Контроль пользовательского доступа на основе технологии 802.1x и цифровых сертификатов

Томилко Виталий Евгеньевич
Системный архитектор

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Предоставление доступа пользователей к внутренним ресурсам

- Наличие последних обновлений антивирусных баз данных на рабочих станциях
- Контроль п/о рабочих станций (OS service pack, HotFixes)
- Контроль техно-парка оборудования (серверы, ноутбуки, рабочие станции, персональные устройства КПК, принтеры, терминалы и т.д)
- Контроль пользователей и привилегий доступа

Защита от неавторизованного подключения и контроль

Протокол 802.1x

- Контроль подключений персональных устройств к сети

Выбор EAP-TLS

(PKI инфраструктура)

(сертификаты X.509)

Цифровые сертификаты X.509

- Идентификация и авторизация сетевых устройств и пользователей при подключении к сети

Защита от неавторизованного подключения и контроль

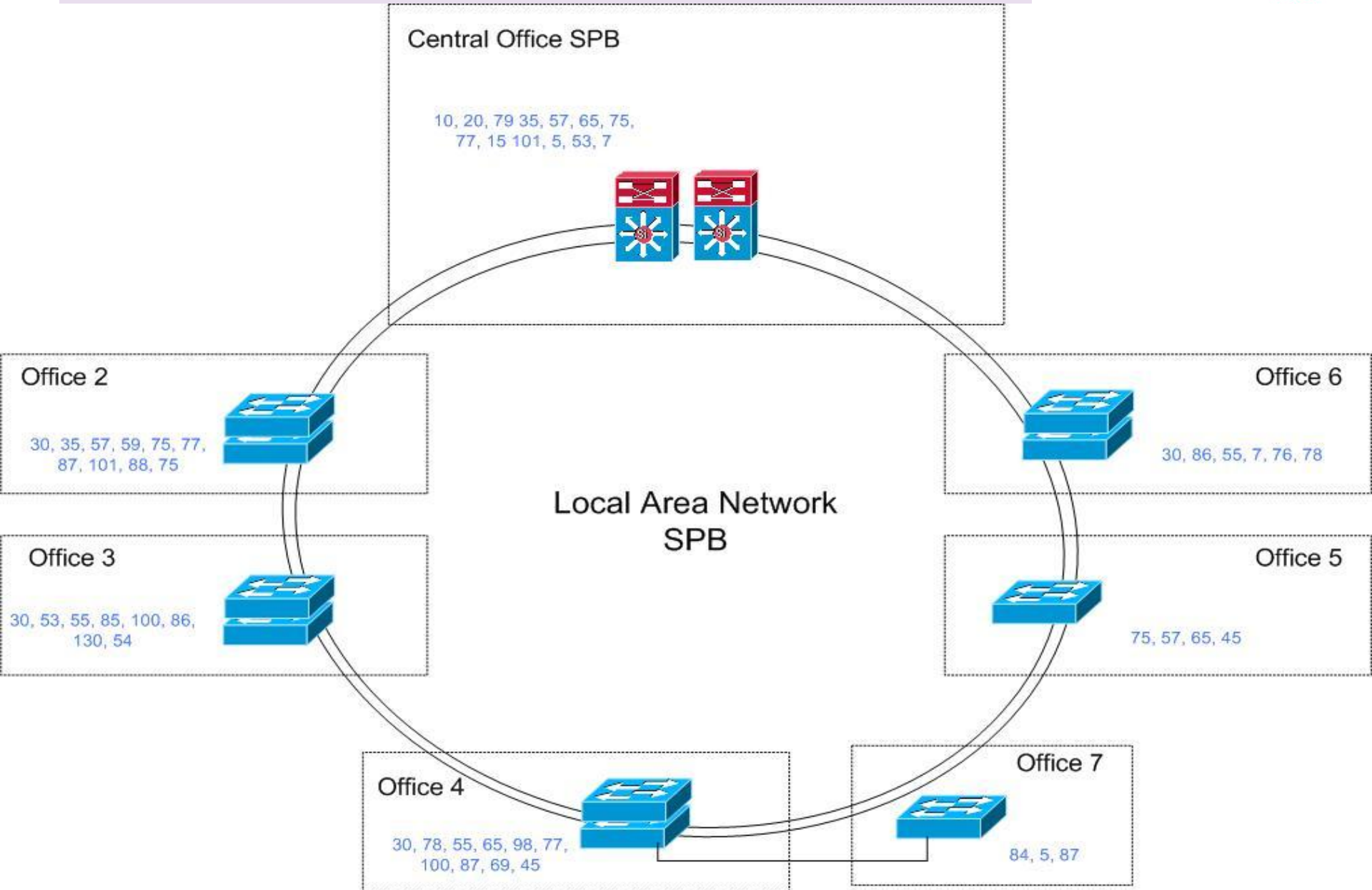
Практические аспекты внедрения решения для территориально-распределенной организации

ОТКРЫТЫЕ ТЕХНОЛОГИИ

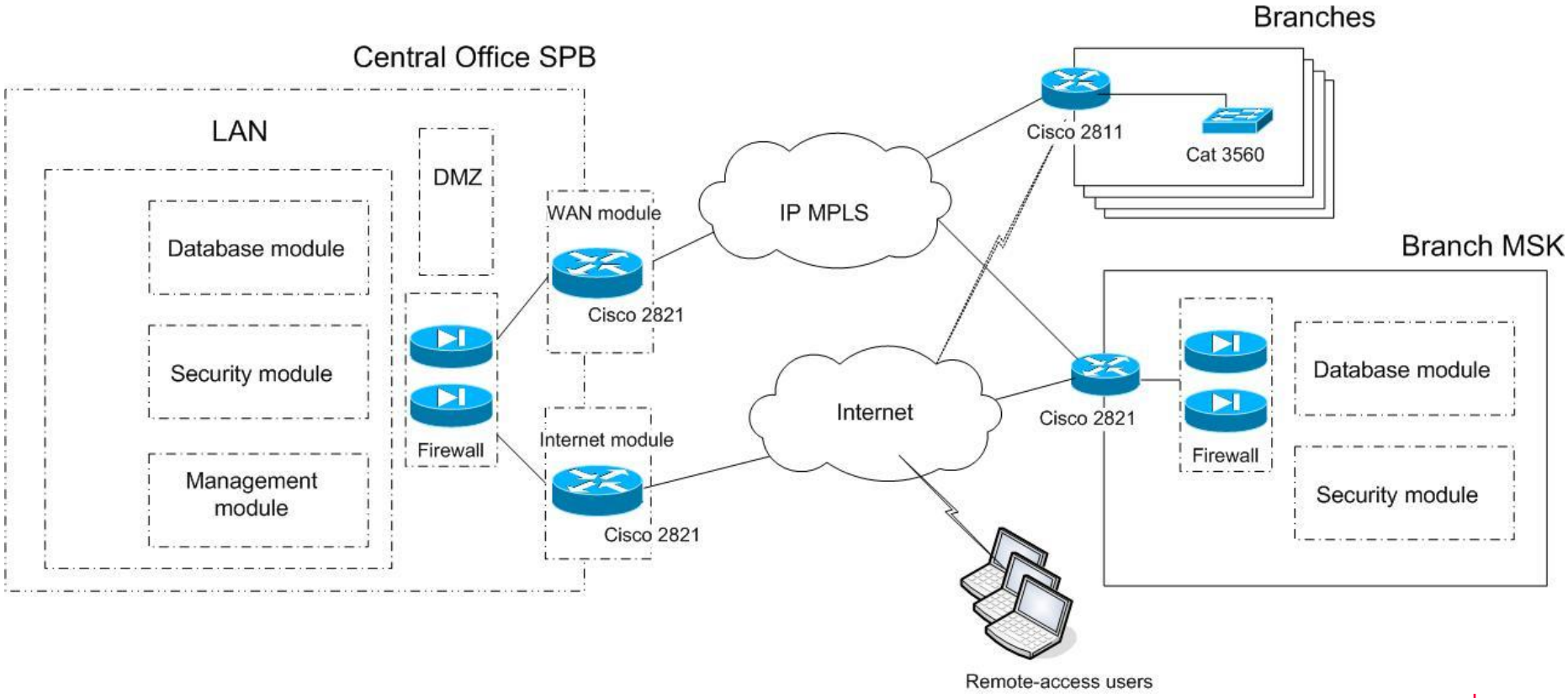
- LAN, WAN топология
- Дизайн Active Directory
- Задачи и пути решения
- Сценарии
- Пример контроля доступа

Защита от неавторизованного подключения и контроль

LAN топология

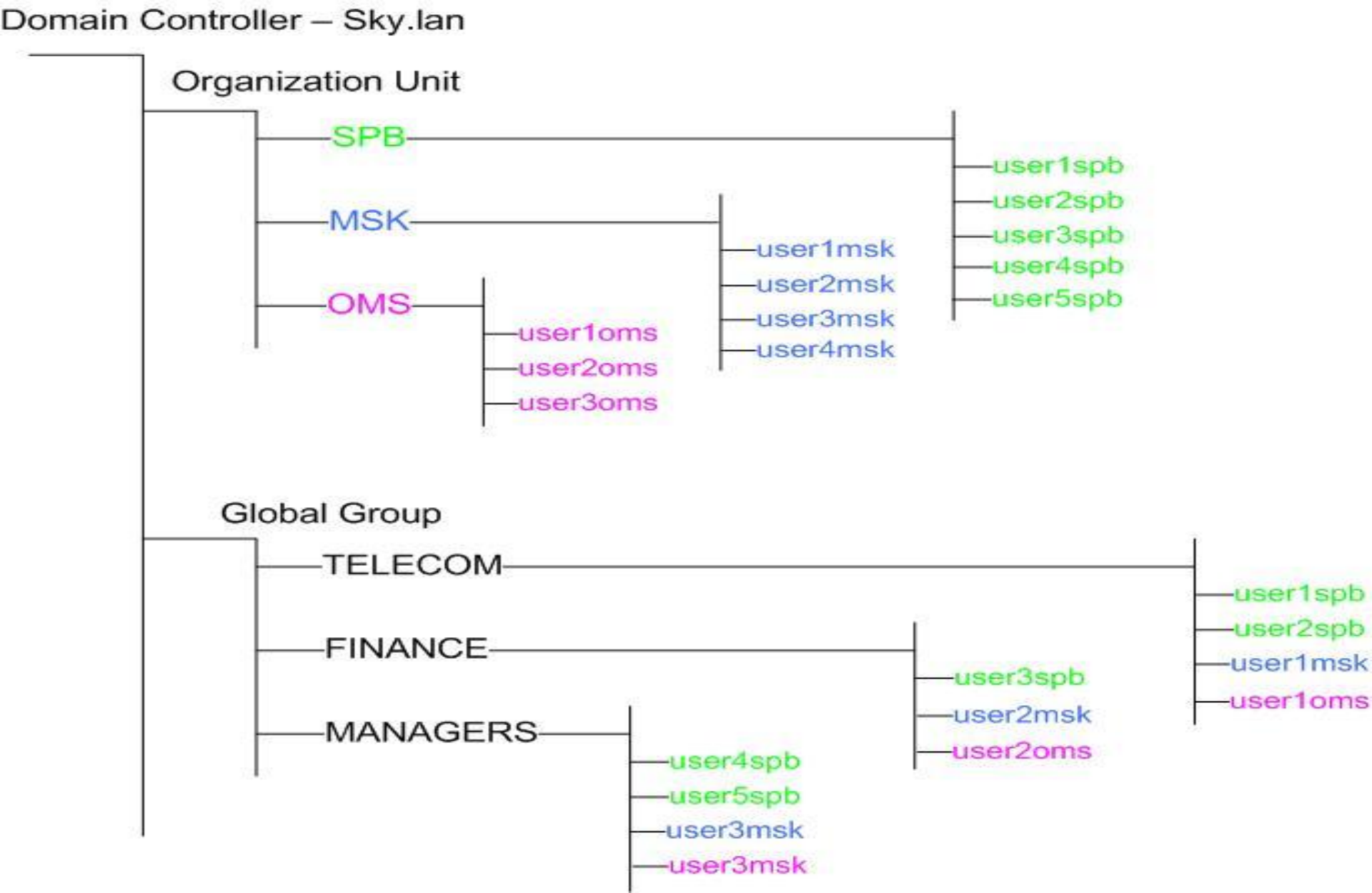


WAN топология



Защита от неавторизованного подключения и контроль

Дизайн Active Directory



Задачи и пути решения

- **Задачи**
- **Сетевой дизайн**
- **Достигаемый результат**

Снижение затрат на управление IT
Идентификация и авторизация
Общее повышение защищенности
Единый носитель сертификата
Диагностика и анализ событий
Интеграция с Active Directory
Внедрение Certification Authority
AAA на базе RADIUS
Идентификация на уровне подключения
Использование Dot1x инфраструктуры
Назначение VLAN ID на порт
Назначение IP адреса на рабочую станцию
Мониторинг и сбор статистики

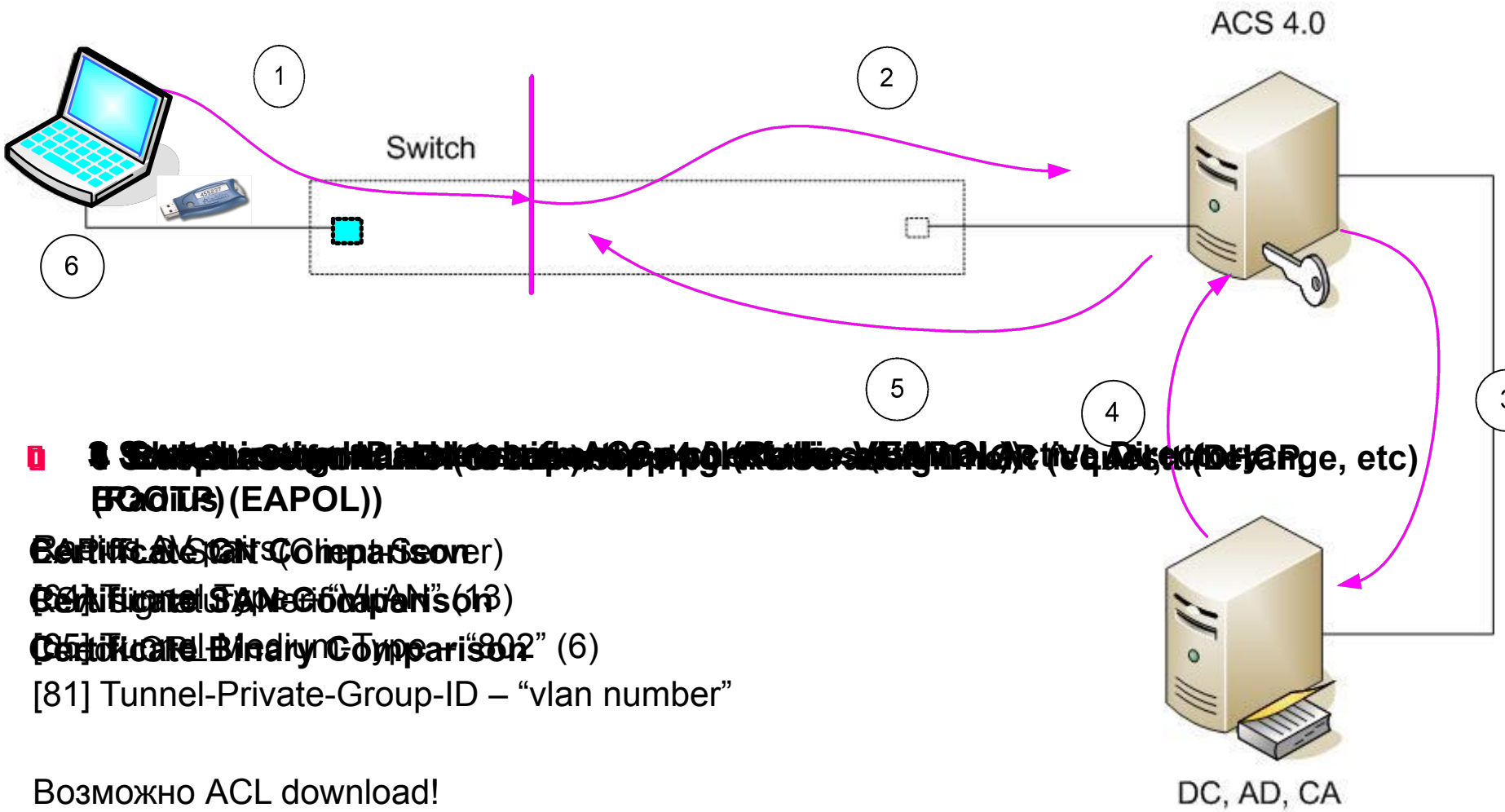
Защита от неавторизованного подключения и контроль

Сценарии

- Переезды пользователей. Концепция свободного рабочего места.
- Посменная работа операторов, кассиров и т. д. Многопользовательская среда.
- Удаленный доступ к ресурсам (из гостиницы, дома). Установление VPN, авторизация на уровне сети и на уровне приложений
- Предоставление гостевого входа (доступ в интернет для заказчика, партнера)
- Подключение принтеров, терминалов и других устройств, не поддерживающих 802.1x

Защита от неавторизованного подключения и контроль

Пример контроля доступа



- 1. Switch sends EAP-Request/Identity (EAPOL)
- 2. Client (Supplicant) responds with EAP-Response/Identity (EAPOL)
- 3. RADIUS Access-Request (EAP)
- 4. RADIUS Access-Challenge (EAP) (Request/MD5-Challenge, etc)
- 5. Client responds with EAP-Response (EAPOL)
- 6. RADIUS Access-Accept (EAP) (Success)

Certificate Comparison

Certificate Binary Comparison

[64] Tunnel-Type – “VLAN” (13)

[65] Tunnel-Medium-Type – “802” (6)

[81] Tunnel-Private-Group-ID – “vlan number”

Возможно ACL download!

[009/001] cisco-av-pair

Защита от неавторизованного подключения и контроль

AD. Users and Computers. Групповые политики

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Users

- Remote access permission (Dial-up or VPN)
- Groups membership (Domain administrators, Domain users, Telecom)

Computers

- Autoenrollment settings (Enroll certificate automatically)
- Smart card removal behavior (Lock Workstation)
- Control local devices (USB, COM, IrDA,Bluetooth, Wi-Fi т. д.)

Развитие. Комплексное решение на основе агентского П/О

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Подключение к сети

Сканирование стека TCP/IP

Анализ реестра

Сбор версий OS, hotfixs, версии антивирусного п/о

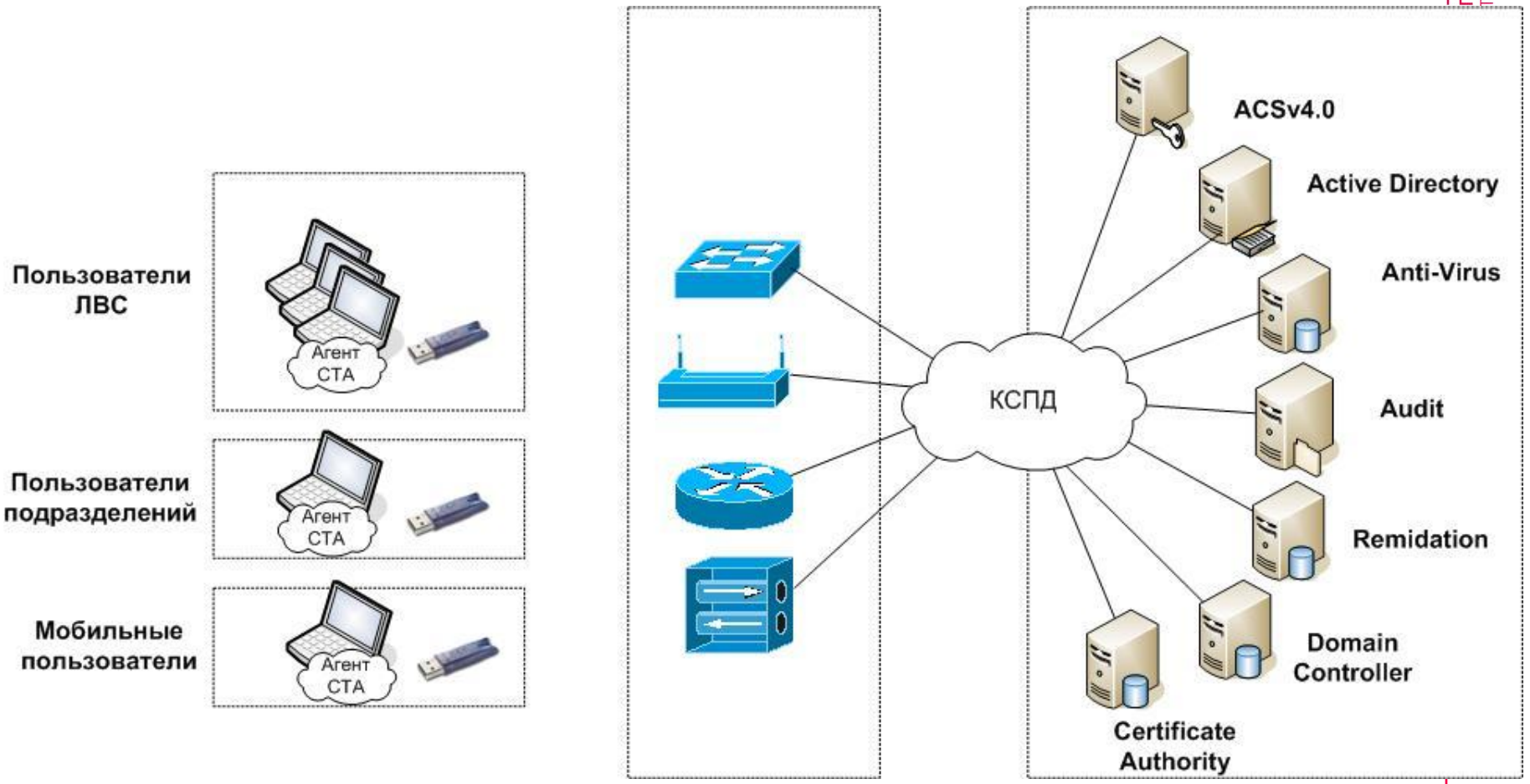
Загрузка обновлений

Повторный аудит

Предоставление доступа

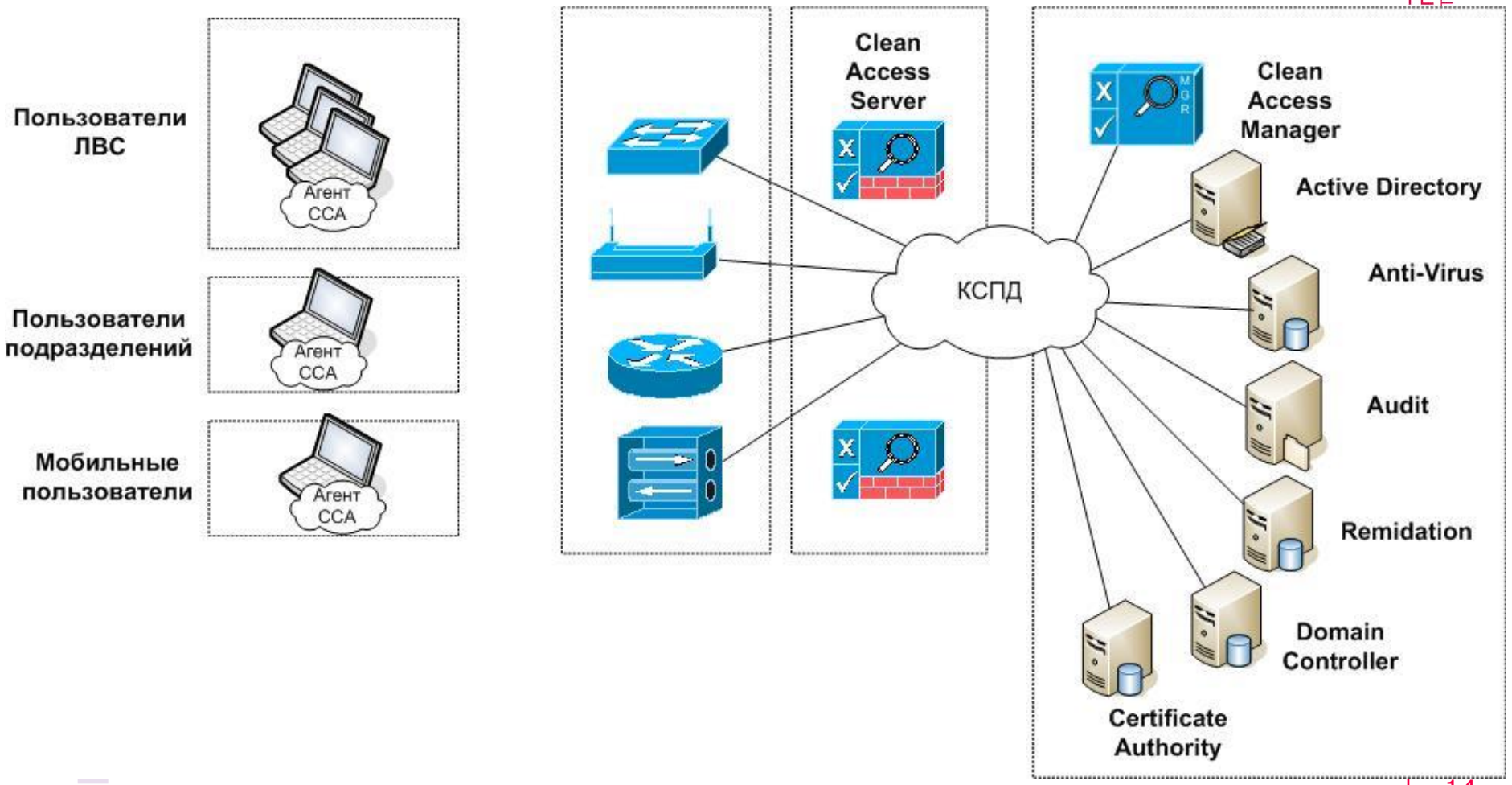
Защита от неавторизованного подключения и контроль

Решения на основе 802.1x инфраструктуры



Защита от неавторизованного подключения и контроль

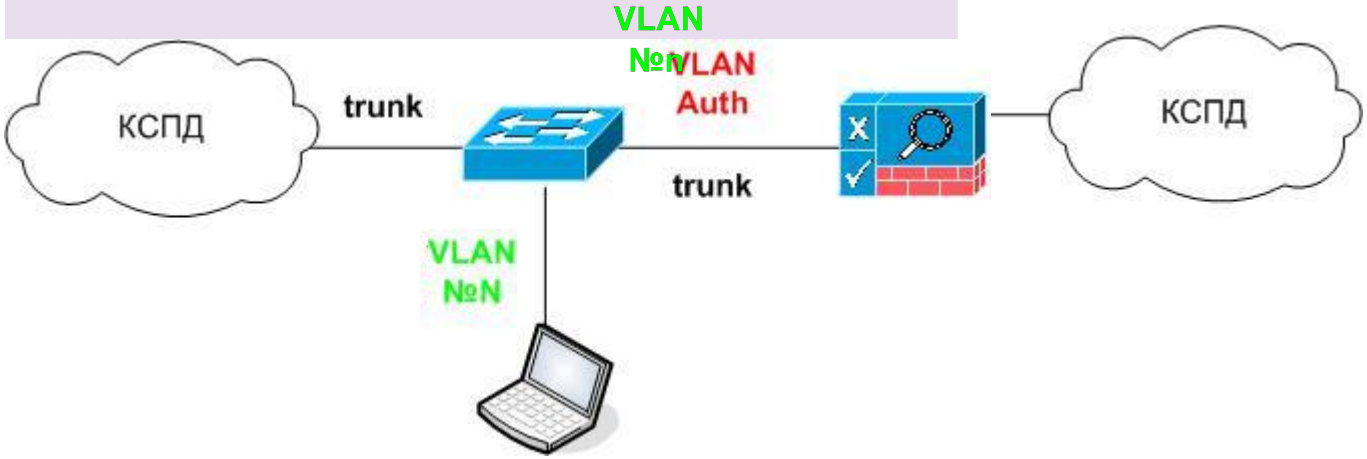
Решения независимые от 802.1x инфраструктуры



Защита от неавторизованного подключения и контроль

Архитектура решения

Внутри полосы (in-band)



Защита от неавторизованного подключения и контроль

Решения на основе 802.1x инфраструктуры

ОТКРЫТЫЕ ТЕХНОЛОГИИ

Преимущества

Недостатки

- тевым ресурсам
- и рабочей станции
- Нет SSO (Single Sign-On)
- При физическом подключении к сети сразу высылается запрос на авторизацию
- Не все операционные системы и
- Использование сертификатов для идентификации пользователя или рабочей станции
- Нет проверки состояния п/о рабочей станции

Защита от неавторизованного подключения и контроль

Решения на основе агентского п/о

ОТКРЫТЫЕ ТЕХНОЛОГИИ

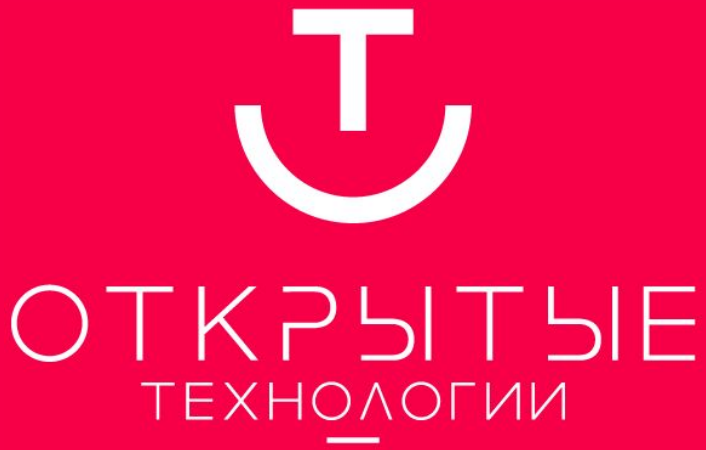
Преимущества

- Контроль подключения к сетевым ресурсам вплоть до уровня приложений
- Независимость от типа операционных систем на рабочих станциях
- Централизованная проверка состояния рабочей станции на соответствие корпоративным правилам
- Централизованное управление всеми коммутаторами (настройки вплоть до порта)
- Возможность реализации SSO (Single Sign-On)

Недостатки

- Очень высокие требования к отказоустойчивости инфраструктуры сети

Защита от неавторизованного подключения и контроль



ТЕХНОЛОГИИ ОТКРЫТИЙ

Россия, 117997, Москва, ул. Обручева, 30, стр. 2
Тел.: (495) 787-08-88, 787-70-27
Факс: (495) 787-70-28, 225-23-58
E-mail: info@ot.ru

www.ot.ru

Table 1-3 EAP Authentication Protocol and User Database Compatibility

Database	LEAP	EAP-MD5	EAP-TLS	PEAP (EAP-GTC)	PEAP (EAP-MS CHAPv2)	EAP-FAST Phase Zero	EAP-FAST Phase Two
ACS	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Windows SAM	Yes	No	No	Yes	Yes	Yes	Yes
Windows AD	Yes	No	Yes	Yes	Yes	Yes	Yes
LDAP	No	No	Yes	Yes	No	No	Yes
ODBC	Yes	Yes	Yes	Yes	Yes	Yes	Yes
LEAP Proxy RADIUS Server	Yes	No	No	Yes	Yes	Yes	Yes
All Token Servers	No	No	No	Yes	No	No	No

Защита от неавторизованного подключения и контроль