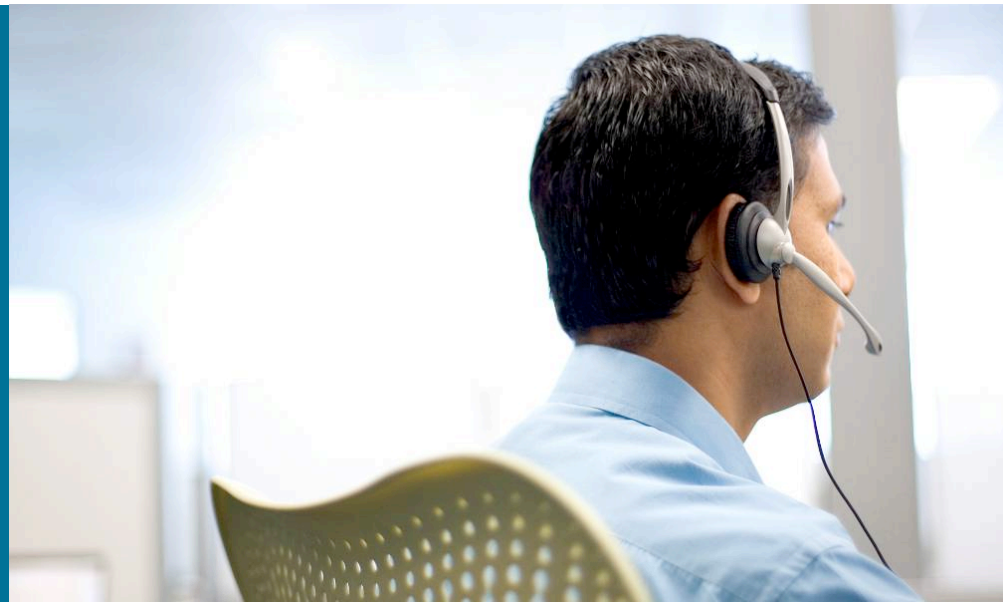
Как решения Cisco по информационной безопасности реализуют требования стандарта PCI DSS…

и не только!



Алексей Лукацкий

Бизнес-консультант по безопасности

Ответьте на 4 вопроса

1. У вас есть сайт электронной коммерции (Интернет-банк, Интернет-магазин и т.д.)?
2. Вы принимаете к оплате кредитные или дебетовые карты?
3. Вы храните, обрабатываете или передаете информацию о кредитных картах?
4. Вы передаете информацию о кредитных картах и их владельцах по телефону, факсу или обычной почте?

Если на какой либо из этих вопросов вы ответили ДА, то вы должны соответствовать требованиям стандарта PCI DSS

Введение в PCI DSS

Стандарт PCI DSS

- Payment Card Industry Data Security Standard (PCI DSS) – стандарт защиты информации в индустрии платежных карт, разработанный международными платежными системами Visa и MasterCard
  - Принят в январе 2005 года. Текущая версия – 1.2.1
  - 12 основных требований, 200+ детальных требований
- PCI DSS объединяет в себе требования программ:
  - Visa Europe & другие регионы: Account Information Security (AIS);
  - Visa USA: Cardholder Information Security (CISP);
  - MasterCard: Site Data Protection (SDP)
- Поддержка AmEx, Diners Club, Discover, JCB

История возникновения и развития

2001 год	• VISA – Cardholder Information Security Program (CISP)
2003 год	• MasterCard – Site Data Protection (SDP)
Октябрь 2004	• Discover – Discover Information Security and Compliance (DISC)
Декабрь 2004 / январь 2005	• PCI – Payment Card Industry Data Security Standard (PCI DSS)
Декабрь 2006	• PCI DSS 1.1
Октябрь 2008	• PCI DSS 1.2
Июль 2009	• PCI DSS 1.2.1

Цели PCI DSS

- Повышение защищенности электронных торговых и платежных систем
- Создание безопасной среды для хранения, обработки и передачи данных платежных карт
- Модернизация и рационализация бизнес-процессов и снижение издержек



К кому применяются требования стандарта PCI DSS?

PCI Data Security Standard

- Требования PCI DSS распространяются на все компании, работающие с платежными системами Visa и MasterCard
- **Применяется ко всем, кто**
  - **Обрабатывает**
  - **Передает**
  - **Хранит: данные владельцев карт**
  - **Как минимум PAN**
- Применяется к компаниям во всем мире

К кому применяется PCI DSS?

- Продавцы

  Компании, продающие товары и услуги

- Провайдеры платежных систем (PSP)

  Компании, обеспечивающие платежные шлюзы продавцам, осуществляющим продажи через Интернет

- Эквайер (Acquiring Bank)

  Банки, помогающие продавцам принимать платежи по кредитным картам

Применимость стандарта

Требования для продавцов

Уровень продавца	Критерий отбора	Проверка
Уровень 1	Свыше 6 миллионов платежных транзакций в год по всем каналам, включая e-commerce Любая пострадавшая от мошенничества компания	▪ Ежегодный аудит ▪ Ежеквартальное сканирование
Уровень 2	1,000,000 - 5,999,999 платежных транзакций в год	▪ Ежегодная самооценка (аудит для MasterCard) ▪ Ежеквартальное сканирование
Уровень 3	20,000 – 1,000,000 электронных платежных транзакций в год	▪ Ежегодная самооценка ▪ Ежеквартальное сканирование
Уровень 4	Менее 20,000 электронных платежных транзакций в год	(Рекомендуется) ▪ Ежегодная самооценка ▪ Ежеквартальное сканирование

Требования для провайдеров

Уровень провайдера	Критерий отбора	Проверка
Уровень 1	Все, кто работает с VisaNet® Платежные шлюзы	▪ Ежегодный аудит ▪ Ежеквартальное сканирование
Уровень 2	Все, кто не относится к Уровню 1 >300К платежных транзакций в год	▪ Ежегодный аудит ▪ Ежеквартальное сканирование
Уровень 3	<300К платежных транзакций в год	▪ Ежегодная самооценка ▪ Ежеквартальное сканирование

«Не Visa»-требования

- Для платежных систем American Express, Discover и JCB критерии отнесения к тому или иному уровню могут быть другими
  - Например, уровень 1 для участников системы American Express начинается с 2,5 миллионов транзакций

Внедрение и соответствие

Внедрить или соответствовать?

- Внедрить стандарт должны ВСЕ без исключения
  - В отличие от оценки соответствия
- Чем больше транзакций проходит через организацию, тем жестче требования к ее проверке
  - И тем серьезнее наказание за несоответствие
- Требования каждая платежная система предъявляет свои
  - У Visa и MasterCard они похожи
- Оценка соответствия проводится в виде
  - Заполнения листов самооценки
  - Ежеквартального сканирования
  - Ежегодного аудита

Ущерб и штрафы за несоответствие

Ущерб от несоответствия

- Рост числа мошенничеств
- Наложение ограничений со стороны платежной системы
- Сложности идентификации поддельных карт
- Риск возмещения «потерянных денег» клиентам
- Штрафы и судебные иски
- Негативное освещение в прессе
- Ущерб репутации
- Снижение курсовой стоимости акций

Штрафные санкции

- Каждая платежная система в каждом регионе имеет свои штрафы
- Пример

  Штраф $25К-100К в месяц

  Понижение на 1 уровень в иерархии

  Банки-эквайеры штрафуются на $25К за каждого несоответствующего требованиям PCI DSS клиента

  При несообщение об инциденте – штраф $100К (до $500К)

10 рекомендаций Cisco

Шаг 1: Составьте план действий

- Цели внедрения стандарта
- Сроки реализации
- Возможные ограничения
- Критерии выбора технических и организационных мер
- Критерии выбора QSA, ASV и т.д.

Шаг 2: Область применимости

- Составьте перечень всех элементов инфраструктуры, хранящих, обрабатывающих или передающих данных платежных карт

  Данные платежных карт (Personal Account Number, имя держателя карты, сервисный код, дата истечения срока действия)

  Данные авторизации, хранение которых запрещено даже при наличии шифрования (полное содержание магнитной полосы, CAV2/CVC2/CVV2/CID, PIN-код/PIN-блок)

- Для этой цели можно использовать CiscoWorks LMS, Cisco MARS и т.п.

Шаг 3: Схема информационных потоков

- Составьте схему потоков данных платежных карт
- Для этой цели можно использовать любое сетевое оборудование Cisco с поддержкой функции анализа сетевого трафика

  ^4[0-9]{12}(?:[0-9]{3})?$ - поиск PAN Visa (без разделителей)

  ^5[1-5][0-9]{14}$ - поиск PAN MasterCard (без разделителей)

  ^((4\d{3})|(5[1-5]\d{2}))(-?|\040?)(\d{4}(-?|\040?)){3}|^(3[4,7]\d{2})(-?|\040?)\d{6}(-?|\040?)\d{5} – поиск PAN Visa, MasterCard и AmEx как в виде строки из цифр, так и с разделителями

- Не забывайте, что PAN могут передаваться и в зашифрованном виде, а также циркулировать локально на ПК, сервере, POS-терминале…

Шаг 4: Не храните лишнего

- Мотивация – от «*а вдруг пригодится*» и «*а я не знаю, как отключить регистрацию дополнительной информации*» до «*а я и не знал, что у меня это обрабатывается и хранится*»
- Данные хранятся в неподходящих местах – БД, журналах регистрации, отладочных файлах, почтовых сообщениях и т.п.
- Чем меньше храним, тем меньше защищать и тратить ресурсов
- Удалите лишние данные и отключите их регистрацию в будущем

Шаг 5: Реализация требований PCI DSS

12 требований PCI DSS

Построение и поддержка защищенной сети	1. Установка и поддержание конфигурации МСЭ для защиты данных 2. Контроль за сменой выставленных по умолчанию производителем системных паролей и других параметров системы безопасности
Защита данных владельцев платежных карт	3. Обеспечение защиты хранящихся данных держателей карт 4. Обеспечение шифрования данных владельцев карт и других важных данных при их передаче через общедоступные сети
Поддержка программу управления уязвимостями	5. Использование и регулярное обновление антивирусного программного обеспечения 6. Разработка и поддержка систем по безопасности и их приложений
Внедрение строгих мер разграничения доступа	7. Разграничение доступа к данным по принципу служебной необходимости и разделения полномочий 8. Присвоение уникального идентификационного номера каждому лицу, располагающему доступом к компьютеру 9. Разграничение физического доступа к данным держателей карт
Регулярный мониторинг и тестирования сети	10. Отслеживание всех сеансов доступа к сетевым ресурсам и данным владельцев карт 11. Постоянный анализ процессов обеспечения безопасности
Поддержка политики информационной безопасности	12. Наличие и выполнение политики по информационной безопасности

Требование 1

- Установка и поддержание конфигурации МСЭ для защиты данных
  - **Документирование и стандартизация конфигурации**
  - **Сегментирование сети передачи данных держателей карт от других участков**
  - **Разграничение доступа для внешних соединений**
  - **Беспроводные сети**
  - **Персональные МСЭ**
  - **ACL на маршрутизаторах**
  - **NAT/PAT**

Требование 2

- Не использовать пароли и настройки безопасности по умолчанию установленные производителями
  - **Изменить заданные по умолчанию пароли**
  - **Беспроводные технологии – изменение настроек заданных по умолчанию, запрет широковещательной рассылки SSID, использование WPA/WPA2**
  - **Реализация одной основной функции на сервер**
  - **Запрет всех нетребуемых и незащищенных протоколов и сервисов**
  - **Шифрование административного доступа**
  - **Стандартизация конфигурации для всех систем**

Требование 3

- Защита хранимых данных

Внедрение системы хранения данных для владельцев платежных карт

Не хранить важные аутентификационные данные (CVV, CVC2, PVV и т.д.)

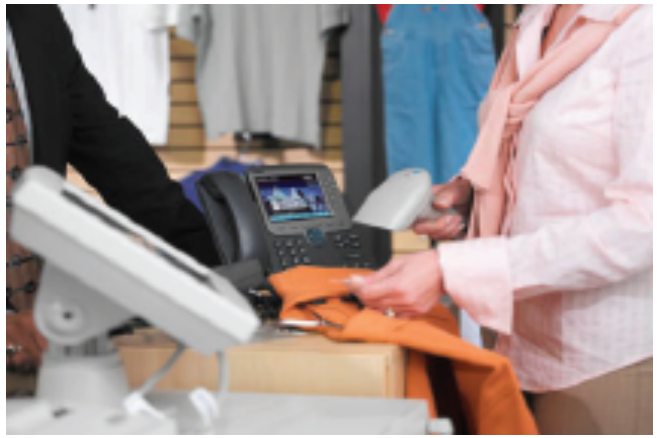
Маскирование персональных данных

Документирование и реализация процессов и процедур управления криптографическими ключами

Шифрование и хэширование данных

Требование 4

- Шифрование данных при передаче через публичные сети
  - **Используйте SSL/TLS или IPSec, WPA для беспроводных сетей**
  - **Если используется WEP**
    - **Используйте минимум 104-битный ключ шифрования и 24-битный вектор инициализации**
    - **Используйте ТОЛЬКО вместе с WPA/WPA2, VPN или SSL/TLS**
    - **Ежеквартально (или автоматически) меняйте ключи shared WEP**
    - **Разграничьте доступ на базе MAC-адресов**
  - **Никогда не посылайте незашифрованных персональную информацию по e-mail**



Требование 5

- Используйте и регулярно обновляйте антивирусное ПО

  Установите антивирусы на все системы, которые могут быть подвержены вирусам и вредоносным программам

  Антивирусы должны быть способны обнаруживать, удалять и защищать против всех известных типов вредоносного ПО, включая шпионское и рекламное ПО

  Убедитесь, что антивирусные механизмы актуализированы, запущены и генерят журнал регистрации

Требование 6

- Разработка и поддержка защищенных систем и приложений

  Установка патчей и обновлений от производителей

  Внедрение процесса идентификации новых уязвимостей

  Разработка ПО на основе индустриальных best practices и стандартов с точки зрения безопасности

  Разработка Web-приложений на основе рекомендаций, например, Open Web Application Security Project (OWASP)

  Web-приложения должны защищаться против известных атак путем установки прикладных МСЭ или путем анализа кода сторонними специализированными организациями

Требование 7

- Ограничение доступа к данным по служебной необходимости

Ограничение доступа к вычислительным ресурсам и данным владельцев платежных кард только сотрудникам, которым доступ необходим для выполнения служебных обязанностей

Установление механизма для многопользовательских систем, который разграничит доступ на основании привилегий пользователей и запретит доступ всем, исключая тех, кому он не будет разрешен отдельно

Требование 8

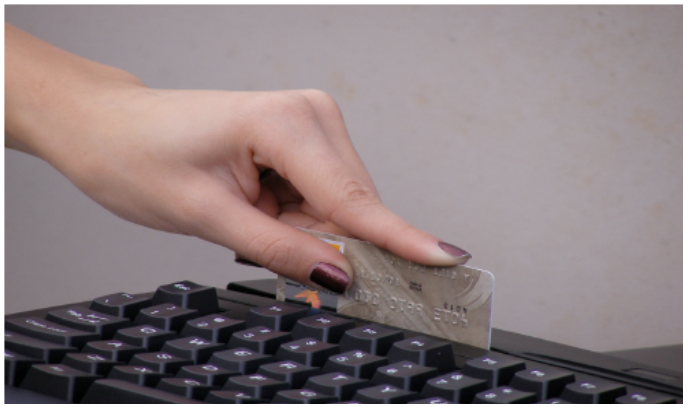
- Связывание уникального ID для каждого сотрудника с доступном к информационным ресурсам

Идентификация всех пользователей с уникальным именем пользователя до разрешения доступа к системным компонентам или данным владельцев платежных карт

В дополнение к идентификации используйте не менее одного метода аутентификации (пароли, токены [SecureID, сертификаты или открытые ключи], биометрия)

Внедрение двухфакторной аутентификации

Шифрование всех паролей в процессе хранения и передачи данных



Требование 9

- Ограничение физического доступа

  Контроль доступа и ограничение физического доступа к системам, которые хранят, обрабатывают или передают данные владельцев платежных карт

  - **Камеры для видеонаблюдения критичных областей**
  - **Ограничение физического доступа к сетевым розеткам, беспроводным точкам доступа, шлюзам и ПК**

  Различие между сотрудниками и посетителями

  Регистрация посетителей, использование физических токенов, авторизация до попадания в критичные области

  Физическая защита носителей с данными владельцев платежных карт

  Уничтожение данных, когда они больше не требуются

Требование 10

- Мониторинг и регистрация всех действий с сетью и данными владельцев карт

Автоматизация регистрации действий

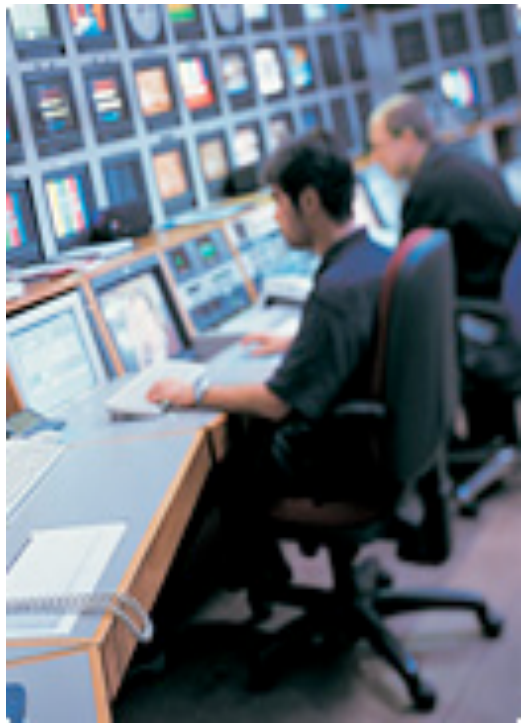
Регистрация широкого набора параметров

Защита журналов регистрации

Ежедневный анализ журналов регистрации

Уничтожение данных, когда они больше не требуются

Хранение журналов регистрации не менее чем в течение года, с обеспечением онлайн-доступности в течение 3-х месяцев



Требование 11

- Регулярное тестирование систем и процессов

  Использование не реже раза в квартал Wi-Fi-анализатора для идентификации всех используемых беспроводных устройств

  Запуск внутреннего и внешнего сканирования уязвимостей не реже раза в квартал, а также после серьезных изменений в сети

  Обеспечение тестирований на проникновение не реже раза в год или после серьезных обновлений и модификаций

  Использование NIDS/IPS, HIDS/HIPS

  Внедрение ПО обеспечения файловой целостности для контроля не реже раза в неделю

Требование 12

- Внедрение и поддержка политики безопасности

  Установка, публикация, поддержка и распространение политики безопасности

  Внедрение политик для всех критичных с точки зрения человеческого фактора технологий

  Внедрение программы повышения осведомленности

  Внедрение плана реагирования на инциденты

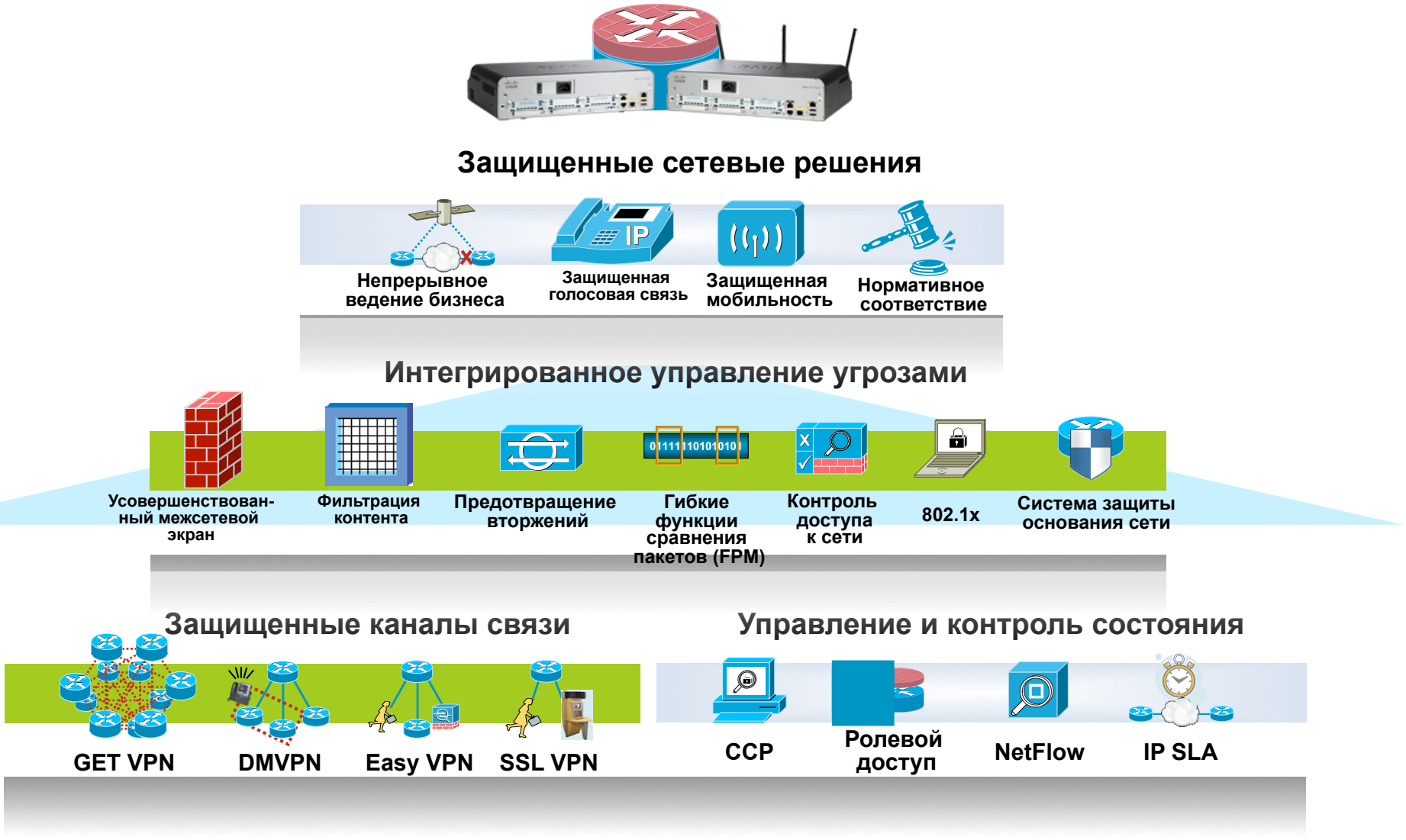
  Если данные владельцев платежных карт разделяются с оператором связи, последний обязан выполнять требования PCI DSS

10 лучших рекомендаций Cisco
Продолжение

Шаг 6: Защищенные приложения

- Организации должны применять приложения, прошедшие сертификацию по стандарту PA DSS
  - 1 июля 2012 года – крайний срок сертификации для производителей приложений
- Организации обязаны работать с теми платежными шлюзами и платежными организациями, которые используют сертифицированные по PA DSS приложения
- Учитывая срок выбора, тестирования и амортизации ПО, остается не так уж и много времени

Шаг 7: Используйте встроенные механизмы защиты



Шаг 8: Периодический контроль и мониторинг

- Целью внедрения PCI DSS является не прохождение аудита или заполнение листа самооценки
  - Фокус на защите данных платежных карт на всем этапе их жизненного цикла, который не заканчивается аудитом
- Обратите внимание на периодически проводимые мероприятия из стандарта PCI DSS
  - Анализ конфигурации межсетевых экранов и защищенных маршрутизаторов – не реже одного раза в полгода
  - Периодическая смена криптографических ключей – не реже одного раза в год
  - Регулярный анализ защищенности Web-приложений от известных атак – не реже одного раза в год, а также по мере внесения изменений в Web-приложения…

Шаг 9: Сохранение соответствия

- Сохранить соответствие гораздо сложнее, чем достичь его
  - Это непрерывный процесс
- Активно используйте цикл Деминга-Шухарта, известный также как PDCA (Plan, Do, Control, Act)
  - Plan – шаги 1-4
  - Do – шаги 5-7
  - Control – шаг 8
  - Act – на основании результатов контроля и мониторинга

Шаг 10: Не забывайте про другие требования

- PCI DSS – только один из возможных нормативных актов / требований
- Национальная система массовых электронных платежей (НСМЭП)
- Базель II
- Евроконвенция по защите персональных данных
- Требования СБУ и ДСТЗИ
- И т.д.

Как сохранить соответствие?

PDCA?.. стандарт ISO 27001?..

- Название – «Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
- В настоящем стандарте устанавливаются требования по созданию, внедрению, эксплуатации, мониторингу, анализу, поддержке и совершенствованию документально оформленной СМИБ в контексте общих бизнес-рисков организации

СУИБ

- СУИБ (СМИБ) - та часть общей системы менеджмента, которая основана на подходе бизнес-рисков при создании, внедрении, функционировании, мониторинге, анализе, поддержке и совершенствовании информационной безопасности
- Целью построения СМИБ является обеспечение выбора адекватных и соответствующих мер (средств) контроля безопасности, с помощью которых обеспечивается адекватная защита информационных активов и создается доверие заинтересованных сторон

Стандарт ISO 17799:2005

- Название – «Методы обеспечения безопасности. Руководство по управлению безопасностью информации»
- Цель – устанавливает основные руководящие принципы для инициирования, реализации, поддержки и усовершенствования управления информационной безопасностью в организации
- Текущая версия – 2-я
- С апреля 2007 года входит в серию ISO 2700x как ISO 27002

Структура стандарта

- 11 областей контроля
- 39 главных категорий безопасности
- Вводный раздел по оценке и управлению рисками
  - Детализация в ISO 27005
- Главная категория описывает
  - Цели контроля
  - Меры безопасности, направленные на достижение целей
- Мера безопасности включает
  - Определение
  - Руководство по реализации
  - Дополнительная информация

Области контроля

- Политика безопасности (1)
- Организация информационной безопасности (2)
- Управление активами (2)
- Безопасность кадровых ресурсов (3)
- Физическая безопасность и безопасность окружения (2)
- Управление средствами связи и операциями (10)
- Контроль доступа (7)
- Приобретение, разработка и обслуживание информационных систем (6)
- Управление инцидентами с информационной безопасностью (2)
- Управление непрерывностью бизнес-процесса (1)
- Соответствие (3)

Основные термины

- Control - средства управления рисками, включая политики, процедуры, руководства, правила или организационные структуры, которые могут быть административного, технического, управленческого или юридического характера

  Синонимы – меры безопасности или контрмеры

ISO 27001/2 vs. PCI DSS

Хорошее соответствие

- Антивирусная защита (PCI DSS 5)

  ‘Защита от вредоносного и мобильного кода’ (ISO 27002 10.4)

- Резервирование (PCI DSS 9.5)

  ‘Резервирование’ (ISO 27002 10.5)

- Мониторинг доступа (PCI DSS 10)

  ‘Мониторинг’ (ISO 27002 10.10)

Хорошее соответствие

- Политика безопасности (PCI DSS 12.1)

  ‘Политика информационной безопасности’ (ISO 27002 5.1)

- Управление информацией и медиа-носителями (PCI DSS 3.1, 9.6-9.10)

  ‘Классификация информации’ (ISO 27002 7.2)

  ‘Управление медиа-носителями’ (ISO 27002 10.7)

- Политика контроля доступа (PCI DSS 7)

  ‘Бизнес-требования для контроля доступа’ (ISO 27002 11.1)

- Политики использования ресурсов (PCI DSS 12.2)

  ‘Приемлемое использование активов ’ (ISO 27002 7.1.3)

Хорошее соответствие

- Контроль изменений (PCI DSS 6.4)

  ‘Управление изменениями’ (ISO 27001 10.1.2)

  ‘Процедуры контроля изменениями’ (ISO 27001 12.5.1)

- Управление уязвимостями (PCI DSS 6.1, 6.2)

  ‘Меру управления техническими уязвимостями’ (ISO 27002 12.6.1)

- Операционные процедуры (PCI DSS 12.2)

  ‘Документированные операционные процедуры’ (ISO 27001 10.1.1)

Хорошее соответствие

- Ответственность за безопасность (PCI DSS 12.4, 12.5)

  ‘Внутренняя организация’ (ISO 27002 6.1)

- Защита персонала (PCI DSS 12.7)

  ‘Защита персонала’ (ISO 27002 8.1.2)

- Повышение осведомленности (PCI DSS 12.6)

  ‘Тренинги, обучение и повышение осведомленности по ИБ’ (ISO 27002 8.2.2)

- Управление инцидентами (PCI DSS 12.9)

  ‘Управление инцидентами ИБ’ (ISO 27002 13)

- Физическая безопасность (PCI DSS 9)

  ‘Защищенные зоны’ (ISO 27002 9.1)

Специфичные требования PCI DSS

- Конфигурация МСЭ (PCI DSS 1)
- Стандартизация системных компонентов (PCI DSS 2.2)
- Шифрование коммуникаций и систем хранения данных (PCI DSS 2.3, 3.4-3.6, 4.1)

  '*Криптографические меры*' (ISO 27002 12.3)
- Пароли и аутентификация пользователей (PCI DSS 8.5)

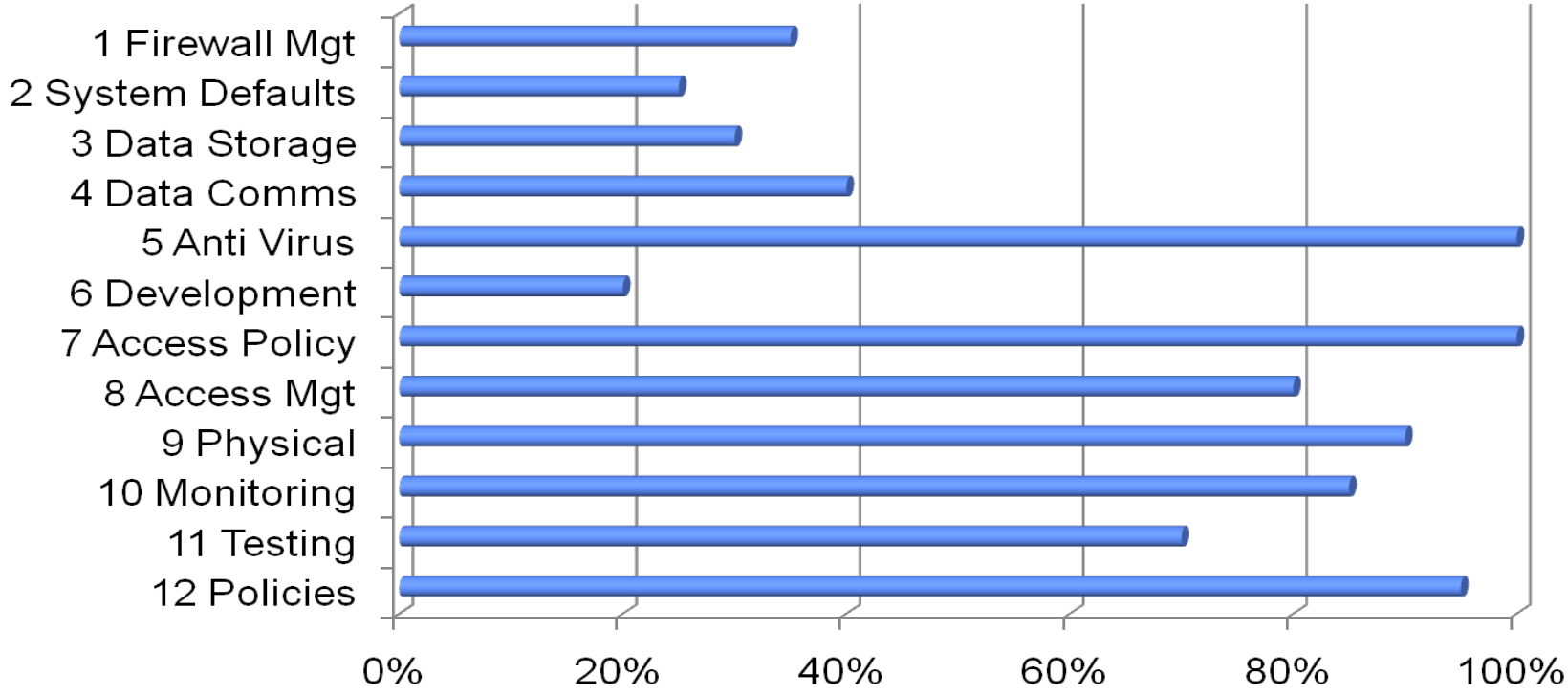
  '*Управление доступом пользователей*' (ISO 27002 11.2)

  '*Контроль доступа в ОС*' (ISO 27002 11.5)

Минимальное присутствие в ISO 27002

- Беспроводные сети (PCI DSS 2.1, 4.1,11.1)
- Мониторинг целостности файлов (PCI DSS 11.5)
- Разработка, тестирование и анализ программного кода (PCI DSS 6.5, 6.6)

Общий рейтинг соответствия



Можно ли сравнивать ISO и PCI?

- Могут ли ISO 27001/27002 использованы для демонстрации соответствия PCI DSS?

  Да, требования ISO 27001 покрывают требования PCI DSS для политик и оценки рисков

  Да, непрерывная поддержка соответствия похожа в обоих стандартах

  Да, многие требования PCI DSS идентичны мерам ISO 27001 / ISO 27002

  НО, требования PCI DSS более спечифичны и обязательны для выполнения

  И не все требования PCI DSS находят соответствие в ISO 27001 / ISO 27002

Выполнение требований PCI DSS с помощью Cisco Self-Defending Network

Продукты Cisco для соответствия PCI

Требование PCI	ASA	FWSM	ISR с IOS	NFP	WLAN	Catalyst	CSA	ACE
1) Установка и поддержка МСЭ для защиты данных	✓	✓	✓	✓	✓	✓	✓	✓
2) Не использовать заданные по умолчанию пароли и настройки	✓	✓	✓	✓	✓	✓	✓	✓
3) Защищать хранимые данные			✓				✓	
4) Шифровать данные, передаваемые по открытым каналам связи	✓		✓		✓			
5) Использовать и регулярно обновлять антивирус							✓	
6) Разрабатывать и поддерживать в защищенном состоянии системы и приложения								
7) Ограничивать доступ к данным	✓	✓	✓	✓	✓	✓	✓	✓
8) Аутентифицировать каждого пользователя с помощью уникального ID	✓	✓	✓	✓	✓			
9) Ограничивать физический доступ к информации								
10) Отслеживать весь доступ к информации о владельцах карт и к сетевым ресурсам	✓	✓	✓	✓	✓	✓	✓	✓
11) Регулярное тестирование систем и процессов			✓		✓			
12) Разработка и поддержка политики безопасности в актуальном состоянии								

Продукты Cisco для соответствия PCI

Требование PCI	IPS	IDSM	DDoS	IOS VPN	RVPN	IPSec SM	AnyConnect	VPN Client
1) Установка и поддержка МСЭ для защиты данных				✓	✓	✓		
2) Не использовать заданные по умолчанию пароли и настройки	✓	✓	✓	✓	✓	✓		
3) Защищать хранимые данные				✓	✓	✓	✓	✓
4) Шифровать данные, передаваемые по открытым каналам связи				✓	✓	v	✓	✓
5) Использовать и регулярно обновлять антивирус	✓	✓	✓					
6) Разрабатывать и поддерживать в защищенном состоянии системы и приложения								
7) Ограничивать доступ к данным							✓	✓
8) Аутентифицировать каждого пользователя с помощью уникального ID				✓	✓	✓	✓	✓
9) Ограничивать физический доступ к информации								
10) Отслеживать весь доступ к информации о владельцах карт и к сетевым ресурсам	✓	✓	✓	✓	✓	✓		
11) Регулярное тестирование систем и процессов	✓	✓	✓					
12) Разработка и поддержка политики безопасности в актуальном состоянии								

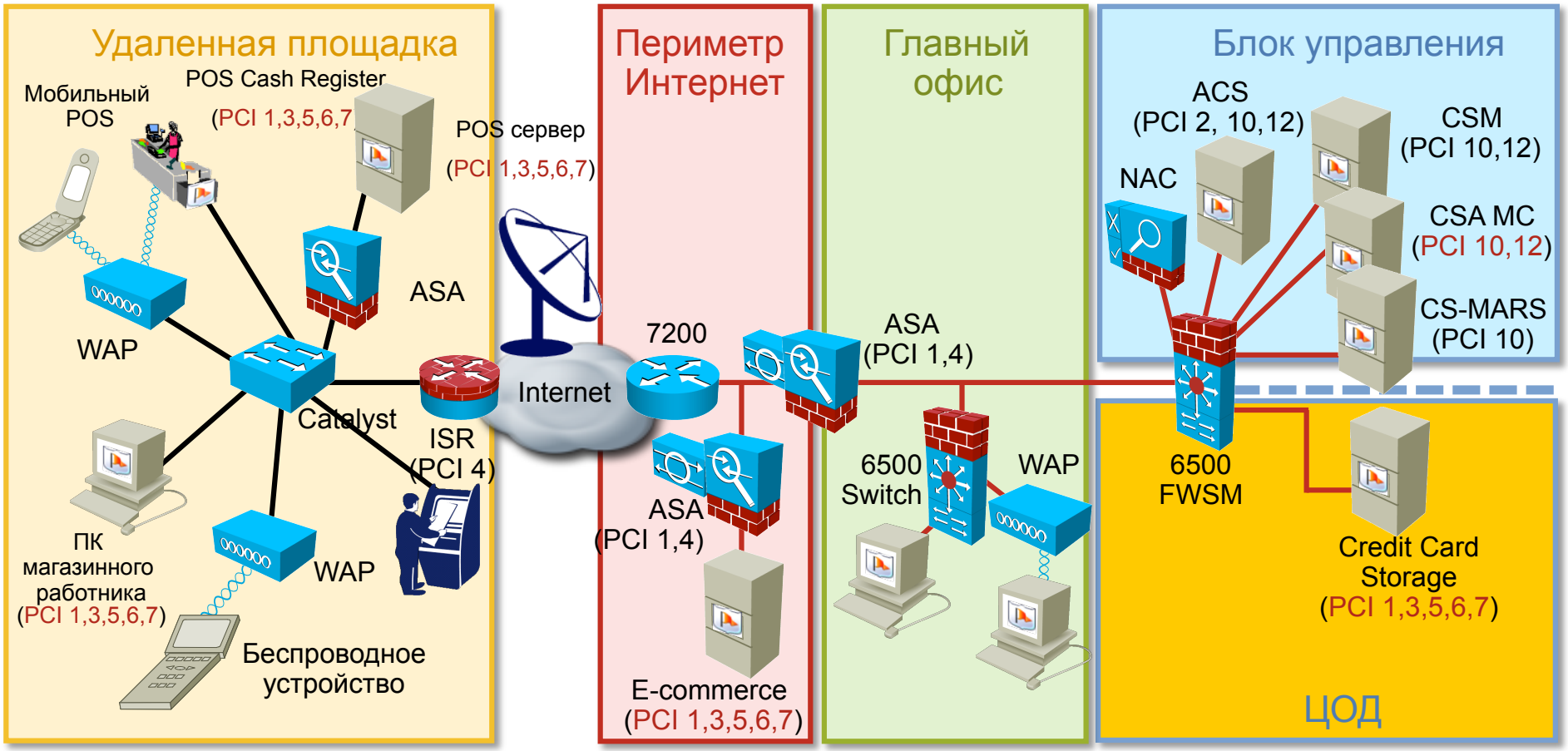
Продукты Cisco для соответствия PCI

Требование PCI	ESA	WSA	CSC	SCE	AON	AXG	NAC Appliance	NAC Guest Server
1) Установка и поддержка МСЭ для защиты данных					✓	✓		
2) Не использовать заданные по умолчанию пароли и настройки	✓	✓	✓	✓	✓	✓	✓	✓
3) Защищать хранимые данные					✓	✓		
4) Шифровать данные, передаваемые по открытым каналам связи	✓				✓			
5) Использовать и регулярно обновлять антивирус	✓	✓	✓	✓			✓	
6) Разрабатывать и поддерживать в защищенном состоянии системы и приложения							✓	
7) Ограничивать доступ к данным		✓		✓		✓	✓	✓
8) Аутентифицировать каждого пользователя с помощью уникального ID	✓				✓		✓	✓
9) Ограничивать физический доступ к информации								
10) Отслеживать весь доступ к информации о владельцах карт и к сетевым ресурсам	✓	✓	✓	✓	✓	✓	✓	✓
11) Регулярное тестирование систем и процессов								
12) Разработка и поддержка политики безопасности в актуальном состоянии								

Продукты Cisco для соответствия PCI

Требование PCI	CSM	MARS	ASDM	NCM	CAS	IntelliShield	ACS
1) Установка и поддержка МСЭ для защиты данных	✓	✓	✓	✓	✓		
2) Не использовать заданные по умолчанию пароли и настройки	✓	✓	✓	✓	✓	✓	✓
3) Защищать хранимые данные							
4) Шифровать данные, передаваемые по открытым каналам связи							
5) Использовать и регулярно обновлять антивирус			✓				
6) Разрабатывать и поддерживать в защищенном состоянии системы и приложения	✓			✓	✓	✓	
7) Ограничивать доступ к данным							✓
8) Аутентифицировать каждого пользователя с помощью уникального ID							✓
9) Ограничивать физический доступ к информации							
10) Отслеживать весь доступ к информации о владельцах карт и к сетевым ресурсам	✓	✓	✓	✓	✓		✓
11) Регулярное тестирование систем и процессов				✓	✓		
12) Разработка и поддержка политики безопасности в актуальном состоянии	✓	✓	✓	✓	✓		✓

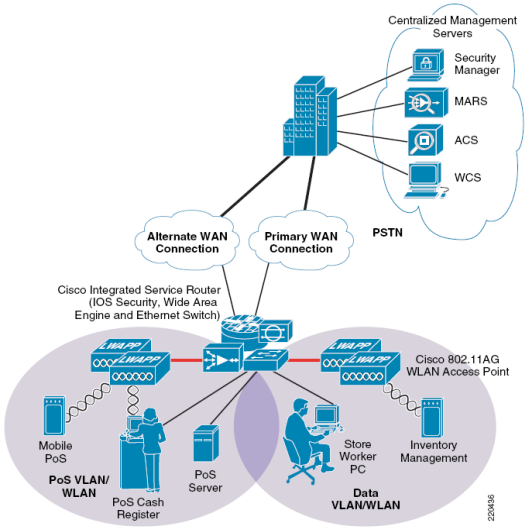
Решение Cisco для PCI DSS



Примечание! Отображена реализация не всех требований

Решение CVD для PCI

- Рекомендованная защищенная архитектура для проводных и беспроводных применений
- Тестирование в реальном окружении, включая POS-терминалы, сервера приложений, беспроводные устройства и системы защиты
- Систему управления конфигурацией, мониторингом и аутентификацией



Партнеры по «железу»:

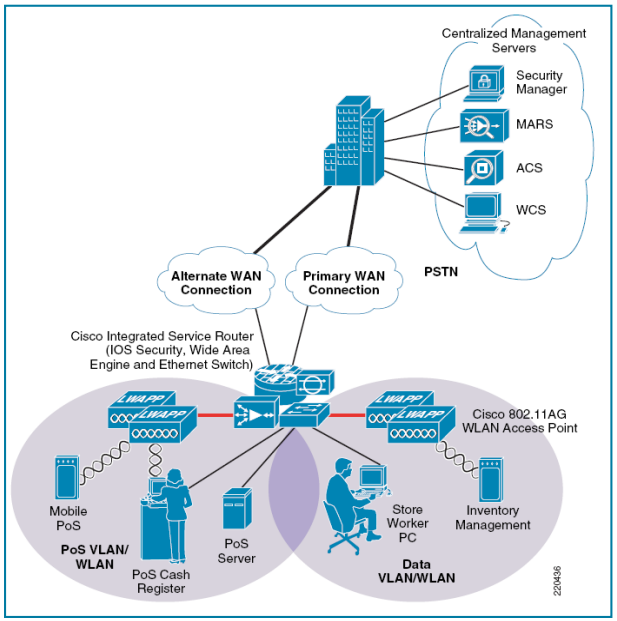
IBM

WINCOR NIXDORF

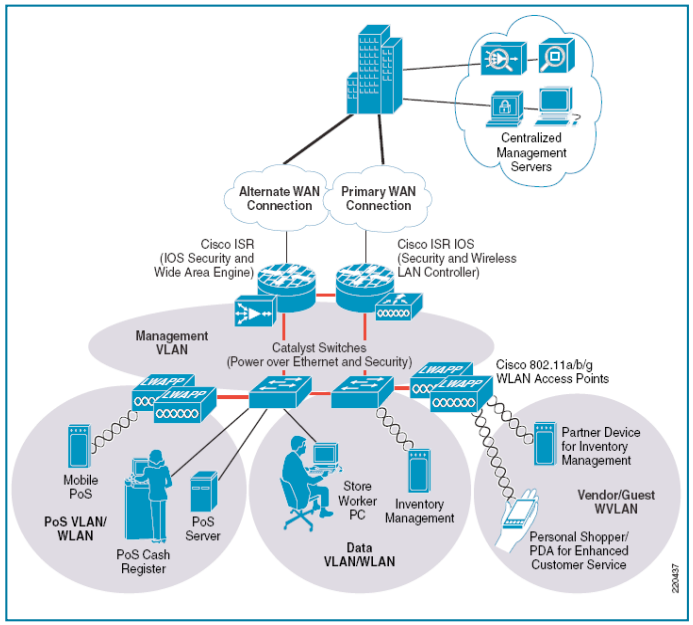
Intermec

Введение в решение CVD для PCI

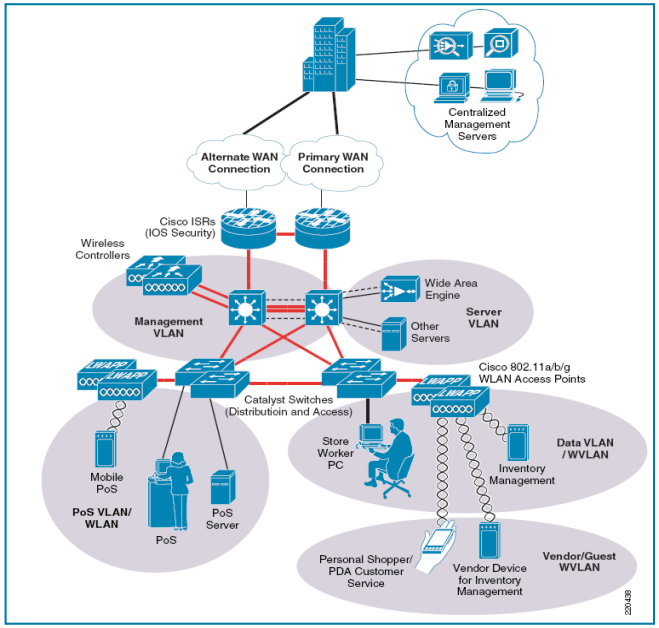
Малая



Средняя



Крупная



- Соответствующие PCI DSS 1.2 архитектуры в зависимости от масштаба предприятия
- Детальный отчет по соответствию
- Руководства по внедрению
- Детальные конфигурации

Пример решения

Требование PCI 1.3.5

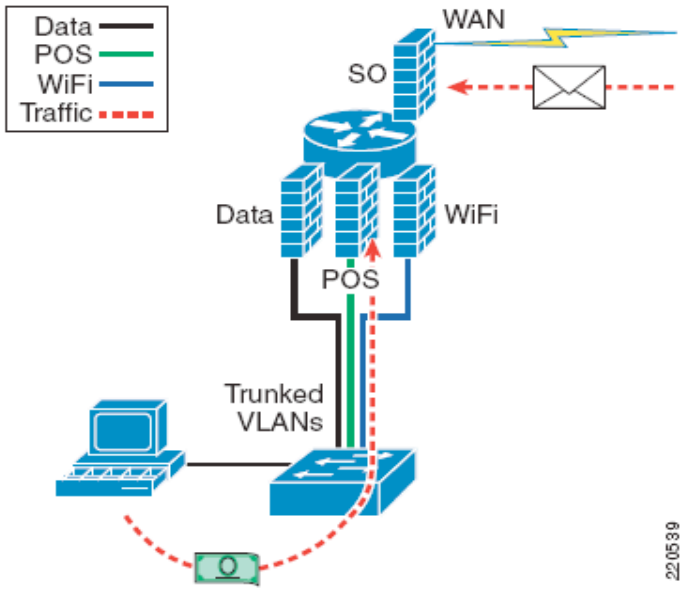
Рекомендации Cisco

Restricting outbound traffic to that which is necessary for the cardholder data environment.

The routers are configured to filter and inspect all traffic inbound from each network segment. Through extensive interview and discussion with the QSA, filtering all inbound network traffic to the router was determined to be an acceptable implementation. This effectively restricts the outbound traffic, and is a common practice in many retailer networks. (See Figure 3-1.)

Иллюстрации обеспечивают ясность

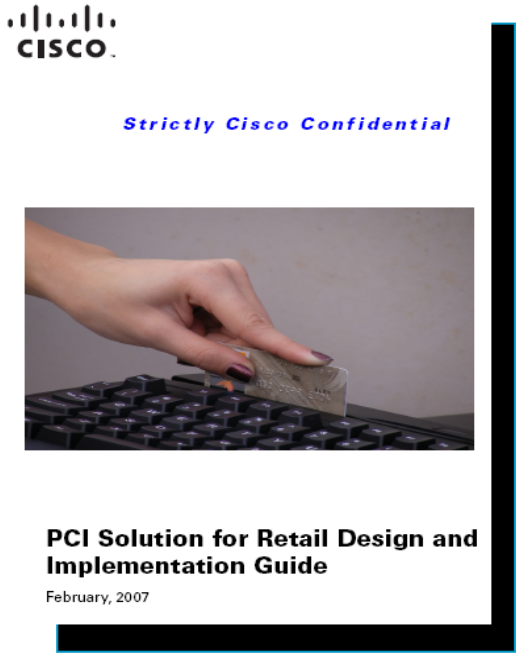
Figure 3-1 Restricting Outbound Traffic



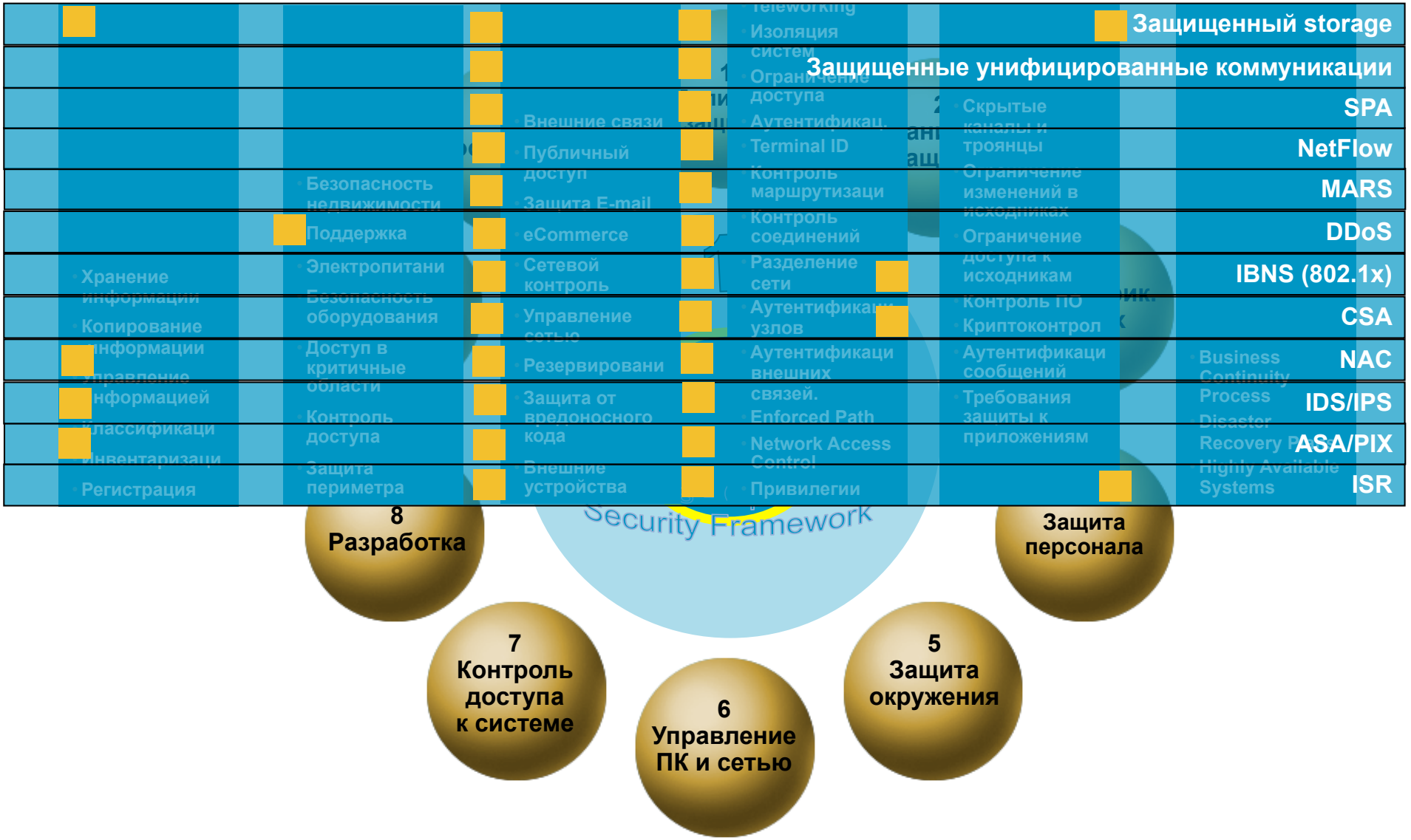
Пример конфигурации

The following is a sample configuration:

```
RLRG-1#
!
interface GigabitEthernet0/0.11
description POINT OF SALE NETWORK
ip access-group CSM_FW_ACL_GigabitEthernet0/0.11 in
ip inspect CSM_INSPECT_1 in
!
```



ISO 17799 и решения Cisco



Как пройти самооценку или подготовиться к аудиту?

Пример требований - PCI DSS

PCI DSS Стандарт защиты информации в индустрии платежных карт	Перечень требований для повышения уровня безопасности в индустрии платежных карт. разработанный международными платежными системами Visa и MasterCard. Поддерживается AmEx, Diners Club, Discover, JCB. Содержит 12 основных требований, 200+ детальных требований
Пример требований	Требование 2.1: Не использовать значения по умолчанию для паролей и других параметров безопасности
Как может быть достигнуто?	Проверка конфигурации на использование стандартных значений ‘public’, ‘private’, ‘cisco’ в SNMP; ‘cisco’, ‘cisco123’, ‘sdm’ для доступа через WEB (например, SDM)

Что значит процесс контроля для служб ИТ и ИБ?

- Постоянный сбор
  - Инвентарной информации
  - Конфигурации устройств
  - Проверка характеристик функционирования устройств
- Проверка характеристик функционирования устройств
- Средства управления должны обеспечивать
  - Сбор
  - Проверку данных
  - Отчетность
  - Ежедневно, в постоянном режиме

Много людей останавливаются на этом этапе

Результаты аудитов сетей

47% изменений не авторизованы или неучтены

60% простоев сетей связаны с человеческими ошибками

Какие решения предлагает Cisco?

- CiscoWorks Network Compliance Manager (NCM)
  - Поддержка разных производителей
  - Поставляется с настройками для некоторых стандартов, в т.ч. PCI DSS
- EMC VoyenceControl
  - Альтернатива NCM
- CiscoWorks LAN Management Solution (LMS)
  - Решение часто уже установлено у пользователей
  - Может выполнять простые функции контроля файлов конфигурации

Обзор Network Compliance Manager

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

Контроль и управление конфигурацией и изменениями

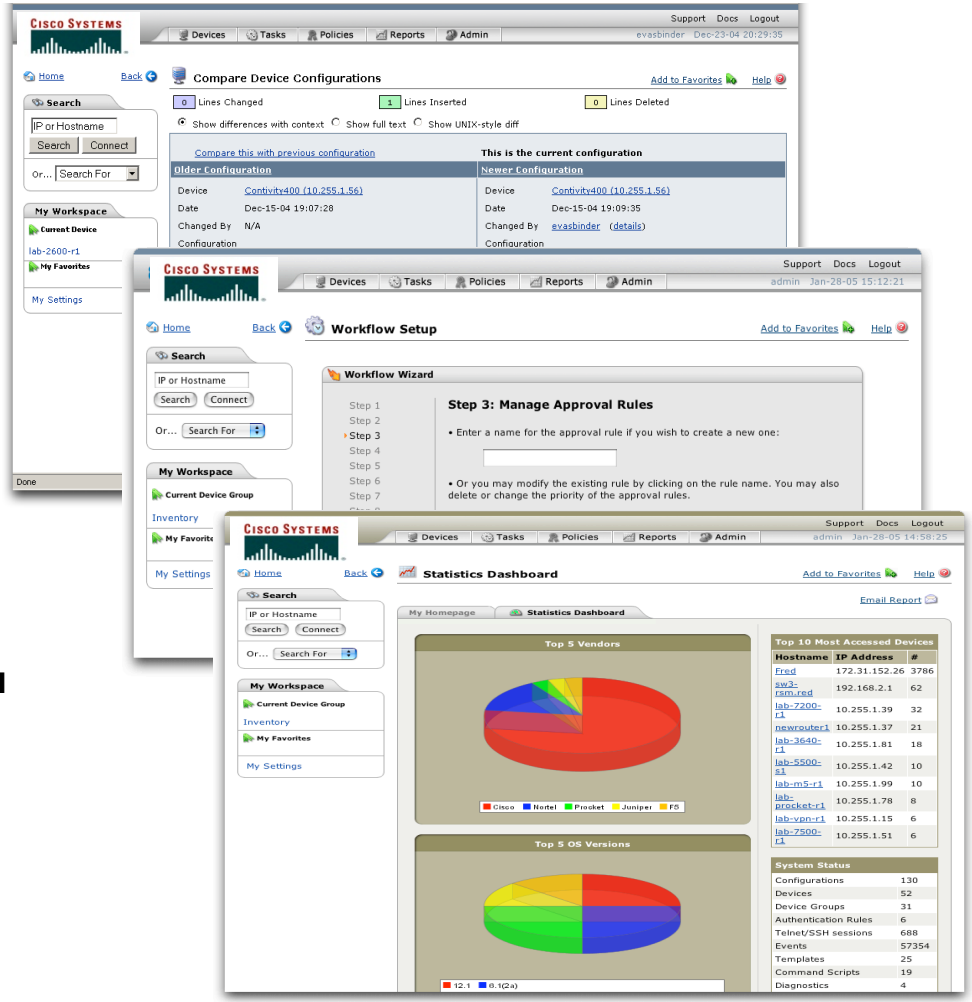
- Контроль изменений в реальном времени
- Контроль непротиворечивости
- Применение политик
- Аутентификация через RADIUS, LDAP, Secure ID, TACACS или Active Directory

Аудит и проверка соответствия

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

Расширенная генерация отчетов

- Статус сети
- Рекомендации по приведению в соответствие



Цели NCM

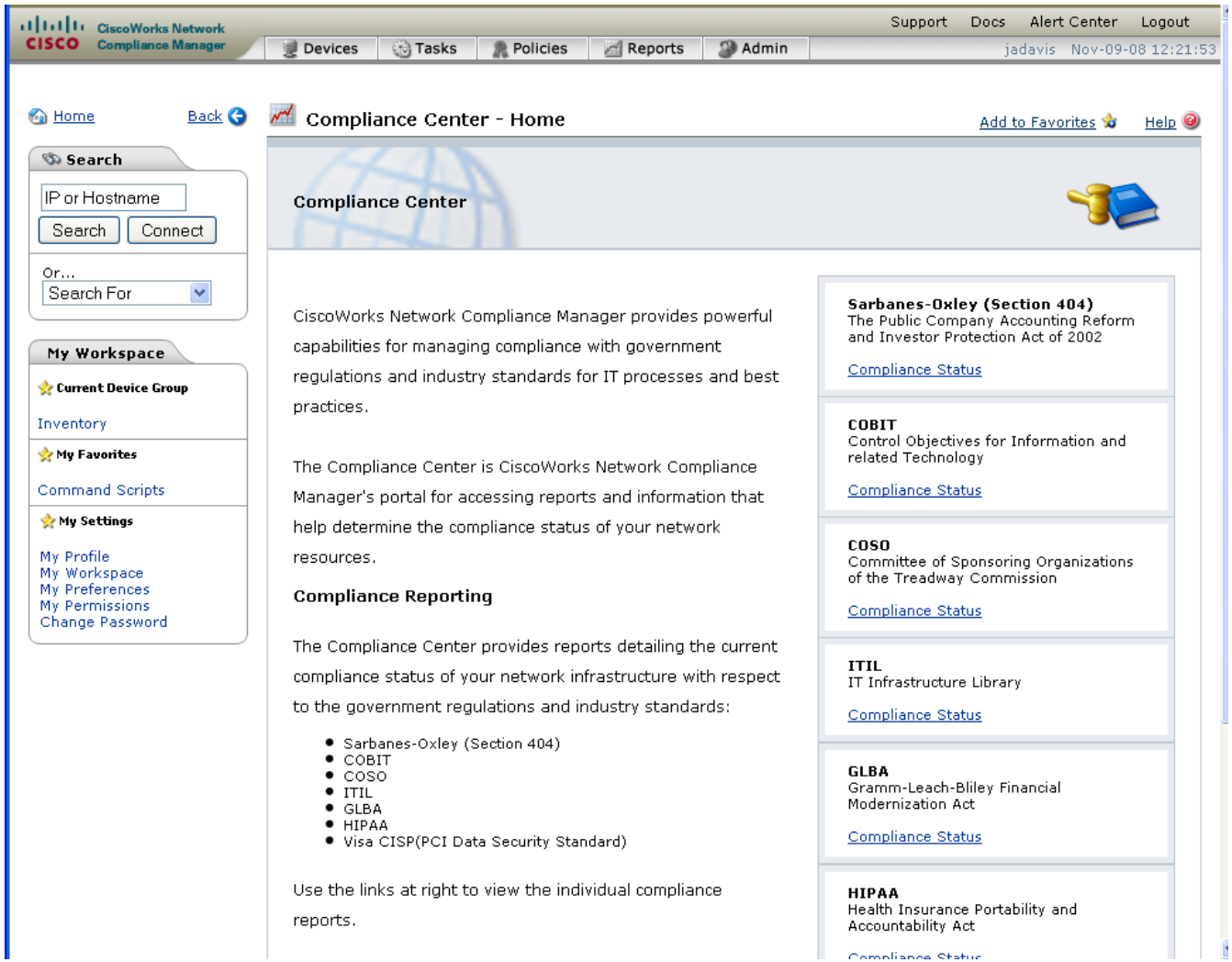
Преимущества NCM

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%**

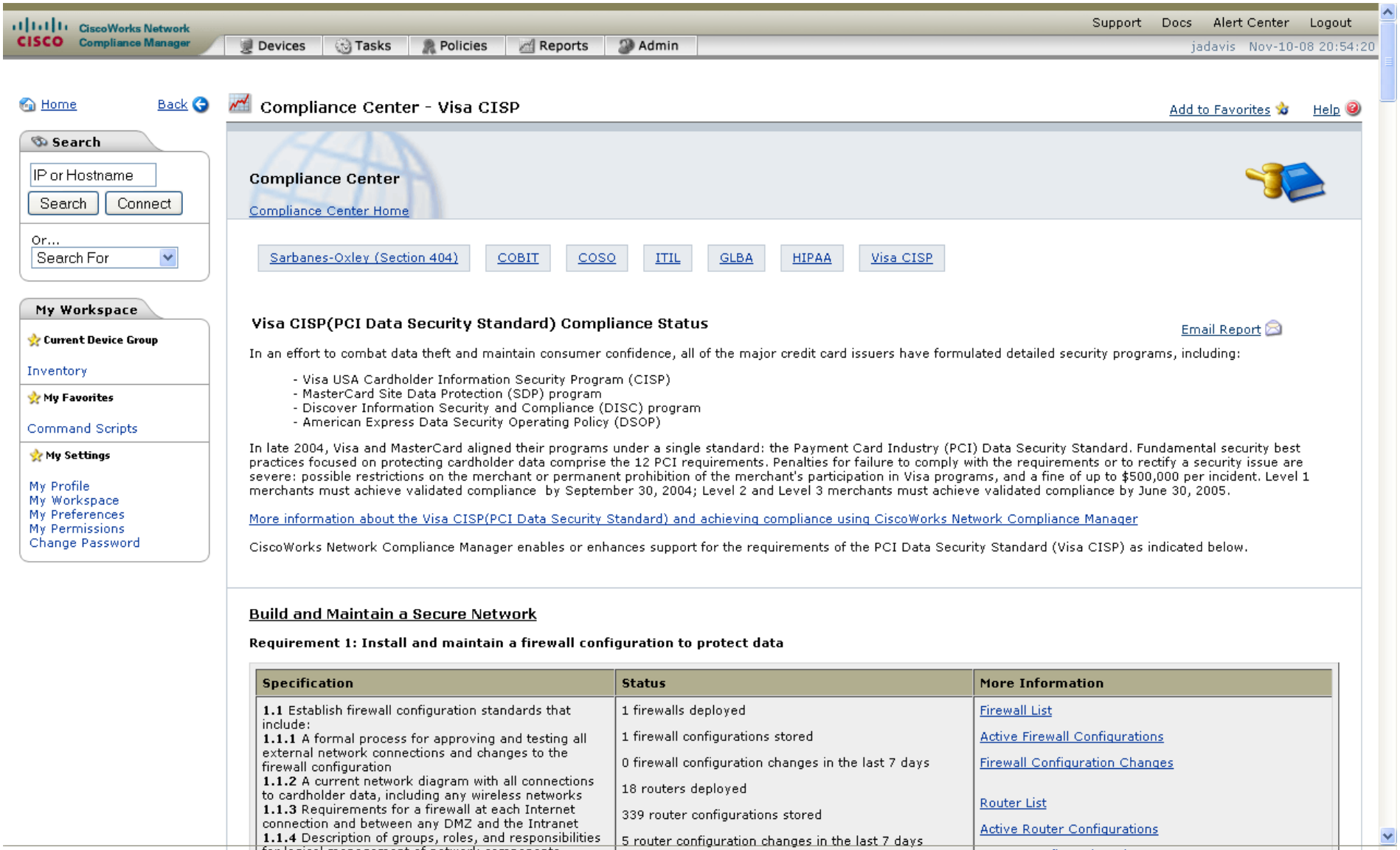
Источник: 2005 EMA Survey и отзывы пользователей

Обзор NCM

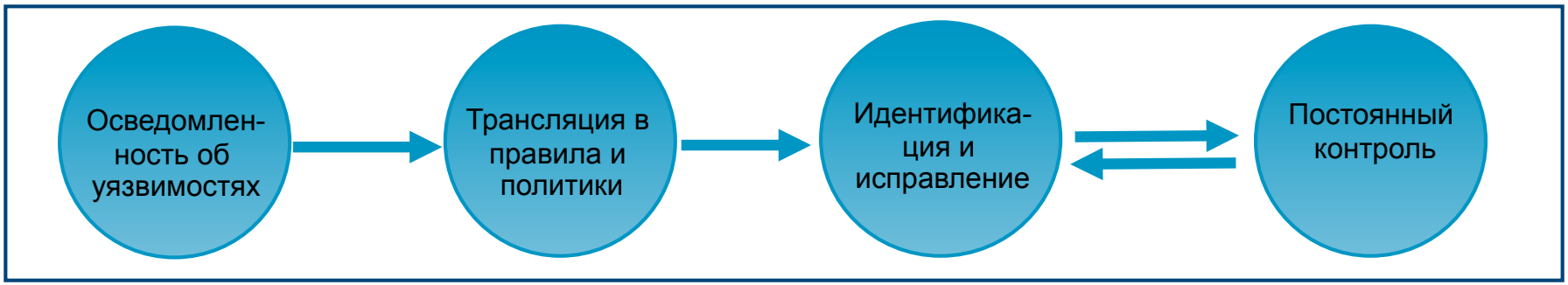
NCM предоставляет готовую отчетность по ряду стандартов



Как только устройство добавлено в систему и по нему получена конфигурация, информация по нему автоматически попадает в отчет.
Вам необходимо нажать одну кнопку...


CiscoWorks Network Compliance Manager
Devices
Tasks
Policies
Reports
Admin
Support
Docs
Alert Center
Logout
jadavis Nov-10-08 20:54:20
Home
Back
Compliance Center - Visa CISP
Add to Favorites
Help
Search
IP or Hostname
Search
Connect
Or...
Search For
My Workspace
Current Device Group
Inventory
My Favorites
Command Scripts
My Settings
My Profile
My Workspace
My Preferences
My Permissions
Change Password
Compliance Center
Compliance Center Home
Sarbanes-Oxley (Section 404)
COBIT
COSO
ITIL
GLBA
HIPAA
Visa CISP
Visa CISP(PCI Data Security Standard) Compliance Status
Email Report
In an effort to combat data theft and maintain consumer confidence, all of the major credit card issuers have formulated detailed security programs, including:
- Visa USA Cardholder Information Security Program (CISP)
- MasterCard Site Data Protection (SDP) program
- Discover Information Security and Compliance (DISC) program
- American Express Data Security Operating Policy (DSOP)
In late 2004, Visa and MasterCard aligned their programs under a single standard: the Payment Card Industry (PCI) Data Security Standard. Fundamental security best practices focused on protecting cardholder data comprise the 12 PCI requirements. Penalties for failure to comply with the requirements or to rectify a security issue are severe: possible restrictions on the merchant or permanent prohibition of the merchant's participation in Visa programs, and a fine of up to $500,000 per incident. Level 1 merchants must achieve validated compliance by September 30, 2004; Level 2 and Level 3 merchants must achieve validated compliance by June 30, 2005.
More information about the Visa CISP(PCI Data Security Standard) and achieving compliance using CiscoWorks Network Compliance Manager
CiscoWorks Network Compliance Manager enables or enhances support for the requirements of the PCI Data Security Standard (Visa CISP) as indicated below.
Build and Maintain a Secure Network
Requirement 1: Install and maintain a firewall configuration to protect data
Specification
Status
More Information
1.1 Establish firewall configuration standards that include:
1.1.1 A formal process for approving and testing all external network connections and changes to the firewall configuration
1.1.2 A current network diagram with all connections to cardholder data, including any wireless networks
1.1.3 Requirements for a firewall at each Internet connection and between any DMZ and the Intranet
1.1.4 Description of groups, roles, and responsibilities for logical management of network components
1.1.5 Documented list of services/ports necessary for business
1.1.6 Justification and documentation for any available protocols besides HTTP and SSL, SSH, and VPN
1.1.7 Justification and documentation for any risky protocols allowed (FTP, etc.), which includes reason for use of protocol and security features implemented
1.1.8 Periodic review of firewall/router rule sets
1.1.9 Configuration standards for routers
1 firewalls deployed
1 firewall configurations stored
0 firewall configuration changes in the last 7 days
18 routers deployed
339 router configurations stored
5 router configuration changes in the last 7 days
16 configuration policies in place
59 violations of NSA Router Security Best Practices policy in last 7 days
0 approved firewall changes in the last 7 days
0 unapproved firewall changes in the last 7 days
Firewall List
Active Firewall Configurations
Firewall Configuration Changes
Router List
Active Router Configurations
Router Configuration Changes
Configuration Policies
NSA Router Security Best Practices Violation Events
Approved Firewall Changes
Unapproved Firewall Changes
1.2 Build a firewall configuration that denies all traffic from "untrusted" networks/hosts, except for:
1.2.1 Web protocols - HTTP (port 80) and Secure Sockets Layer (SSL) (typically port 443)
1.2.2 System administration protocols (e.g., Secure
0 firewalls in configuration policy non-compliance
0 firewall configuration non-compliance events in the last 7 days
Non-Compliant Firewalls
Firewall Non-Compliant Events

NCM Alert Center



Автоматическое получение данных об уязвимостях	Получение готовых политик	Быстрый поиск и исправление проблемы	Автоматическое извещение о проблемах
Ответственные люди получают данные своевременно	▪ Данные об уязвимостях получаются в виде готовых политик ▪ Пользователь может выбрать политики, которые должны работать на сети	▪ Автоматический поиск всех устройств с уязвимостями и вывод отчета ▪ NCM обеспечит исправление проблемы	Извещение о появлении новых проблем или новых устройств, установленных на сети со старыми проблемами

CiscoWorks LMS или NCM?

- NCM частично пересекается с LMS по функционалу в приложении RME (инвентарные данные, управление конфигурациями и ПО)
- Преимущества NCM:

  Поддержка 30+ производителей – CiscoWorks работает только с оборудованием Cisco

  Масштабирование – архитектура NCM позволяет работать с гораздо большими сетями

  Отчетность – в стандартной поставки предоставляются готовые отчеты по PCI DSS, ITIL, COBIT ...

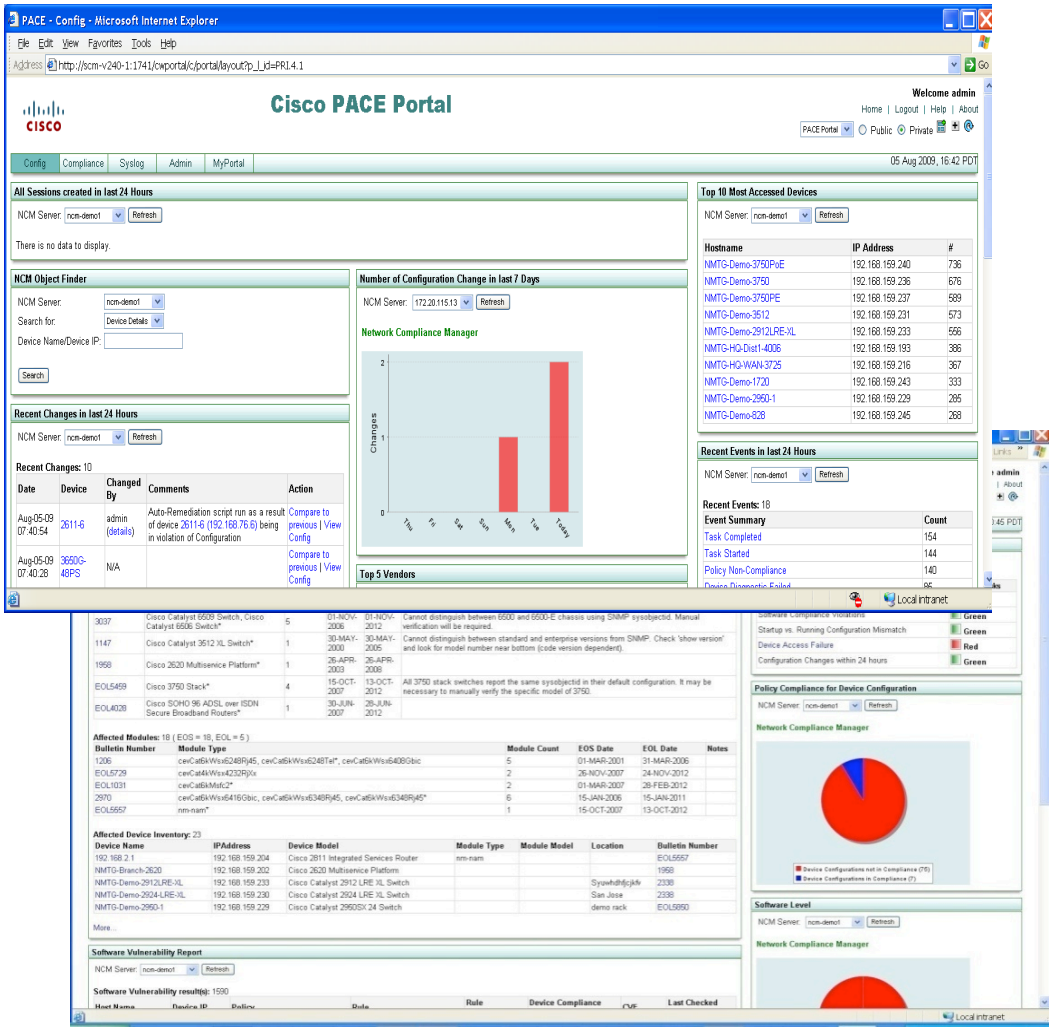
  Workflow – возможность создания алгоритмов согласования изменений

  API – гибкие возможности по интеграции (SOAP, PERL, другие)

- Решения дополняют друг друга в PACE

Обзор PACE 2.0

- PACE Portal – единая точка получения данных с
  - CiscoWorks LMS
  - Network Compliance Manager
  - QoS Policy Manager
  - Cisco Network Collector
- Поставляется бесплатно в составе NCM
- Услуги Cisco AS – опциональная часть PACE



Заключение

Ресурсы Cisco

- Cisco PCI Compliance Advisor

  http://www.ciscowebtools.com/pcicomplianceadvisor/

- WP “PCI Compliance Using the Cisco SDN”
- Retail PCI Architectures

  http://www.cisco.com/go/retail (на английском языке)

- Ресурсы Cisco

  http://www.cisco.com/go/compliance (на английском языке)

  http://www.cisco.com/go/security (на английском языке

Внешние ресурсы

- PCI Security Standards Council
  http://www.pcisecuritystandards.org
- American Express
  http://www.americanexpress.com/datasecurity
- MasterCard
  http://www.mastercard.com/sdp
- Discover
  http://www.discovernetwork.com/resources/data/data_security.html
- JCB
  http://www.jcb-global.com/english/pci/index.html
- Visa Europe и США
  http://www.visaeurope.com/aboutvisa/security/main.jsp
  http://usa.visa.com/merchants/risk_management/cisp.html
  http://corporate.visa.com/pd/security/main.jsp

Вопросы?

Дополнительные вопросы Вы можете задать по электронной почте security-request@cisco.com
или по телефону: +38 044 391-3600