Сеть без границ

Что движет современной ИБ

Алексей Лукацкий

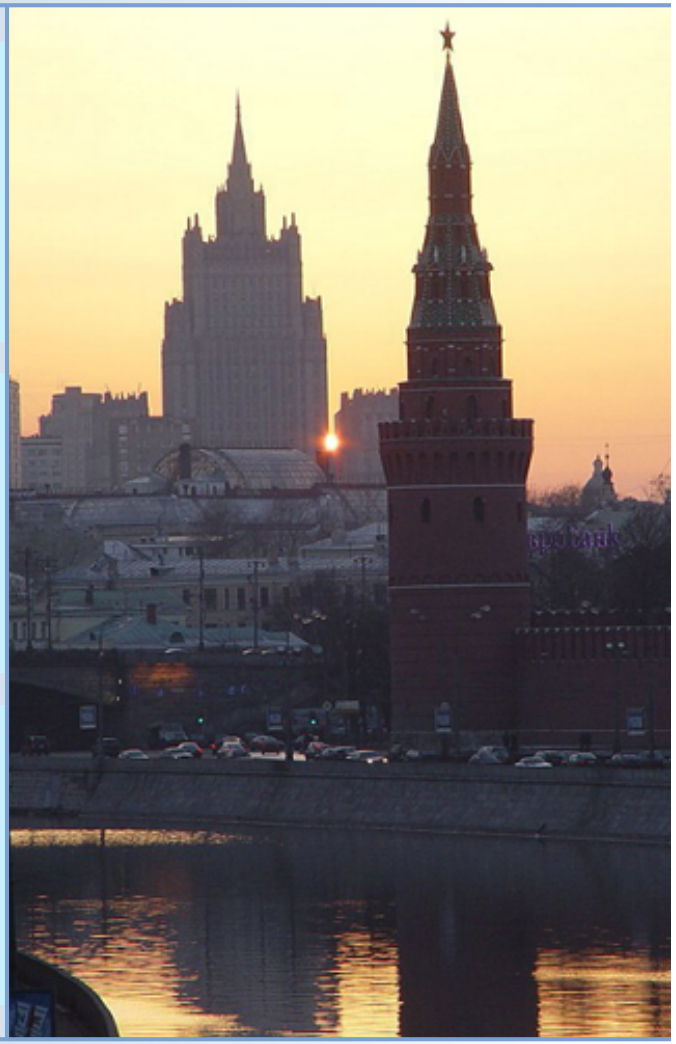
Бизнес-консультант по безопасности

О чем пойдет речь?

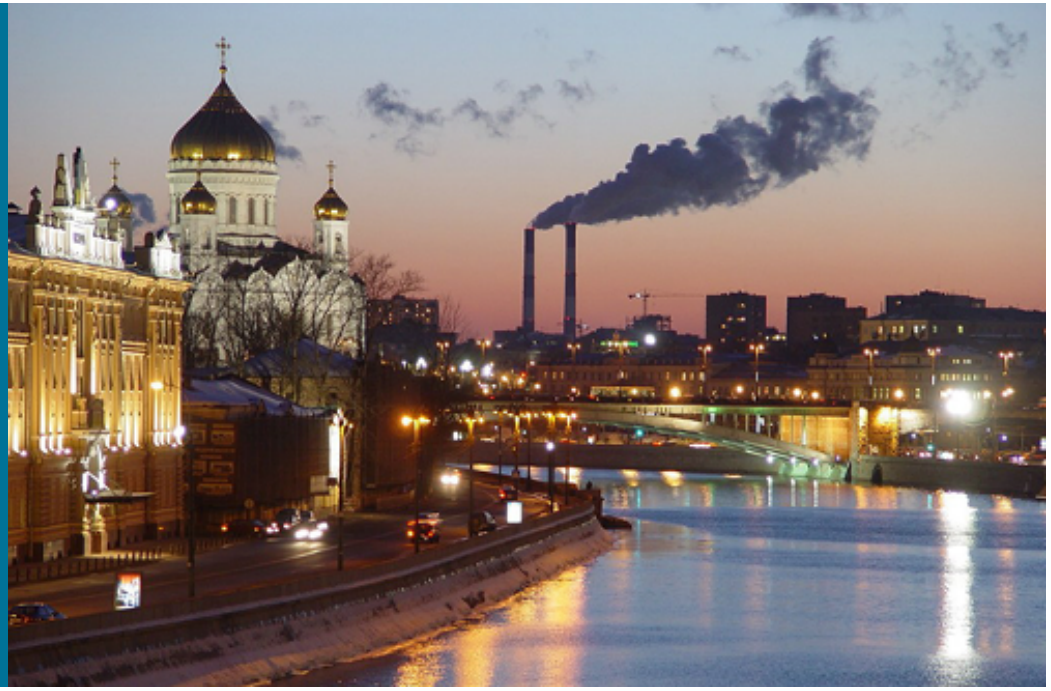
Тенденции угроз, бизнеса, регуляторов и ИТ

Сеть без границ (Borderless Network)

Дополнительная информация



Что движет безопасностью?



Угрозы

- Угрозы носят заказной и криминальный характер
- Угрозы и криминалитет становятся быстрее, умнее & неуловимее
- Точечные (даже лучшие в своем классе) решения не справляются в одиночку с ростом угроз
- Заказчики не могут защищать свои ресурсы в режиме 24x7

ИТ и ИБ

Мобильность и пользователи

Взаимодействие

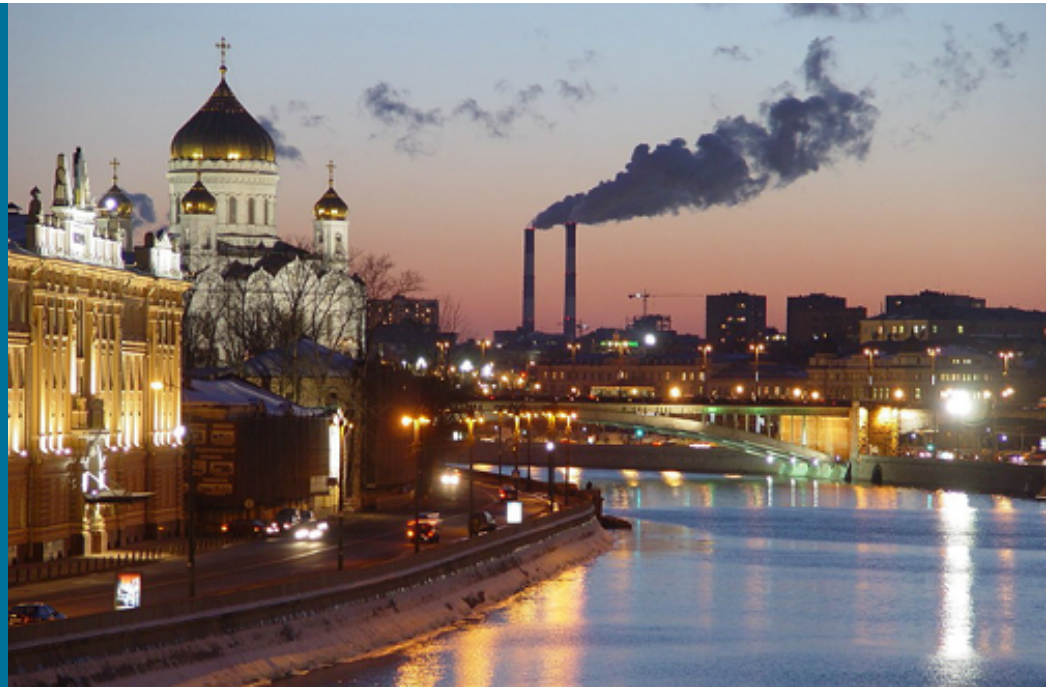
Виртуализация

Соответствие

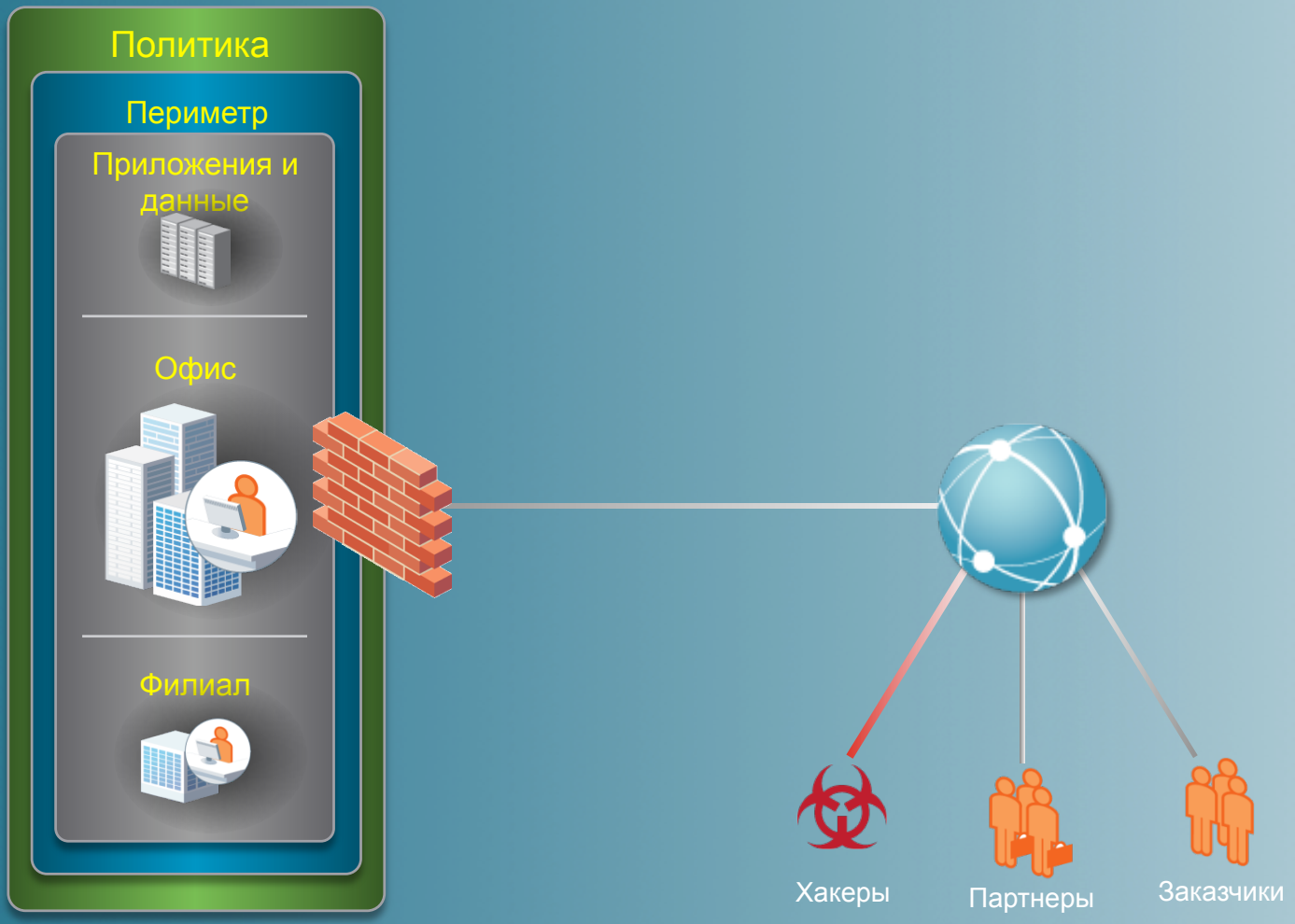
Интересы бизнеса

- Рост (доли рынка, маржинальности, доходности…)
- Экспансия (новые рынки, новые целевые аудитории)
- Рост продуктивности сотрудников
- Соответствие требованиям
- Инновации и новые бизнес-практики
- Реинжиниринг бизнес-процессов
- Взаимоотношения с клиентами (лояльность)
- …

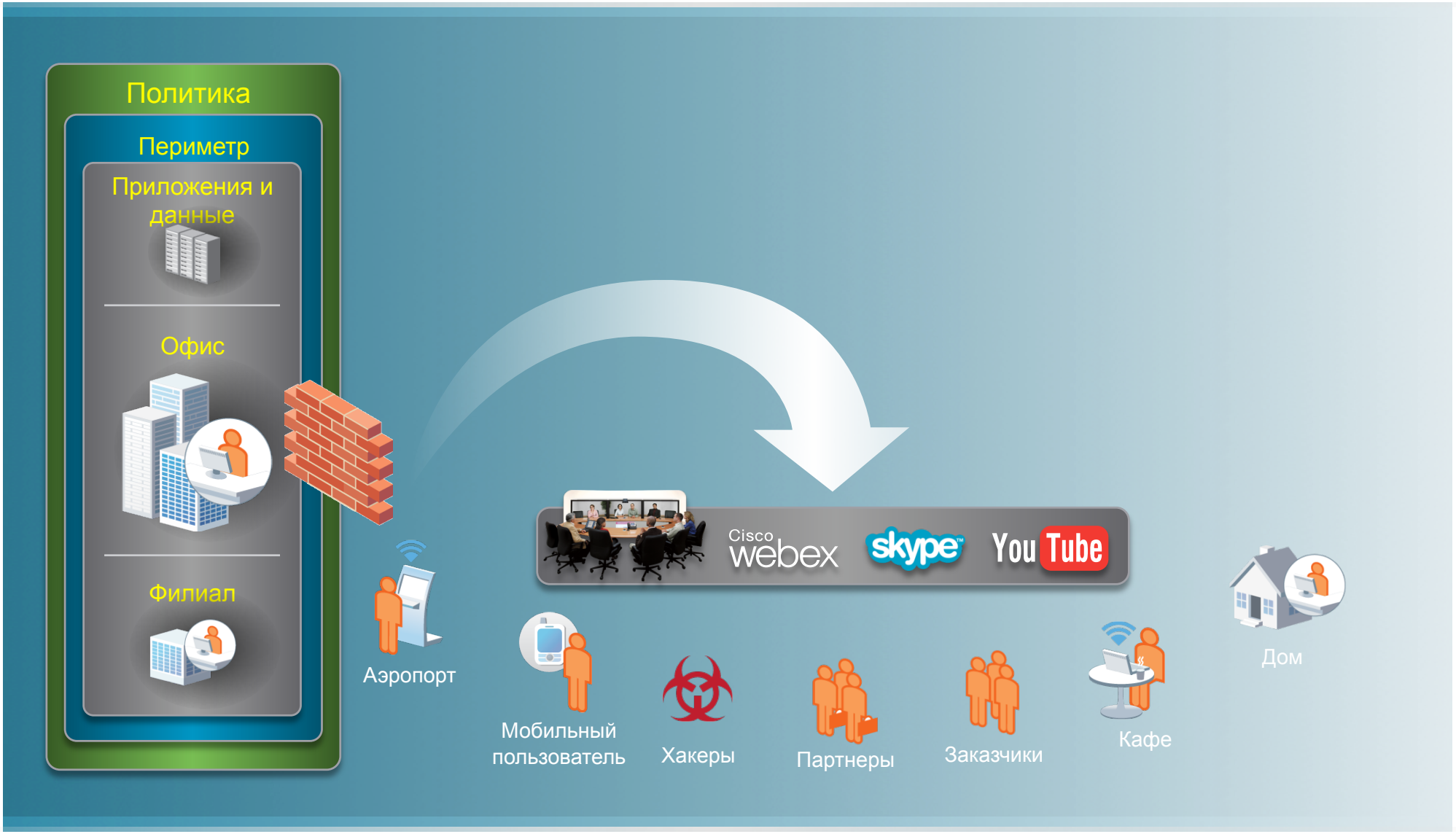
Сеть без границ
Эволюция подходаCisco



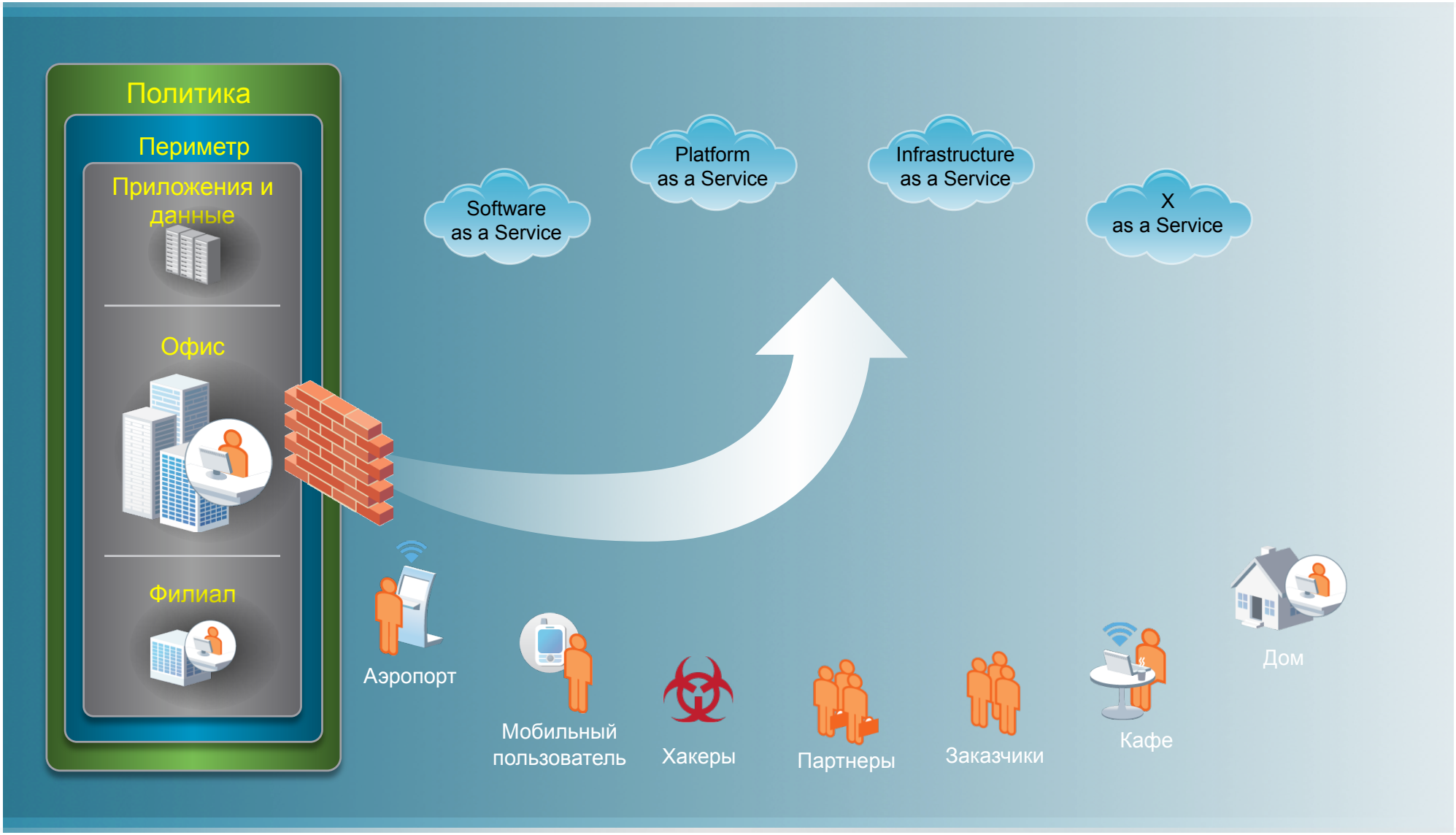
Традиционный периметр



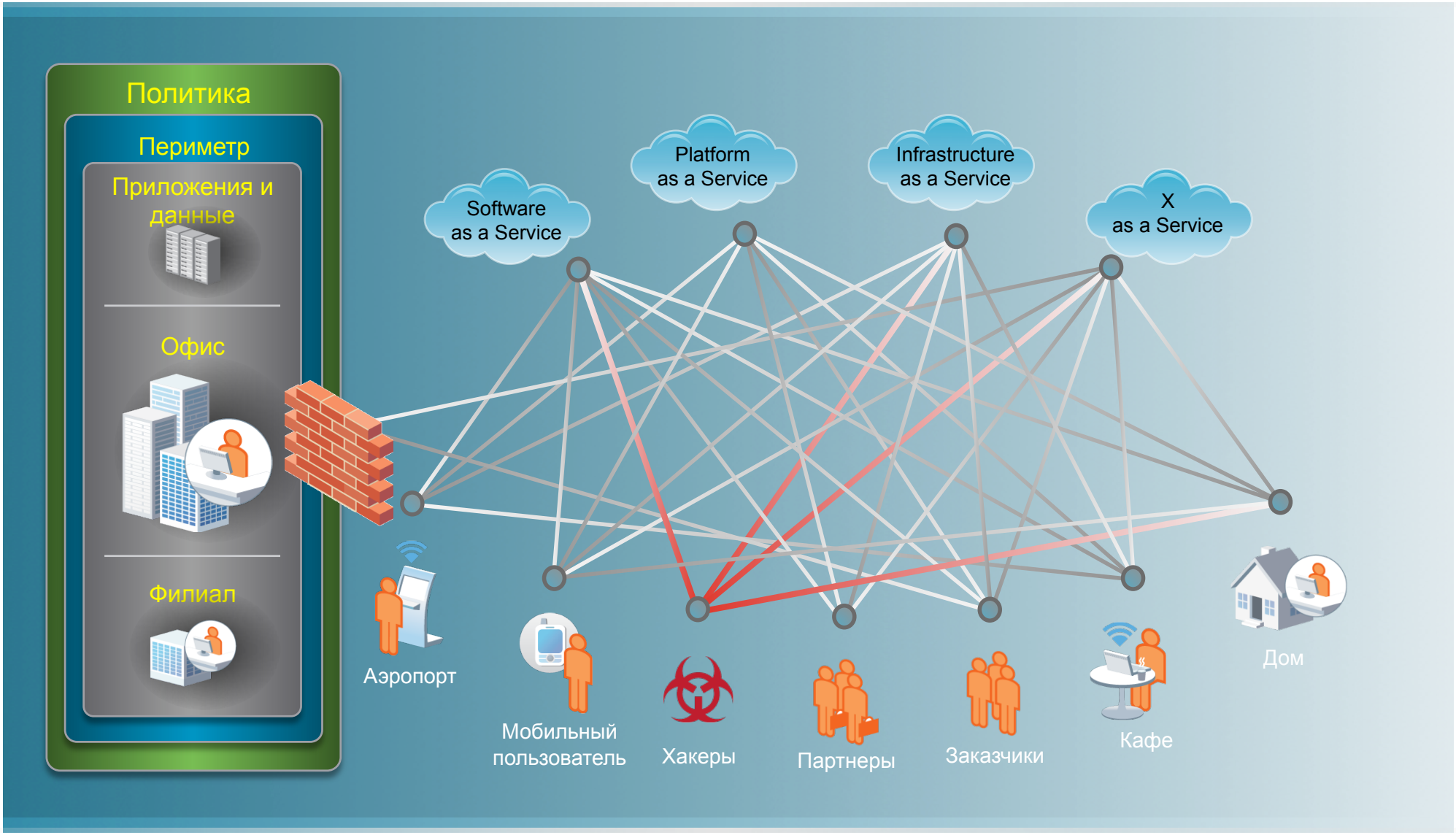
Мобильность и взаимодействие растворяют Интернет-периметр



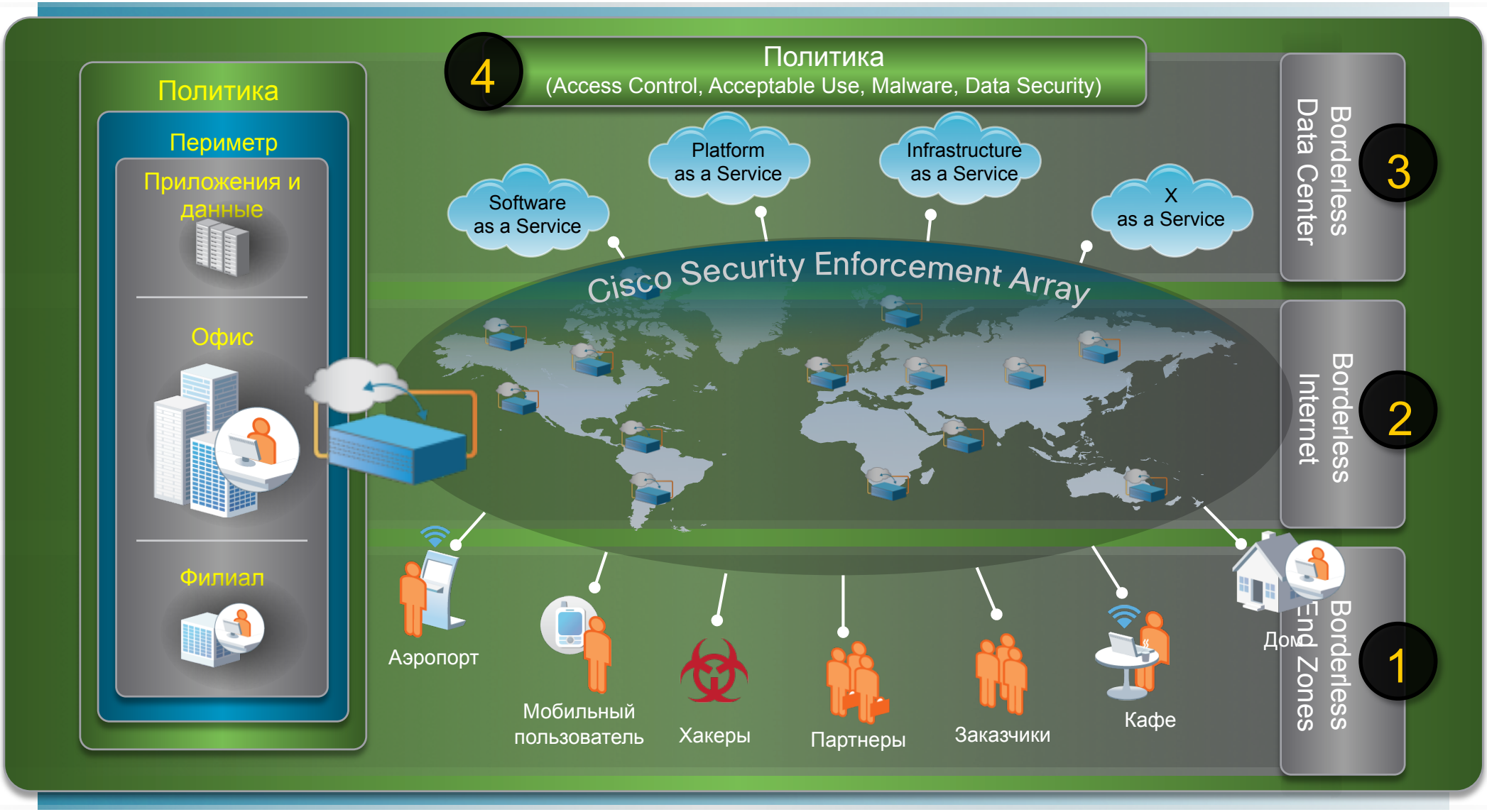
Cloud Computing растворяет границу ЦОД



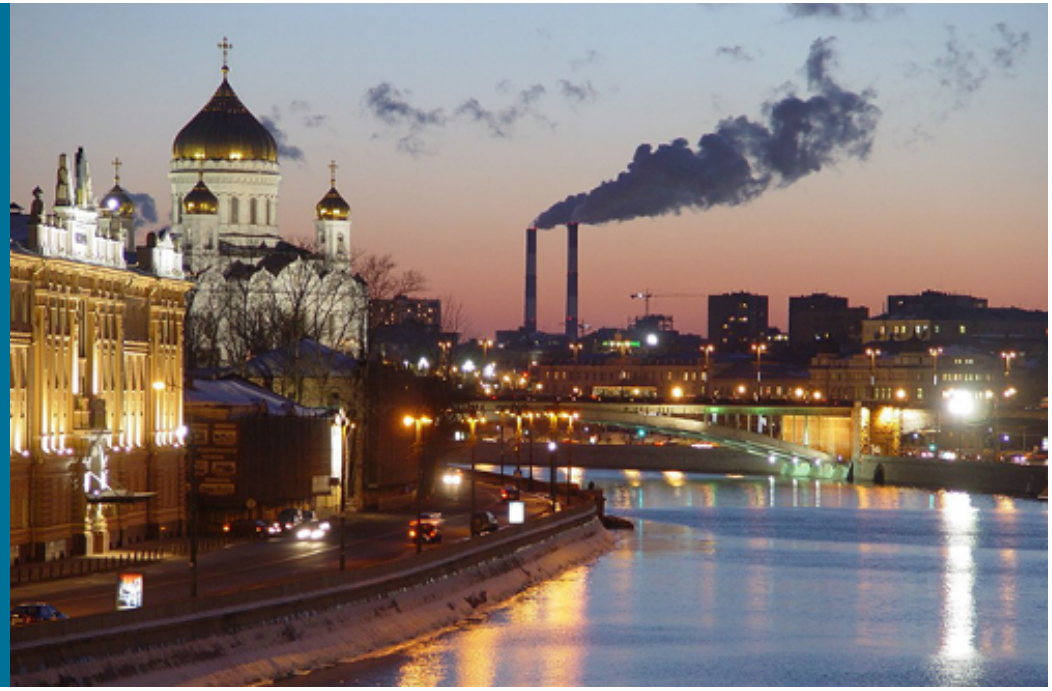
Пользователи хотят вести бизнес без границ



Концепция Cisco: сеть без границ



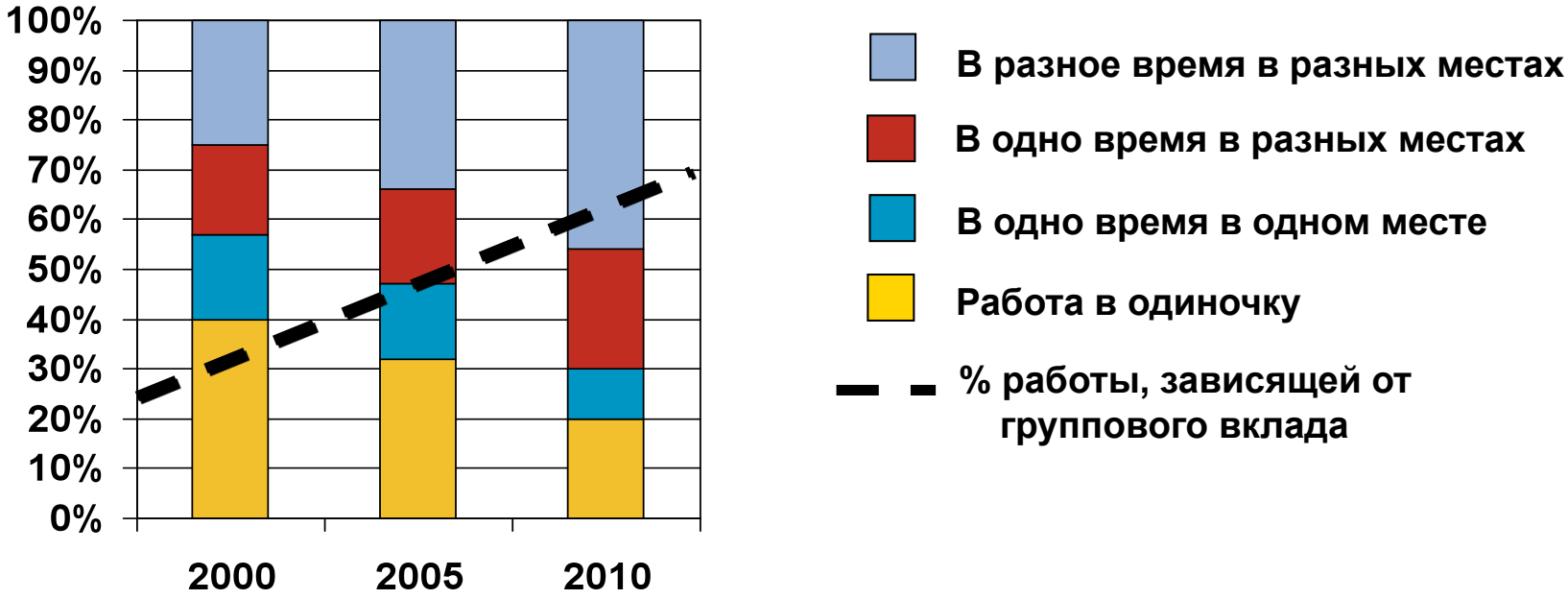
Один из сценариев
Удаленный доступ



Работа происходит везде

- В ДОРОГЕ
  (отели, аэропорты, бизнес-центры)
  - 280 миллионов бизнес-поездок в год
  - Спад производительности >60–65%
- ДОМА (teleworking)
  - 137 миллионов надомных работников в 2003г.
  - 40% надомных работников в США из крупных компаний и среднего бизнеса
- НА РАБОТЕ
  (филиалы, отделения, партнеры)
  - E-business требует быстрых сетей
  - Филиал должен быть там где люди

Трансформация бизнеса



- Сотрудничество – драйвер роста
- Взаимодействие с другими, но не лицом к лицу
- Рост продуктивности невозможен без поддержки этой тенденции

Элемент 1: Borderless End Zone

Умная маршрутизация трафика оконечных устройств

Широкое покрытие

Большинство ОС и протоколов

Windows Mobile

Apple iPhone

Постоянное соединение

Всегда на связи, определение места

Автоматическое определение Head-End

IPsec , SSL VPN, DTLS

Расширенная безопасность

Строгая аутентификация

Быстрая, надежная защита

Контроль политики

Мобильный Интернет

Новый большой виток вычислений

Мейнфрейм
Вычиления
1950-х

Мини
Вычисления
1960-х

ПК
Вычисления
1980-х

Интернет+ПК
Вычисления
1990-х

Мобильный Интернет
Вычисления
2000-х

Всеобщая мобилизация

- Пользователи (особенно руководство) хотят получать доступ к корпоративным ресурсам даже с мобильных устройств
- Пользователи хотят выбирать мобильные устройства самостоятельно
- Спектр выбираемых устройств очень широк

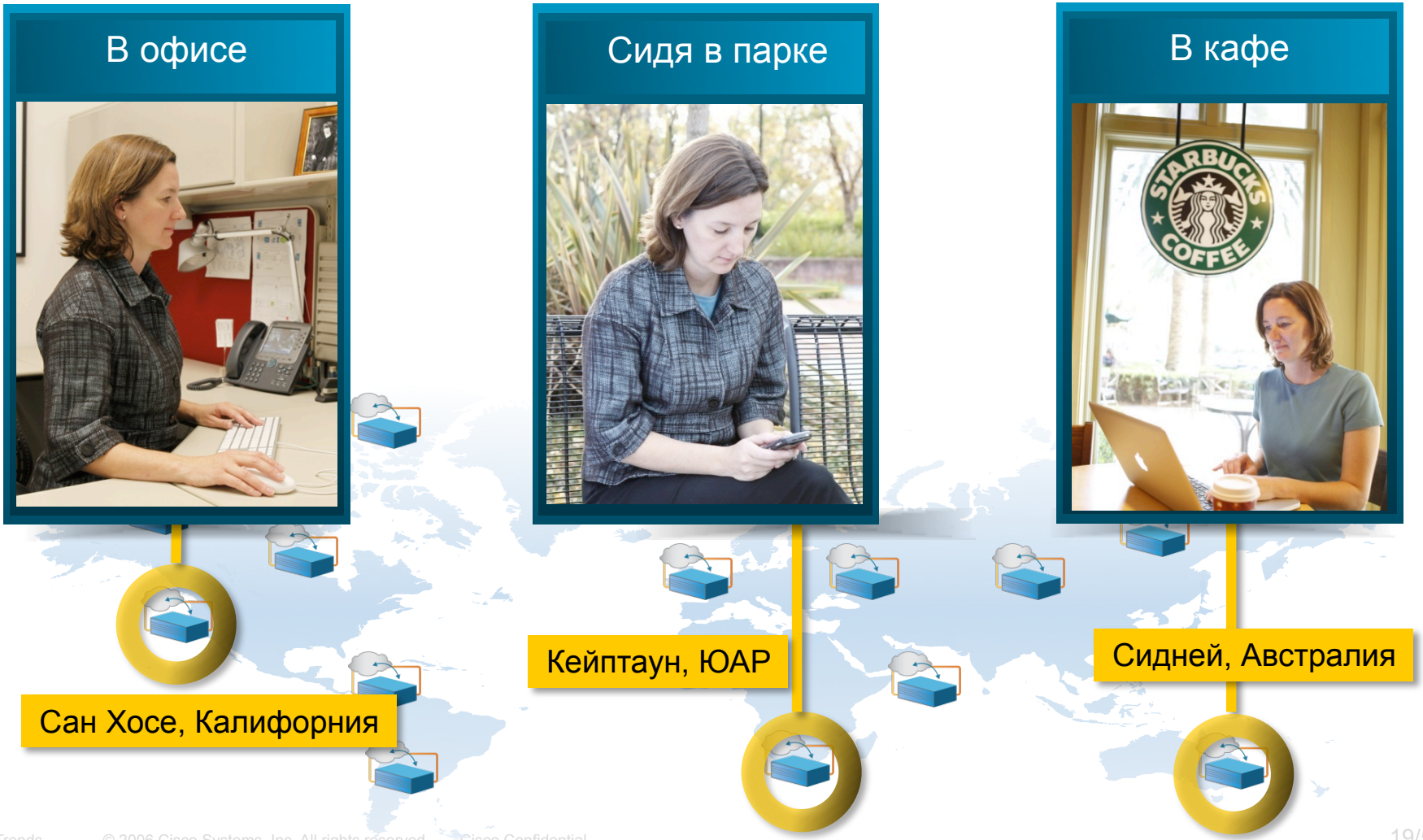
  ОС: iPhone, Windows Mobile, Symbian, BlackBerry

  Платформа: iPhone, Nokia, HTC, LG, Samsung, BlackBerry

- Адекватных средств защиты для мобильных устройств не так много

Вы там, где офис ⇔ офис там, где Вы?

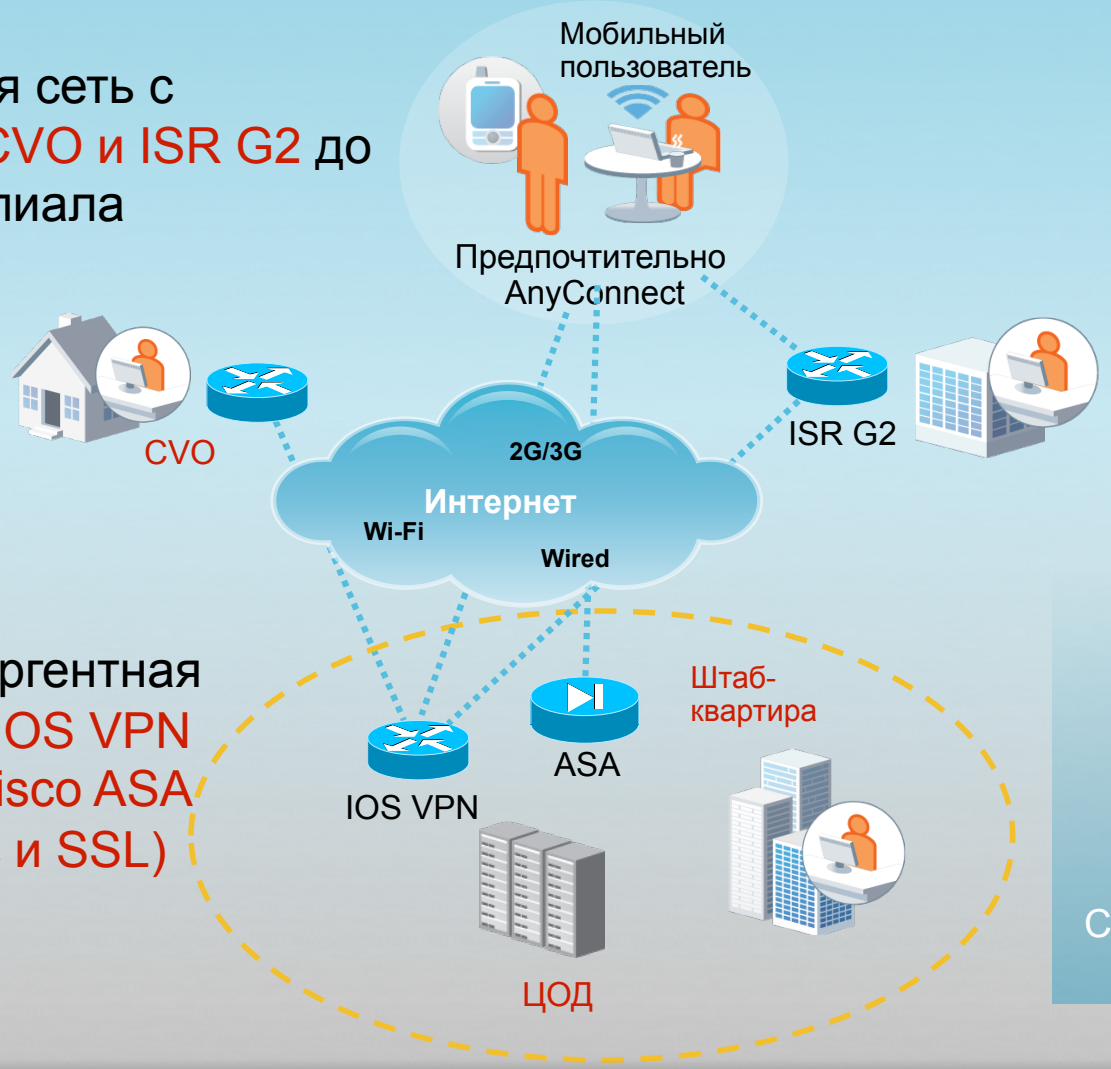
Всегда под защитой



Решение Cisco Virtual Office

Оптимальный сценарий удаленного доступа

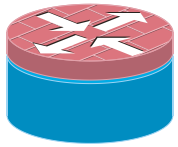
Доверенная сеть с помощью CVO и ISR G2 до дома и филиала



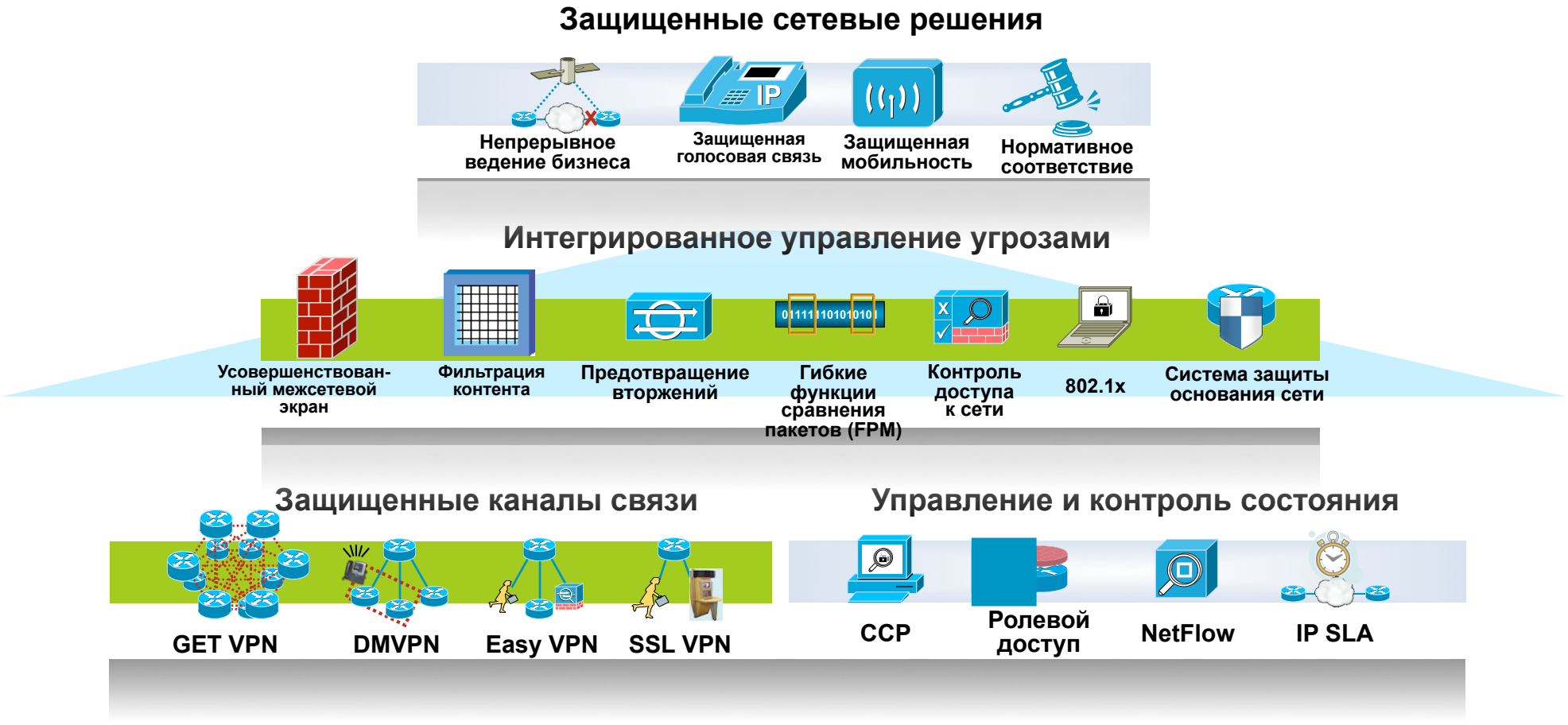
CVO = Cisco Virtual Office

Хороший маршрутизатор хорошей компании

Что еще нужно чтобы встретить старость ;-)

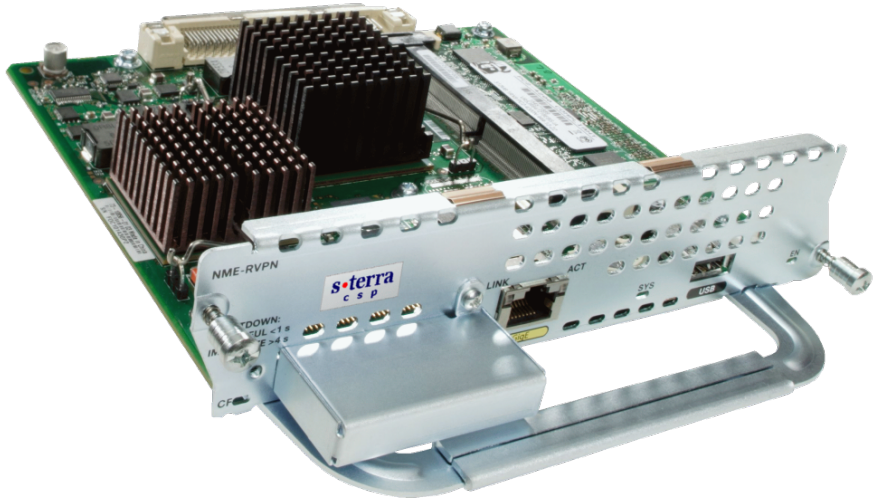


Cisco ISR G2



Cisco и Криптон / УСС

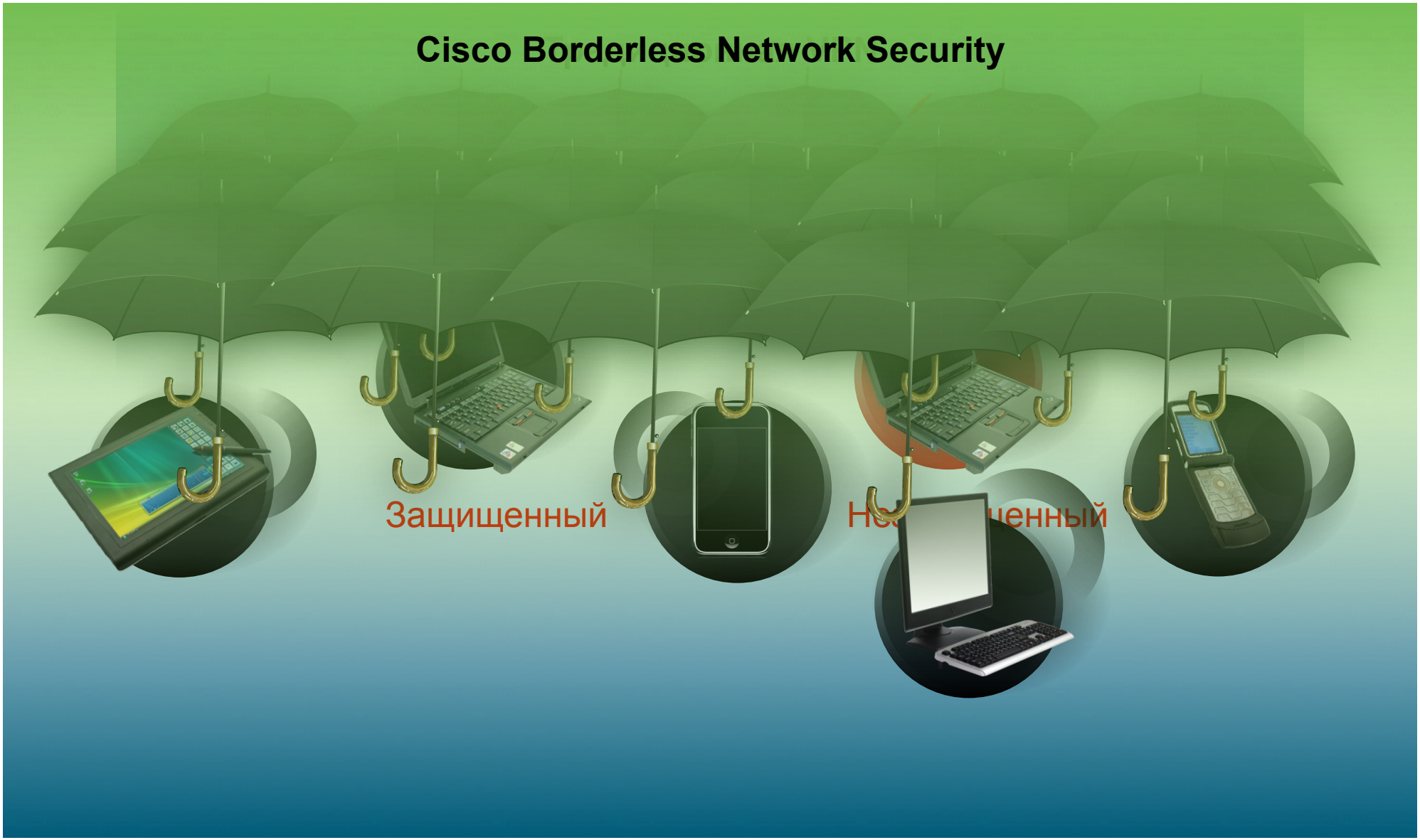
- Компаниями Cisco Systems, ООО НВФ «Криптон» и ГП «Украинские специальные системы» разработан VPN-модуль NME-UVPN, поддерживающий национальные криптоалгоритмы
  - Поддержка Cisco ISR 2800, 2900, 3800 и 3900



Cisco + Лаборатория Касперского

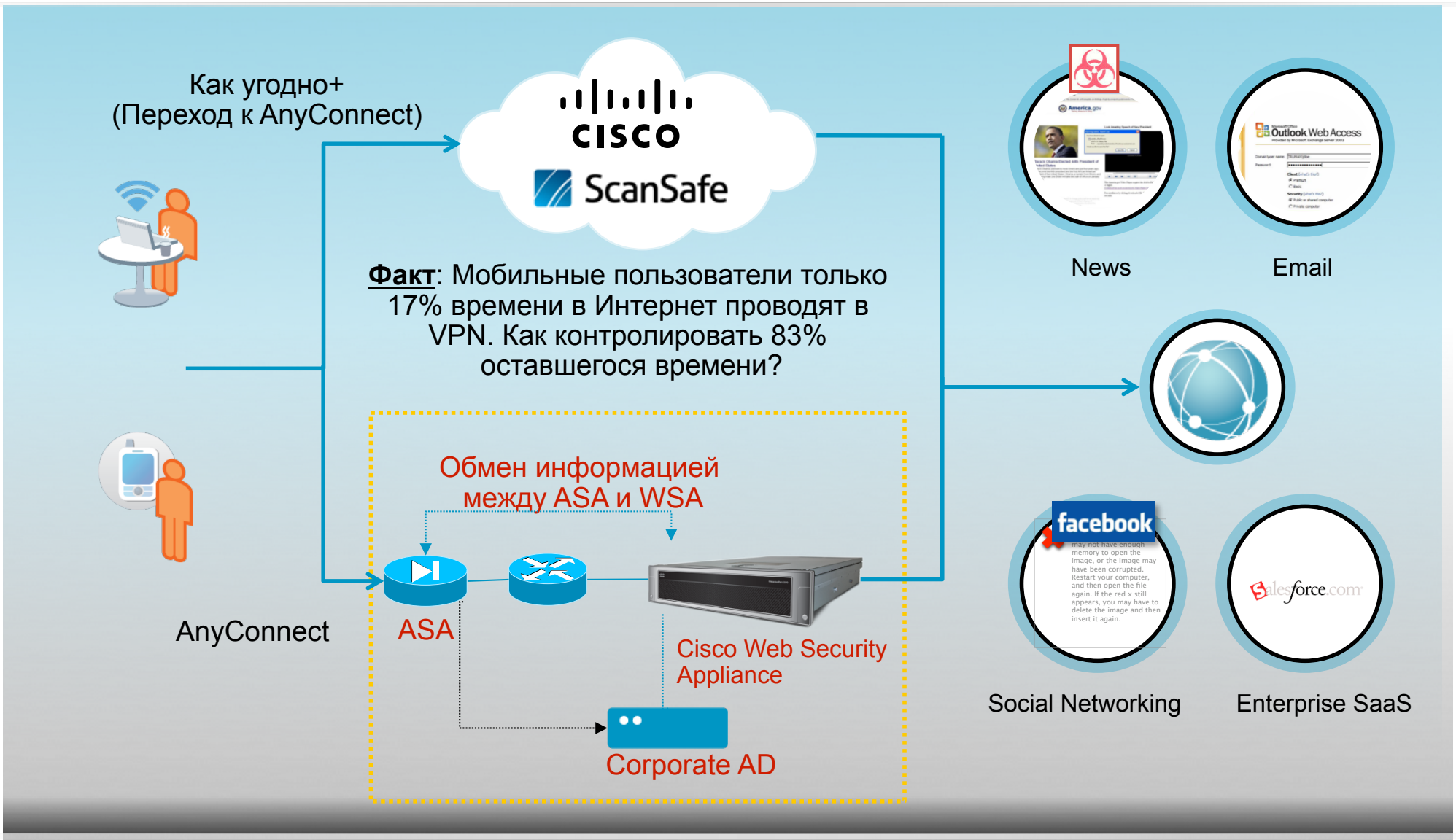
- Компаниями Cisco Systems и Лабораторией Касперского создан модуль «антивирус + антиспам» для маршрутизаторов Cisco
  - Поддержка маршрутизаторов Cisco ISR 1800, 1900, 2800, 2900, 3800, 3900, а также 800 Series
- Форм-фактор
  - AXP-NME
  - AXP-AIM

Всегда под защитой



Защита мобильных пользователей

Выбор реализации: облако или на предприятии



Облачная безопасность Cisco

Ядро ScanSafe

- 1 млрд. Web-запросов в день
  - 28M уникальных JavaScript в день
  - 560K уникальных PDF в день
  - 244 уникальных ShockWave в день
- 2 антивирусных движка (Symantec+ЛК)
- False Positive \ False Negative rate < 0,0004%
- Гарантированная доступность – 99,999%

Безопасность любого подключения

Модули обеспечения безопасности

Контроль доступа
Управление сервисами и приложениями

Допустимое использование
Фильтрация контента, управление контентом

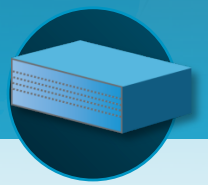
Защита данных
Защита информации и доступа

Защита от угроз
Противодействие ВПО и атакам

Платформы

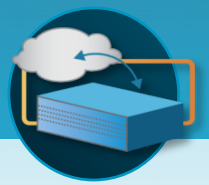
ПО VM
Образы VM на объекте заказчика

Устройства
Выделенные устройства на объекте заказчика

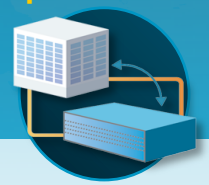


"Облако"
SaaS-инфраструктура на базе "облака"

Гибридная
Сочетание решений на объекте и в "облаке"



Управляемая
На объекте, полностью управляемая



Расширенный анализ трафика

Криптоанализ

Анализ контекста

Анализ сигнатур

Лексический анализ

Анализ приложений

Единые механизмы анализа для разного трафика

Web-трафик

Сетевой трафик

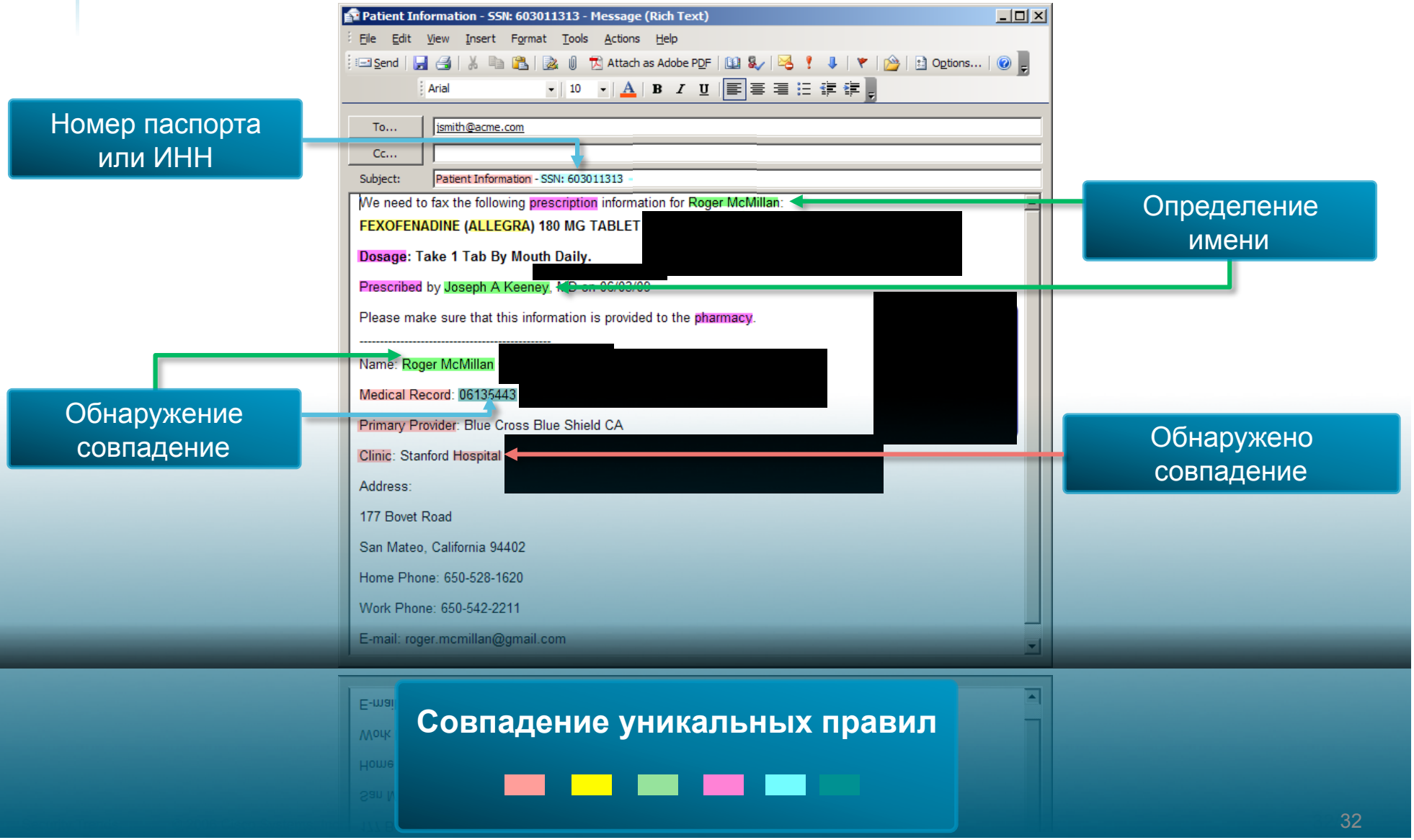
Email-трафик

Понимание контекста

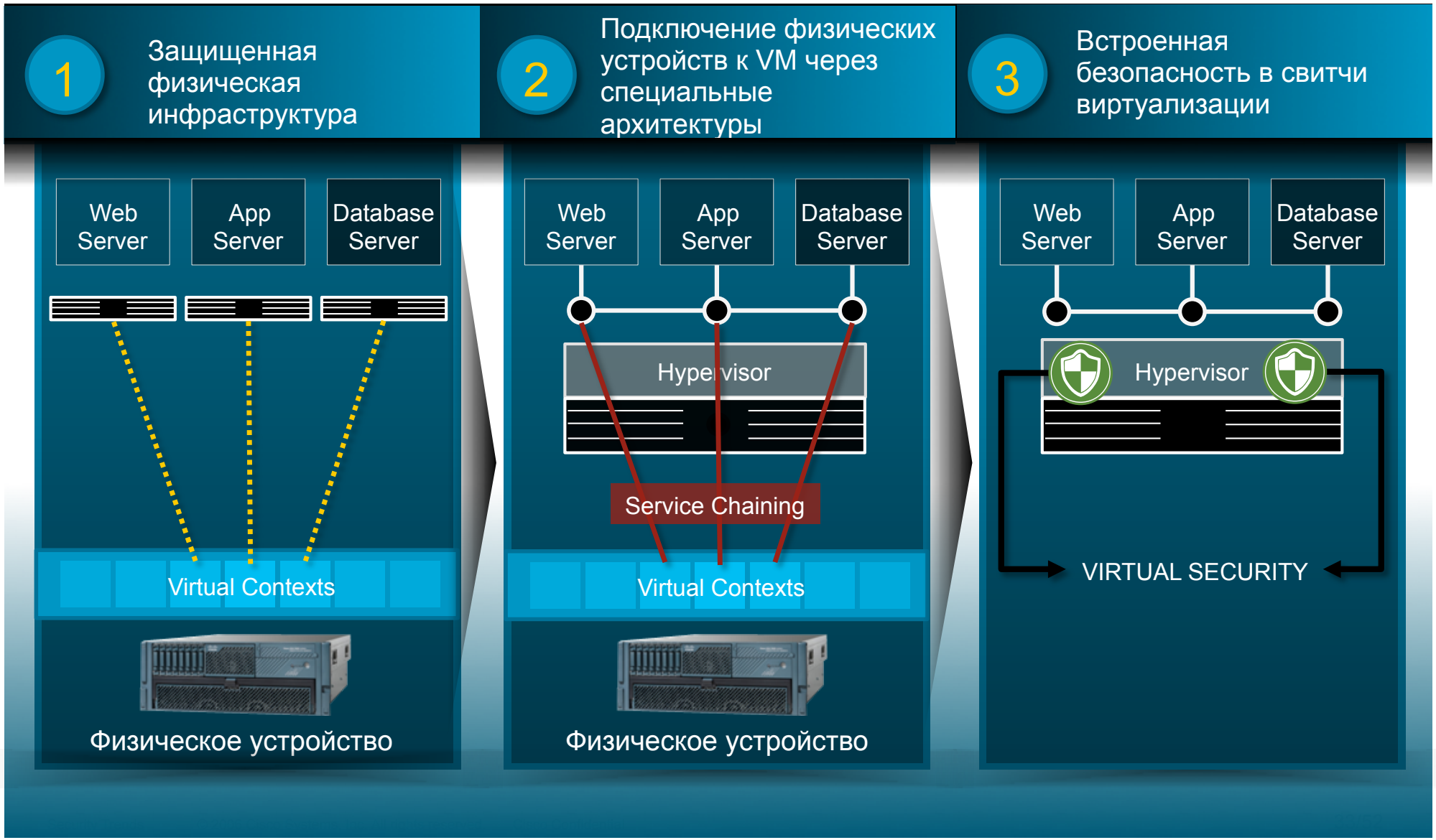
HTTP – это новый TCP

Понимание Web-трафика

Расширенный анализ контента



Элемент 3: Виртуализация, ЦОД и ИБ



Элемент 4: Полный, но прозрачный контроль на основе политик

1. Политики доступа

2. Динамические политики

3. Политики на периметре, на устройствах, на XaaS

Вопросы доступа в современных сетях

Политика доступа

Авторизованный доступ

- Кто в моей сети?
- Могу я управлять рисками ПК в своей сети?
- Общие правила доступа когда я в сети, дома или в дороге?
- ПК соответствуют политике?

Гостевой доступ

- Могу я дать гостям доступ только к Интернет?
- Как управлять гостевым доступом?
- Они могут работать через Wi-Fi или Wired?
- Как мониторить активности гостей?

Неуправляемые устройства

- Как отслеживать неуправляемые устройства?
- Как определить что они делают?
- Могу я контролировать их доступ?

Аутентификация и авторизация

Информация о пользователях

Группа:
Сотрудник

Группа:
Контрактник

Группа:
Гость

+

Другие условия

Время и дата

Статус

Место

Тип доступа

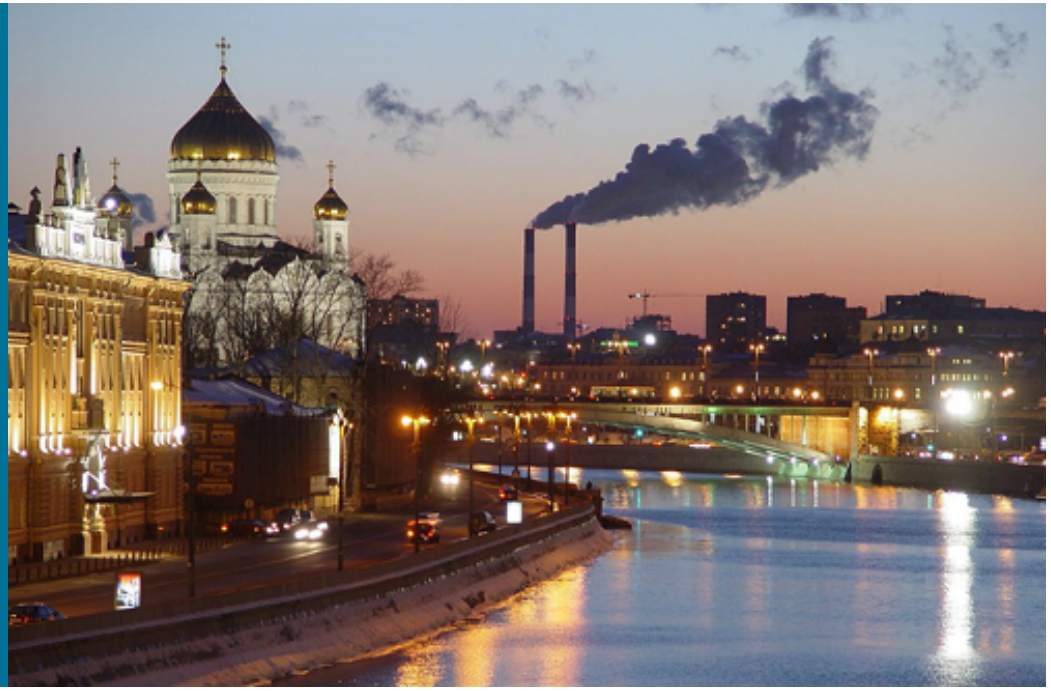
Авторизация (контроль доступа)

- Полный доступ
- Ограничения доступа
- Гость/Internet
- Карантин
- Запрет доступа

Контроль и отчетность

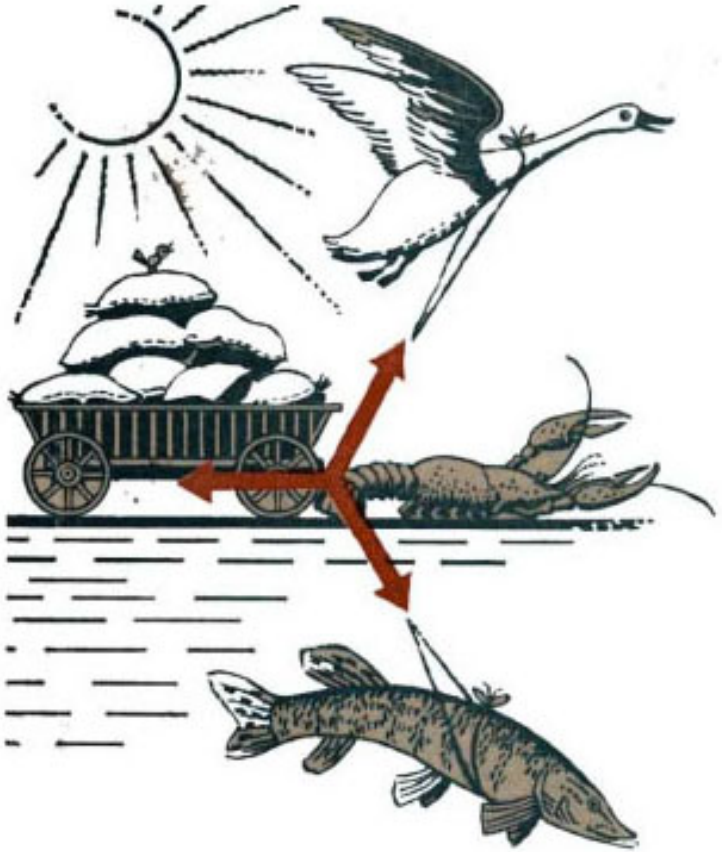
Есть и другие сценарии

Архитектурный подход



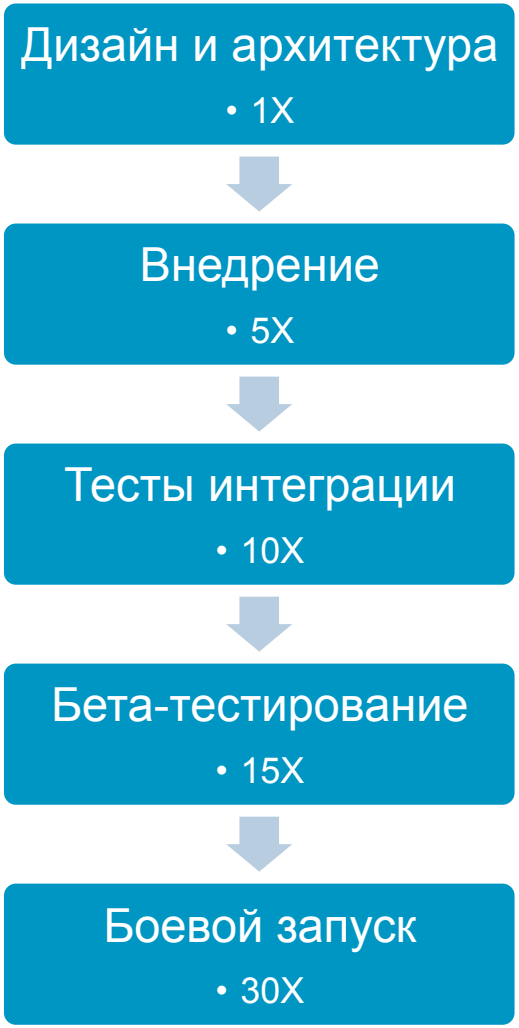
«Технологические» проблемы…

- Отсутствие стандартизации и унификации технологий, продуктов, методов и подходов
  - Рост операционных затрат
  - Сложность поддержки и интеграции
- Повтор и избыточность
  - Не путать с резервированием
  - Нехватка ресурсо-затрат
- Упущения неочевидных вещей
- Отсутствие планов развития
  - Нехватка гибкости и адаптивности к новым требования



…приводят к глобальным проблемам…

- Финансирование по остаточному принципу
- Неудовлетворенность пользователей, снижение их продуктивности и рост цены их поддержки
- Потенциальные наезды со стороны регуляторов
- Неэффективность ИБ в виду забывчивости в отношении некоторых направлений бизнеса
- Несогласованность отделов



Принципы построения защищенной сети

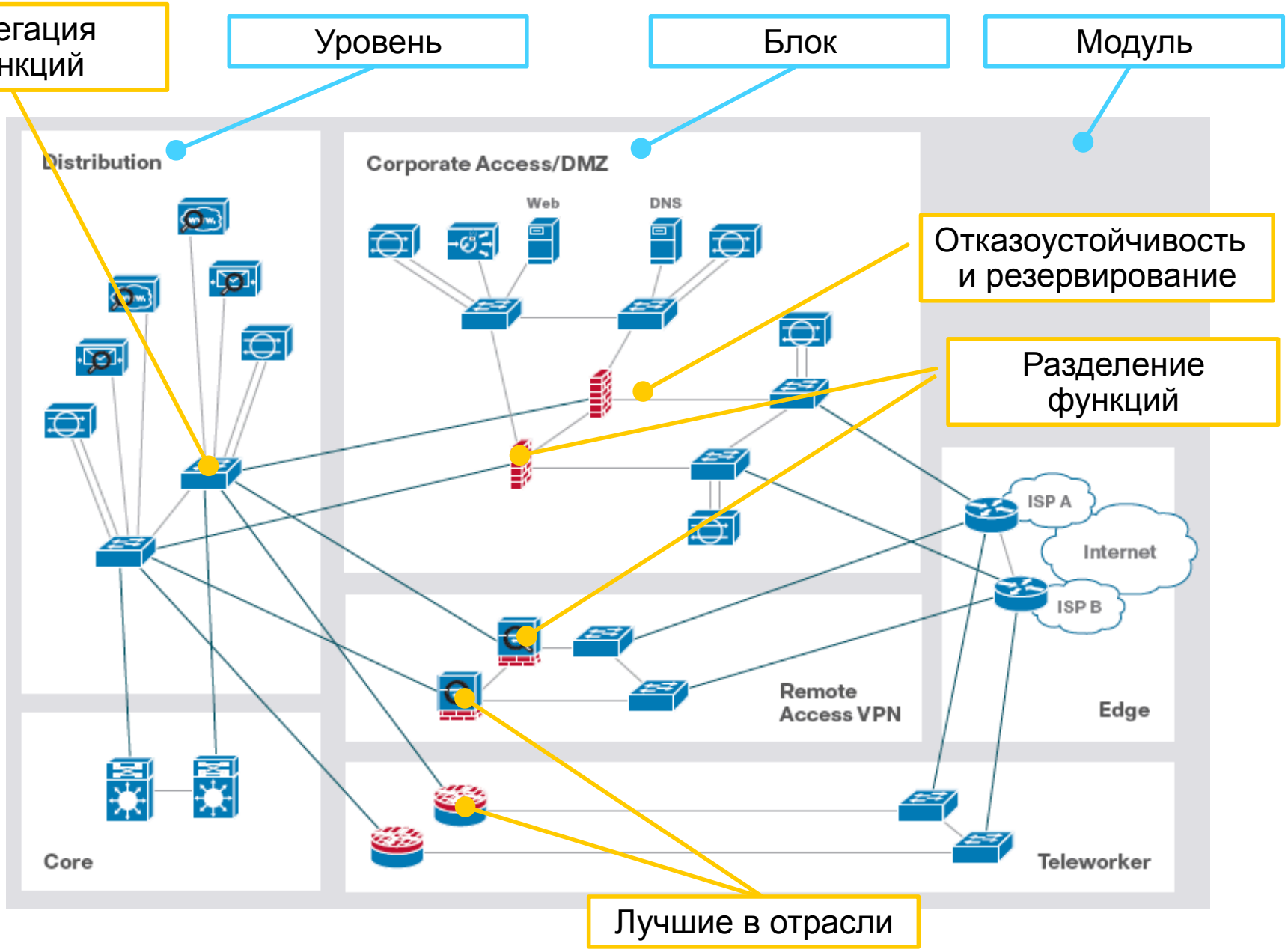
Принципы ИТ

- Модульность / поэтапность
- Снижение TCO
- Стандартизация / унификация
- Гибкость
- Надежность
- Поддержка новых проектов
- Адаптивность / автоматизация
- Масштабируемость

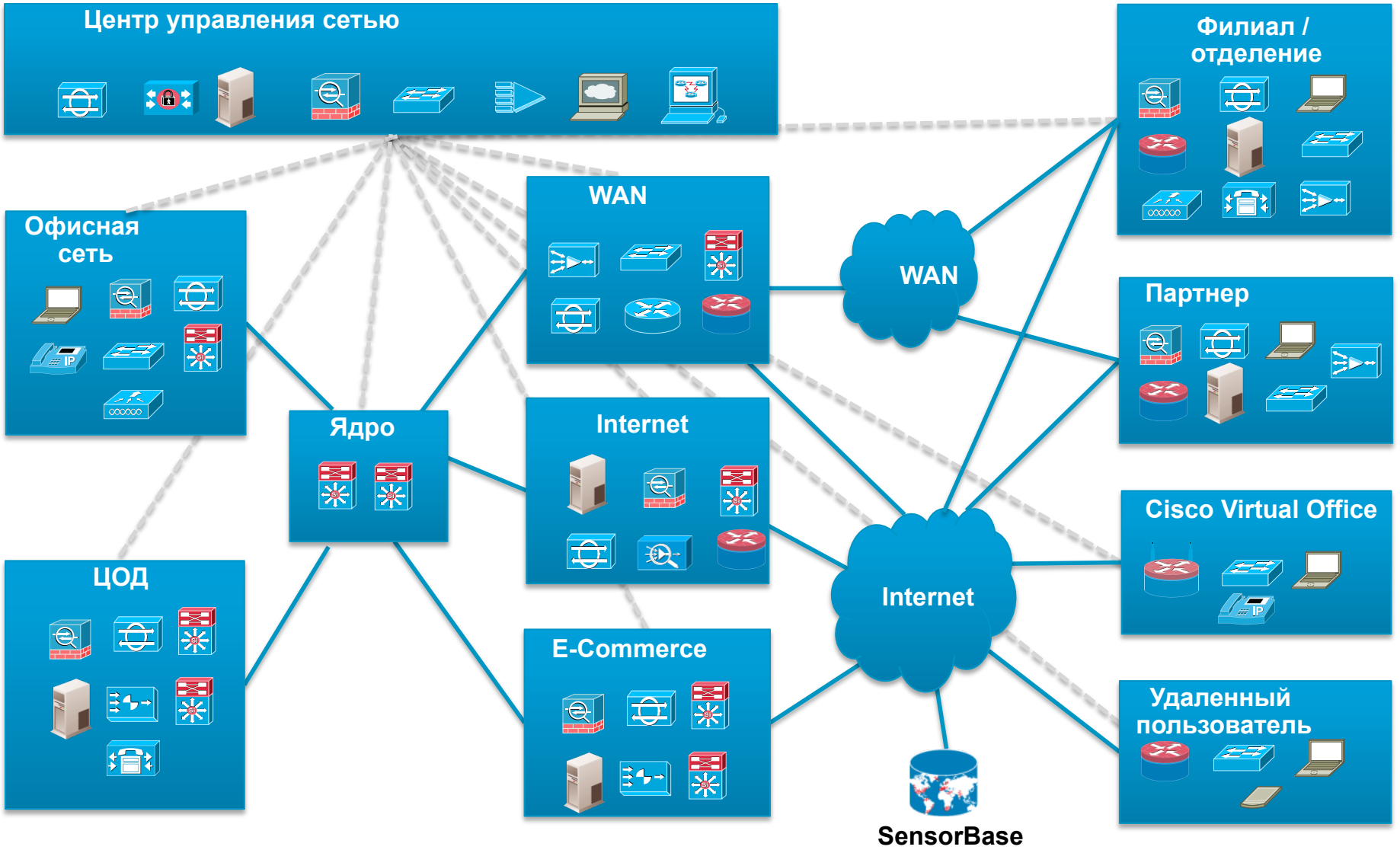
Принципы ИБ

- Безопасность как свойство, а не опция
- Цель – любое устройство, сегмент, приложение
- Эшелонированная оборона
- Независимость модулей
- Двойной контроль
- Интеграция в инфраструктуру
- Соответствие требованиям

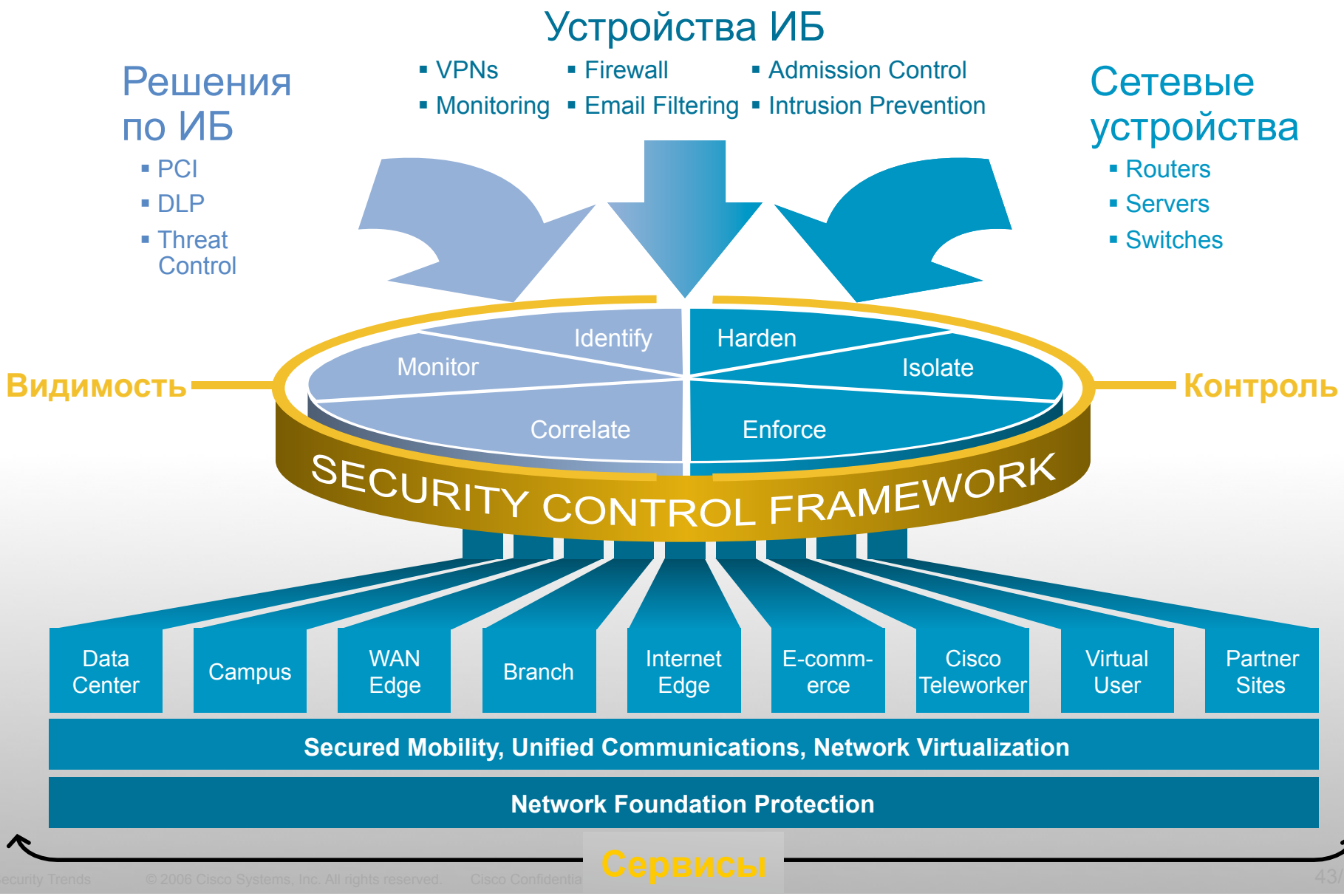
Фрагмент дизайна – Интернет-периметр



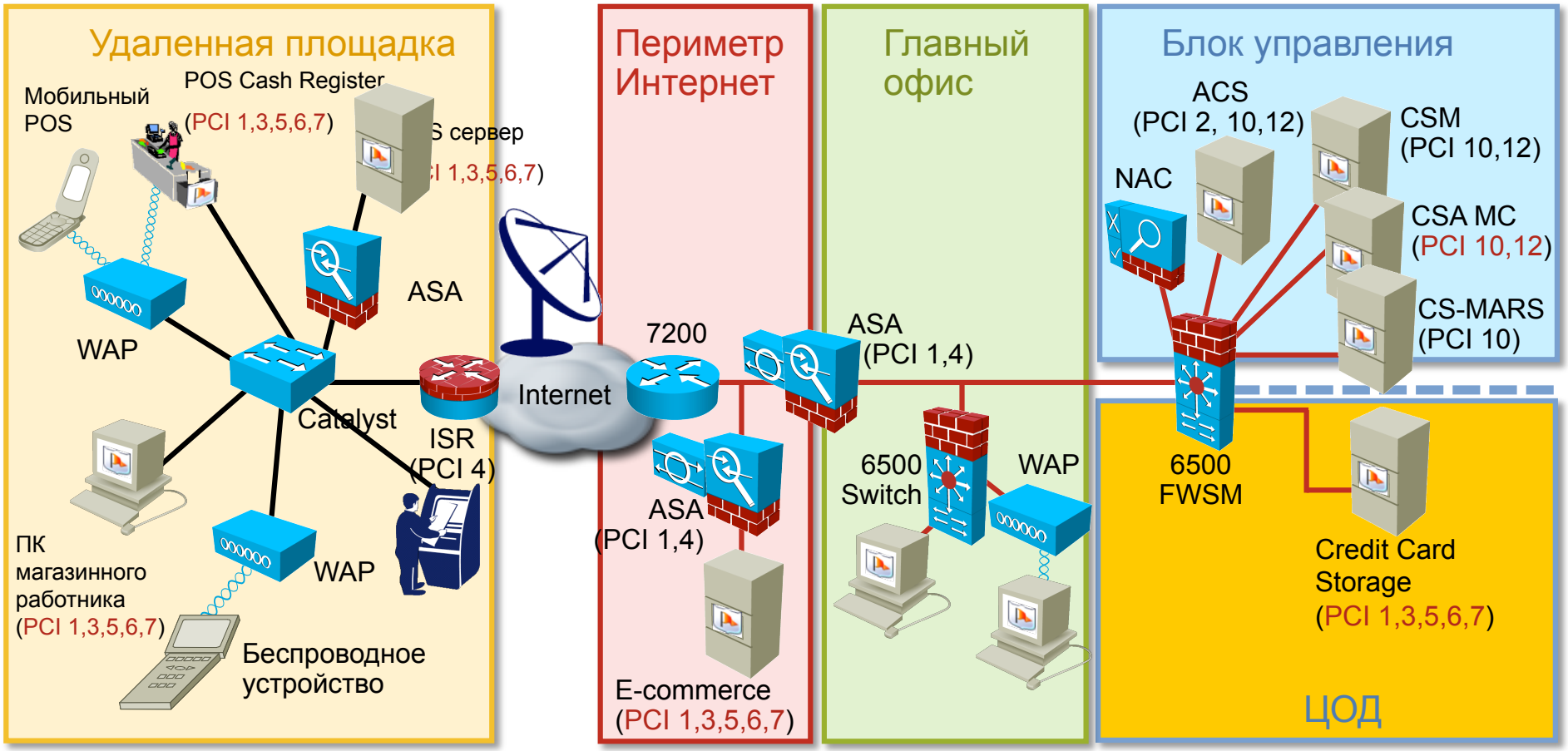
Архитектура защищенной сети



SAFE в современной сети

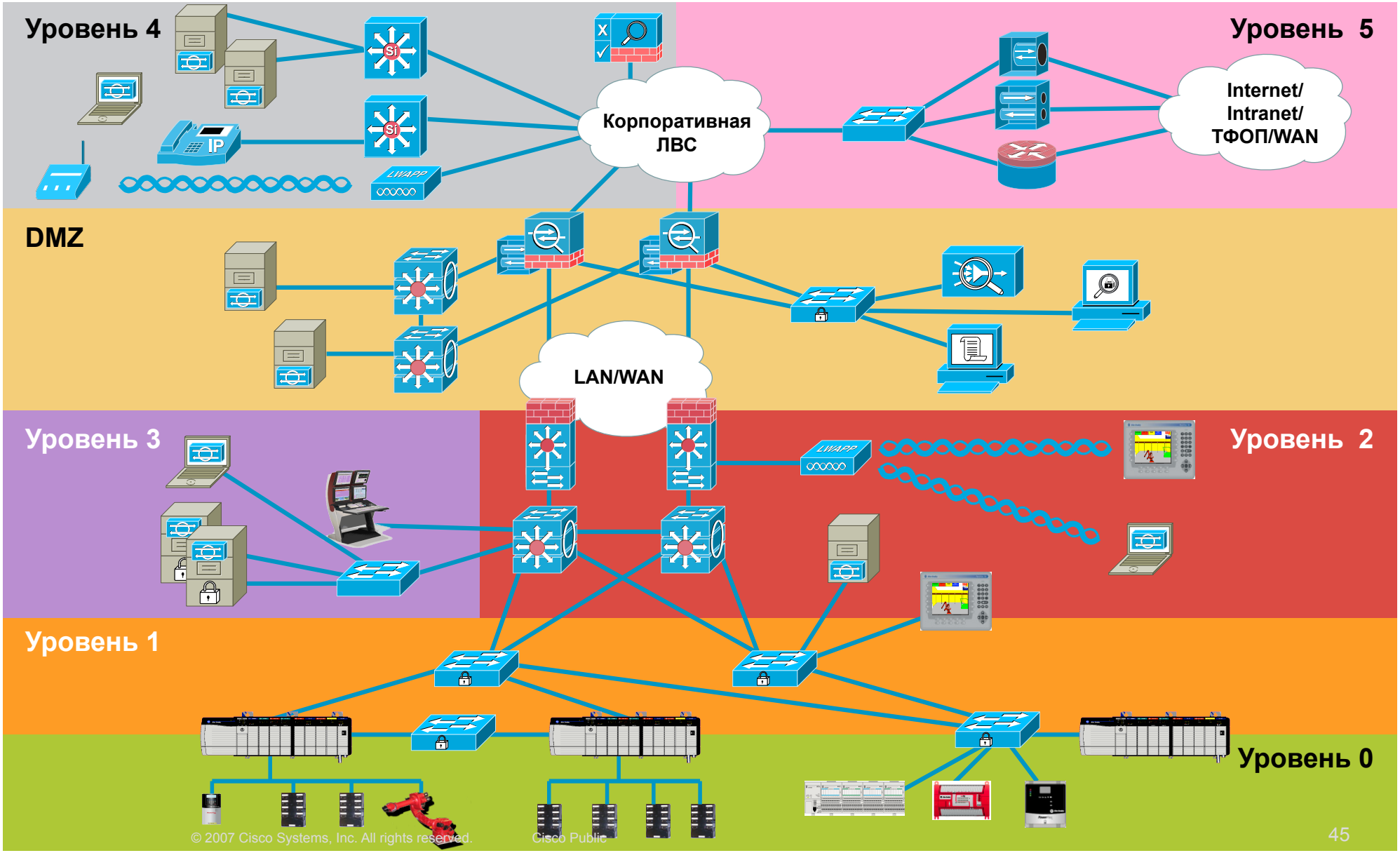


Вертикальные архитектуры
Решение Cisco для PCI DSS

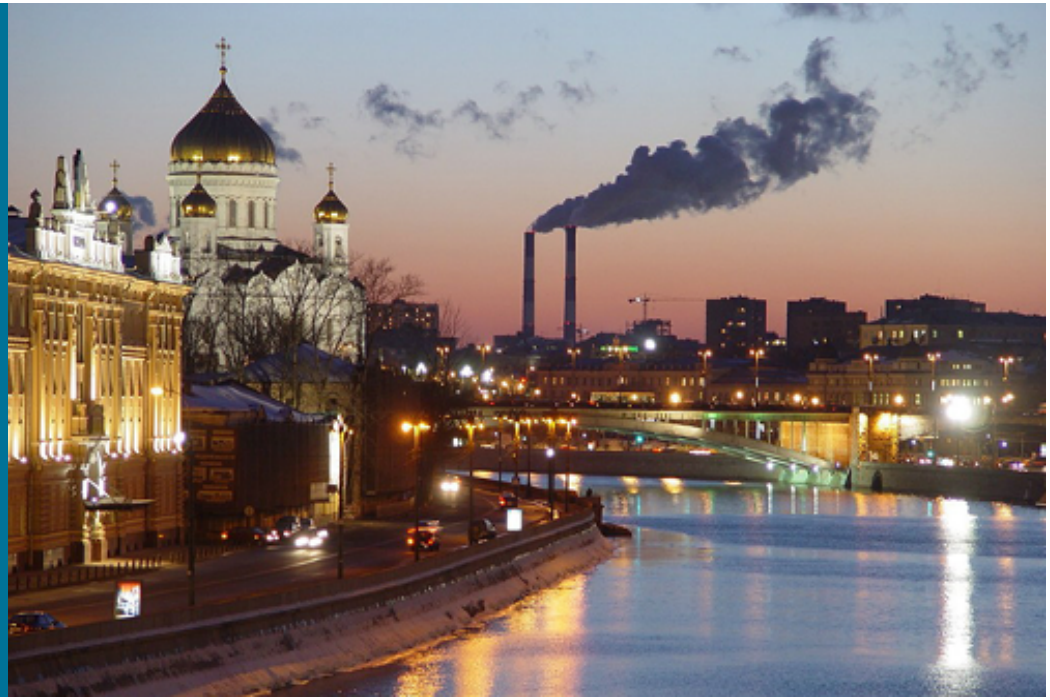


Примечание! Отображена реализация не всех требований

Вертикальные архитектуры
Решение Cisco для АСУ ТП (SCADA)



Заключение



Лидер в области безопасности

39% мирового рынка ИБ, =

сеть – это платформа для реализации поставленных бизнес-целей защищенным образом в соответствие с требованиями регуляторов

Дополнительная информация

Новые документы

- Каталог продуктов по ИБ (8-е издание)
- WP «Стратегия и архитектура Cisco в области ИБ»
- WP «Информационная безопасность в условиях кризиса. Рекомендации Cisco»
- И многое другое на www.cisco.ua

Онлайн-ресурсы Cisco по ИБ

- Cisco Security Center
  http://www.cisco.com/security
- PCI Compliance Advisor
  http://www.pcicomplianceadvisor.com/
- Security Business Advisor
  http://www.securitybusinessadvisor.com/
- Security Solution Designer
  http://www.ciscowebtools.com/designer/
- Cisco SenderBase
  http://www.senderbase.org/

Вопросы?

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