agent

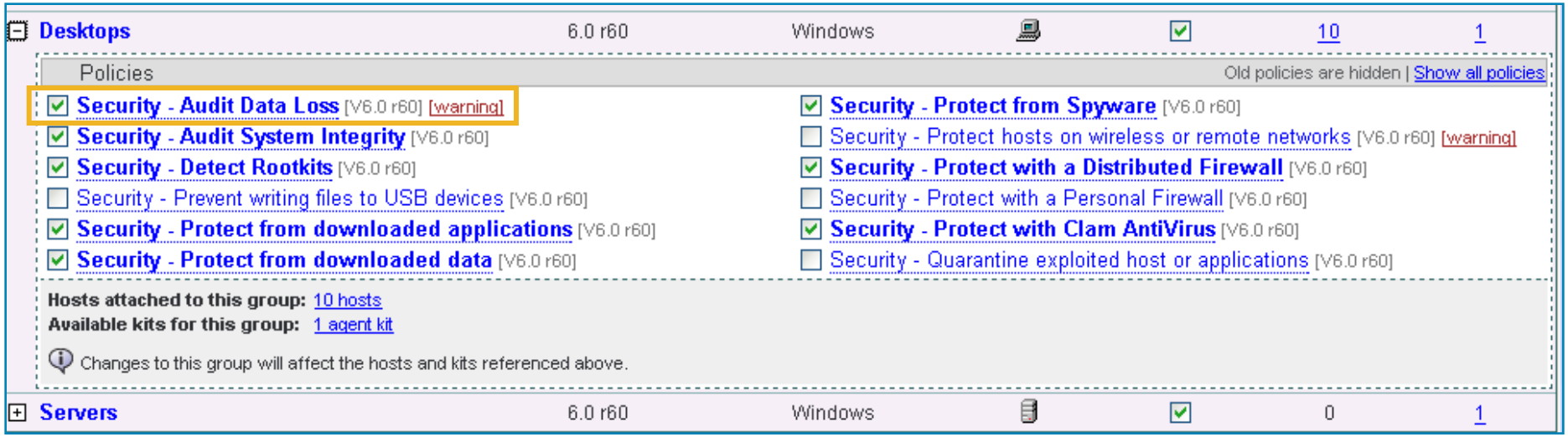
- Предотвращение утечки данных:
  - Сканирование файлов в поиска важных данных
  - Блокирование копирования на внешние носители (USB flash и disk, порты IR/Bluetooth)
  - Предотвращение копирования в коммуникационные приложения (e-mail, IM, броузер)
- Предотвращение обхода сетевой защиты IronPort



Storage Media Encryption

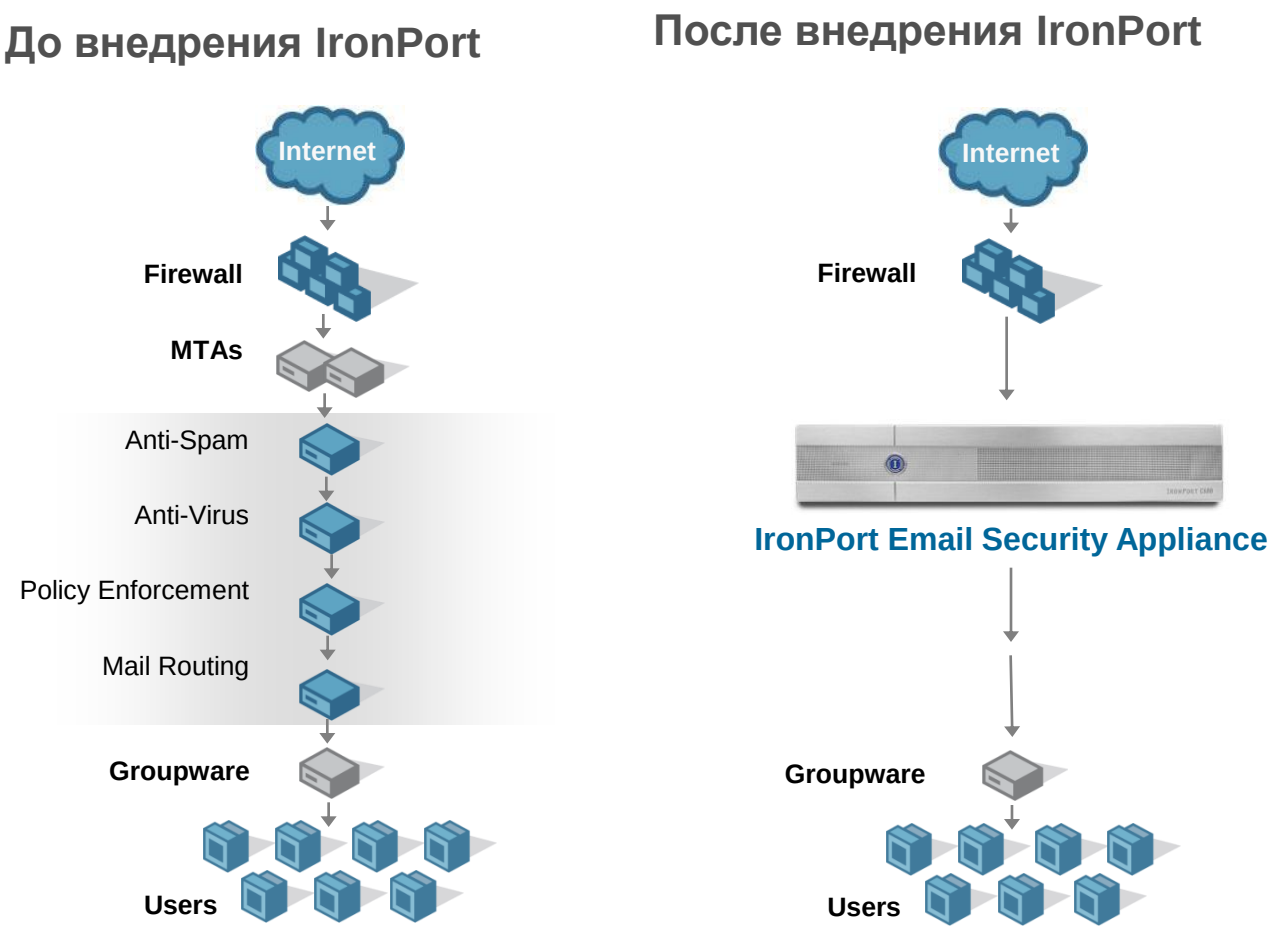
- Шифрование данных в SAN

Предотвращение утечек информации



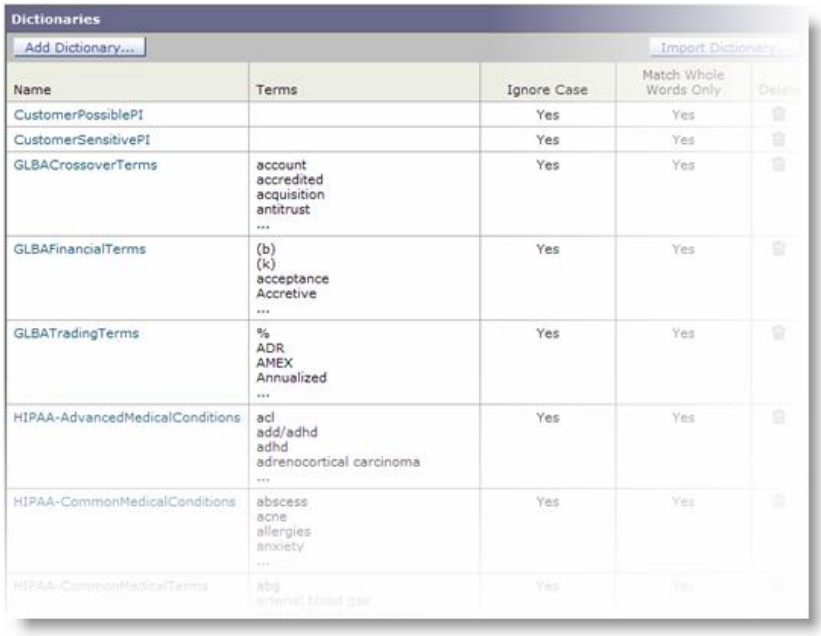
- Агент сканирует файловую систему и ищет важную информацию, определенную в настройках “Global Data Classification”
- Если важная информации найдена, она метится соответствующим образом и к ней применяется соответствующая политика безопасности (Audit Data Loss Policy)
- Политика Audit Data Loss Policy защищает важную информацию внутренних пользователей от вредоносных и неавторизованных действий, включая копирование на внешние носители и через буфер обмена, а также печать на принтере
- Политика Audit Data Loss Policy также определяет правила для мобильных и удаленных пользователей

Что дает IronPort ESA?

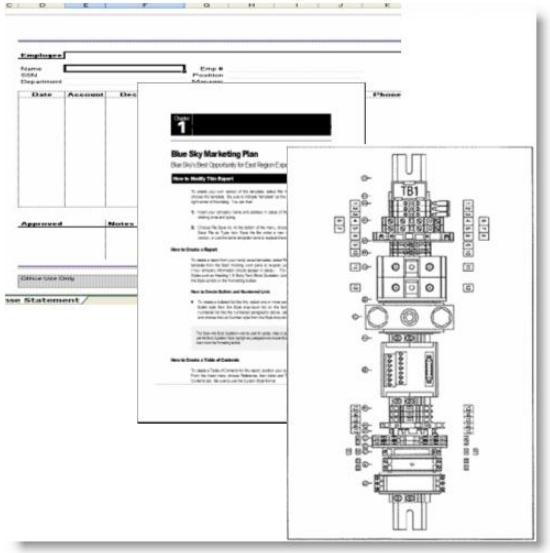


Контроль утечки информации

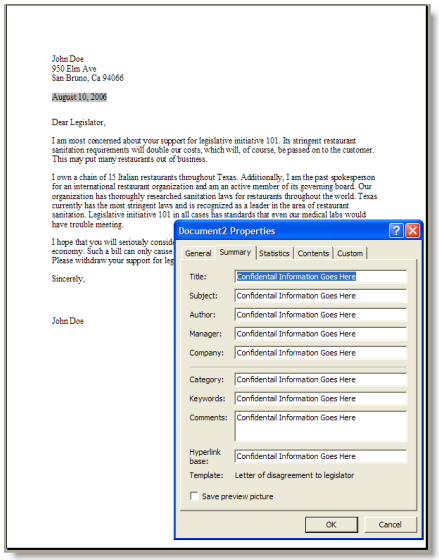
- Предустановленные шаблоны и политики для распространенных требований по безопасности
- Механизм поиска по образцу **снижает число ложных срабатываний**
- Высокопроизводительный механизм TLS позволяет обеспечить защиту передаваемой почты



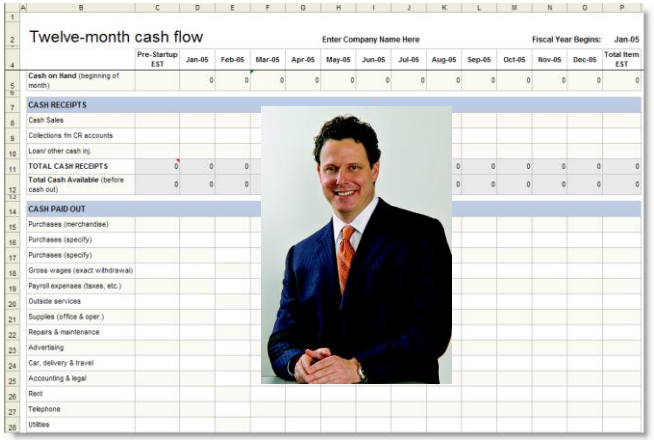
Контроль содержимого



Анализ текста в файлах 390+ форматов



Анализ метаданных



Обнаружение внедренных объектов в файлах Excel и Word:

EXE, DLL, JPEG, GIF, BMP

Снижение капитальных затрат

Снижение капитальных затрат

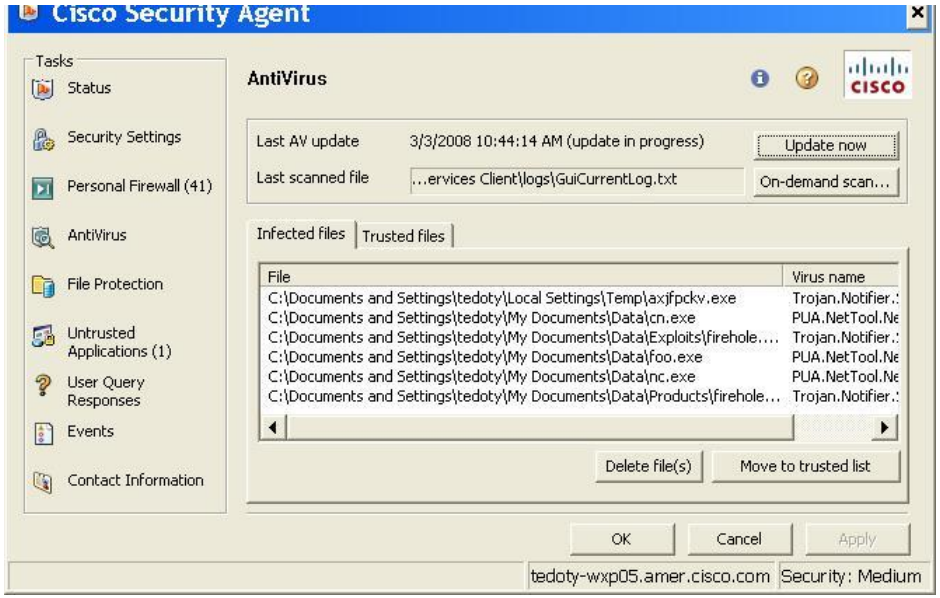
- Снижение капитальных затрат → экономия на ПО → отказ от отдельного антивируса → Cisco Security Agent
- Выгоды:

  Экономия на антивирусном ПО
- Дополнительно

  Защита ПК, лэптопов от широкого спектра угроз

Интегрированный агент CSA
с Clam Antivirus

- Сканирующий модуль ClamAV интегрирован с CSA в единый продукт
- Защита серверов и ПК Windows без дополнительных затрат
  - Аккуратное обнаружение вредоносного ПО
  - Предотвращение исполнения вредоносного ПО
  - Удаление или помещение в карантин вредоносного ПО



- CSA Management Center управляет политиками агента и обновлениями сигнатур
- Действительно единый агент – единая консоль управления

Пример ROI
Интегрированный антивирус

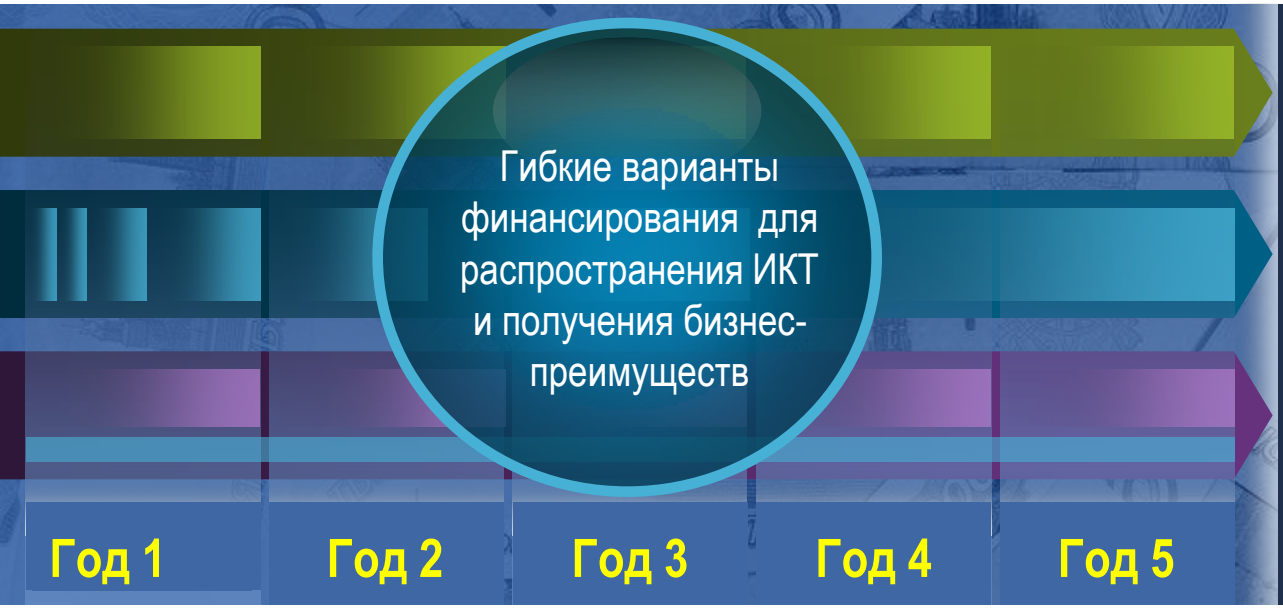
- Несмотря на малую цену антивирус для одного узла очень дорог в среднесрочной перспективе
- ~$10 на ПК в год (усредненная цена) для 50,000 узлов
- Цена на CSA по GPL (бессрочная лицензия) на 50,000 ПК:
  - $625K на продукт (с 42%-ой скидкой) $12.51 на ПК
  - $106K на поддержку (скидка 28%) $2.12 на ПК в год
- Сравнение цен в среднесрочной перспективе:
  - 1-й год $731K Cisco $500K у конкурентов
  - 2-й год $837K Cisco $1M у конкурентов
  - 3-й год $943K Cisco $1.5M у конкурентов

Для антивируса Clam не требуется оплаты поддержки – она включена в стандартную поддержку CSA

Снижение капитальных затрат

- Снижение капитальных затрат → переход на лизинг → Cisco Capital
- Выгоды:
  - CapEx переходит в OpEx
  - Ускоренная амортизация (коэффициент – 3)
  - Снижение налога на прибыль и имущество
  - Не снижает Net Income, EBITDA
  - Нет проблем списания оборудования
  - Отсрочка платежа
- Дополнительно
  - Использования актуальной версии оборудования и ПО

Финансирование проектов по ИБ



Большой опыт работы в Украине, в России и других странах СНГ

Заслуживающий доверия финансовый консультант

Инновационные решения в области финансирования, отвечающие требованиям каждого заказчика

Резюме

ИБ в условиях кризиса

- Чтобы эффективно существовать в условиях кризиса службы ИБ должны понимать бизнес и не только идти за ним, но и направлять его в нужном направлении
- Чтобы понимать бизнес, обратитесь к консультантам Cisco Customer Advocacy
- Посетите презентацию «Измерение отдачи при внедрении системы ИБ»

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +7 495 961-1410