Защищенный удаленный доступ

Михаил Кадер

Инженер

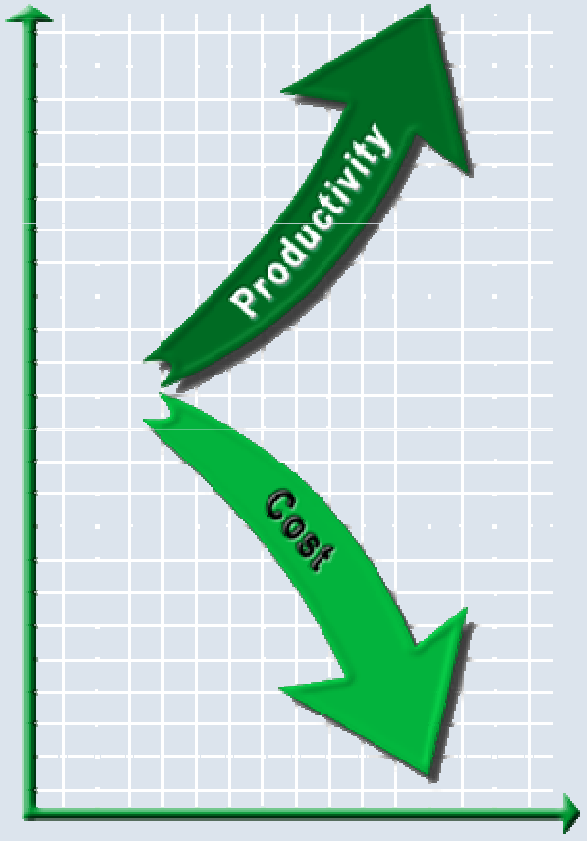
О чем пойдет речь

- Когда нужен удаленный доступ?
- Защищенная архитектура сети предприятия
  - Удаленный доступ мобильных работников
- Требования к защите удаленного доступа
- Защищенный доступ со стороны клиента
- Защищенное подключение
- Расширенная защита приложений удаленного доступа

Когда нужен удаленный доступ?
2 стороны медали

Потребности и возможности

- Достичь большего при тех же ресурсах и с теми же активами
- Сокращение штатов, ограничение бюджетов и давление со стороны конкурентов заставляет предприятия
  - Увеличивать продуктивность
  - Увеличивать взаимодействие
  - Снижать затраты
  - И еще… поддерживать лояльность сотрудников, удовлетворенность работой и психологический климат
- Глобализация экономики требует работать не только в режиме 8x5, но и в нерабочие часы

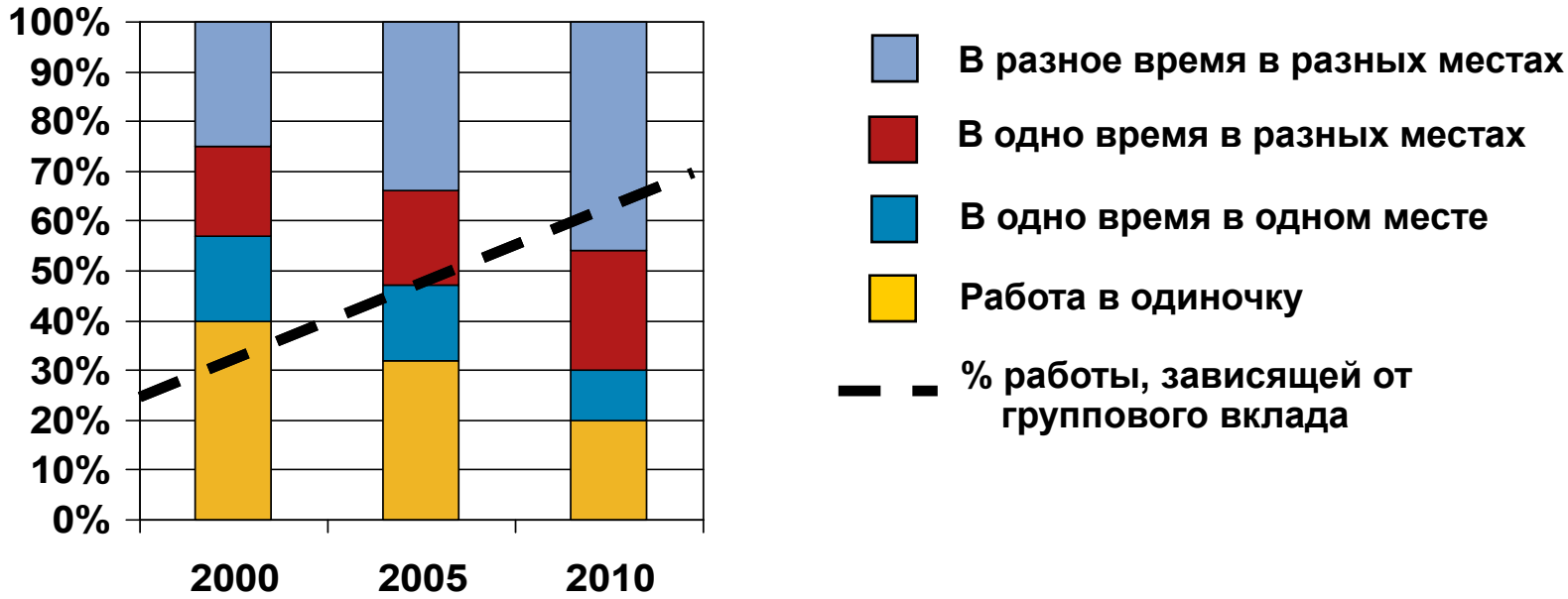


Работа происходит везде

- 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

**Источник: Gartner, Cahners Instat,
Wharton Center for Applied Research**

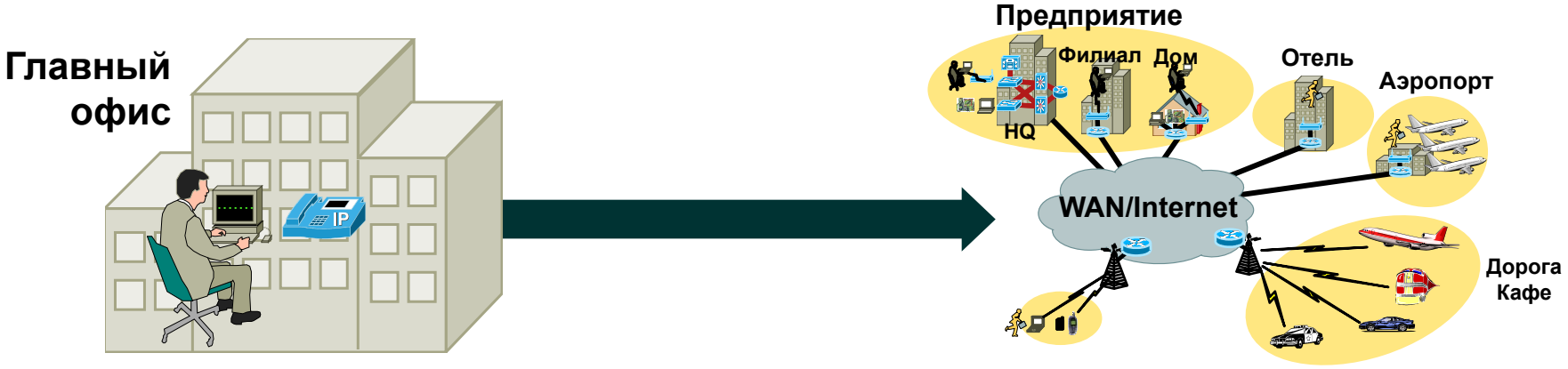
Трансформация бизнеса



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

Источник: Gartner Group

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

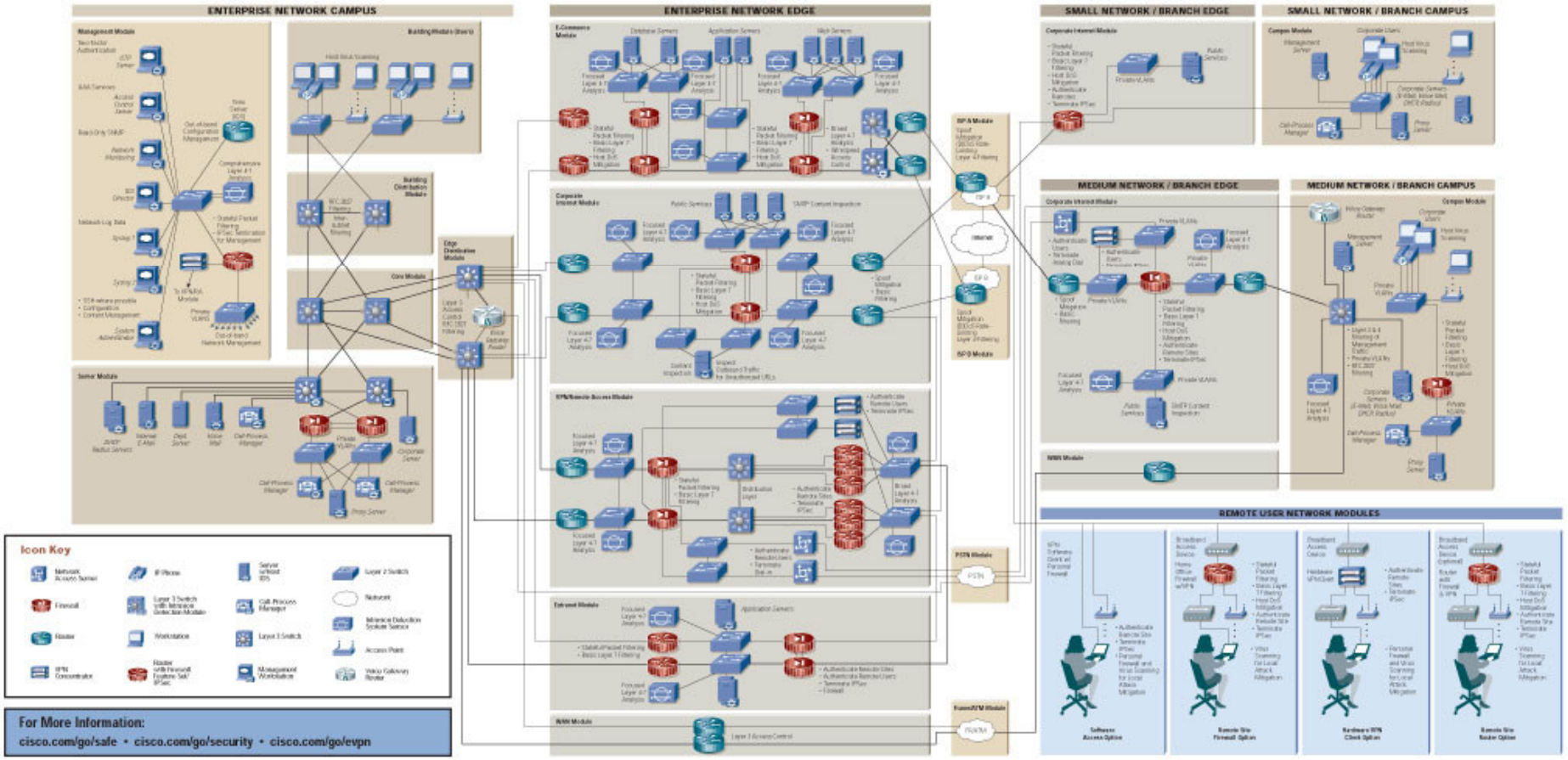
- Многие компании фокусируются на предоставлении сервиса на своей территории (зарплата, билеты, документооборот…)
- Сотрудник в среднем тратит только 30–40% времени в офисе

Архитектура защищенного предприятия

Компромисс удобства и безопасности

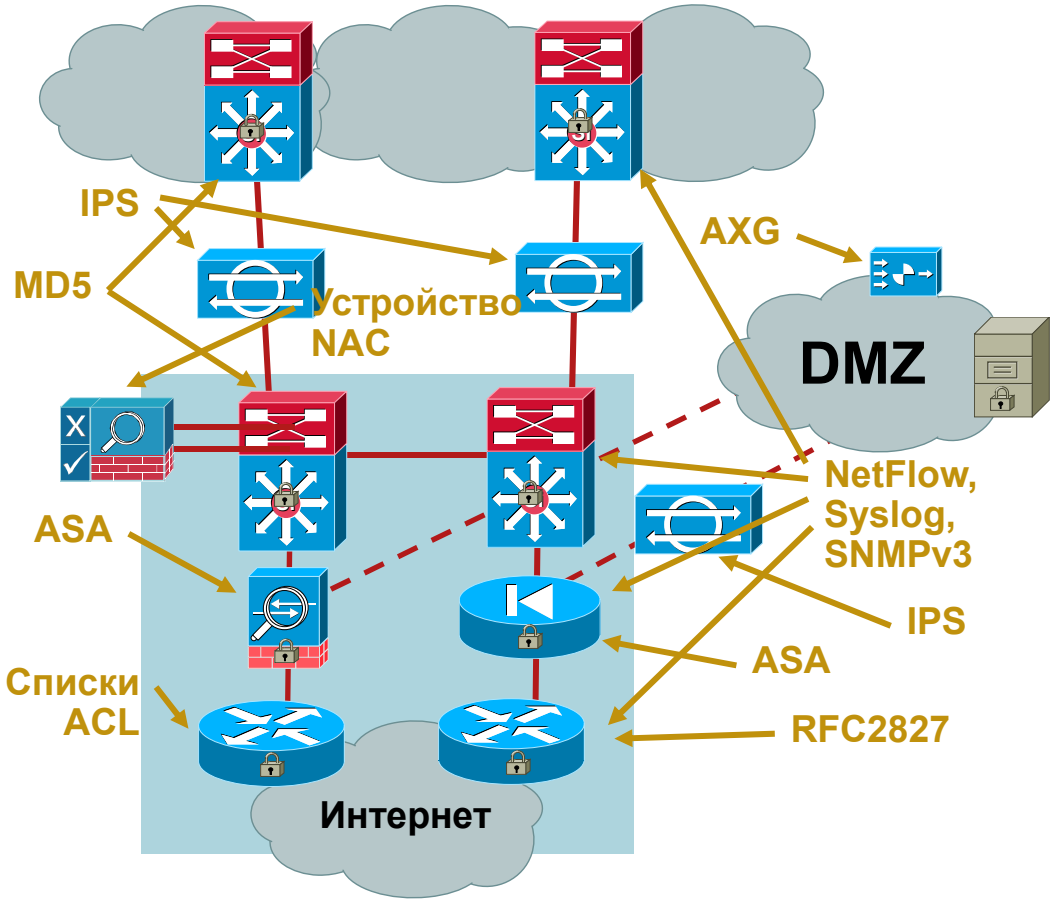
- Многие руководящие документы, стандарты, требования по ИБ рассматривают безопасность, как самоцель

Удаленный доступ к корпоративной сети из Интернет



Загрузить брошюру «Cisco SAFE» можно на сайте my.cisco.ru

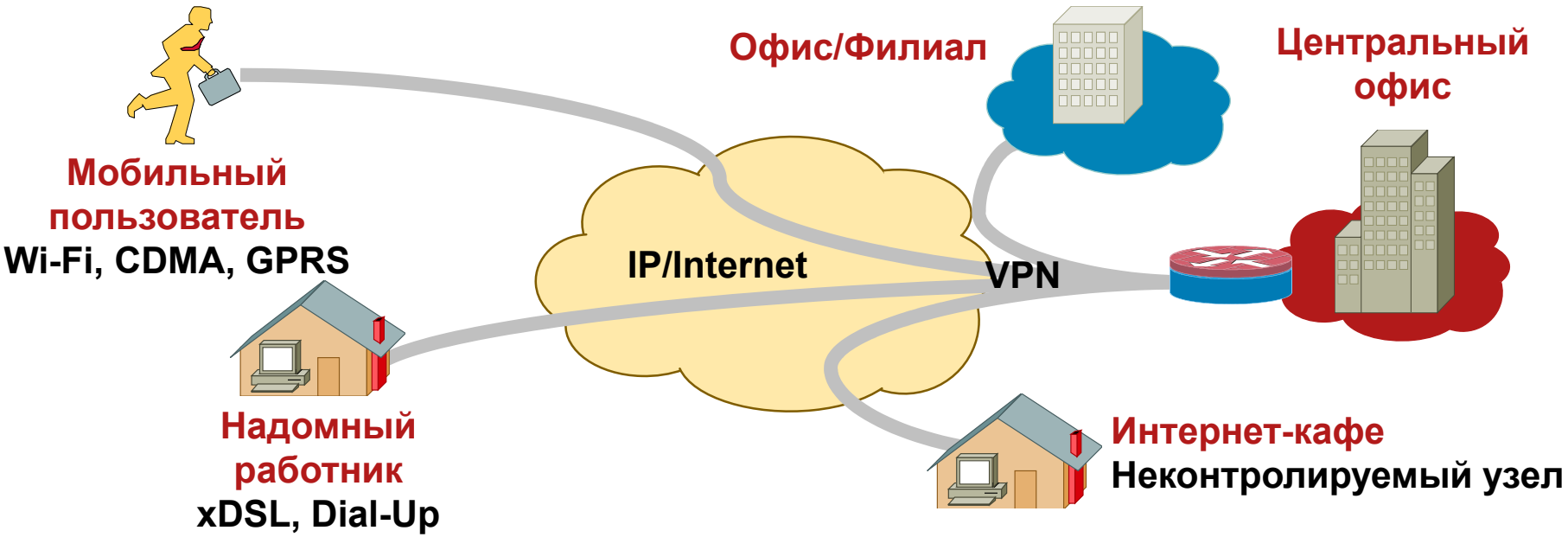
Защищенный удаленный доступ
Взгляд со стороны корпоративного центра



- Идентификация и управление доступом:
  - Межсетевые экраны, IPSec, SSL VPN, списки ACL, NAC
- Выявление и подавление угроз:
  - NetFlow, Syslog, SNMP, MARS, NIPS, HIPS
- Защита инфраструктуры:
  - AAA, CoPP, SSH, RFC2827, SNMP v3, IGP/EGP MD5
- Безопасность приложений:
  - ACE, ACE XML Gateway
- Управление безопасностью:
  - CSM, MARS, NCM

Защищенный удаленный доступ
Взгляд со стороны клиента

Защита удаленного клиента



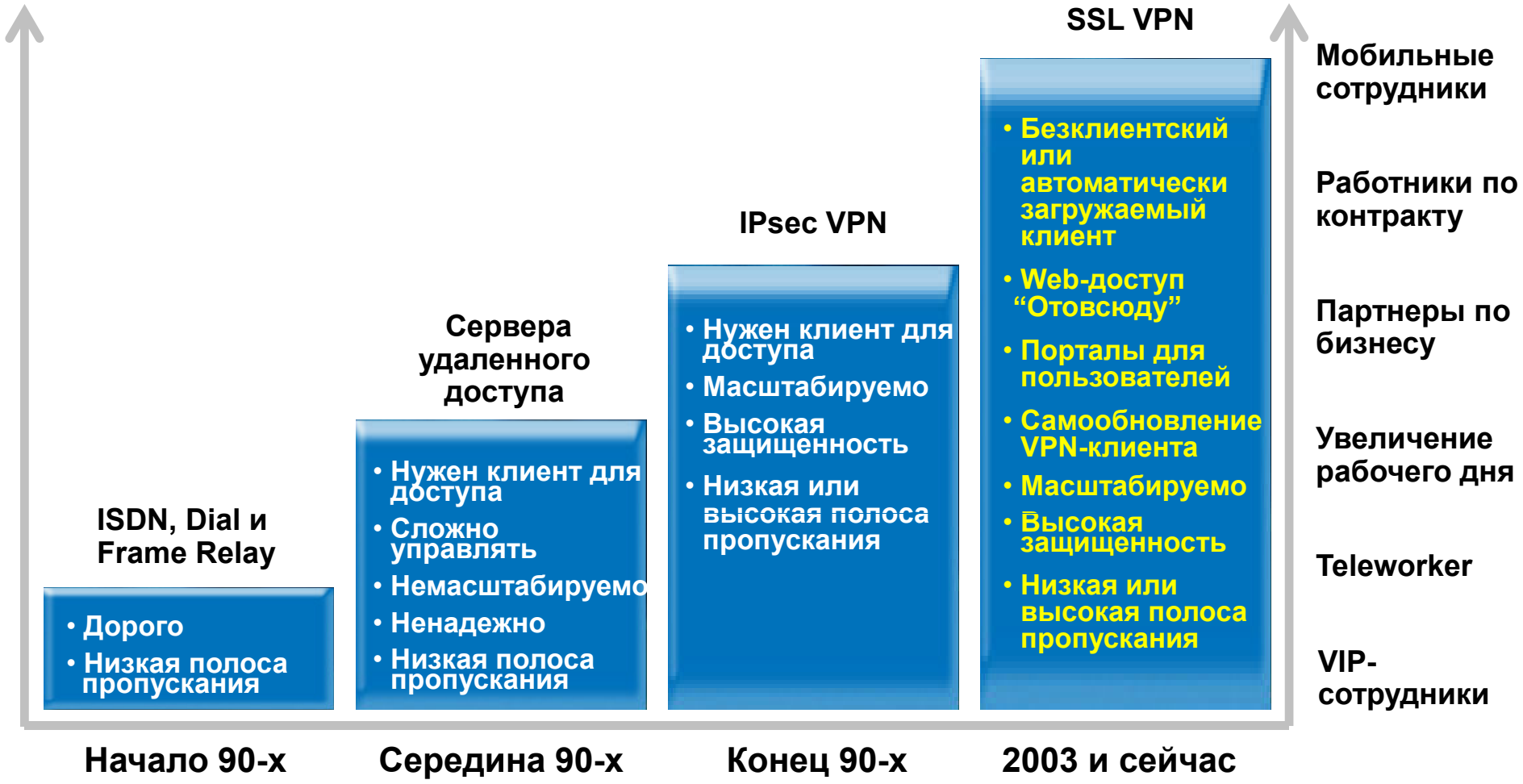
- Защита хранимых и передаваемых с клиента данных
- Выполнение требований регуляторов и корпоративной политики
- Обеспечение работы с недоверенных компьютеров
- Интеграция в корпоративную систему обеспечения ИБ
- Отсутствие помех работе бизнес-приложений

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?

Защищенное подключение

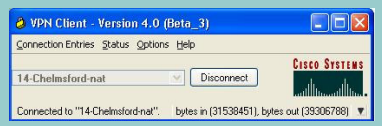
Эволюция удаленного доступа



Сравнение технологий удаленного доступа

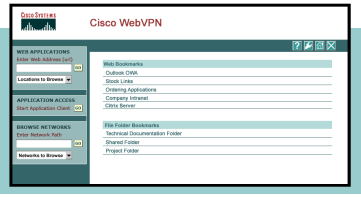
Существует 2 основные технологии удаленного доступа: IPSec и SSL. SSL – более новая технология; обычно более дешевая и обеспечивающая лучший доступ для партнеров и контрактников (по сравнению с IPSec). SSL обеспечивает более быструю связь, чем IPSec.

IPSec VPN



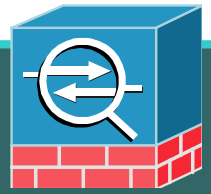
- Широко распространенная, отработанная технология
- Хорошо подходит для расширенного доступа сотрудников с корпоративнымы компьютерами

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

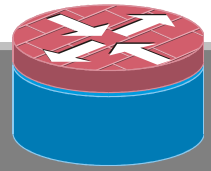
Cisco ISR или Cisco ASA как VPN?



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

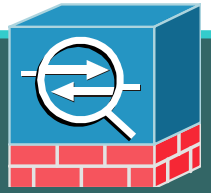
Cisco ISR Router



- 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

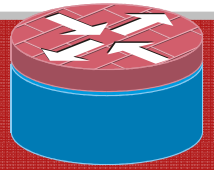
Cisco ASA или Cisco ISR для SSL VPN?



Cisco ASA 5500

- Ключевой продукт Cisco для удаленного доступа
- Ориентирован на любой сегменте – от SMB до крупного предприятия
- Поставляется как «чистый» VPN или UTM+VPN

Cisco ISR Router



- Первый маршрутизатор в мире с SSL VPN
- Ориентирован на SMB
- Использует сделанные инвестиции в маршрутизаторы

	ASA 5500	ISR Routers
Масштабируемость	От 10 до 5000 сессий	От 10 до 150 сессий
Функции Clientless	Расширенные	Стандартные
Функции Client	Расширенные	Расширенные
Интеграция СЗИ	Лидирующая	Выше среднего
Гибкость	Расширенная	Не применимо
Балансировка	Расширенная	Не применимо

Cisco ASA 5500

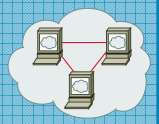
МСЭ / Защита приложений

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

IPS / Анти-вирусная защита

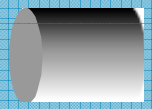
- Защита от сетевых червей и вирусов
- Обнаружение и фильтрация вредоносного кода
- Технология аккуратного предотвращения и упреждающее реагирование
- Корреляция событий и упреждающее реагирование

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

Cisco SSL VPN: расширенные функции

Доступ отовсюду

Доступ с большинства платформ

Расширенная защита

Защита до, в процессе и после

Эффективный контроль

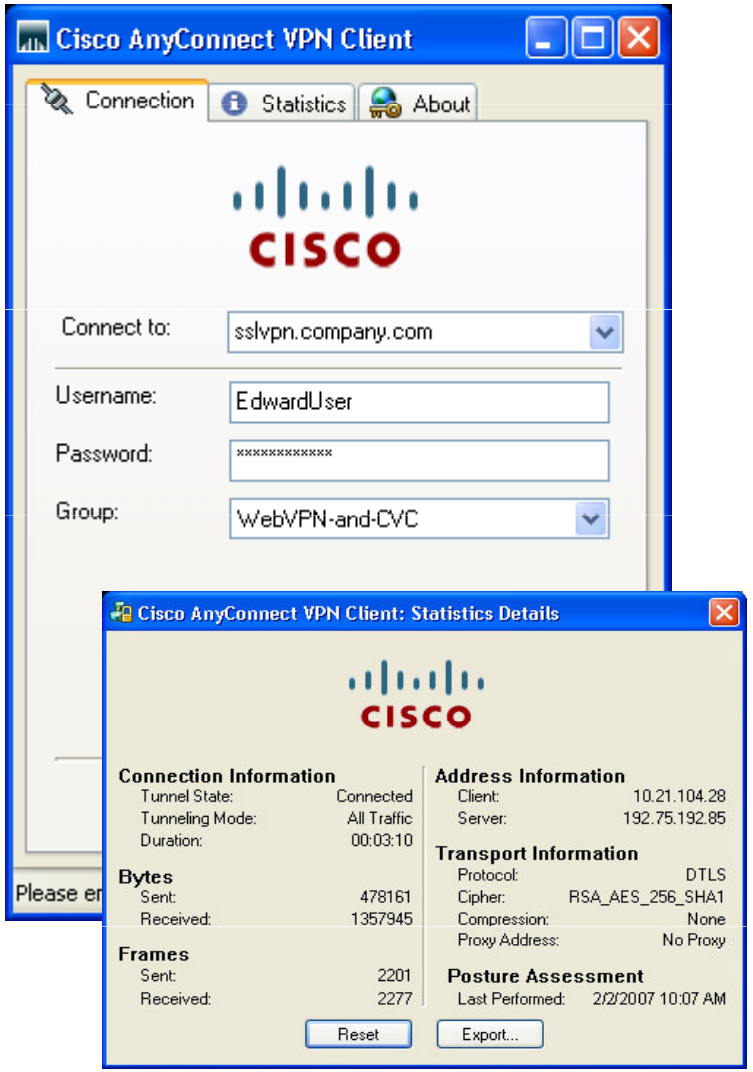
Мониторинг и анализ

Простота управления

Интуитивно понятный интерфейс

Cisco AnyConnect Client

- VPN-клиент, доступный на многих платформах:
  - Windows Vista 32/64-bit, Windows XP 32/64-bit и Windows 2000
  - Mac OS X 10.4 (Intel и PPC)
  - Intel-based Linux
  - Windows Mobile 5\6 Pocket PC Edition
- Стандартный клиент или автоматически скачиваемый через Интернет
  - Автоматическое обновление
- Старт до входа в систему



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

Сравнение VPN-протоколов

	HTTPS/SSL	DTLS/SSL	IPsec / IKEv1
Блокирование на МСЭ	Да	Нет	Через TCP tunneling
Совместимость с прокси-серверами	Да	Нет	Нет
Высокопроизводительный транспорт	Нет	Да	Да
Резервный протокол	Не применимо	HTTPS/SSL (TCP)	
Поддержка QoS (DSCP Preservation)	Нет	Возможно	Да
Поддержка мобильности	Да	Да	Нет (IKEv2/Mobile IKE)
Транспорт	TCP	UDP	ESP, UDP, Fake TCP
Ценность для клиента ($$s)	$$$	$$$	$

Cisco Secure Desktop

Перед установлением соединения выполняется проверка:

- Местонахождение – управляемый/неуправляемый компьютер?
- Установленное ПО: AV, МСЭ, malware?

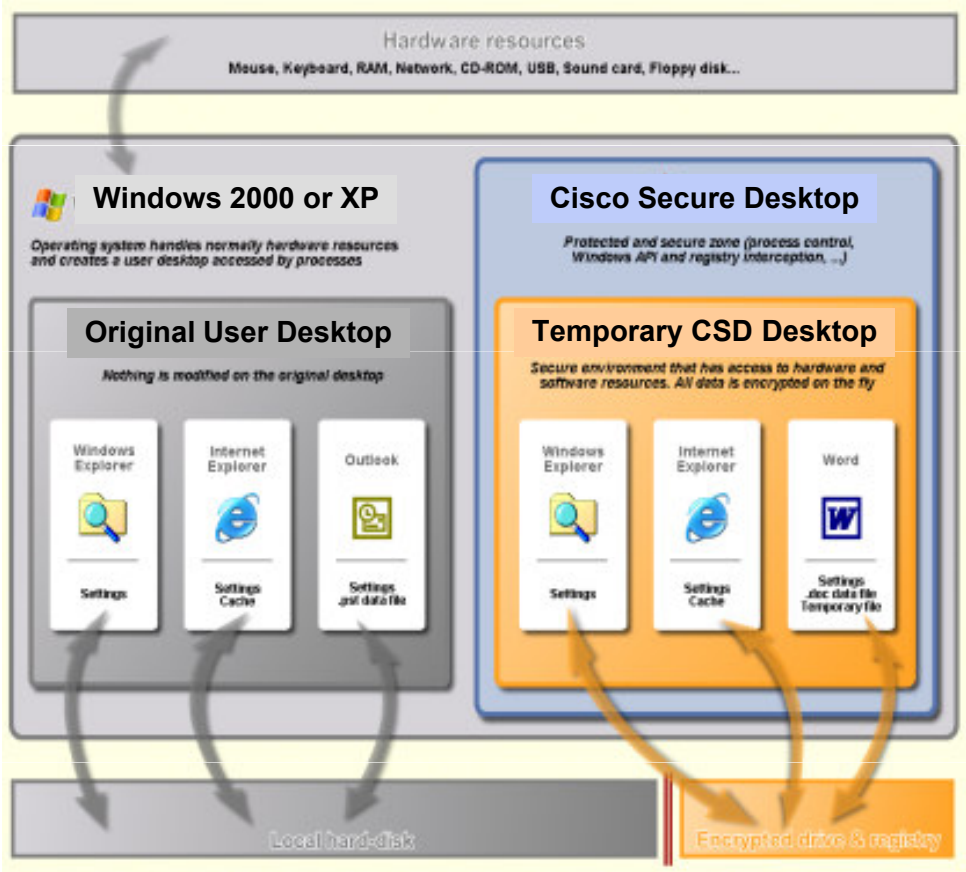
Максимальная защита сессии:

- Выделенный сегмент защищает данные на компьютере
- Обнаружение Malware с помощью Microsoft free anti-spyware software

Удаление данных после завершения соединения:

- Защищенный сегмент очищается
- Cache, history и cookie удаляются
- Скачанные файлы удаляются
- Пароли удаляются

Работает с гостевыми правами
Не требует полномочий администратора

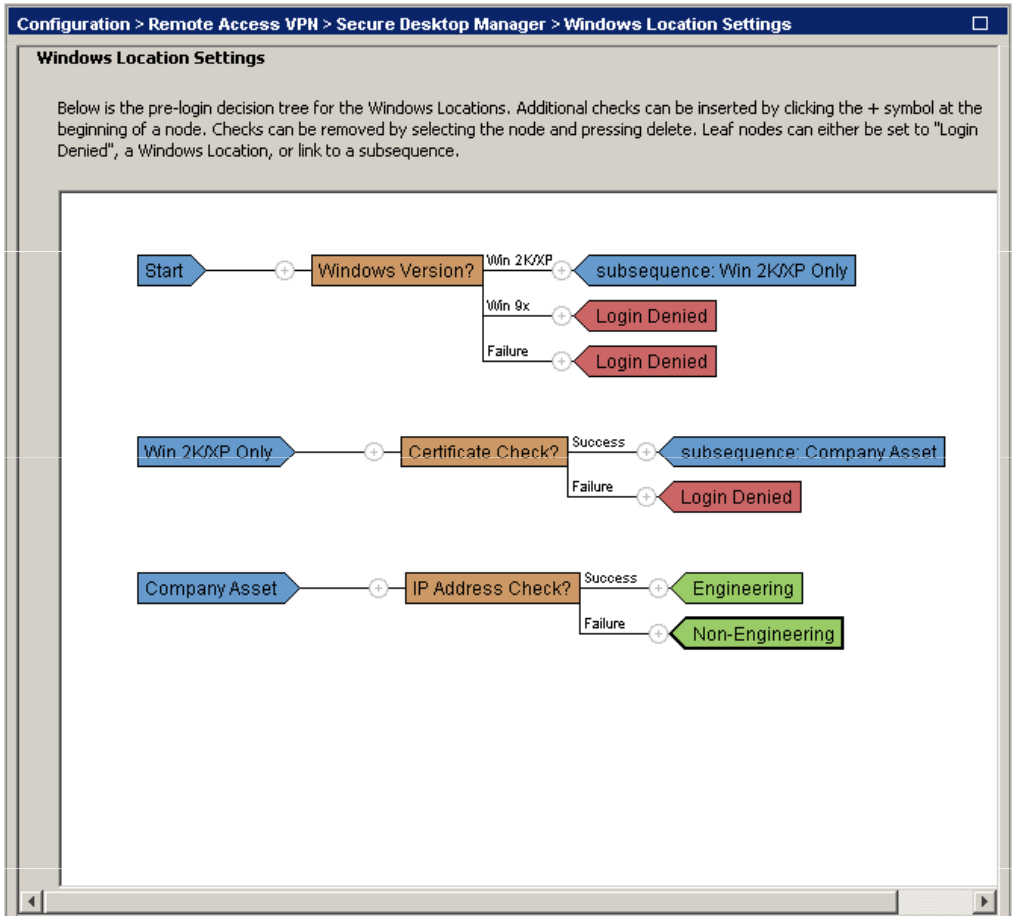


Расширенная защита ПК

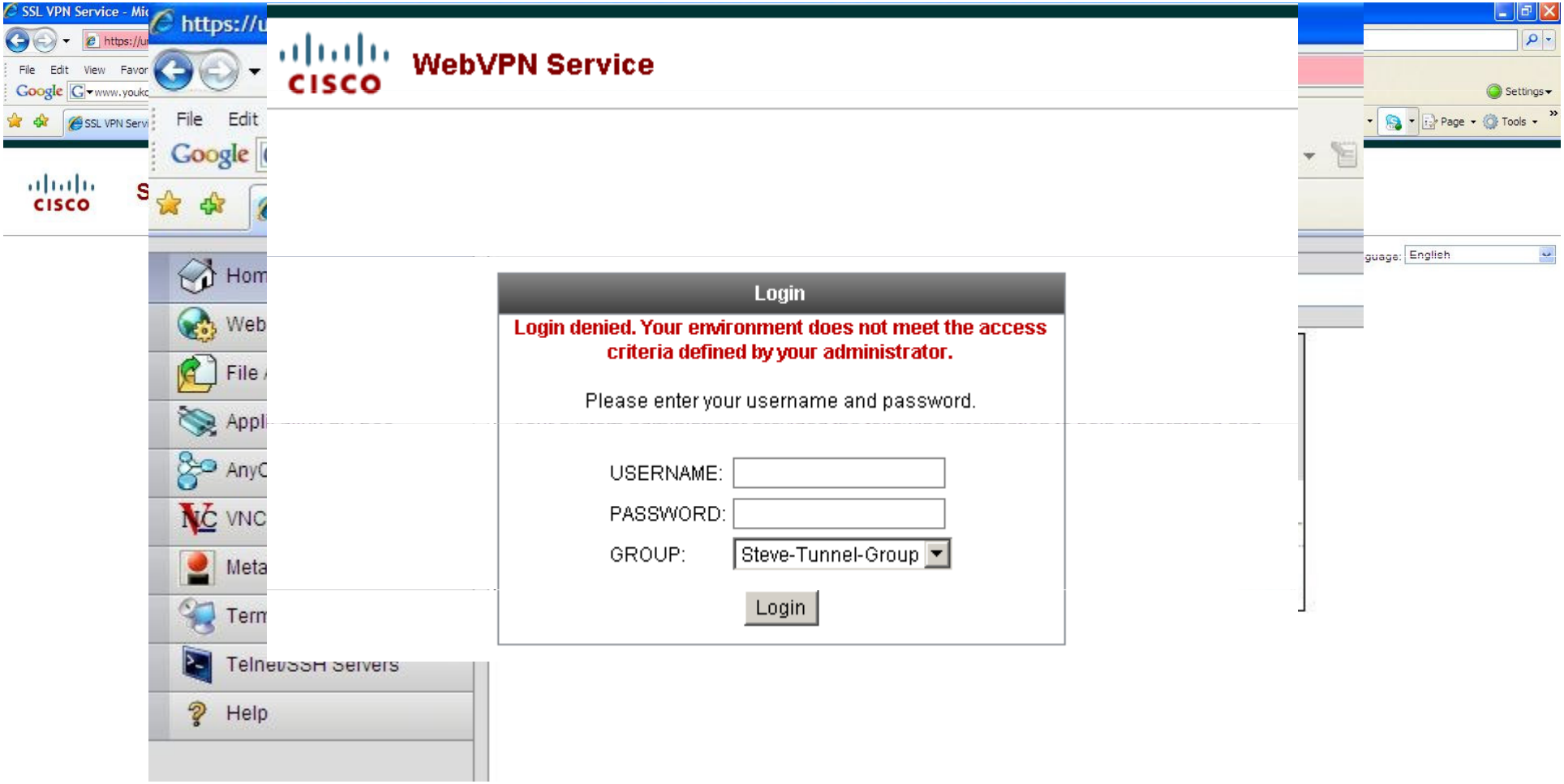
- Cisco Secure Desktop (CSD) поддерживает сотни предустановленных приложений
  - Антивирусы, anti-spyware, персональные МСЭ и др.
- 4 основных функции
  - Host Scan (Windows)
  - Advanced Endpoint Assessment
  - Secure Vault (Windows 2K/XP)
  - Cache Cleaner (Windows, Mac OS X и Linux)

Собственные проверки

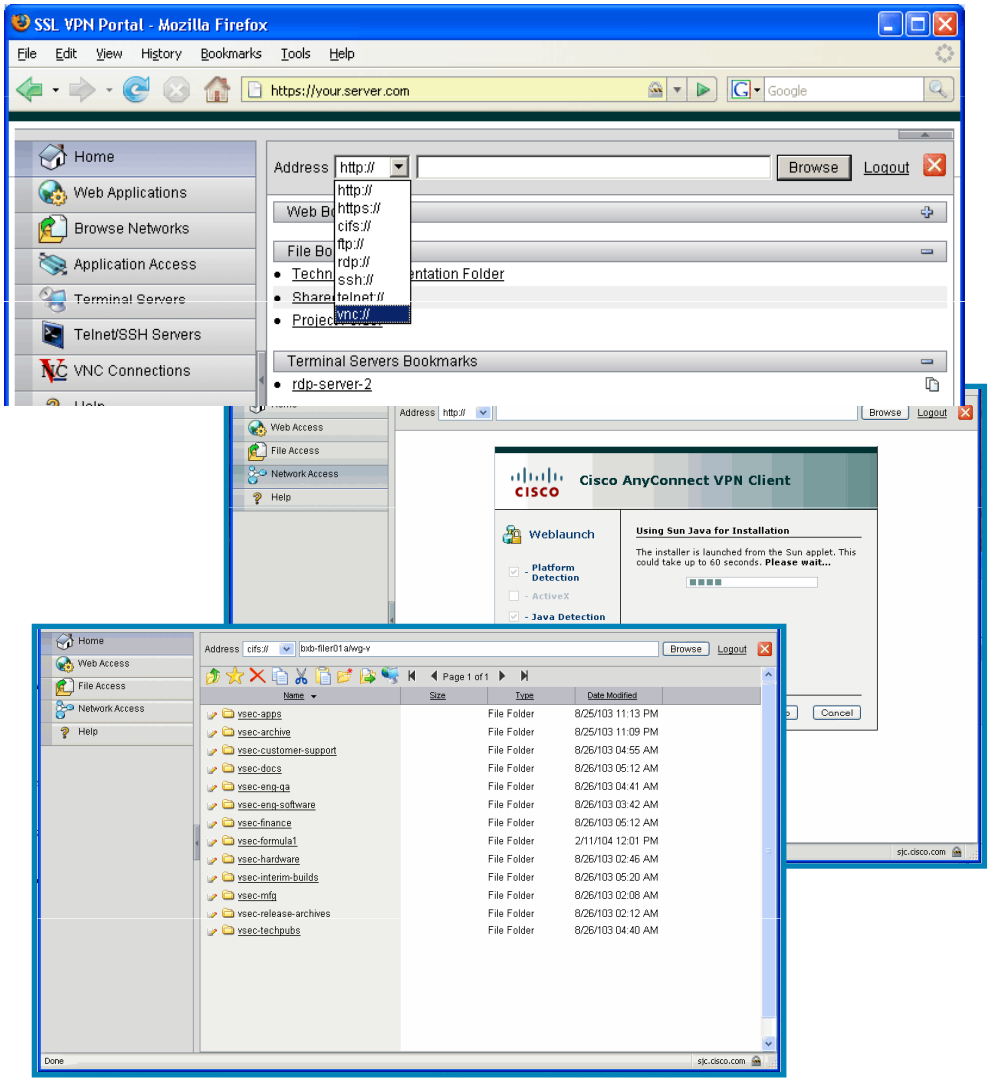
- Поддерживаемые проверки
  - Проверки реестра
  - Проверки файлов
  - Проверки сертификатов
  - Проверка версии Windows
  - Проверка IP-адресов
- Визуализация облегчает конфигурирование и снижает число ошибок



Что после проверки?



Пользовательский портал

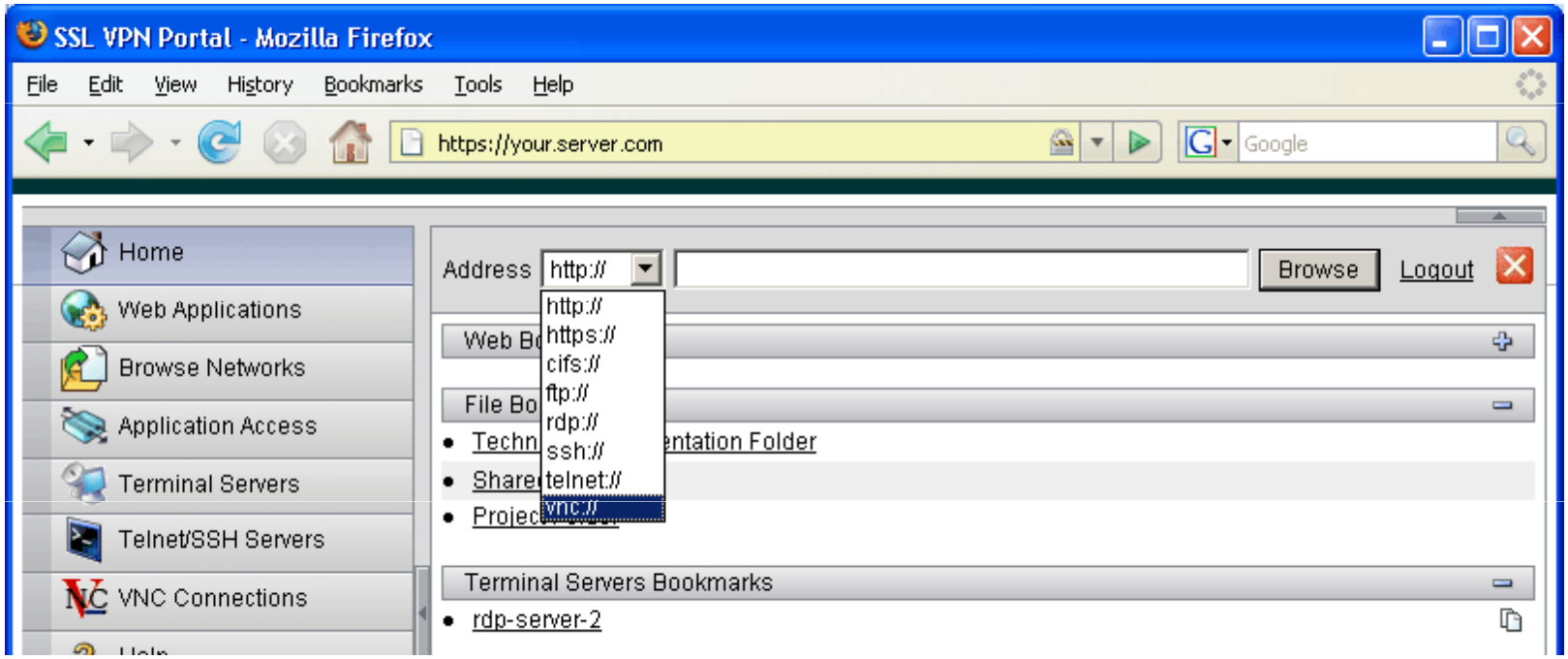


- Доступ к отдельным ресурсам
- Новый дизайн портала
  - Локализация
  - RSS
  - Персональные закладки
  - Доступ с AnyConnect Client
- Доступ к файлам (FTP/CIFS)
- Поддержка Flash
- Поддержка удаленного управления через telnet, SSH, RDP и VNC
- Перенаправление запросов на доступ к Windows-приложениям (Smart Tunnel)

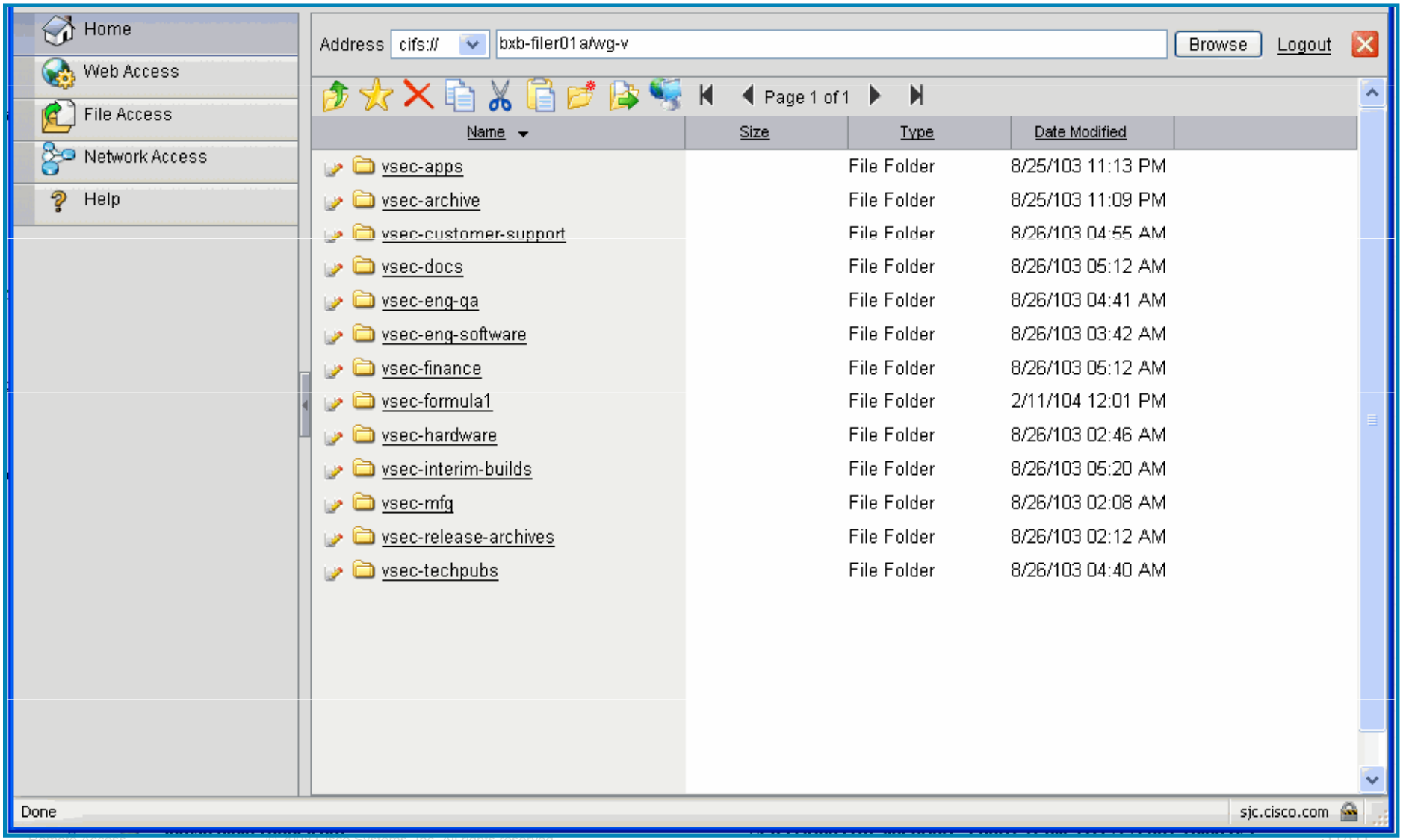
Доступ к различным ресурсам

- Обеспечивается доступ к web- и традиционным приложениям через браузер
- Технология Smart Tunnel обеспечивает доступ TCP приложениям

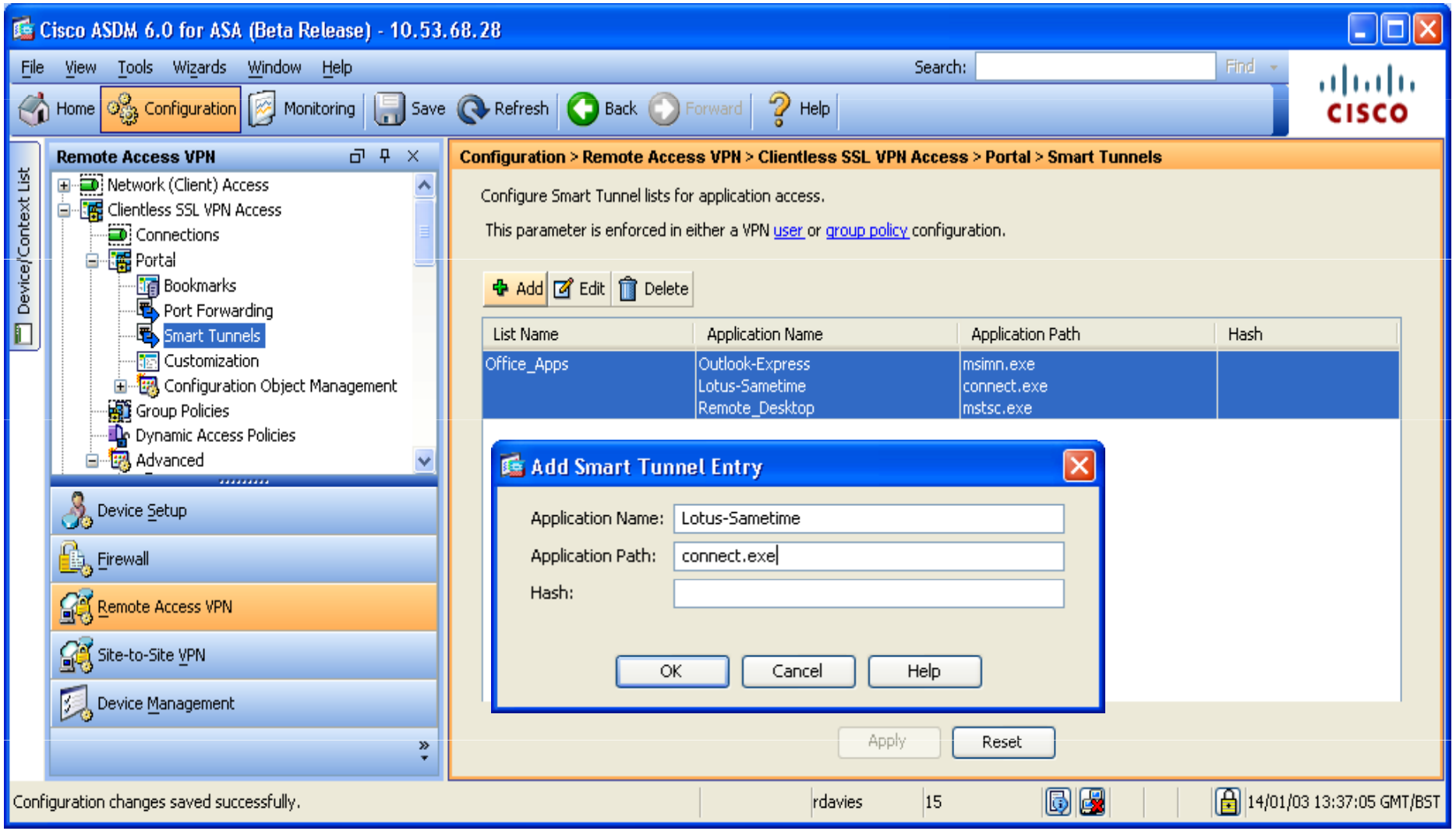
  Не требуется полномочий администратора на ПК



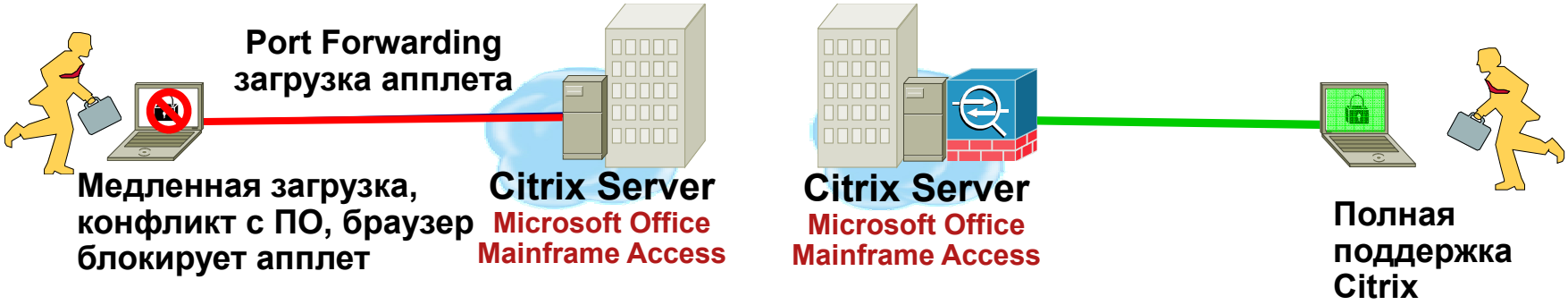
Доступ к файловым ресурсам



Smart Tunnel – работа приложений через SSL



Полная поддержка Citrix



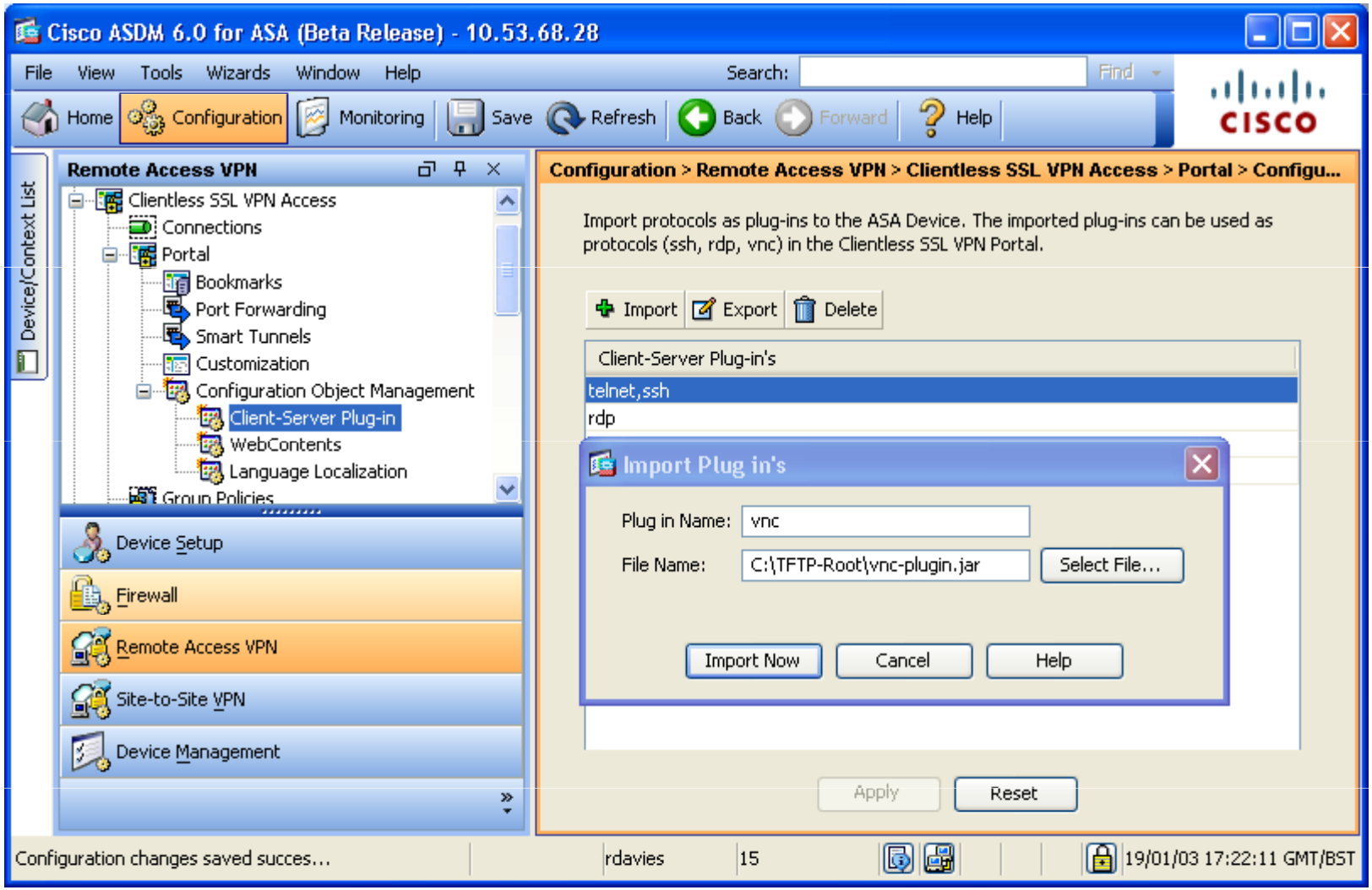
Типичная поддержка Citrix SSL VPN

- Поддержка Citrix требует специального SSL-клиента или Java-апплета или иного резидентного ПО
  - Медленная инициация приложения
  - Может не работать из-за настроек безопасности браузера
  - Потенциальные конфликты ПО, особенно на неуправляемых узлах

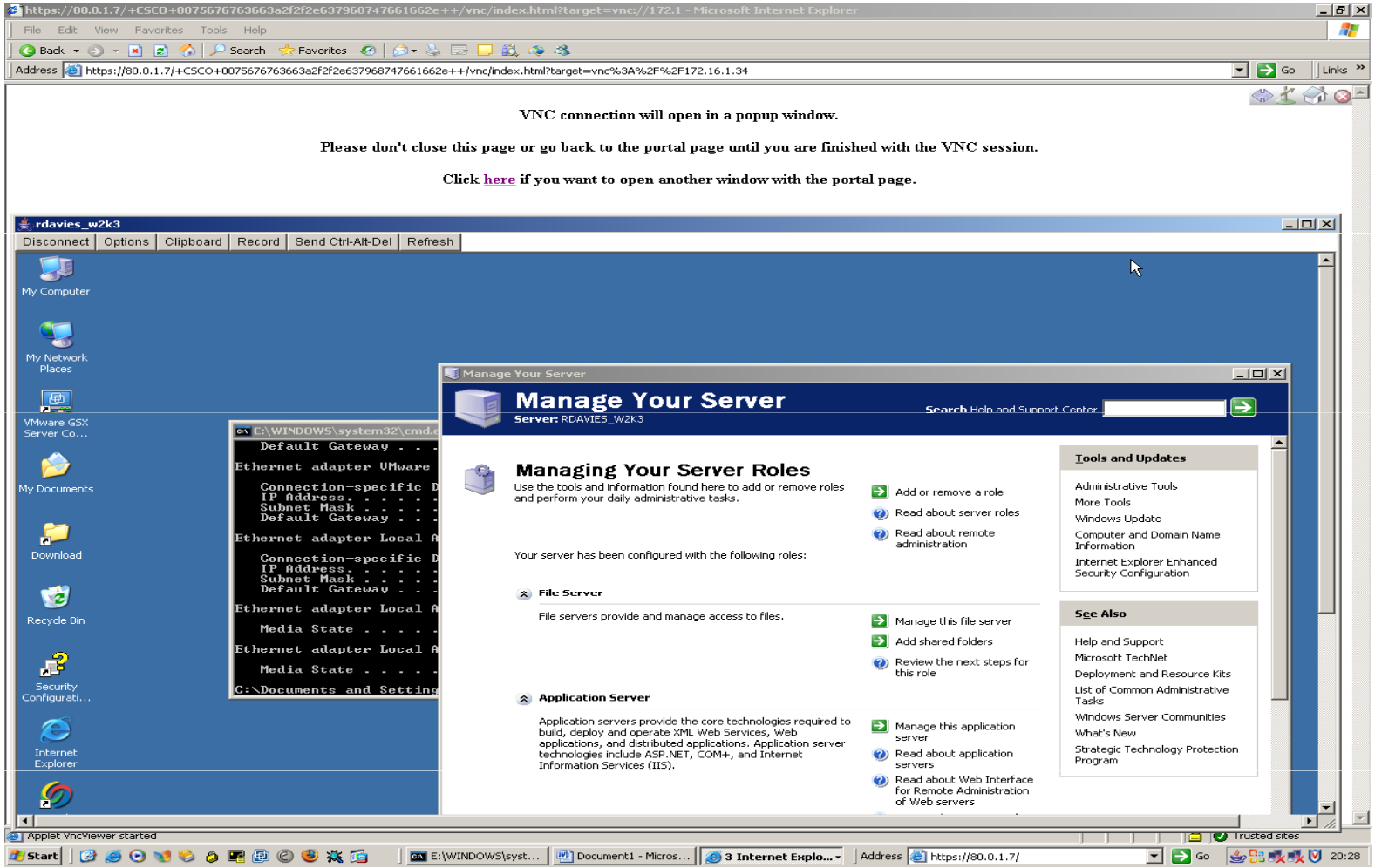
Поддержка Cisco Citrix

- Полная поддержка Citrix без специального клиента
  - Быстрое время инициализации – ничего не надо загружать
  - Высокая производительность – нет локального приложения-транслятора
  - Не зависит от настроек безопасности и браузера
  - Высокая стабильность – нет потенциальных конфликтов с ПО

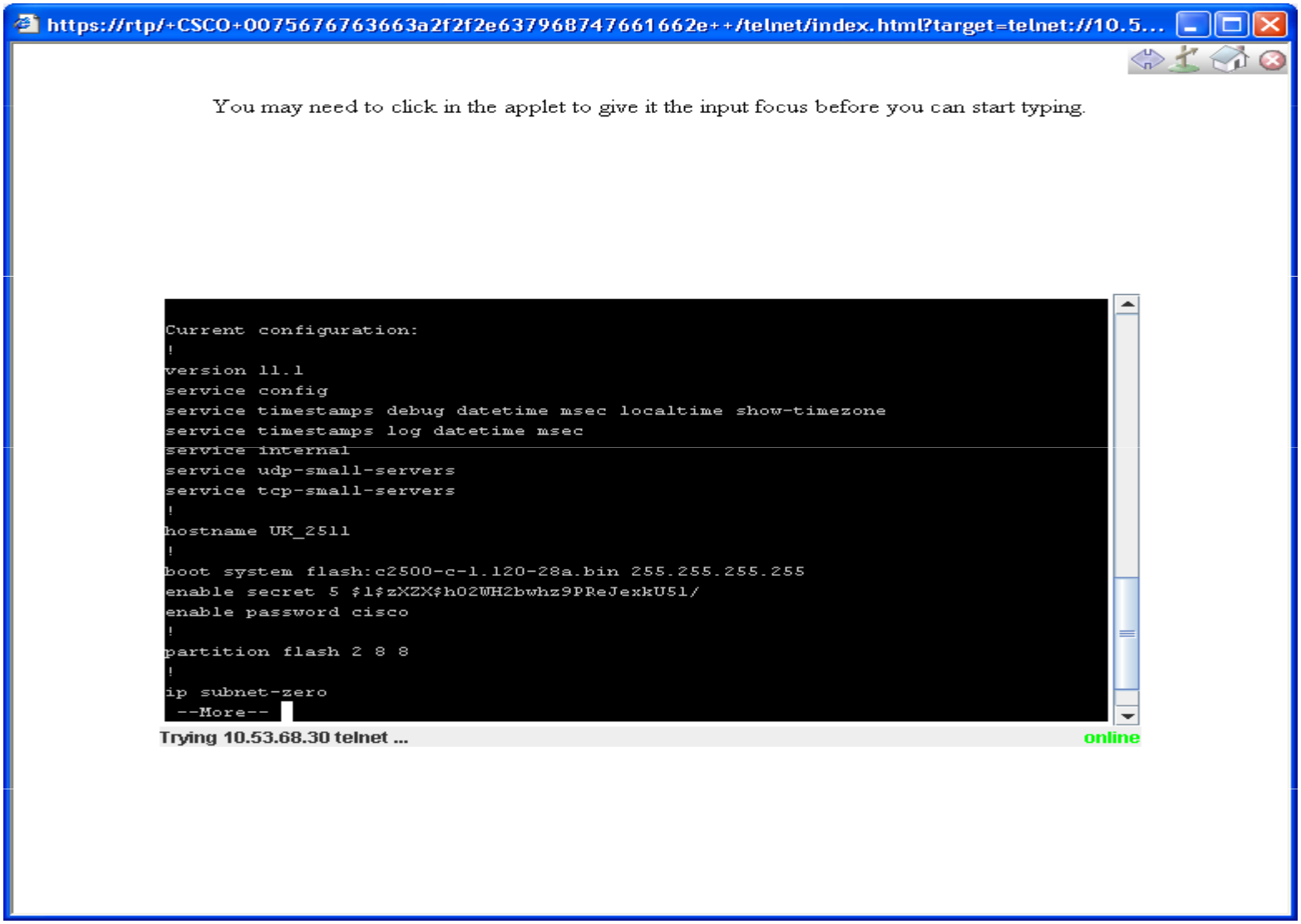
Терминальный доступ



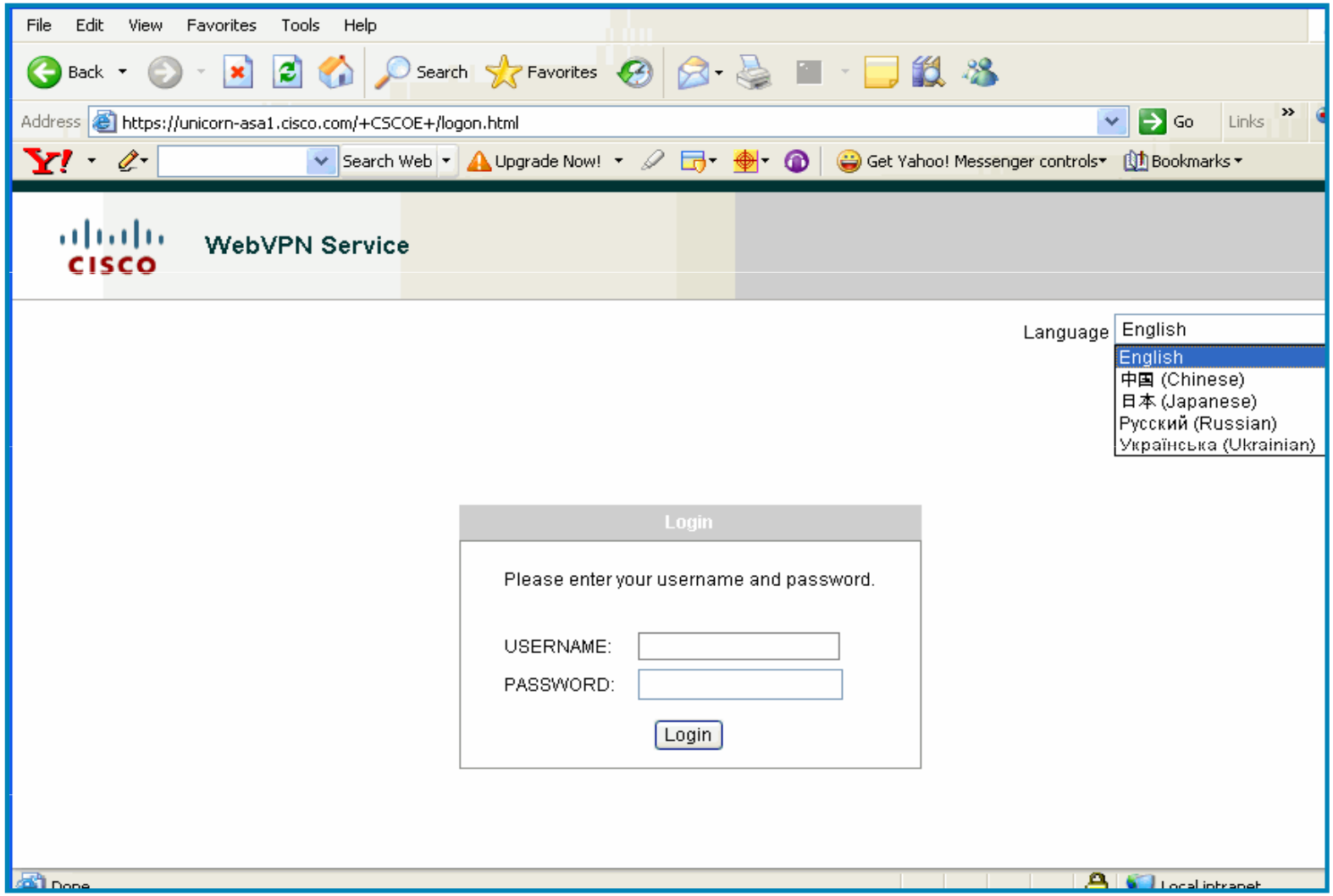
Поддержка VNC/RDP



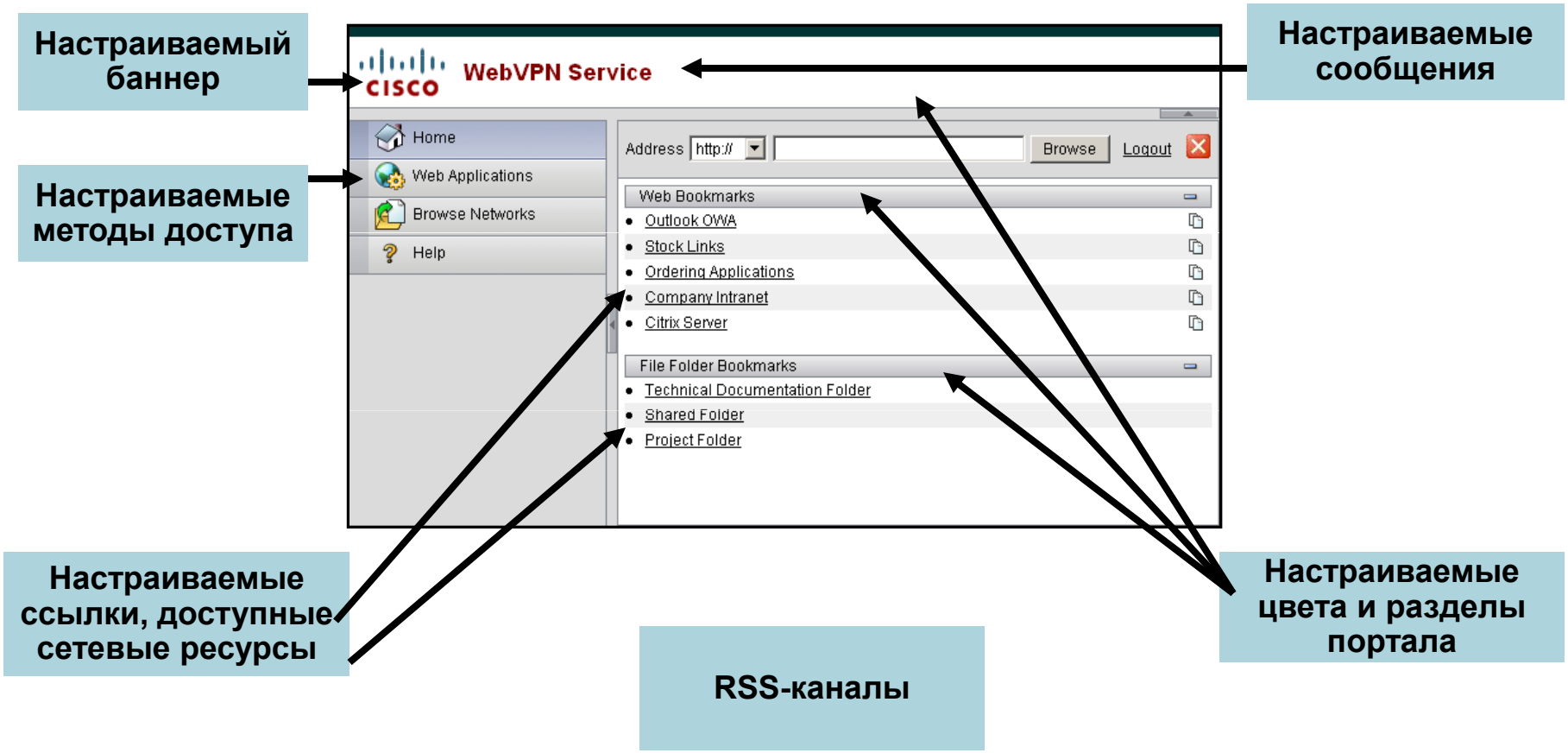
Поддержка Telnet/SSH



Локализация интерфейса

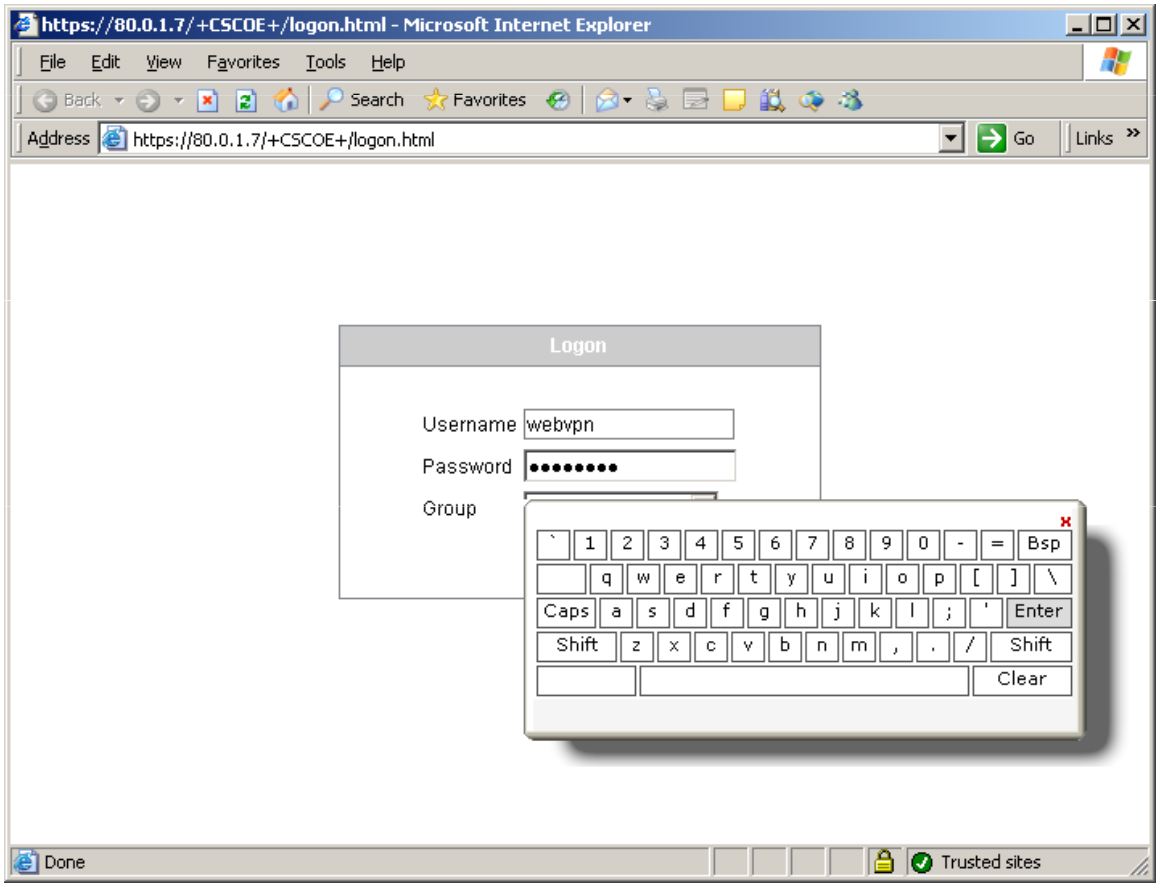


Персонализированный портал



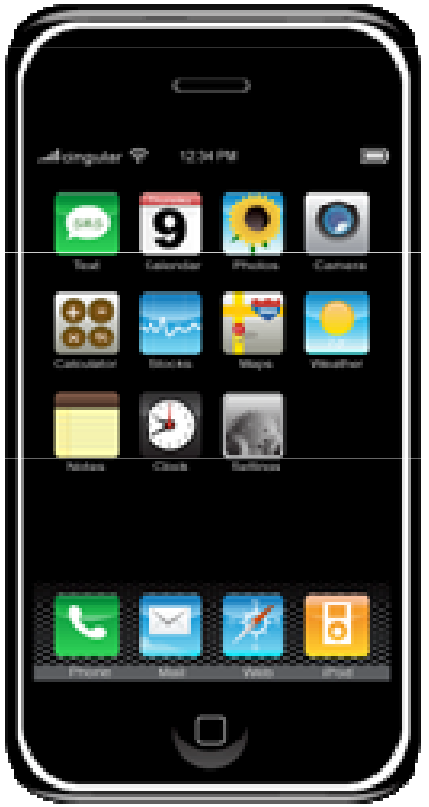
Виртуальная клавиатура

- Основное назначение – защититься от перехватчиков ввода с клавиатуры
- Может быть использована на любой странице, где требуется ввести пароль



Дополнительные особенности

- Поддержка Group/User-to-VLAN mapping
- Расширенные механизмы AAA
  - Аутентификация на LDAP, RADIUS и т.п.
  - Встроенный Certificate Authority (CA)
  - SAML Single Sign-On (SSO) совместно с RSA Access Manager (бывший ClearTrust)
- API для интеграции с внешними системами
  - Контроль соединений, получение статуса, разрыв соединения
- Cisco IPSec VPN-клиент включен в Apple iPhone



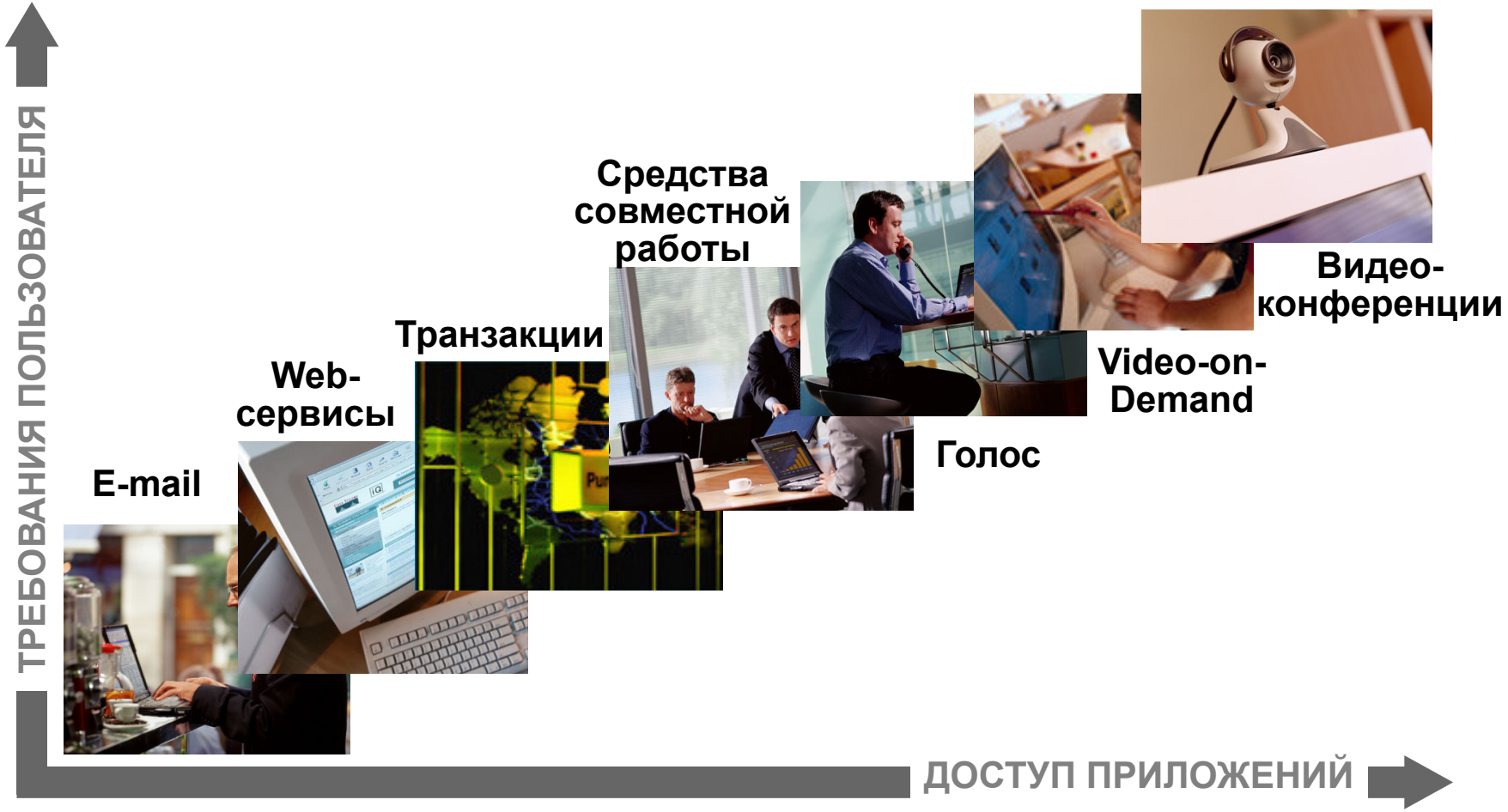
Расширенная защита приложений удаленного доступа

Понимание удаленных пользователей

- Какие приложения нужны для работы?
  - Web-сервисы (включая Web-почту)
  - Тонкий клиент (TCP)
  - Полный сетевой доступ
- Откуда они могут получать доступ?
  - Контролируемые компанией компьютеры
  - Неконтролируемые компьютеры
  - Интернет-кафе
- Как долго пользователь может оставаться «на связи»?
  - 24x7 или в течение бизнес-часов
  - Ограниченный период времени

Как меняются требования приложений?

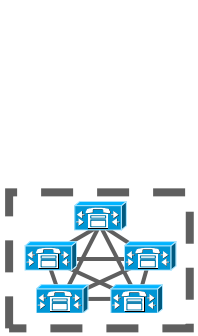
Удаленные пользователи требуют доступа к тем же приложениям, что и сотрудники центрального офиса

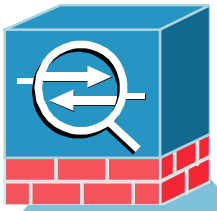


Защита IP-телефонии

- 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)

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

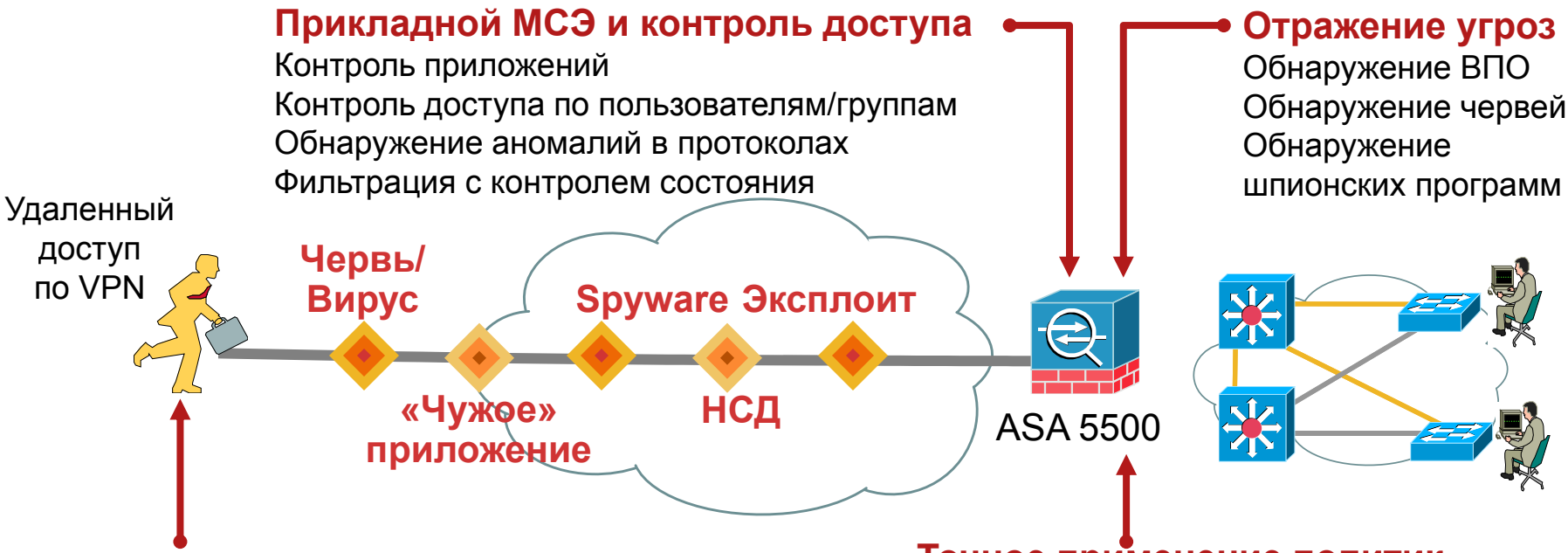
- Инспекция RTP/RTCP
- SIP и SCCP Video Endpoints – IP phones, VT Advantage, Cisco Unified Personal Communicator
- Политики - разрешить/запретить звонки с незарегистрированных телефонов, абонентов, whitelist, blacklist

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**

Интеграция защитных функций



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

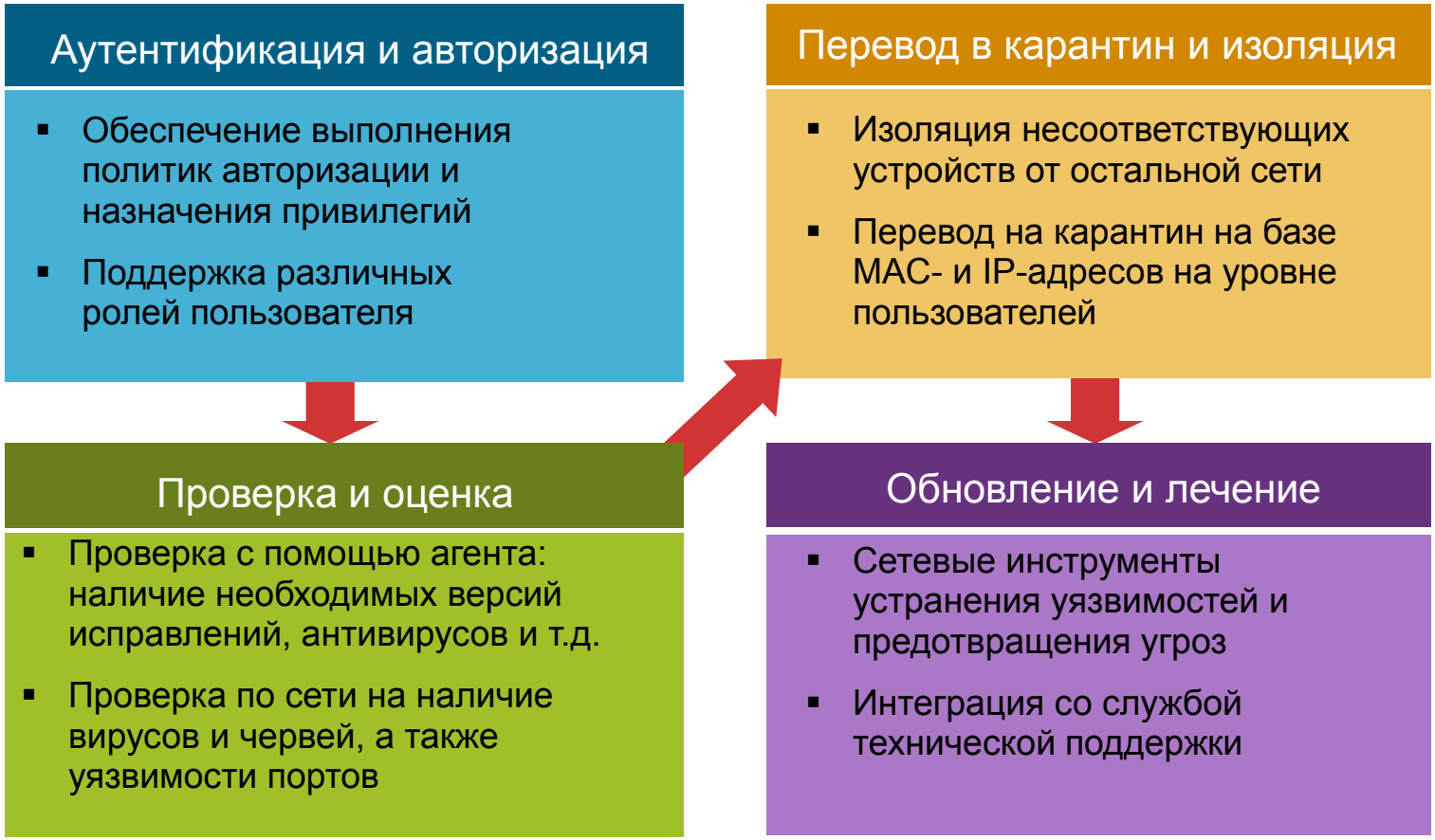
Другие требования по защите удаленного доступа

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:

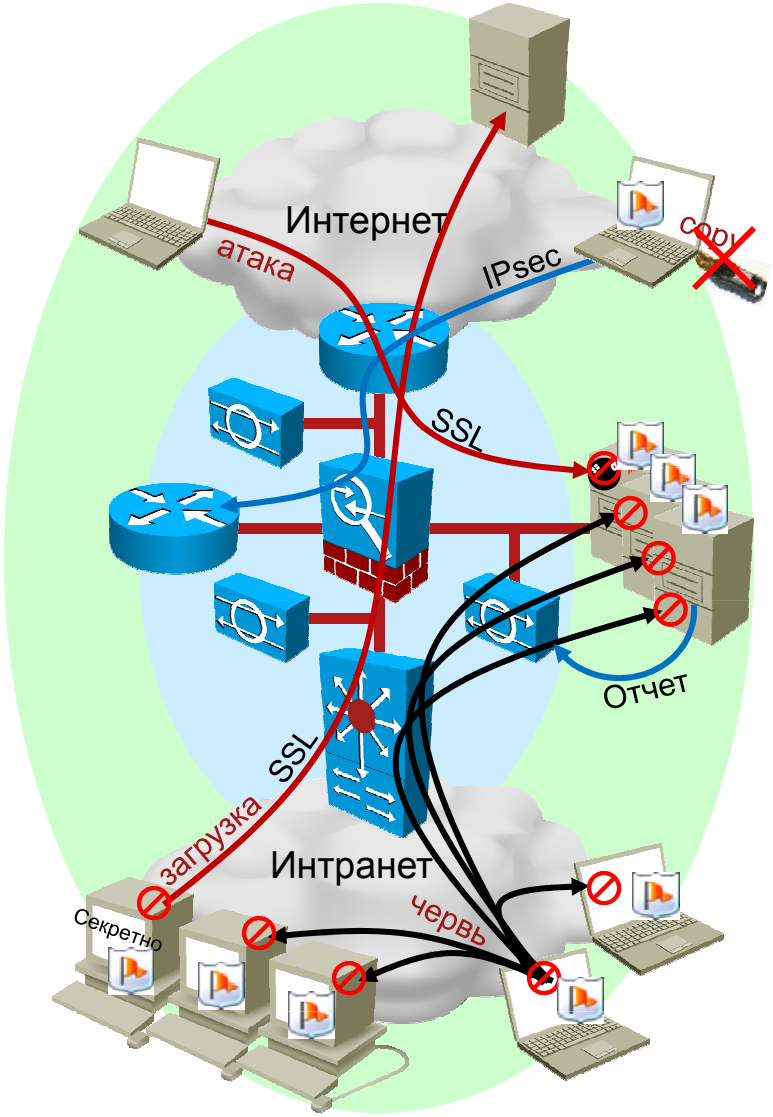


НЕТ СООТВЕТСТВИЯ = НЕТ ДОСТУПА К СЕТИ

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.



Cisco Case Study

История: 1999 год

- С ростом Интернет и широкополосного доступа ИТ начинает проект по организации удаленного широкополосного доступа для сотрудников с рядом операторов связи
- Главная проблема: Множество поставщиков, неполное покрытие

  Наша цель - обеспечить лучший сервис для всех сотрудников по разумной цене
- Rhythms NetConnections был выбран для обеспечения защищенного xDSL-доступа для сотрудников в США

  Сервис Rhythms DSL был эффективным «частным" DSL сервисов, предлагающим прямое виртуальное соединение с корпоративной сетью Cisco

Кризис удаленного доступа

- Август 2001: Rhythms NetConnections обанкротился; более 9000 сотрудников оказались без доступа, ранее обеспечиваемого с помощью Rhythms DSL service

  Задача – обеспечить доступ 9000 сотрудников за один месяц

- Из опыта ИТ знали, что миграция на другой сервис обойдется дороже и потребует в 10 раз больше человеческих ресурсов, чем было в наличии

VPN-решение

- Кризис удаленного доступа заставил ИТ задуматься о других вариантах
- Из множества сценариев была выбрана новая модель:
  - Пользовательская модель на базе программного VPN-клиента
  - Пользователь сам выбирал способ подключения к сети (GPRS, CDMA, Wi-Fi, DSL и т.д.)
  - Cisco оплачивает подключение к оператору связу
  - Cisco IT обеспечивает и поддерживает VPN-соединение через Интернет-шлюз в корпоративную сеть Cisco

Влияние на бизнес

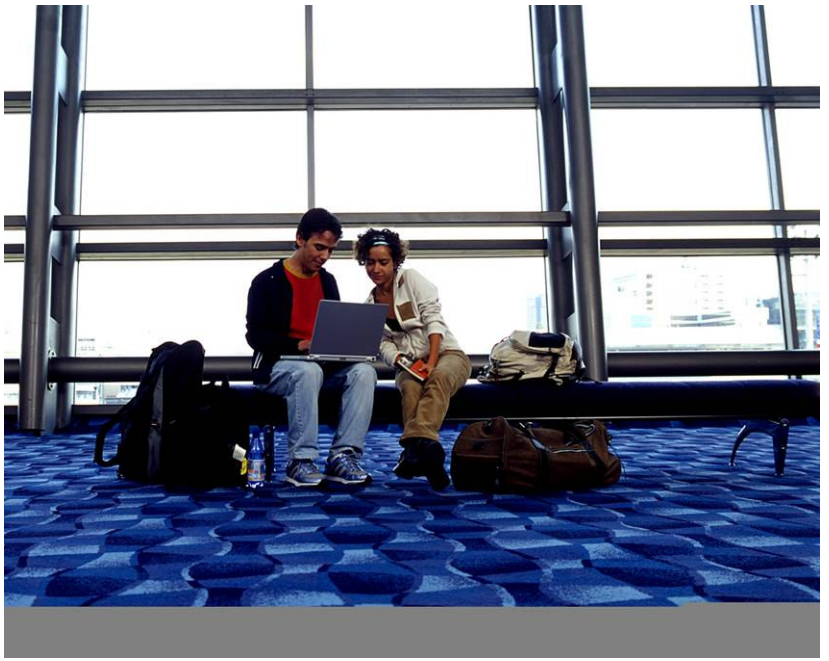
- Рост продуктивности

  Удаленный доступ означает возможность работать из дома или в дороге. Для многих пользователей это значит увеличение продуктивности на 10-40% в день

- Рост удовлетворенности

  Сотрудники находят баланс между работой и семьей, имея возможность подключаться к корпоративной сети в любое время.

  В 2001 Cisco® имело 9000 DSL пользователей, а в 2003 их стало уже 23,000.



Влияние на бизнес

- Глобализация

  Глобальная компания должна предоставлять эффективную возможность работать всем сотрудникам, находящимся в разных часовых поясах, в разных точках земного шара.

- Гибкость

  Удаленный доступ обеспечивает гибкость во время кризисов, эпидемий, катастроф и т.д.

- Поддержка

  Т.к. большинство сотрудников Cisco используют собственное подключение к оператору связи, мы не тратим усилия на поддержку и разбор проблем, связанных с подключением к Интернет

Заключение

Унифицированный доступ с ASA

Вопросы?

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