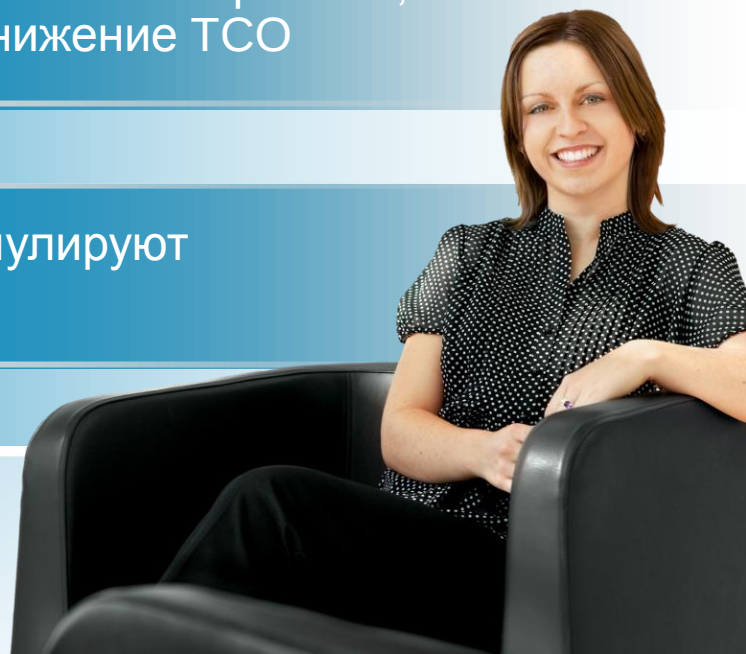
Филиал без границ

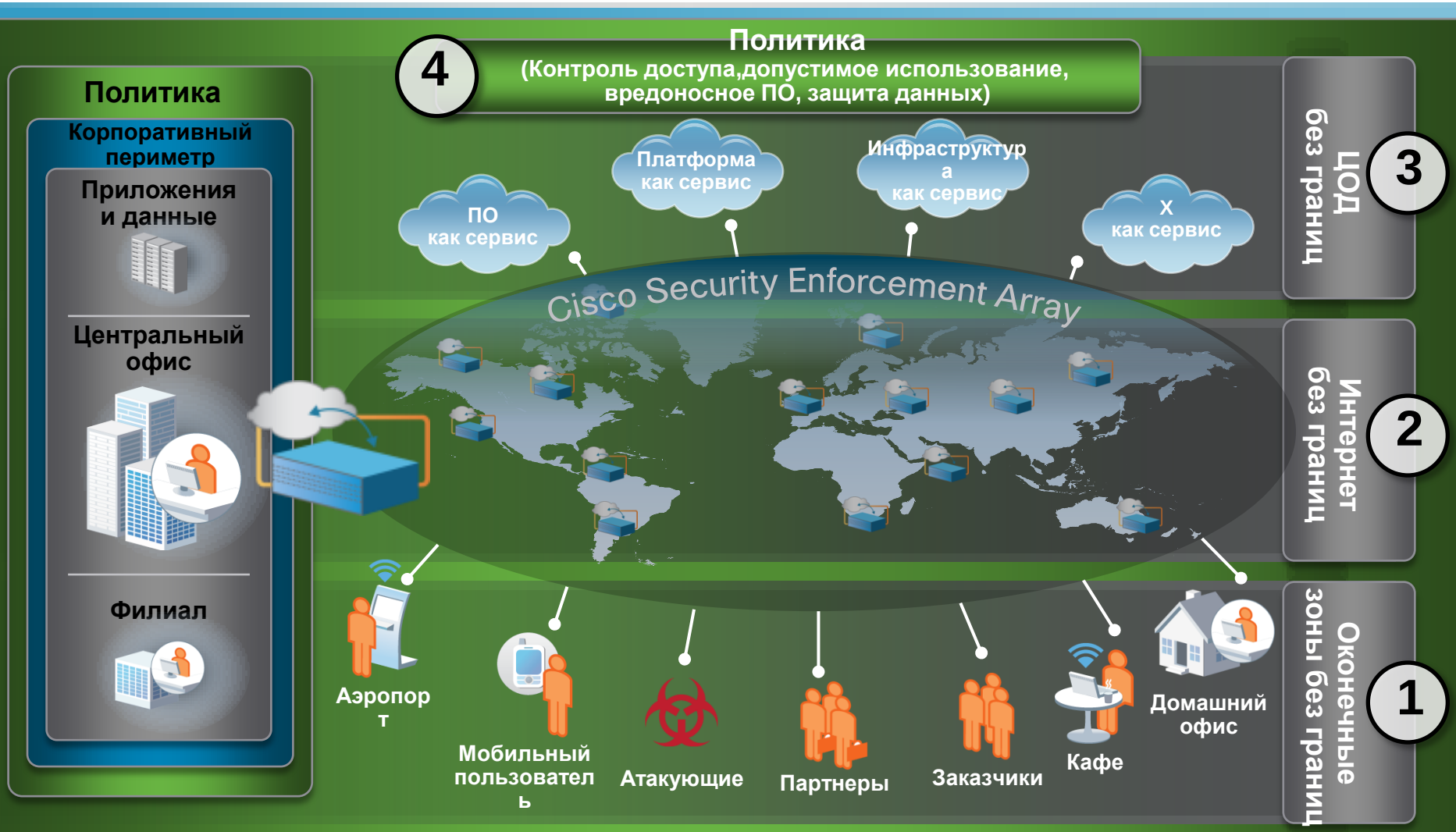
Ноябрь 2009 г.

Основные предпосылки

1. Эволюция филиалов без границ является основным условием работы в сети без границ
2. Cisco ISR G2 обеспечивает высочайшее качество работы, повышенный уровень безопасности и снижение TCO
3. Архитектуры филиалов без границ стимулируют бизнес-инновации



Архитектура системы безопасности сети без границ



Филиал без границ

На 2010 год запланирован 17-процентный рост

Стиль работы

- Существенный рост популярности видео; 75% организаций стремятся улучшить совместную работу и повысить эффективность работы

Эффективность эксплуатации

- Централизация данных и средств их обработки обеспечивает упрощение эксплуатации, экономию средств и улучшение показателей ROI

Филиалы: окна в мир потребителей

Банк

Магазин

Больница

Аудитория

Источник: Nemertes Research

Безопасность филиала без границ
Обеспечение надежной работы

Приложения для работы заказчиков и компании

Защищенные видеосервисы

Защищенные сервисы для надомных работников

Инновационные сервисы

Защищенные сервисы мобильности

Сервисы безопасности

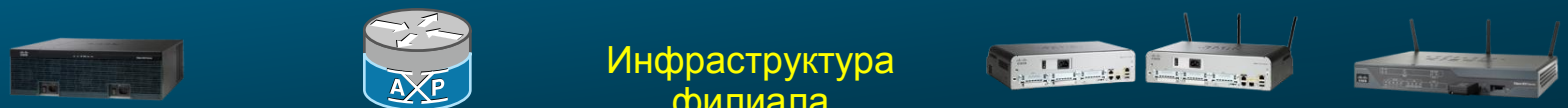
Поли-тика

Защита от интернет-атак

Безопасность уровня ядра

Защищенные подключения

GET VPN



Инфраструктура филиала

Безопасность филиала 2.0

Проблемы заказчиков при создании защищенного филиала без границ

Контроль доступа к ресурсам филиала

- Контроль подключений
- Управление методом доступа
- Управление пользователями и приложениями

Отражение интернет-угроз

- Защита периметра
- Предотвращение вторжений
- Защита контента

Защищенное подключение с учетом приложений

- Защищенный доступ из филиала к ЦОД/главному офису
- Обеспечение производительности приложений
- Защищенная MPLS-сеть

Создание зон подключения без границ

Задача: контроль доступа к ресурсам филиала

«Кто, что, когда, где и как» или подключение к сети

Контроль подключений

- Разрешение/запрет доступа или карантин оконечных устройств в соответствии с их состоянием
- Сегментация пользователей в домена доверия локальной сети на основании идентификационной информации
- Защита от кражи идентификационных данных на уровне 2

Управление методом доступа

- Поддержка систем обеспечения физической безопасности, включая систему видеонаблюдения
- Обнаружение точек беспроводного доступа злоумышленника, обеспечение надежной аутентификации и надежного шифрования в беспроводной сети
- Управление подключениями к корпоративной сети по VPN удаленного доступа

Управление пользователями и приложениями

- Обеспечение доступа к корпоративным ресурсам в соответствии с политиками
- Обнаружение и контроль доли пропускной способности сети, используемой приложениями
- Шифрование трафика управления, ведение журналов аудита в соответствии с нормативными требованиями

Создание зон подключения без границ

Решение: многоуровневый контроль доступа

Преимущества:

- Несколько уровней аутентификации и сегментации, например, пользователь, устройство, VLAN
- Доступ в Интернет для гостей/ членов семьи
- Автоматизированное развертывание защищенной среды домашнего офиса

Аутентификация в беспроводной сети

- 802.11a/b/g, WEP/WPA/WPA2 для корпоративных и домашних сетей, Cisco Secure Services Client с поддержкой 802.1

Прокси системы аутентификации

- Доступ к корпоративной сети предоставляется только пользователям, прошедшим процедуру аутентификации; остальным пользователям предоставляется только доступ в Интернет
- IP-телефоны проходят аутентификацию в особом порядке с использованием средств анализа SCCP на МСЭ

Интеграция AAA/ACS

- Средства AAA интегрируются со средствами 802.1x, прокси система аутентификации, 802.11 и PKI; защита концентраторов Cisco Virtual Office путем аутентификации узлов перед установкой IPSec-туннелей

Контроль доступа для приложений

- Контроль доступа с учетом особенности работы приложений для приложений, использующих несколько протоколов, например, IM/P2P, с помощью NBAR

Физическая безопасность

- Интегрированные средства управления потоками архивного видео и прямой видеотрансляции с использованием Cisco Video Surveillance Manager на модуле SRE

НОВОЕ!

Аппаратный модуль NAC

- Обслуживание пользователей проводной и беспроводной сети и удаленных пользователей
- Функциональные возможности NAC appliance

Создание зон подключения без границ
Пример: система видеонаблюдения

VMSS — система управления и хранения видео

Функциональные возможности и преимущества:

- Интегрированные средства управления потоками архивного видео и прямой видеотрансляции с использованием Cisco Video Surveillance Manager
- Локальное архивирование и хранение данных системы видеонаблюдения
- Удаленный доступ к видео/данным в реальном времени
- Обеспечение безопасности за счет тонких настроек системы контроля доступа

Новые возможности Cisco ISR G2:

- Поддержка SRE (SM-700 и SM-900)
- Полная интеграция системы видеонаблюдения с системой хранения данных на модуле
- Высокая производительность означает меньшее время реакции

Работа в сети Интернет без границ

Задача: отражение угроз на уровне филиала

Филиалы являются точками проникновения вредоносного ПО в корпоративную ИТ-инфраструктуру

Контроль периметра

- Защита сети филиала и ее сегментация с помощью МСЭ
- Глубокий анализ и управление трафиком, связанным с портом 80, и обнаружение нарушений правил использования других протоколов
- Защита доступа к приложениям, размещенным в распределенных сетевых сервисах

Предотвращение вторжений

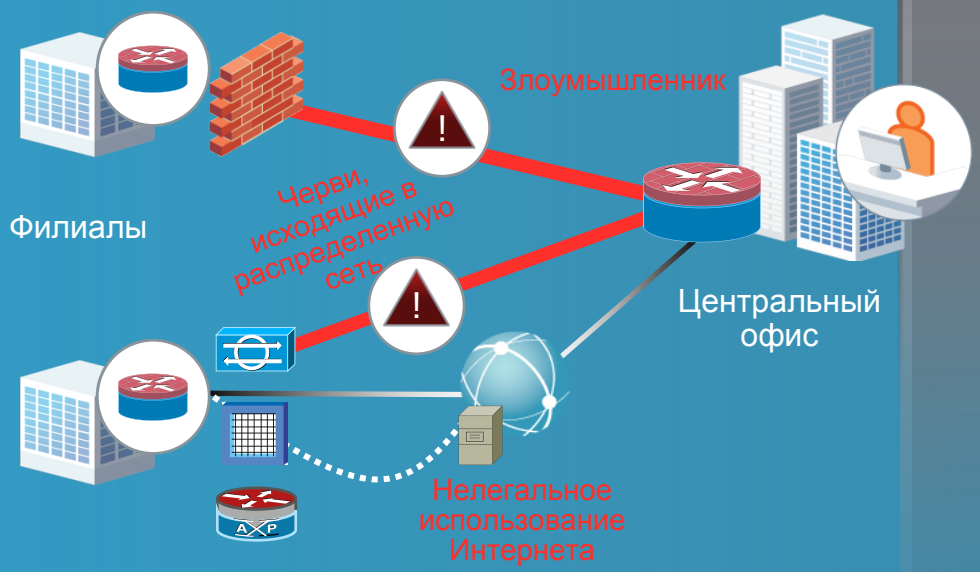
- Обнаружение и реакция на известные угрозы и совершенно новые угрозы
- Корреляция угроз и динамическая реакция на угрозы
- Снижение числа ложных срабатываний

Безопасность контента

- Ограничение использования интернет-ресурсов, фильтрация web-сайтов в соответствии с их репутацией
- Борьба с вредоносным программным обеспечением: вирусами, троянскими конями и средствами проведения атак типа "фишинг"
- Борьба со спамом

Работа в сети Интернет без границ

Решение: интегрированные средства отражения угроз



Преимущества:

- Защищенный доступ к системам филиала по Интернету без установки дополнительных устройств
- Контроль угроз прямо в ИТ-инфраструктуре филиала; снижение нагрузки на канал подключения к распределенной сети
- Возможность доступа к распределенным сетевым сервисам

Контроль периметра с помощью МСЭ

- Защита внешней и внутренней сети: внутренняя сеть больше не считается доверенной
- Обнаружений аномалий трафика и контроль состояния сеансов

Сетевая IPS

- Глобальная корреляция угроз, снижение числа ложных срабатываний
- Обнаружение совершенно новых атак

Безопасность контента

- Контроль действий пользователей в Интернете

Модули SRE

- Сетевой модуль IPS : функции аппаратного сенсора
- Средства фильтрации по репутации web-сайта и борьбы с вредоносным программным обеспечением

Сервисы безопасности уровней 2–7

- Использование существующих сетевых устройств для сбора сведений о трафика, настройка ловушек для злоумышленников

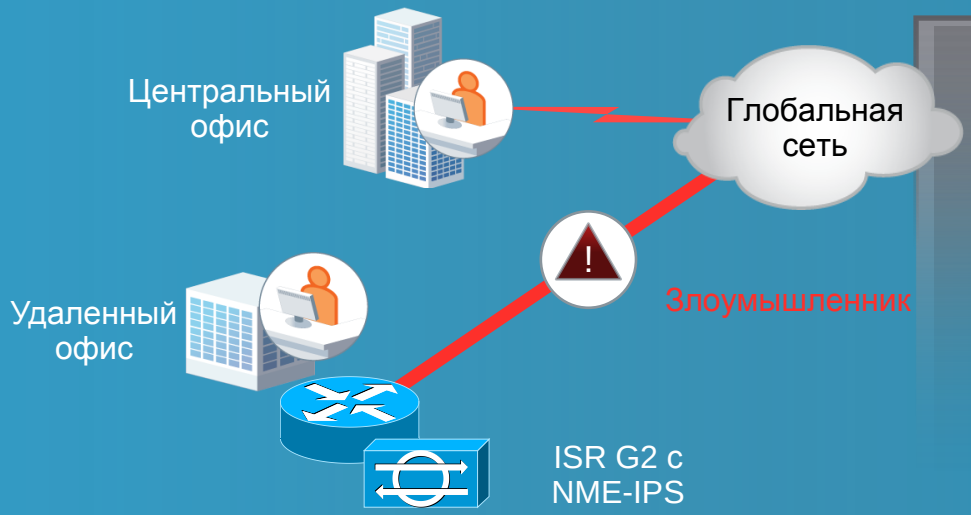
Системное управление

- Унифицированные средства управления безопасностью и анализа угроз для маршрутизаторов и устройств безопасности

Работа в сети Интернет без границ

Пример: предотвращение вторжений

Сетевой модуль системы предотвращения вторжений (IPS)



Новые возможности Cisco ISR G2:

- Поддержка нового решения Cisco для глобальной корреляции и обнаружения угроз на основе репутации
- Повышенная надежность, эффективность и способность противостоять большему числу совершенно новых атак
- Требуется плата адаптера ISR G2

Функциональные возможности и преимущества:

- Бесшовная интеграция с другими системами обеспечения безопасности филиала (VPN, МСЭ и т. п.) , функционирующими на маршрутизаторе ISR G2
- Полнофункциональная высокопроизводительная система защиты от угроз сети филиала или малого предприятия
- Не требует установки дополнительных устройств, прокладки дополнительных кабелей или обеспечения дополнительного электропитания
- Поддерживает каналы подключения к распределенной сети всех типов: T1/E1, T3/E3, Ethernet, xDSL, MPLS, 3G WWAN

Создание ЦОД без границ

Задача: защищенное подключение

Требования к средствам шифрования и общей производительности продолжают расти

Защищенная MPLS-сеть

- Поддержка масштабируемой инфраструктуры шифрования в MPLS-сети
- Выделенный уровень управления для поддержки аутсорсинга услуг
- Доступ к закрытым распределенным сетевым сервисам в соответствии с политиками использования виртуальных ресурсов

VPN по Интернет

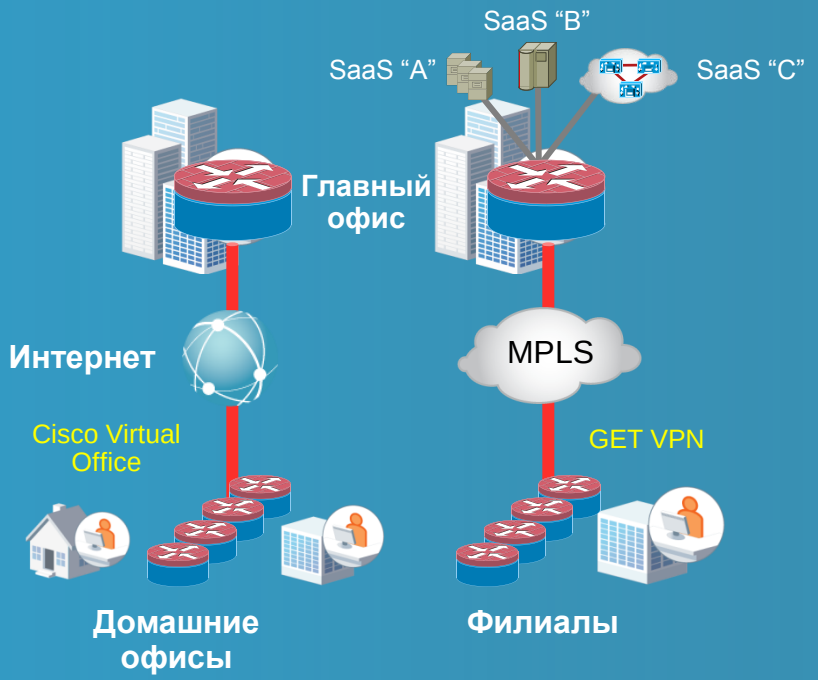
- Масштабируемые и гибкие архитектуры (топологии: звезда и полносвязная сеть)
- Защита сети и абонентских устройств от интернет-угроз
- Автоматизация управления для поддержки самообслуживания удаленных объектов

Производи-тельность приложений

- Повышение производительности работы по глобальной сети
- Повышение приоритета критически важного трафика для оптимизации производительности

Создание ЦОД без границ

Решение: защищенный доступ без границ



Преимущества:

- Защищенный MPLS-доступ к приложениям в ЦОД
- Возможность взаимодействия филиалов и надомных работников по сети VPN через Интернет
- Оптимизация производительности приложений и подключений к глобальной сети

Средства шифрования MPLS для филиалов и ЦОД

- Защищенная сеть MPLS с GET VPN обеспечивает создание масштабируемой полносвязной сети без использования туннелей
- Возможность ограничения прав доступа до определенного приложения SaaS в ЦОД

VPN типа "сеть-сеть"

- Решение Cisco Virtual Office обеспечивает защищенный интернет-доступ к филиала/удаленных сотрудников/мобильных сотрудников к приложениям, размещенным в ЦОД
- Интеграция средств шифрования DMVPN и Easy VPN с MCЭ, IPS, средствами защиты контента и PKI

Производительность приложений

- WAAS обеспечивает высокую производительность приложений при работе по защищенным каналам связи по распределенной сети (сравнимую с работой в локальной сети)
- Интеграция расширенных средств обеспечения QoS и средств передачи трафика с групповой адресацией с IPsec обеспечивает требуемый уровень производительности для передачи аудио и видео

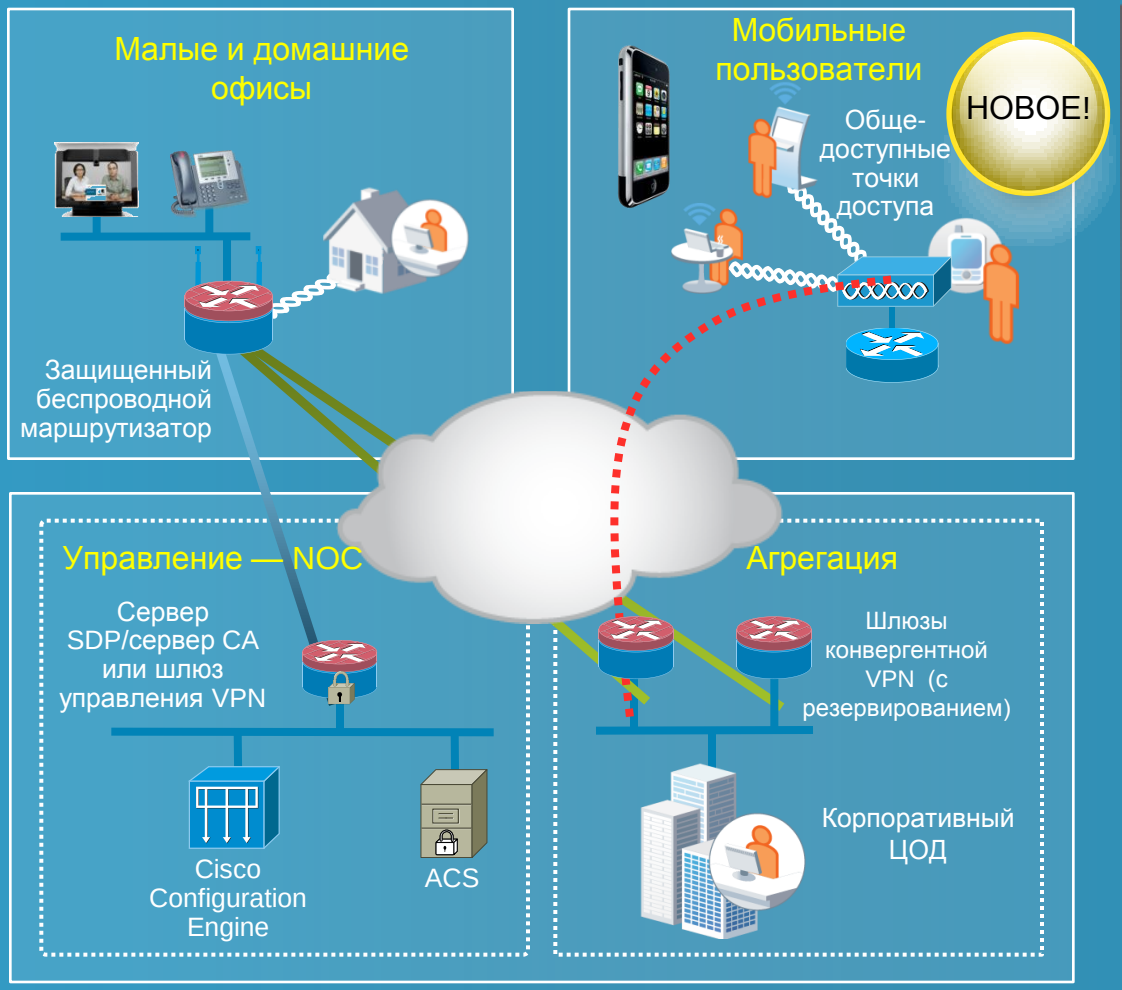
Доступность

- Аварийное переключение с сохранением состояния сеансов и с учетом маршрутизации
- Резервирование каналов связи и устройств

Управление VPN

- Средства управления серверами сторонних производителей
- Системы управления CiscoWorks и CSM

Cisco Virtual Office Express



- Упрощенная архитектура концентратора
- Аутентификация удаленных устройств с использованием PKI
- Конвергентное VPN-подключение к корпоративной ИТ-инфраструктуре обеспечивает активный резервный туннель для упрощения оперативного аварийного переключения
- Архитектура обеспечивает возможность использования внешнего центра управления (NOC)
- Туннель управления постоянно активен, что обеспечивает возможность централизованного распространения изменений политик
- Гибкие средства поддержки смартфонов (Nokia)
- Поддержка сервисов мобильности (роуминг, унифицированные коммуникации, совместная работа)

Можно ли защитить ИТ-инфраструктуру филиала и управлять ей, обеспечивая производительность и совместную работу?

Технологическое лидерство

- Cisco Virtual Office, GET VPN
- Гибкие варианты подключения
- Интеграция с архитектурой корпоративной системы совместной работы
- Гибкие средства анализа трафика (HTTP, HTTPS, FTP, SMTP и т. п.)
- Анализ контента, учет специфики приложений

Реализация

- Высокопроизводительные маршрутизаторы
- Модули SRE
- Сервисы ИБ с использованием IPS
- Гибкие средства сетевого управления и управления ИБ

Защищенные маршрутизаторы Cisco ISR G2

Лучшие средства для защиты филиалов

Эффективная защита от угроз, гибкие варианты защищенных подключений, снижение операционных затрат и поддержка модулей SRE

Апробированные средства защиты от угроз

- Интеграция и расширение самых популярных средств МСЭ/IPS/фильтрации контента платформы Cisco ISR
- Основаны на опыте эксплуатации более 6 млн. ISR по всему миру и более 10 лет новаторства

Лучшие в отрасли средства организации сетей VPN

- Интеграция и расширения самых популярных средств организации VPN (сеть-сеть и удаленного доступа) платформы ISR с поддержкой SSL и IPsec VPN

Интеграция расширенных сервисов безопасности

- МСЭ с поддержкой системы унифицированных коммуникаций, систем совместной работы и передачи видео
- Интеграция средств безопасности в сетевые механизмы (протоколы маршрутизации/ QoS/NAT/передача голоса…)

Средства мониторинга и управления

- Развитые средства мониторинга для упрощения эксплуатации сетей
- Средства управления системой ИБ, обеспечивающие настройку, управление и мониторинг системы ИБ

Преобразование стиля работы филиала:

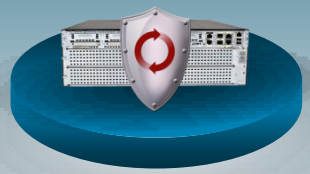
Любой сервис | **Любой филиал** | **Любая точка мира**

Сервисные модули и интерфейсные карты для обеспечения безопасности

- Широчайший спектр защищенных сервисов для проводной и беспроводной сети
- 16, 24 или 48 портов GE
- 802.1X /PVLAN/WEP

Новые сервисные модули: EtherSwitch (ESM) и контроллер WLAN (NME)

- Встроенный криптомодуль, работа драйвера криптомодуля в режиме "run-to-completion", отсутствие задержек



Встроенные средства организации VPN устраняют необходимость в AIM-VPN

- NAC и IPS в формате NME
- Полная функциональность
- Поддержка глобальной корреляции в версии 7.0
- 2911-3945

NME-NAC-K9 NME-IPS-K9 с адаптером SM

- Система обеспечения физической безопасности: сетевой модуль 16-портового шлюза аналогового видео
- Система видеонаблюдения: SRE 700 SM, SRE 900 SM февр. 2010 г.

Сервисный модуль системы видеонаблюдения 1 кв. 2010 фин. г.

Набор сервисов на базе ISR G2

Сетевые сервисы и сервисы ИБ		Сервисы совместной работы	Сервисы и приложения для вычислений	
Сетевые сервисы	Сетевая и физическая безопасность	Система унифицированных коммуникаций	Инфраструктура приложений	Отраслевые приложения
			 	
ИТ-инфраструктура филиала и управление	Защита и обеспечение соответствия нормативным требованиям	Системы связи и совместной работы	Консолидация приложений филиала, высокая производительность	Приложения для отдельных отраслей
▪ Контроллер WLAN (WLC) ▪ Основные сетевые сервисы Infoblox (AXP) ▪ Cisco Network Analysis (NAM) ▪ Cisco Wide Area Application Services (WAAS)	▪ Управление доступом и доверительными отношениями ▪ Расширенные сервисы безопасности ▪ Защищенные подключения ▪ Управление и мониторинг ▪ Система видеонаблюдения	▪ Модуль Cisco Unity® Express (гол. почта, IVR) ▪ Система аудиозаписи NICE (AXP) ▪ Sagem Interstar Fax over IP (AXP) ▪ SingleWire Informacast (AXP)	▪ Платформа Cisco Application Extension (AXP) ▪ Интегрированная система хранения данных ▪ Средства виртуализации ▪ Windows Server	▪ ICW Healthcare Connector на платформе AXP ▪ Tiani Medical Data Exchange (AXP) ▪ Global Protocols Skipware (AXP)

▪ Выпущено ▪ Разработка

Новые возможности ISR G2

Лучшие в отрасли устройства…стали еще лучше!

Cisco ISR		Cisco ISR G2
До 45 Мбит/с с сервисами	Производительность каналов WAN	До 150 Мбит/с с сервисами
Одноядерный	Сетевой процессор	Многоядерный
X (160 Гбайт)	Производительность и емкость сервисных модулей	До 7X при использовании двухъядерного процессора и системы хранения емкостью 1 Тбайт
До 200 Мбит/с	Производительность системы ИБ	Повышение производительности до 5 раз по сравнению с ISR
Защищенная передача голоса, защищенная мобильность	Сервисы безопасности	Защищенная передача голоса и видео, защищенная мобильность, поддержка распределенных сетевых сервисов
Несколько	Образы IOS	Единый универсальный образ IOS
Аппаратная привязка	Развертывание сервисов	Виртуальные сервисы "по запросу"
Одна материнская плата	Резервирование	Резервируемые источники питания.Материнская плата, модернизируемая на месте установки
EnergyWise	Эффективность энергопотребления	EnergyWise с управлением на уровне слота

Пятикратное повышение производительности.
Тот же уровень цень.

Эволюция филиала без границ

Резюме

- Эволюция филиала без границ является основным этапом создания сети без границ
- Маршрутизаторы Cisco ISR G2 обеспечивают превосходные возможности для работы пользователей, стимулируют бизнес-инновации и характеризуются лучшими показателями TCO в отрасли. Кроме того, они позволяют внести свой вклад в защиту окружающей среды.