



# Обеспечение безопасности для пользовательских устройств



**Михаил Кадер**

[mkader@cisco.com](mailto:mkader@cisco.com)

[security-request@cisco.com](mailto:security-request@cisco.com)

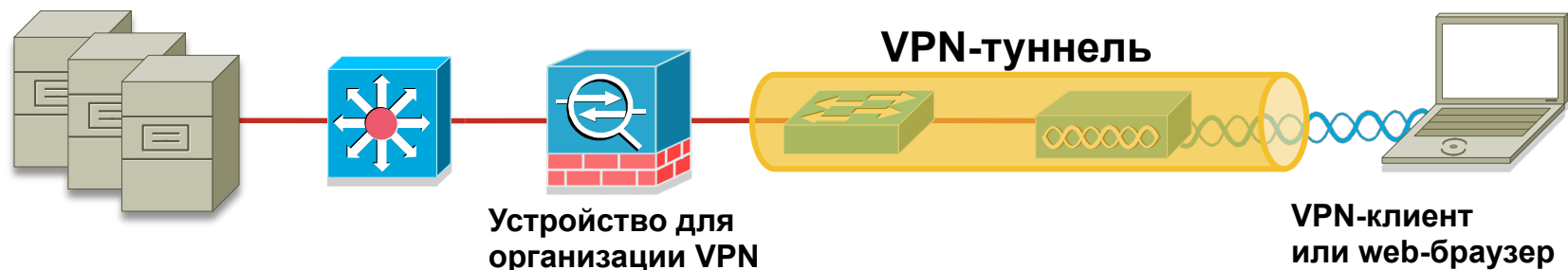
# План презентации

- Начальные сведения о VPN удаленного доступа
- Соображения по проектированию и развертыванию
- Безопасность оконечных устройств
- Управление SSL VPN
- Вопросы и ответы

# НАЧАЛЬНЫЕ СВЕДЕНИЯ О VPN УДАЛЕННОГО ДОСТУПА

# Обзор сетей VPN: IPsec и SSL

- Механизм защиты взаимодействия по IP-сети
  - Аутентификация (проверка подлинности/статуса доверенности узла)
  - Целостность (отсутствие изменений/подмены)
  - Конфиденциальность (невозможность НСД)
- Компоненты VPN удаленного доступа (RA VPN)
  - Клиент (мобильный или фиксированный)
  - Устройство терминирования (для большого числа конечных устройств)



# VPN удаленного доступа по Интернету

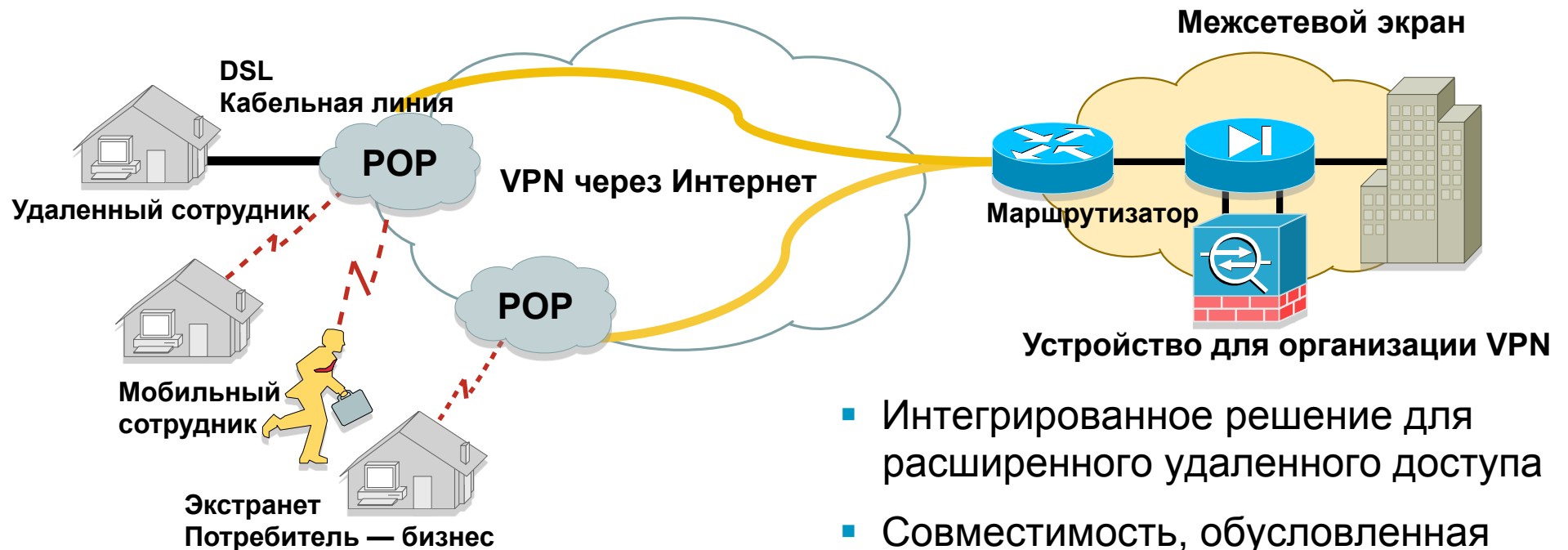
## Клиент удаленного доступа

AnyConnect, IPsec VPN — уровень 3 —  
Microsoft Windows, Mac OS X (L2TP/IPsec), iPhone

SSL VPN "без использования клиента" —  
уровень 7 — Web browser

## Корпоративная инфраструктура — центральный офис

Маршрутизатор, межсетевой экран и  
устройство для организации VPN:  
терминирование VPN-туннеля



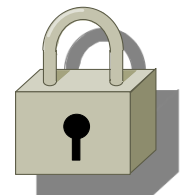
- Интегрированное решение для расширенного удаленного доступа
- Совместимость, обусловленная следованием стандартам

# Обзор SSL

- "Защищенный протокол", разработанный Netscape для безопасной электронной коммерции.
- В 1994 году был опубликован стандарт SSL 2.0, впоследствии замененный SSL 3.0. Затем был опубликован стандарт TLS, который продолжает развиваться. В настоящее время используется TLS 1.2.
- Создает туннель между web-браузером и web-сервером
  - Аутентификация и шифрование (RC4, 3DES, DES, AES)
- **https://**

Стандартный порт: 443

*Закрытый замок указывает на использование SSL!*



*TLS 1.0 описан в RFC 2246*

*TLS 1.1 описан в 4346 (2006 г.)*

*TLS 1.2 описан в RFC 5246 (2008 г.)*

# DTLS (TLS по UDP) – RFC 4347

## Причины разработки DTLS

- Ограничения TLS при использовании туннелей SSL VPN
  - TLS используется для туннелирования TCP/IP-трафика с использованием порта TCP/443
  - TCP обеспечивает повторную передачу потерянных пакетов
  - При обнаружении потери пакетов повторная передача инициируется **и приложением, и TLS**
- DTLS позволяет решить проблему "передачи TCP-трафика по протоколу TCP"
  - При использовании DTLS вместо TCP/443 используется UDP/443
  - DTLS использует TLS для согласования параметров и установки DTLS-соединения (управляющие сообщения, обмен ключами)
  - По DTLS передаются только данные
- Дополнительные преимущества
  - Низкие задержки для приложений, работающих в режиме реального времени
  - Использование DTLS является необязательным, всегда существует возможность возврата на TLS при необходимости

# Осознание потребностей удаленных пользователей

- Какие приложения будут использоваться для доступа?
  - Web-браузер (включая web-интерфейс серверов электронной почты)
  - "Толстые" клиенты (ТСР)
  - Полный доступ к сети
- Откуда будет осуществляться доступ?
  - Управляемые и контролируемые корпоративные ПК
  - Неуправляемые компьютеры
  - Интернет-кафе/общедоступные системы
- Какова длительность подключения пользователей?
  - 24x7 или целый рабочий день
  - Ограниченный период времени

# Варианты доступа по SSL VPN

## Без использования клиента

- Базовый web-доступ
- Доступ к системе электронной почты
- Доступ к ресурсам CIFS (Common Internet File System)
- Настраиваемый пользовательский экран

## С использованием "тонкого клиента"

- Перенаправление портов только для приложений, использующих TCP
- Режим Smart tunnel

## С использованием клиента

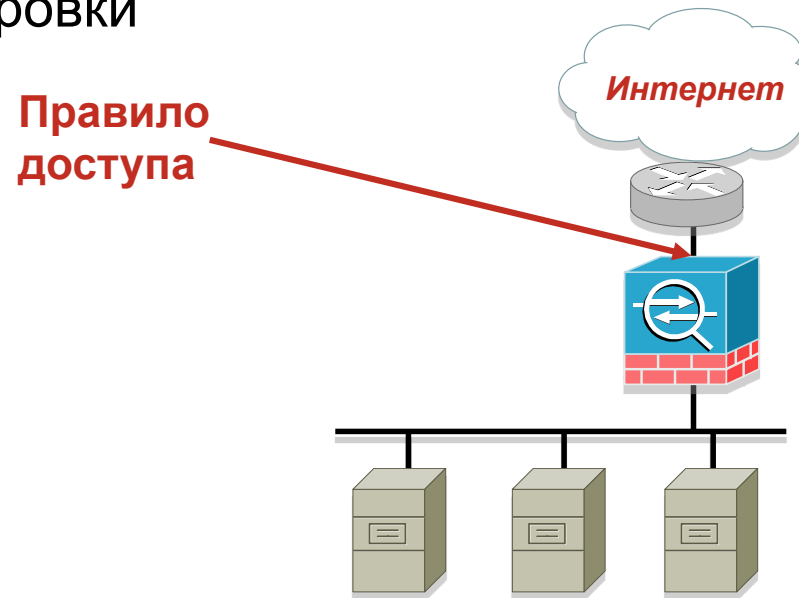
- AnyConnect (полнофункциональный SSL-туннель)

# ОБЩИЕ СООБРАЖЕНИЯ ПО РАЗВЕРТЫВАНИЮ

# Местоположение и настройка МСЭ

Использование Cisco ASA5500 в качестве МСЭ и для организации SSL VPN

- В ASA реализован функционал МСЭ и SSL VPN, эти сервисы могут функционировать одновременно
- Трафик terminates на ASA и может анализироваться после расшифровки

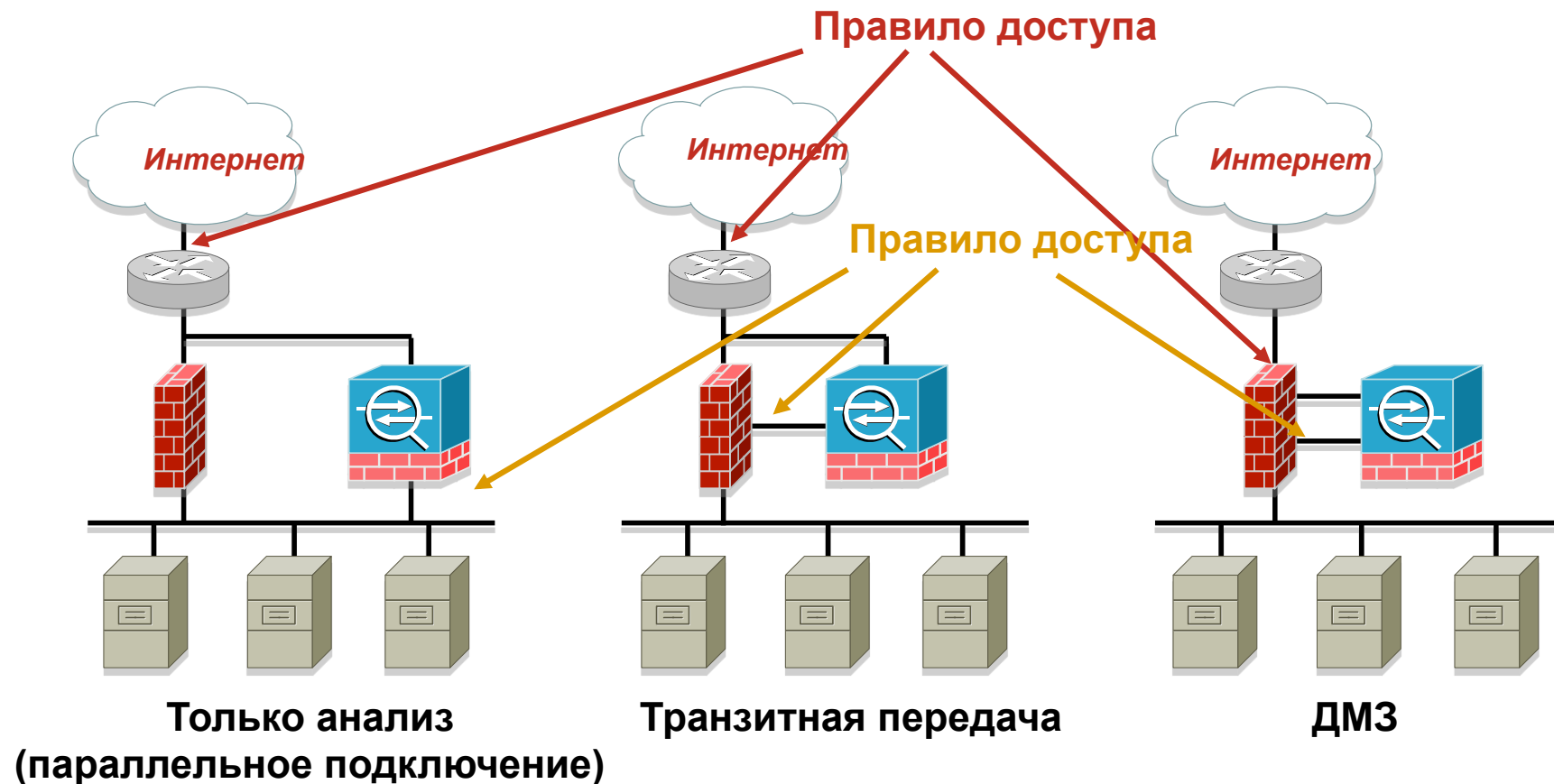


**Использование ASA в качестве МСЭ  
и для организации VPN**

# Местоположение и настройка МСЭ

Контроль доступа между внешними/внутренними интерфейсами

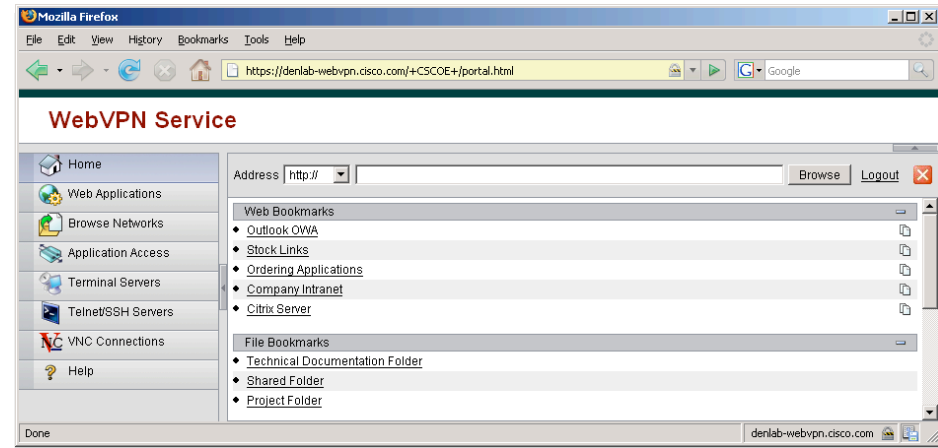
- Ограничение входящего трафика: только SSL
- Использование МСЭ для анализа IP-трафика после расшифрования



# Передача трафика через МСЭ

Порты, используемые различными сервисами SSL

- HTTPS — TCP/443
- DTLS — UDP/443
- HTTP — TCP/80
  - Если требуется HTTP-перенаправление
- Чтобы удаленные пользователи могли успешно подключаться к сетевым ресурсам, необходимо разблокировать указанные порты и протоколы



# Разделение трафика

## Удаленный доступ с использованием AnyConnect

**Без** разделения трафика



Максимальная  
безопасность

**С** разделением трафика



Максимальная  
производительность  
доступа в Интернет

# Разделение трафика

## Пример конфигурации в ASDM



Приводится  
для справки

- Необходимо выбрать значения в списках "POLICY" и "NETWORK LIST"

**Edit Internal Group Policy: Cert-auth**

Split tunneling network lists distinguish networks that require traffic to go through the tunnel and those that do not require tunneling. The security appliance makes split tunneling decisions on the basis of a network list, which is an ACL that consists of list of addresses on the private network.

DNS Names:  Inherit

Policy:  Inherit Tunnel Network List Below

Network List:  Inherit anyconnect\_acl [Manage...](#)

Intercept DHCP Configuration Message from Microsoft Clients

# Проектирование системы аутентификации клиентов

- Для централизованной аутентификации в сетях VPN могут использоваться базы данных различных типов

Имя пользователя и пароль

Токены

Цифровой сертификат/смарт-карты

- Проверка при аутентификации

Какие базы данных могут использоваться для проверки введенных данных при аутентификации

RADIUS

Active Directory (AD)/Kerberos

Домен NT

RSA SecurID

LDAP

Другой сервер одноразовых паролей (OTP), поддерживающий RADIUS

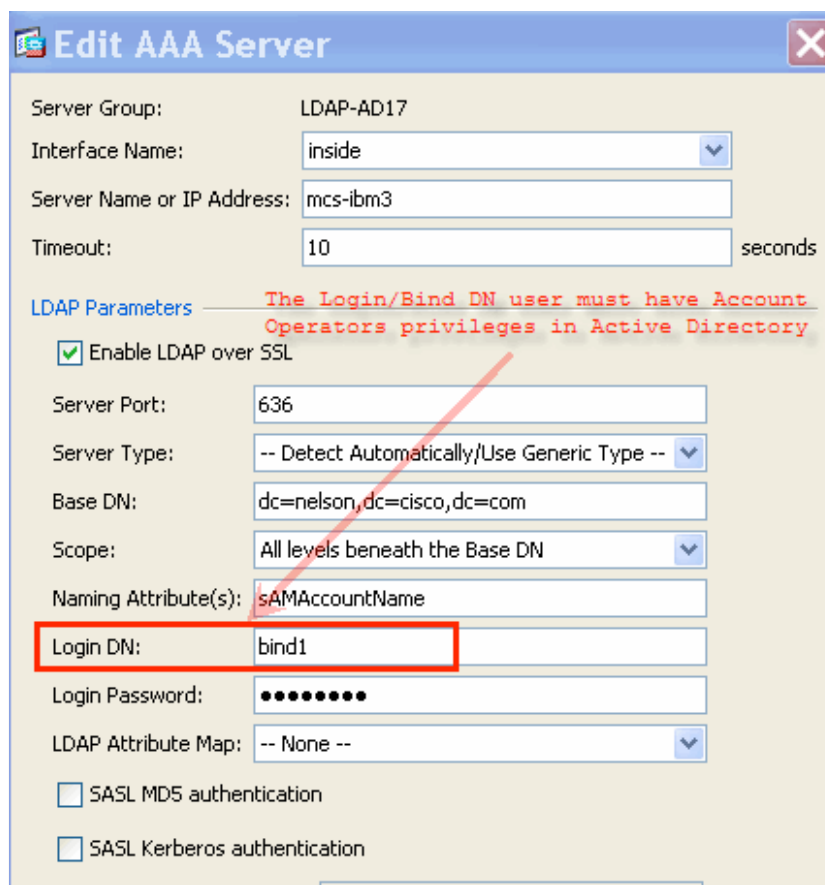
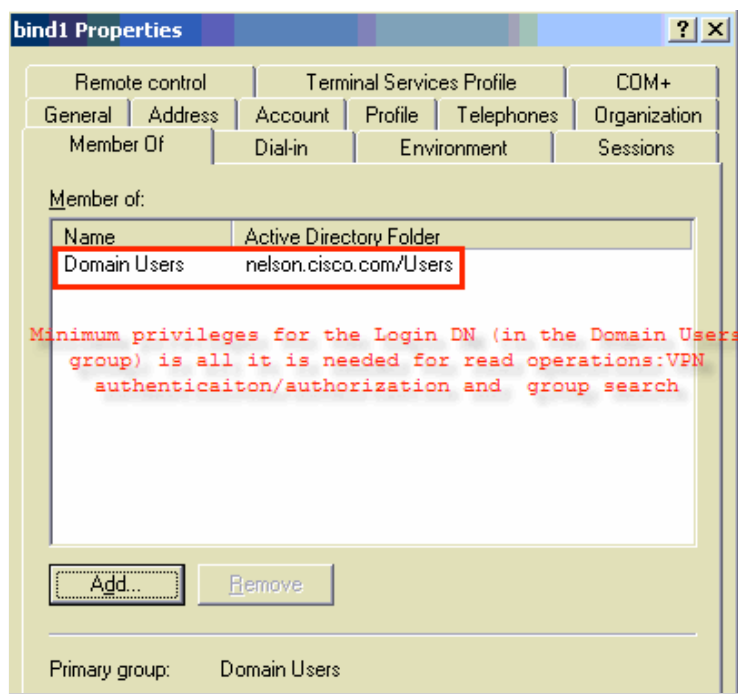
# Аутентификация



Приводится  
для справки

## Пример интеграции с LDAP

Имя Login DN представляет собой имя пользователя на сервере LDAP, которое используется для установления доверительных отношений между клиентом LDAP (т. е. ASA) и сервером LDAP в процессе обмена данными привязки до начала поиска сведений о пользователе на сервере.



Для управления паролями/изменения настроек VPN имени пользователя Login DN необходимо присвоить привилегии Account Operators.

# Аутентификация с использованием LDAP

- Необходимо знать базовое имя DN LDAP
- Его можно определить с помощью браузера LDAP

The screenshot displays the Apache Directory Studio interface. On the left, the LDAP Browser shows a tree view of the directory structure. The entry `DC=fieldlab,DC=cisco,DC=com (14)` is selected and circled in red. A red arrow points from this entry to a larger, torn-edge callout box on the right. This callout box shows a detailed view of the selected entry, including its DN (`CN=adoeschl,CN=Users,DC=fieldlab,DC=cisco,DC=com`), its object classes (`organizationalPerson`, `person`, `top`, `user`), and its instance type (`user`). The `sAMAccountName` attribute is also circled in red and points to the value `adoeschl`. Below the callout box, a small window shows the user's attributes, including `name (1)`, `objectCategory (1)`, `displayName (1)`, `objectGUID (1)`, and `distinguishedName (1)`.

# Аутентификация с использованием LDAP

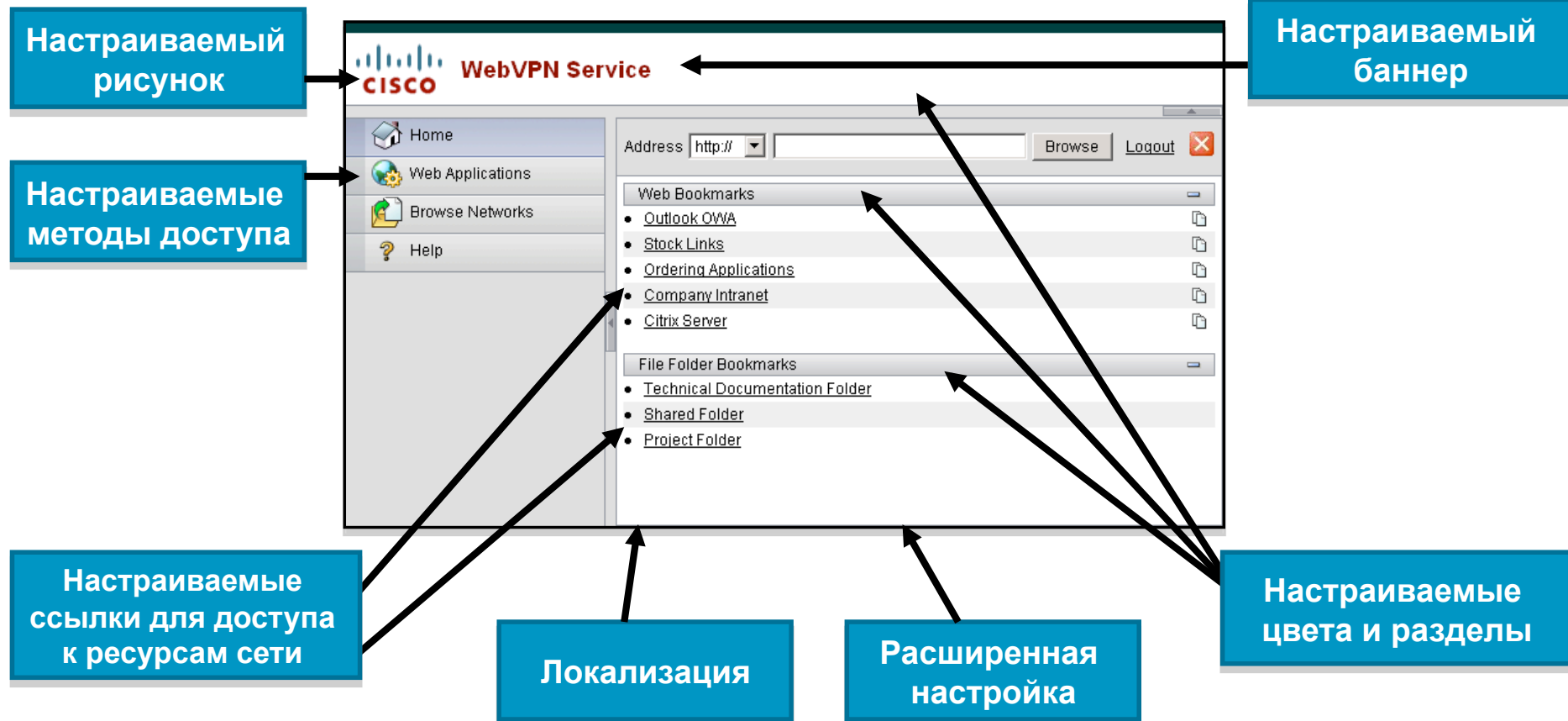
- Для аутентификации в VPN и поиска по группам для имени пользователя Login DN достаточно прав доступа "только чтение"
- Для управления паролями необходимо задать привилегии Account Operator

The screenshot shows the 'Add AAA Server' configuration window. The 'LDAP Parameters for VPN authentication/authorization' section is expanded. The 'Login DN' field is highlighted with a red oval and contains the text 'labops'. The 'Login Password' field is also highlighted with a red oval and contains a series of dots. Other fields include 'Server Group' (LDAP-FIELDLAB), 'Interface Name' (INSIDE), 'Server Name or IP Address' (munlab-aaa.fieldlab.cisco.com), 'Timeout' (10 seconds), 'Server Port' (389), 'Server Type' (Microsoft), 'Base DN' (DC=fieldlab,DC=cisco,DC=com), and 'Scope' (One level beneath the Base DN). The 'LDAP Parameters for Group Search' section is also visible at the bottom.

# **РАЗВЕРТЫВАНИЕ VPN ДЛЯ ДОСТУПА БЕЗ ИСПОЛЬЗОВАНИЯ КЛИЕНТОВ**

# Настройка SSL VPN без использования клиента (L7)

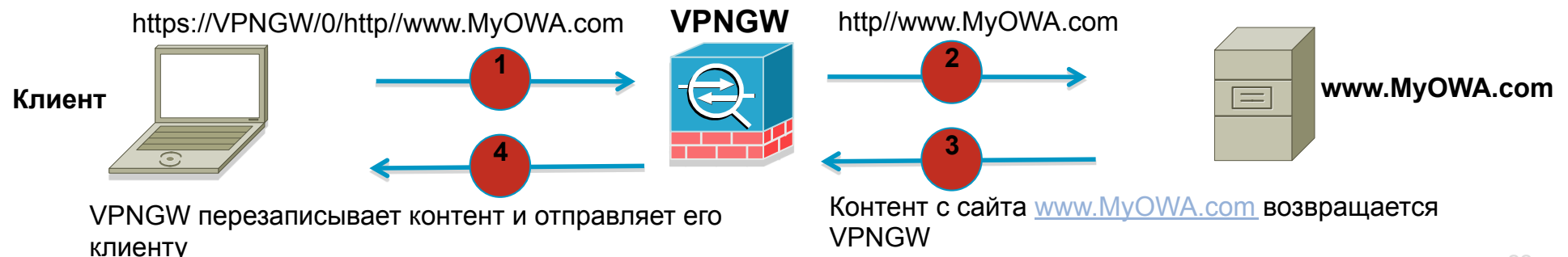
Без использования клиента



# SSL VPN: без использования клиента (перезапись контента)

## Стандартный браузер

- Шлюз передает трафик HTTP(S) по SSL-соединению
- Ограничение: web-страницы  
HTML-страницы  
Web-приложения
- Перезапись контента подразумевает изменение URL и Java-обращений к сокетам
- Перезапись контента может выполняться шлюзом или клиентом.
- Основная операция: корректировка URL:



# SSL VPN: без клиента (трансляция приложений)

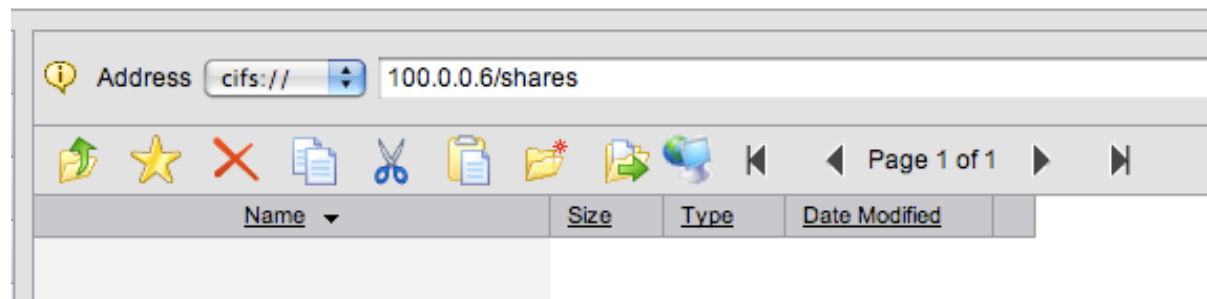
## Стандартный браузер

- При трансляции приложений устройство VPN "превращает приложение в web-приложение"

Трансляция протокола в HTTP → Необходимы подробные сведения о приложении

Реализация HTML-стиля

Возможность использования изначально не-web- приложений  
CIFS (совместный доступ к файлам (NT и Active Directory))



Без использо-  
вания клиента

С использованием  
"тонкого клиента"

# Сложная обработка контента

- Среда настройки профилей приложений
- Режим разделения трафика
  - Позволяет TCP-приложениям, использующим **Winsock v2**, использовать устройство терминирования VPN в качестве прокси для доступа в закрытую область сети
- Перенаправление портов
  - Локальный "тонкий" клиент выполняет функции прокси
  - Туннелирование и перенаправление трафика приложений
- Подключаемые модули
  - Cirtix ICA, RDP, SSH/TELNET, VNC предоставляются Cisco
  - Расширяемая среда для поддержки других популярных протоколов

# Среда настройки профилей приложений (APCF)

Без использования клиента

## Модуль Application Helper

- Позволяет устройству безопасности поддерживать работу нестандартных приложений и web-ресурсов, чтобы обеспечить возможность работы с ними по каналу SSL VPN без использования клиента
- Профили

В профиле APCF содержится скрипт, который указывает когда (pre, post), где (header, body, request, response) и какие данные следует преобразовывать для конкретного приложения

Скрипт написан на XML, для преобразования строк используется синтаксис sed (stream editor)

**Профиль предоставляется Cisco TAC**

# Режим Smart Tunnel

Приложения используют устройство VPN в качестве прокси

- Необходимо создать список "авторизованных" процессов
- Механизм Smart Tunnel загружает модуль-заглушку для каждого авторизованного процесса, перехватывает обращения к сокетам и перенаправляет их через устройство VPN. Привилегии администратора не требуются.
- Родитель каждого авторизованного процесса передает информацию (cookie и т. п.) своим потомкам, если потомок также является авторизованным процессом

Пример

Запуск telnet-сеанса с использованием telnet.exe

telnet.exe должен являться авторизованным процессом

# Причины использования Smart Tunnel

- Нельзя установить VPN-клиент
- Нет доступного подключаемого модуля
- Перенаправление портов невозможно
- Привилегии администратора невозможно получить
- Требуется доступ к локальному приложению
- Требуется поддержка трансформации контента по URL для WEBVPN (оптимальный метод!)

# Результат использования Smart-Tunnel

С использованием "тонкого клиента"

The image shows a Windows Task Manager window with a list of processes on the left and a detailed view of a process on the right. The process list includes:

- iPassPeriodicUpdateService.exe
- iPodService.exe
- iTunesHelper.exe
- leventmgr.exe
- lsass.exe
- mcshield.exe
- MDM.EXE
- mfeann.exe
- mfevtps.exe
- MDM.exe** (highlighted in yellow)
- okclient.exe
- POWERPNT.EXE
- procexp.exe
- putty.exe** (circled in red)
- rapiMgr.exe
- services.exe
- shstat.exe
- smax4pnp.exe
- smss.exe
- Snagit32.exe
- SnagPriv.exe
- spoolsv.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- svchost.exe
- SynTPEnh.exe
- SynTPLpr.exe
- System
- System Idle Process
- TaskSwitch.exe

The detailed view of the process shows:

- 2752 iPass Periodic Update Service iPass, Inc.
- 5908 iPodService Module Apple Inc.
- 4956 iTunesHelper Module Apple Inc.

The **putty.exe: 2900 Properties** dialog box is open, showing the **Strings** tab. The **Threads** section is expanded, showing a list of loaded modules:

- putty.exe+0x1747f
- Relay.dll!DForceLoad+0x4887** (circled in red and labeled "Injected DLL")
- mswsock.dll!wSPStartup+0x102b

Other details in the dialog box include:

- Thread ID: 4404
- Start Time: 15:55:42 08.01.2010
- State: Wait:UserRequest
- Kernel Time: 0:00:00.000
- User Time: 0:00:00.000
- Context Switches: 99
- Base Priority: 8
- Dynamic Priority: 8

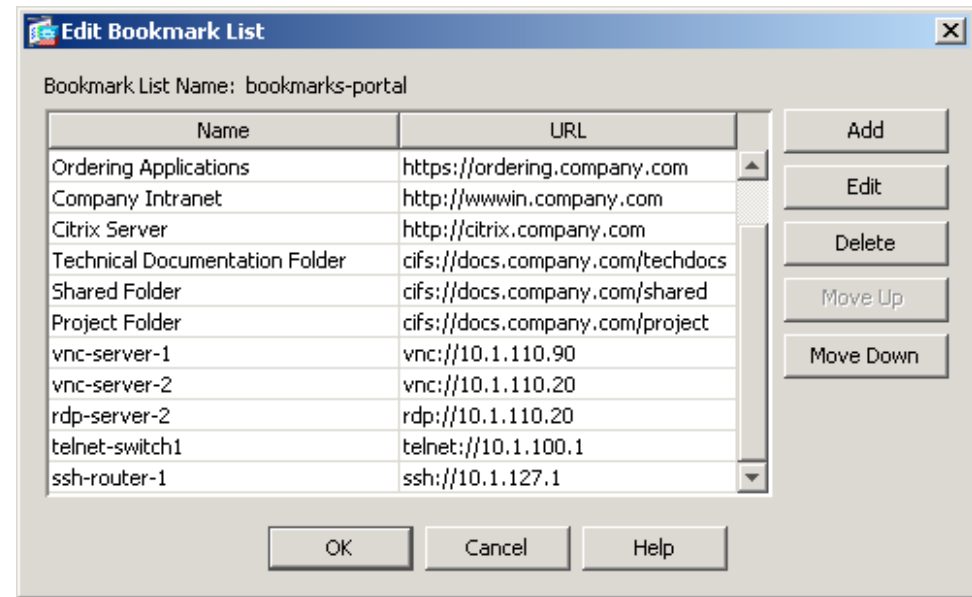
Buttons for **Kill**, **Suspend**, **Module**, **Stack**, **OK**, and **Cancel** are visible at the bottom of the dialog.

# Подключаемые модули для клиента сервера

С использованием  
"тонкого клиента"

## Обзор функциональных возможностей

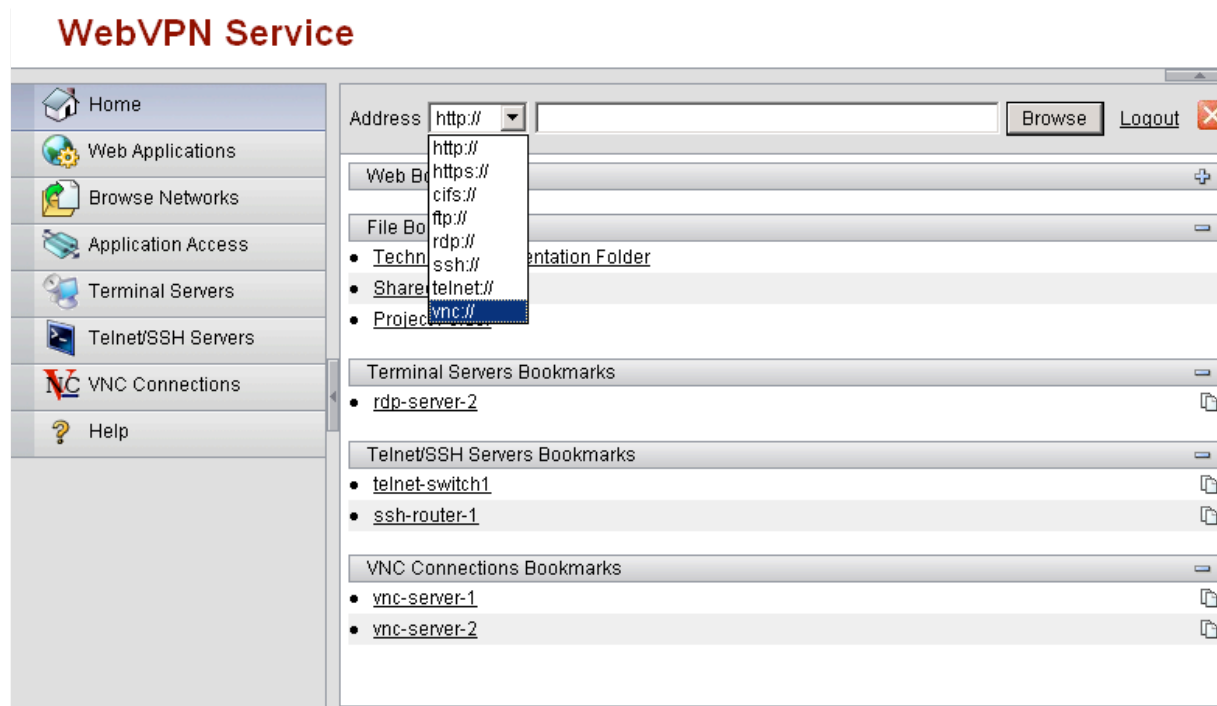
- Назначение подключаемых модулей:
- ASA версии 8.0 поддерживает множество типовых клиентских/серверных приложений с использованием подключаемых модулей Java/ActiveX, включая
  - Windows Terminal Server (RDP)
  - Telnet/SSH
  - Citrix ICA Client
  - VNC
- Ресурс определяется с помощью URL с указанием типа протокола  
rdp://сервер:порт
- Поддержка приложений сторонних производителей обеспечивается с помощью автономных файлов .jar



# Подключаемые модули для клиента

С использованием  
"тонкого клиента"

- При переходе по ссылке на ресурс генерируется динамическая страница, содержащая элемент ActiveX/апплет Java
- При необходимости выполняется перезапись и повторное подписание Java-апплета, перезапись параметров ActiveX и включение в цепочку обработки вспомогательного ActiveX для перенаправления портов
- Java-апплет прозрачно кэшируется (заносятся в кэш шлюза)



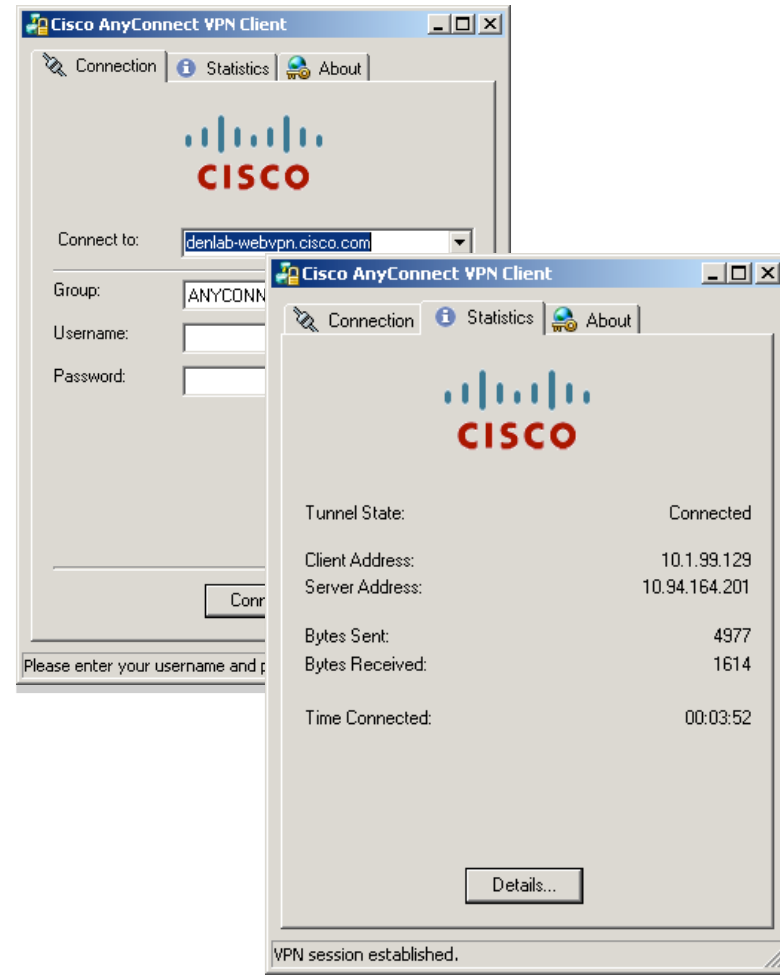
# **РАЗВЕРТЫВАНИЕ VPN С ИСПОЛЬЗОВАНИЕМ КЛИЕНТОВ (ANYCONNECT)**

# Туннелирование SSL VPN: клиент AnyConnect

С использованием  
клиента

Постоянно работающий клиент: "толстый"/"с поддержкой полного туннелирования"

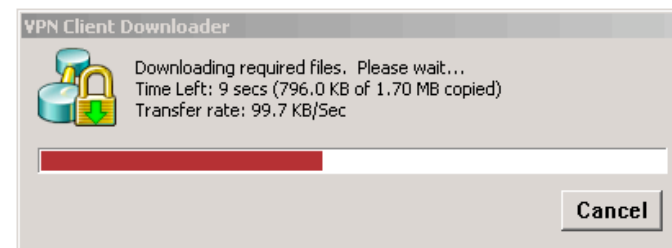
- Традиционный клиент автоматически загружается на компьютер пользователя
- Для начальной установки требуются права администратора
- Заглушка установщика была заменена отдельным пакетом MSI
- Может использовать TLS или DTLS в качестве транспорта
- Поддерживается обновление предыдущей версии



# VPN-клиент Cisco AnyConnect

## Варианты установки

- С web-страницы
  - Запуск из web-браузера
  - Вход на портал
  - Автоматическая загрузка (ActiveX/Java)
  - Загрузка вручную
- Вручную
  - Установщик MSI



# VPN-клиент Cisco AnyConnect

## Варианты подключения

- Запуск с web-страницы  
Портал



- Автономный режим

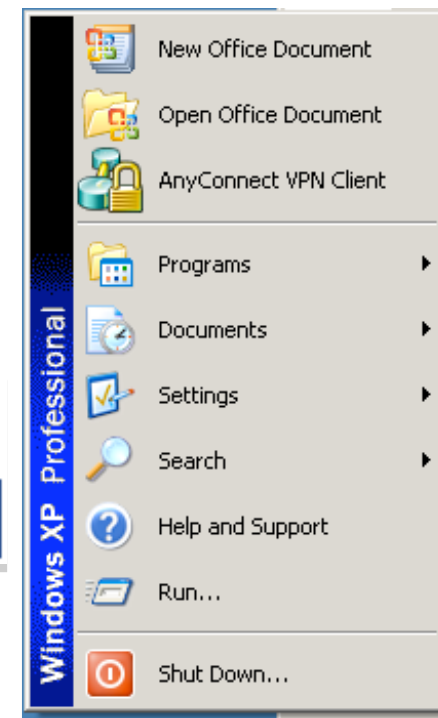
Ярлык

Меню "Пуск"

Командная строка

```
Command Prompt
C:\Program Files\Cisco\Cisco AnyConnect UPN Client>vpnccli connect denlab-webvpn.
cisco.com
Cisco AnyConnect UPN Client (version 2.0, 0300).
Copyright (C) 1998-2007 All Rights Reserved.

>> warning: No profile is available. Please enter host to "Connect to".
>> registered with local UPN subsystem.
>> state: Disconnected
>> notice: UPN session ended.
UPN> >> contacting host (denlab-webvpn.cisco.com) for login information...
>> Please enter your username and password.
0) ANYCONNECT
1) Internal
2) PORTAL
Group: [ANYCONNECT]
Username: [agroudan]
Password: [*****]
>> notice: Authentication succeeded. Checking for updates...
>> state: Connecting
>> notice: Establishing connection to denlab-webvpn.cisco.com.
>> state: Connected
>> notice: UPN session established.
UPN>
C:\Program Files\Cisco\Cisco AnyConnect UPN Client>
```



# Сравнение клиентов

## Основные отличия

	Cisco VPN Client	Cisco AnyConnect
Примерный размер	~10 Мбайт	~1,2 Мбайт
Начальная установка	Дистрибутив	Автозагрузка Дистрибутив
Требуются ли права администратора?	Да	Да Только при установке
Протокол	IPsec	DTLS, TLS
Поддерживаемые ОС	Различные*	Различные**
Головное устройство	Cisco ASA®/Cisco PIX®/ Cisco IOS®	Cisco ASA/Cisco IOS
Требуется ли перезагрузка клиента?	Да	Нет
Лицензирование	Бесплатно	Платно (2 по умолчанию)

\* W2K/XP x32, Vista x32, Mac OS X 10.4/10.5, ядро Linux 2.6, Solaris UltraSparc

\*\* W2K x32, XP x32/x64, Vista x32/x64, Mac OS X 10.4/10.5/10.6, ядро Linux 2.6, Windows Mobile, Windows 7 x32/x64

# Маршрутизация для AnyConnect на ASA

С использованием клиента

- Маршрут по умолчанию на ASA обычно направлен "наружу"
- ASA будет маршрутизировать незашифрованный трафик от VPN-клиентов на шлюз по умолчанию (если подходящий маршрут не обнаружен)
- Ключевое слово "tunneled" позволяет задать маршрут по умолчанию для расшифрованного трафика (обычно получатель находится во внутренней области сети)

[Configuration](#) > [Device Setup](#) > [Routing](#) > [Static Routes](#)

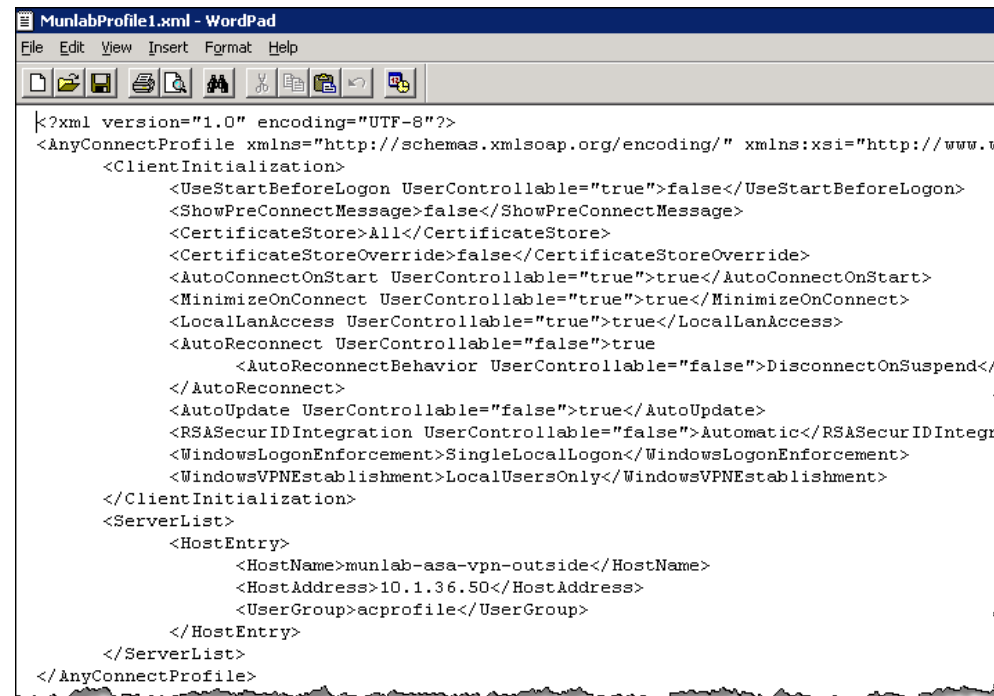
Specify static routes.

Filter:  Both  IPv4 only  IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
inside	0.0.0.0	0.0.0.0	10.1.30.12	255	Tunneled
inside	10.1.99.0	255.255.255.0	10.1.30.12	1	None
inside	144.254.0.0	255.255.0.0	10.1.30.12	1	None
outside	0.0.0.0	0.0.0.0	10.1.36.12	1	None

# Профиль AnyConnect

- Настройки клиентов хранятся в профилях
- Профили могут динамически загружаться на клиентов при подключении к VPN-шлюзу
- Профили записаны на языке XML

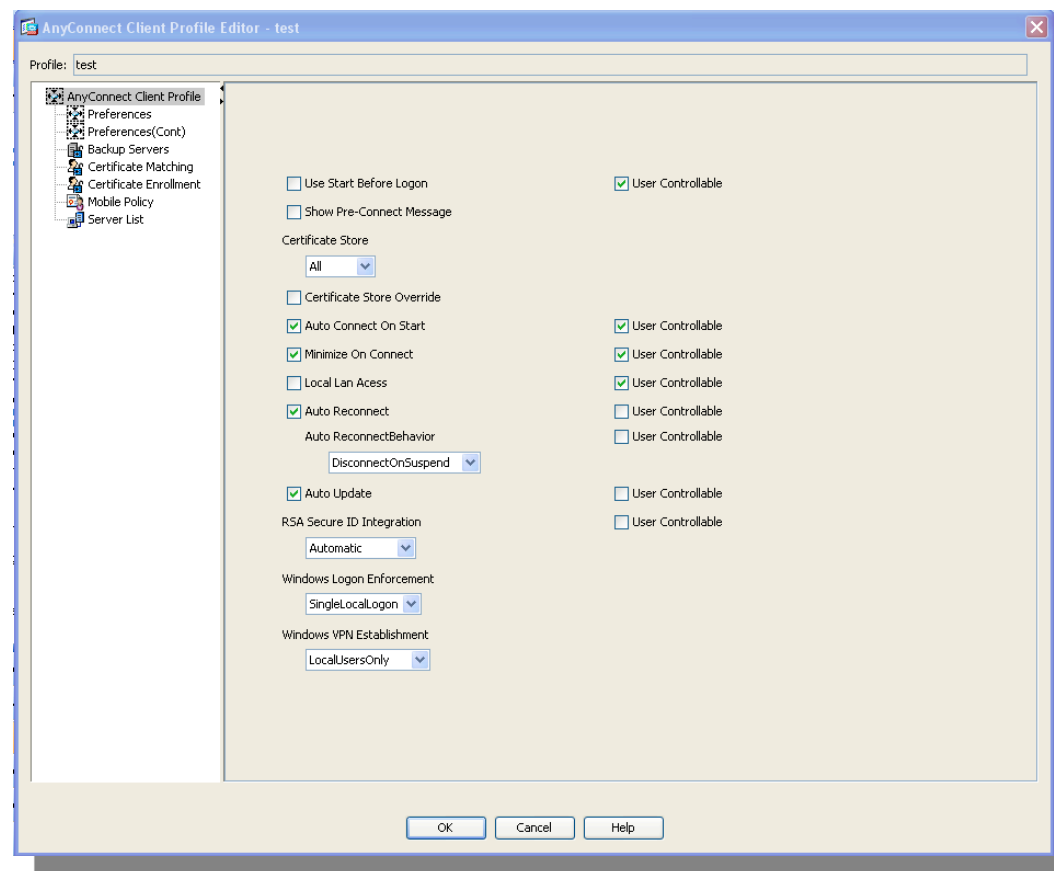


```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/" xmlns:xsi="http://www.w
  <ClientInitialization>
    <UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
    <ShowPreConnectMessage>>false</ShowPreConnectMessage>
    <CertificateStore>All</CertificateStore>
    <CertificateStoreOverride>>false</CertificateStoreOverride>
    <AutoConnectOnStart UserControllable="true">>true</AutoConnectOnStart>
    <MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
    <LocalLanAccess UserControllable="true">>true</LocalLanAccess>
    <AutoReconnect UserControllable="false">>true
      <AutoReconnectBehavior UserControllable="false">DisconnectOnSuspend</
    </AutoReconnect>
    <AutoUpdate UserControllable="false">>true</AutoUpdate>
    <RSA SecurID Integration UserControllable="false">Automatic</RSA SecurID Integr
    <WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
    <WindowsVPNEstablishment>LocalUsersOnly</WindowsVPNEstablishment>
  </ClientInitialization>
  <ServerList>
    <HostEntry>
      <HostName>munlab-asa-vpn-outside</HostName>
      <HostAddress>10.1.36.50</HostAddress>
      <UserGroup>acprofile</UserGroup>
    </HostEntry>
  </ServerList>
</AnyConnectProfile>
```

# Профиль AnyConnect Profile — настройка

С использованием клиента

- Средства поддерживаются как часть ASDM (ASA версии 8.3 и ASDM версии 6.3)
- Управление большинством параметров клиентов, включая
  - AlwaysOn
  - LocalLan Access
  - и многое другое...
- Сохранение в формате XML-файла



# Профиль AnyConnect Profile — настройка

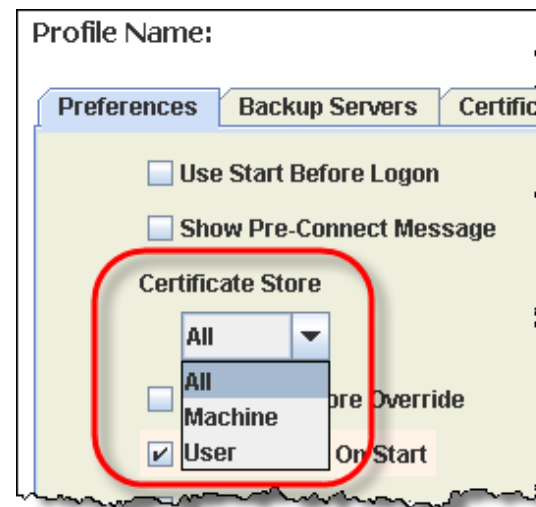
С использованием клиента

- Профиль автоматически загружается клиентом при подключении
- При установке соединения проверяется контрольная сумма профиля. Если локальный профиль был модифицирован, он заменяется профилем из централизованного хранилища.



# AnyConnect и сертификаты

- До AnyConnect версии 2.3:  
Клиенту требовались права администратора для считывания сертификатов из **хранилища компьютера**
- AnyConnect версии 2.3 и более поздних  
Клиент может считывать сертификаты из хранилищ **пользователя** и **компьютера**  
Хранилище сертификатов определяется в профиле AnyConnect



Без использо-  
вания клиента

С использованием  
клиента

# AnyConnect и сертификаты

- AnyConnect поддерживает аутентификацию с использованием сертификата и последующим запросом имени пользователя

Authentication

Method:  AAA  Certificate  Both

AAA Server Group:  Manage...

Use LOCAL if Server Group fails

# Предварительное указание имени пользователя из сертификата

Без использования клиента

С использованием клиента

- Имя пользователя может быть извлечено из сертификата
- Имя пользователя может быть скрыто от пользователя
- Настройка в профиле подключения

Username Mapping from Certificate

Pre-fill Username from Certificate

Hide username from end user

Specify the certificate fields to be used as the username

Primary Field: CN (Common Name)

Secondary Field: OU (Organization Unit)

Use the entire DN as the username

Use script to select username

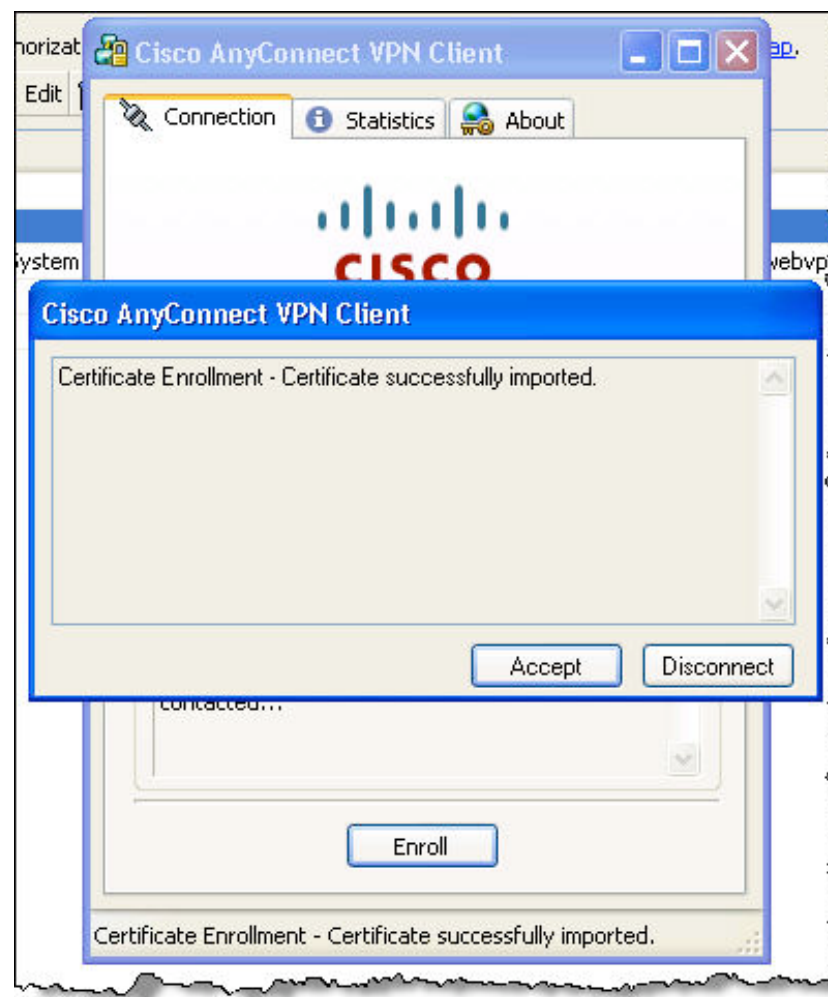
-- None --

+ Add Edit Delete

# Распространение сертификатов с помощью SCEP

С использованием клиента

- Клиентские сертификаты могут распространяться с помощью Active Directory и GPO (рекомендуется для Windows)
- Кроме того, клиентские сертификаты могут запрашиваться по SCEP
- Параметры распространения по SCEP определяются в профиле клиента AnyConnect



# Пример: SCEP

## Параметры SCEP в редакторе профиля

Cisco AnyConnect Client Profile Editor - Beta

File Help

CISCO

Profile Name:

Certificate Match Certificate Enrollment Server List Mobile Policy

Preferences Preferences (cont) Backup Servers

Certificate Enrollment

Certificate Expiration Threshold (days)

Automatic SCEP Host

CA URL

Prompt For Challenge PW

Thumbprint

Certificate Contents:

Name (CN)  Qualifier (GEN)

Department (OU)  Qualifier (DN)

Company (O)  City (L)

State (ST)  Title (T)

State (SP)  CA Domain

Country (C)  Key Size

Email (EA)   Display Get Certificate Button

Domain (DC)

# Дополнительно: распространение сертификатов по SCEP



Приводится  
для справки

## Хранилище сертификатов после запроса SCEP

### Windows:

- Персональное хранилище сертификатов пользователя
- Хранилище компьютера при наличии достаточных привилегий

### Mac OS:

- Сертификаты, полученные по запросу SCEP, добавляются только в цепочку "login"

### Linux:

- На Linux поддерживается хранилище сертификатов браузера Firefox

## Уведомление об истечении срока действия сертификата

- Администраторы AnyConnect могут настроить профиль клиента таким образом, что пользователи будут получать уведомление об истечении срока действия сертификата

# Сопоставление сертификатов группе

Без использо-  
вания клиента

С использованием  
клиента

- Пользователь запускает AnyConnect -> профиль выбирается на основании заданных критериев
- Подключение ОДНИМ ЩЕЛЧКОМ

The screenshot shows the Cisco ASA configuration interface for 'Certificate to SSL VPN Connection Profile'. The left pane shows the 'Device List' with 'asa1.stgbu.cisco.com' and IP '172.16.254.10'. The main pane shows the configuration for 'labmap' with a rule priority of 10, mapped to the 'Cert-Auth' profile. The 'Mapping Criteria' table shows a rule for 'Subject' with component 'Organization (O)', operator 'Equals', and value 'cisco'. Two red callout boxes highlight the 'labmap' row and the 'Subject' row in the mapping criteria table.

**Connection Profile to be mapped**

Map Name	Rule Priority	Mapped to Connection Profile
labmap	10	Cert-Auth

**Profile is mapped if the criteria is matched**

Field	Component	Operator	Value
Subject	Organization (O)	Equals	cisco



# ОБЕСПЕЧЕНИЕ БЕЗОПАСНОЙ МОБИЛЬНОСТИ

# Безопасная мобильность

- Возможность централизованного контроля состояния безопасности и управления политиками
  - Если головное устройство недоступно,
    - переход в состояние fail-open (прямой доступ к сети)
- ИЛИ
- переход в состояние fail-closed (нет доступа к сети)



# Постоянное включение/ поддержание безопасности Конфигурация ASA



Приводится  
для справки

**Edit Internal Group Policy: DfltGrpPolicy**

- General
- Servers
- Advanced
  - Split Tunneling
  - IE Browser Proxy
  - SSL VPN Client**
  - IPsec Client

Keep Installer on Client System:  Yes  No

Compression:  Enable  Disable

Datagram TLS:  Enable  Disable

Keepalive Messages:  Disable Interval:  seconds

MTU:

Client Profile to Download:

Service Profile to Download:

Optional Client Modules to Download:

Always-On VPN:  Disable  Use AnyConnect Profile setting

**Включение  
Always-On VPN  
в зависимости  
от профиля**

Find:

# Задание WSA на ASA



Приводится  
для справки

Configuration > Remote Access VPN > Network (Client) Access > Mobile User Security

Mobile User Security service let WSA (Web Security Appliance) to scan traffic from AnyConnect clients to ensure no virus enter the enterprise network.

Service Access Control

Specify the addresses of the hosts/networks from where WSAs can communicate with this security appliance.

+ Add Edit Delete

Interface	IP Address	Mask/Prefix Length
-----------	------------	--------------------

Service Setup

Enable Mobile Use Security Service

Service Port:

WSA Access Password:

Confirm WSA Access Password:

MUS Host:

Show WSA Sessions

Apply Reset

<admin> 15 8/26/09 9:49:28 AM PDT

**Обеспечение взаимодействия с WSA**

# Настройка WSA



Приводится для справки

Membership Definition	
<i>Membership is defined by any combination of the following options. All criteria must be met for the policy to take effect.</i>	
Define Members by User Location:	<input type="radio"/> Local Users Only ? <input checked="" type="radio"/> Remote Users Only ? <input type="radio"/> Both
Define Members by Subnet:	<input type="text"/> <small>(examples: 10.1.1.1, 10.1.1.0/24, 10.1.1.1-10)</small>
Define Members by Protocol:	<input checked="" type="radio"/> All protocols <input type="radio"/> HTTP/HTTPS Only ? <input type="radio"/> Native FTP Only
Define Members by Authentication:	Identify Users Transparently through Cisco ASA Integration ? Select a Realm or Sequence: 1
Authentication Surrogate for Transparent Proxy Mode	Surrogate Type: ? <input checked="" type="radio"/> IP Address <input type="radio"/> Persistent Cookie <input type="radio"/> Session Cookie  Explicit Forward Request: ? <input type="checkbox"/> Apply same surrogate settings to explicit forward requests <small>If this option is not selected, no surrogates will be used with explicit forward requests and NTLM credential caching will not be available to these requests.</small>
▶ Advanced	<small>Define additional group membership criteria.</small>

Cancel Submit

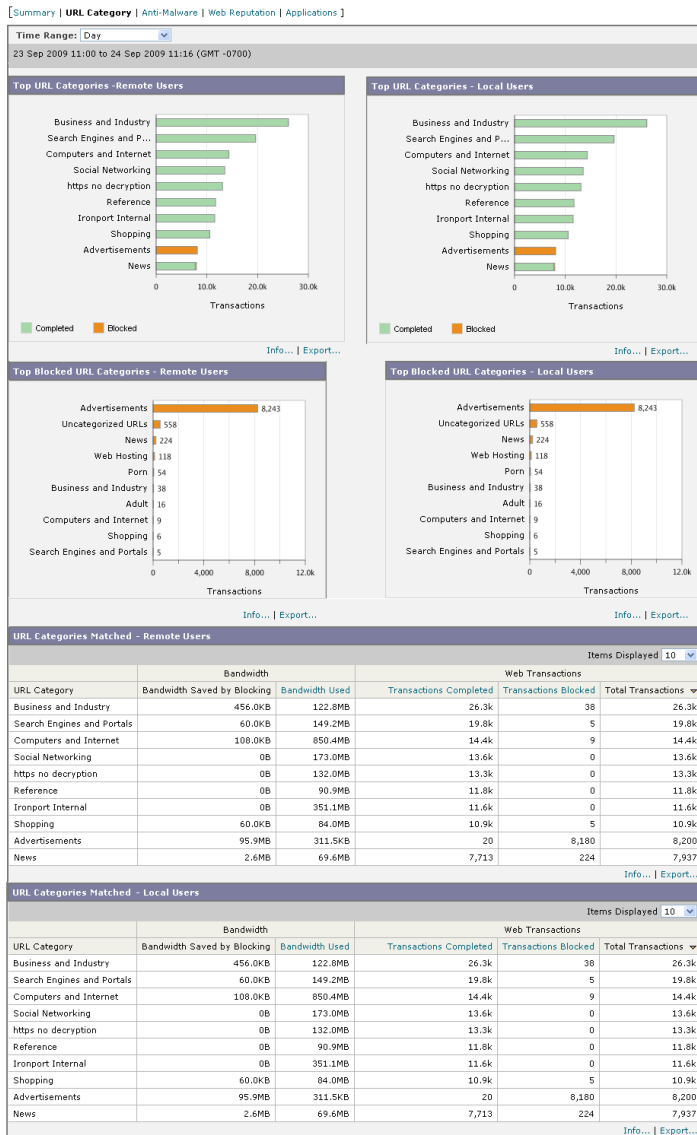
Политики удаленных/мобильных пользователей

ASA SSO

# Отчеты WSA о пользователях



Приводится для справки



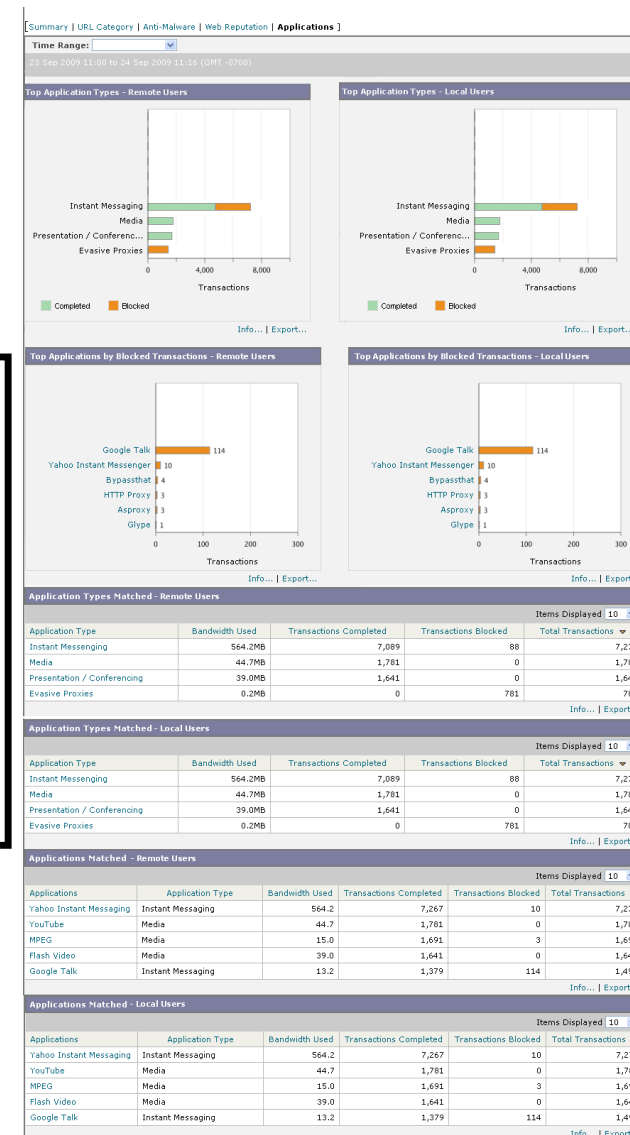
**Раздел удаленного доступа**

**Категории URL**

**Категории блокируемых URL**

**Популярные типы приложений**

**Экономия пропускной способности**



# БЕЗОПАСНОСТЬ ОКОНЕЧНЫХ УСТРОЙСТВ

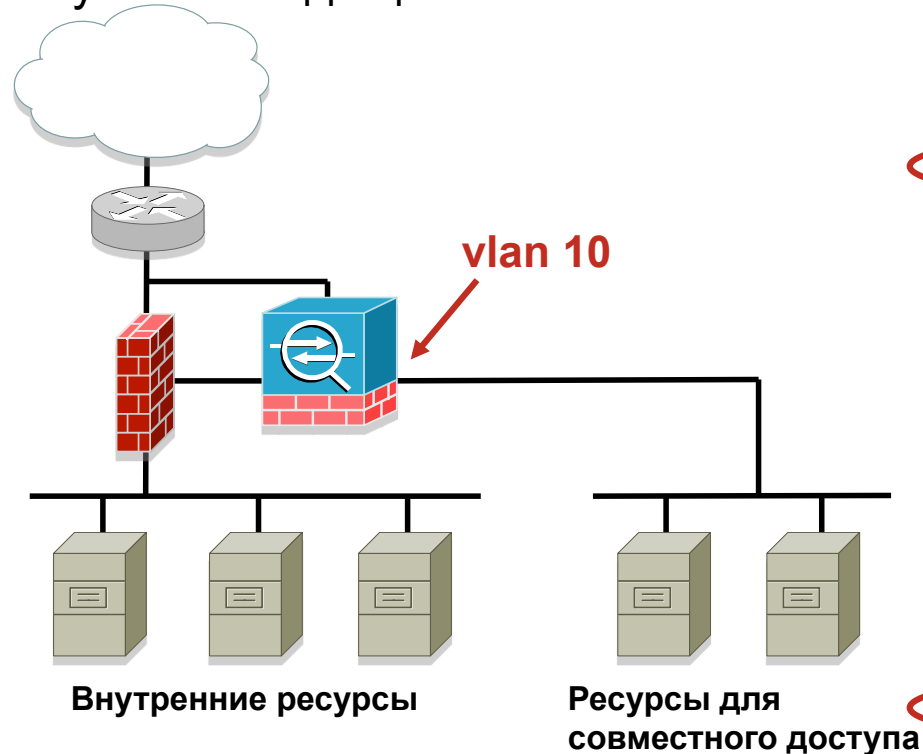
# Средства защиты конечных устройств

- Встроенные возможности устройства организации VPN
  - Разрешение доступа в зависимости от времени суток
  - Списки ACL для сети
  - Списки ACL для интернет-ресурсов
  - Cisco Secure Desktop (CSD)
  - Сканирование хостов
  - Динамические политики доступа (DAP)
- Расширенные возможности при использовании NAC
  - Устройство NAC Appliance

# Маршрутизация: интерфейсы/сети VLAN

## Политики на основании пользователей/групп

- Сопоставление пользователей группам на основании ролей
- Использование групповой политики для ограничения доступа к исходящим сетям VLAN



Name:

Banner:  Inherit

Address Pools:  Inherit

**More Options**

Tunneling Protocols:  Inherit  Clientless SSL VPN  SSL VPN Client  IPsec  L2TP/IPsec

Filter:  Inherit

NAC Policy:  Inherit

Access Hours:  Inherit

Simultaneous Logins:  Inherit

Restrict access to VLAN:  Inherit

Name:

Banner:  Inherit

Address Pools:  Inherit

**More Options**

Tunneling Protocols:  Inherit  Clientless SSL VPN  SSL VPN Client  IPsec  L2TP/IPsec

Filter:  Inherit

NAC Policy:  Inherit

Access Hours:  Inherit

Simultaneous Logins:  Inherit

Restrict access to VLAN:  Inherit

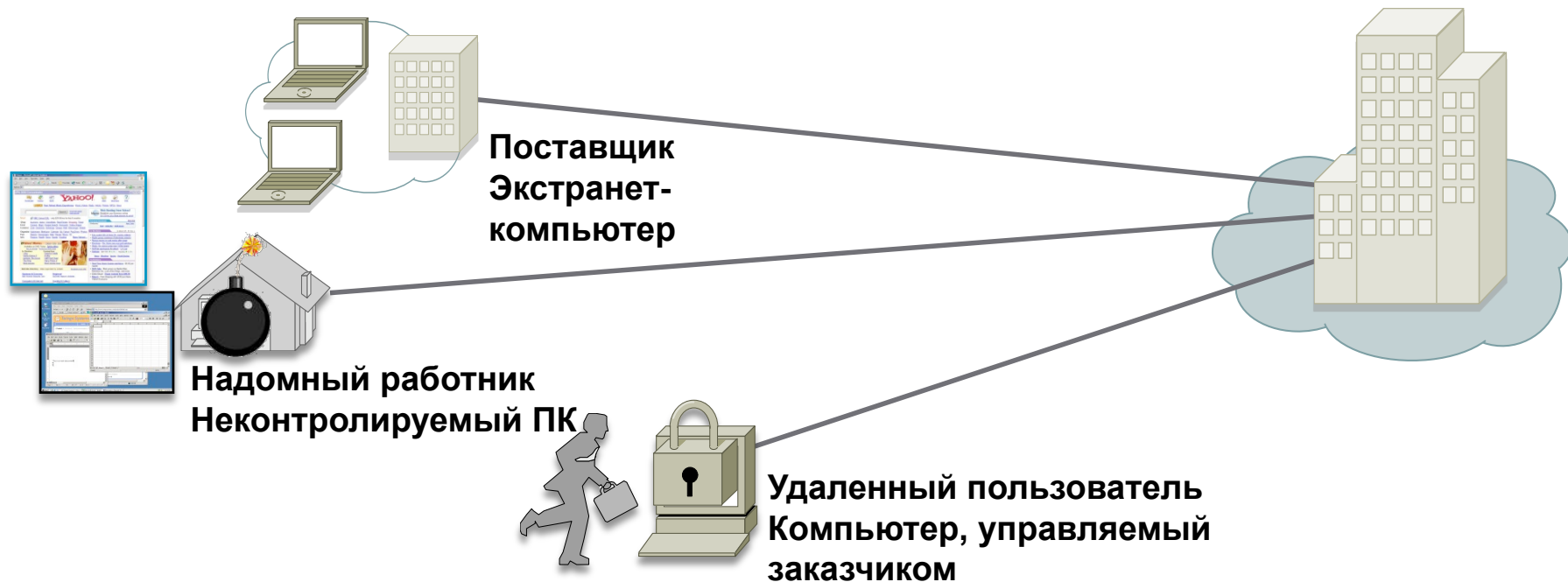
Потенциальная интеграция с VRF

# Безопасность оконечных устройств

## Рекомендации по методу доступа

- Полное туннелирование (AnyConnect)
  - Рассматривать как удаленный узел сети
  - Предоставлять условный доступ на основании идентификационных данных и результатов оценки безопасности
  - Использовать сетевые списки ACL для ограничения доступа
- SSL VPN без использования клиента
  - Предоставлять доступ только к определенным приложениям
  - Предоставлять условный доступ на основании идентификационных данных и результатов оценки безопасности
  - Использовать списки ACL для интернет-ресурсов для ограничения доступа
  - Обеспечивать защиту от утечки конфиденциальных данных

# Соображения по защите SSL VPN



## Перед сеансом SSL VPN

Кто контролирует оконечное устройство?  
Оценка защищенности оконечного устройства:  
антивирус, персональный МСЭ?  
Запущено ли вредоносное ПО?

## В ходе сеанса SSL VPN

- Защищены ли данные о сеансе?
- Защищены ли вводимые пароли?
- Запущено ли вредоносное ПО?

## После сеанса SSL VPN

- Web-страницы в кэше браузера?
- Пароли сохранены в браузере?
- Удалены ли загруженные файлы?

# Управление оконечными устройствами для создания туннеля SSL

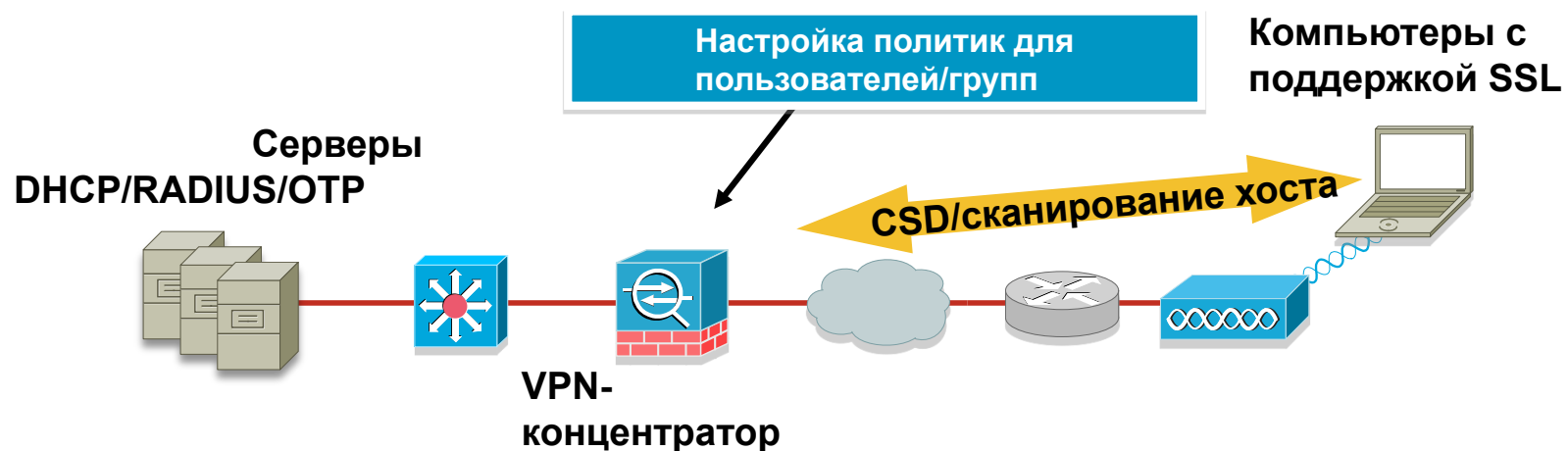
## Клиент AnyConnect

- Политики пользователей и групп
  - Назначение IP-адреса на основании сведений о пользователе/группе
  - Применение сетевого списка ACL
  - Ограничение доступа с помощью VLAN
- Политики, применяемые на основании критериев оконечного устройства
  - Cisco Secure Desktop (CSD)
  - Динамическая политика доступа (DAP)



# Управление оконечными устройствами для SSL VPN без использования клиента

- Политики пользователей и групп
  - Ограничение доступа с помощью VLAN
  - Применение списка ACL для интернет-ресурсов
  - Контроль ввода URL
  - Контроль подключения к файловому серверу и просмотра ресурсов
- Политики, применяемые на основании критериев оконечного устройства
  - Cisco Secure Desktop (CSD)
  - Динамическая политика доступа (DAP)



# Защита конфиденциальной информации

## Риски использования VPN на системах общего пользования

- Файлы cookie
  - Имена пользователей и пароли
- Журнал URL
- Страницы в кэше
  - Конфиденциальные данные
- Загруженные файлы

# Cisco Secure Desktop

Поддержка сеансов без использования клиента и с использованием AnyConnect

- **Оценка перед подключением:**

Оценка местоположения —  
управляемый или неуправляемый ПК?  
Сбор данных о компьютере

- **Защита сеанса:**

Изоляция данных и использование шифрования для защиты сеанса

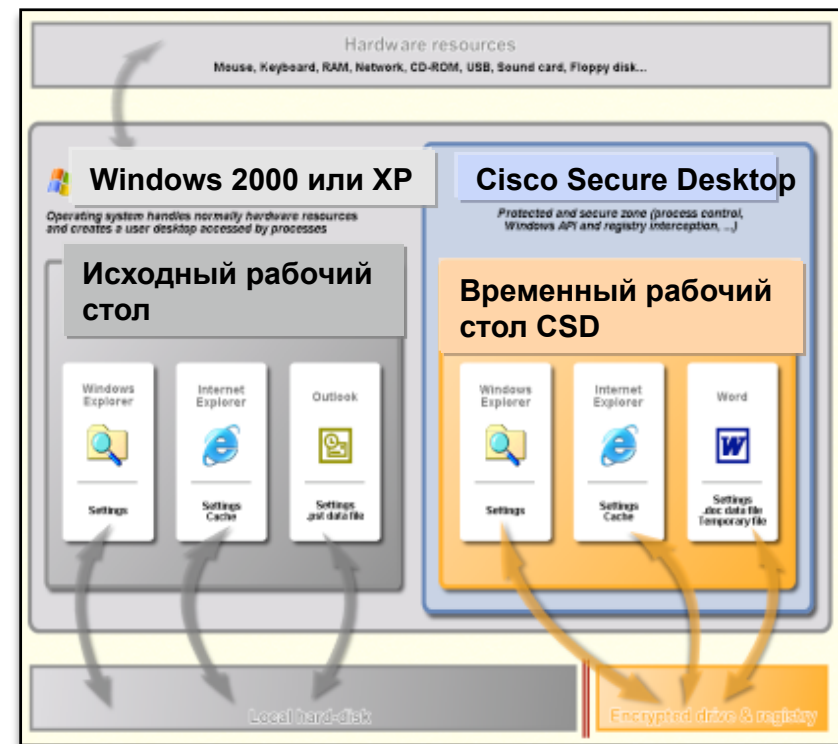
- **Очистка после сеанса работы:**

Перезапись зашифрованного раздела  
(не просто удаление)

Перезапись кэша, истории и файлов cookie

Перезапись загруженных файлов и вложений  
электронной почты

Перезапись записей средств  
автоматического дополнения паролей



# Cisco Secure Desktop

## Схема работы (перед процедурой входа)

- **Шаг 1.** Удаленный пользователь подключается к VPN-концентратору по SSL.
- **Шаг 2.** VPN-концентратор загружает на ПК Secure Desktop.
- **Шаг 3.** С помощью проверок определяется состояние ПК (или вход запрещается).
- **Шаг 4.** На основании параметров удаленного ПК применяются политики CSD.



# Cisco Secure Desktop

## Дерево принятия решений перед входом

- Поддерживаемые проверки

Проверка реестра

Проверка файловой системы

Проверка сертификатов

Проверка версии Windows

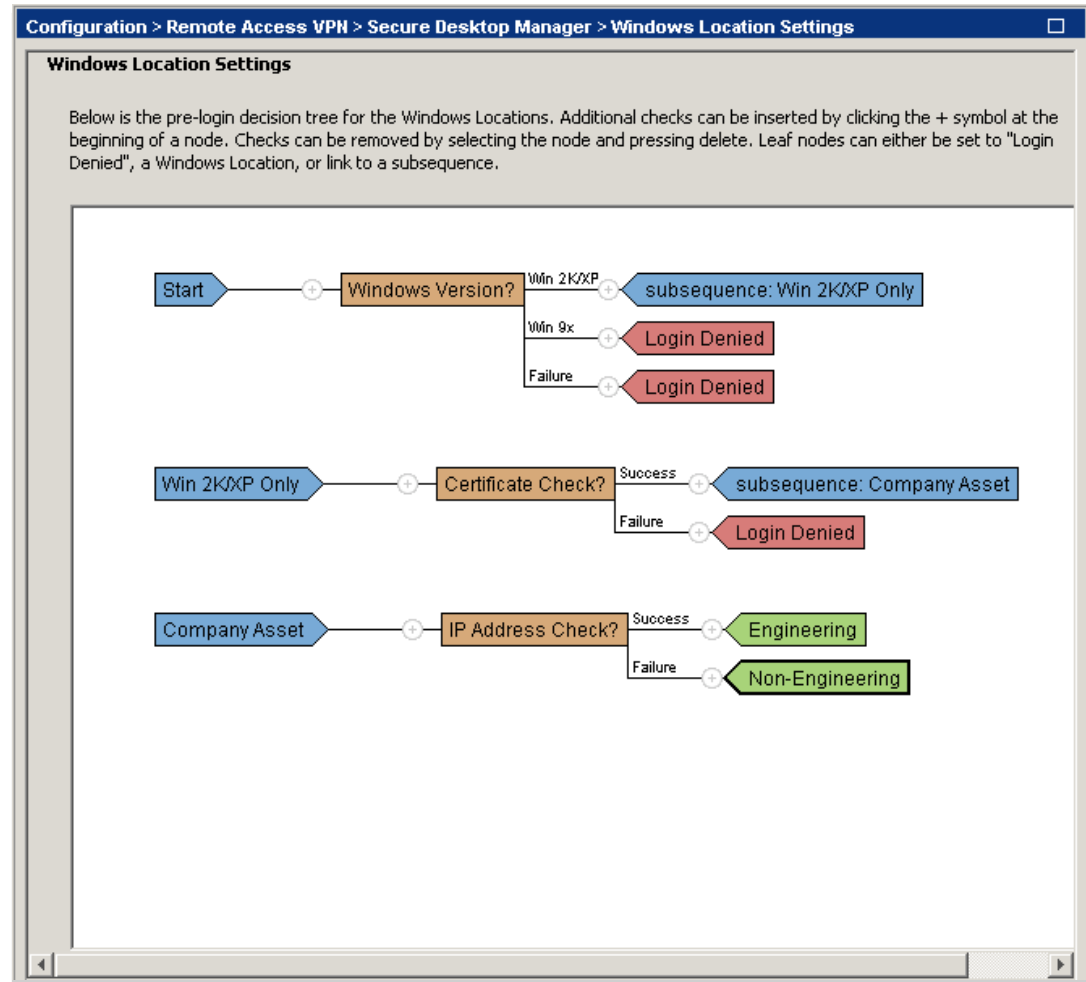
Проверка IP-адреса

- Конечные узлы

Вход запрещен

Параметры местоположения

Дополнительная процедура



# Cisco Secure Desktop

## Параметры местоположения

- Secure Desktop (защищенное хранилище) или система очистки кэша
- Система обнаружения средств регистрации нажатий клавиш и сред эмуляции

**Secure Desktop General**

Enable switching between Secure Desktop and Local Desktop

Enable Vault Reuse (User chooses a password)

Suggest application uninstall upon Secure Desktop closing

Force application uninstall upon Secure Desktop closing

Enable Secure Desktop inactivity timeout

Timeout After:  minute(s)

Enable Secure Desktop inactivity timeout audio alert

Open following web page after Secure Desktop closes

URL:

Secure Delete:  pass(es)

Launch the following application after installation:

Program Files\

**Secure Desktop Settings**

Restrict application usage to the web browser only

Disable access to network drives and network folders

Do not encrypt files on network drives

Disable access to removable drives and removable folders

Do not encrypt files on removable drives

Disable registry modification

Disable command prompt access

Disable printing

Allow email applications to work transparently

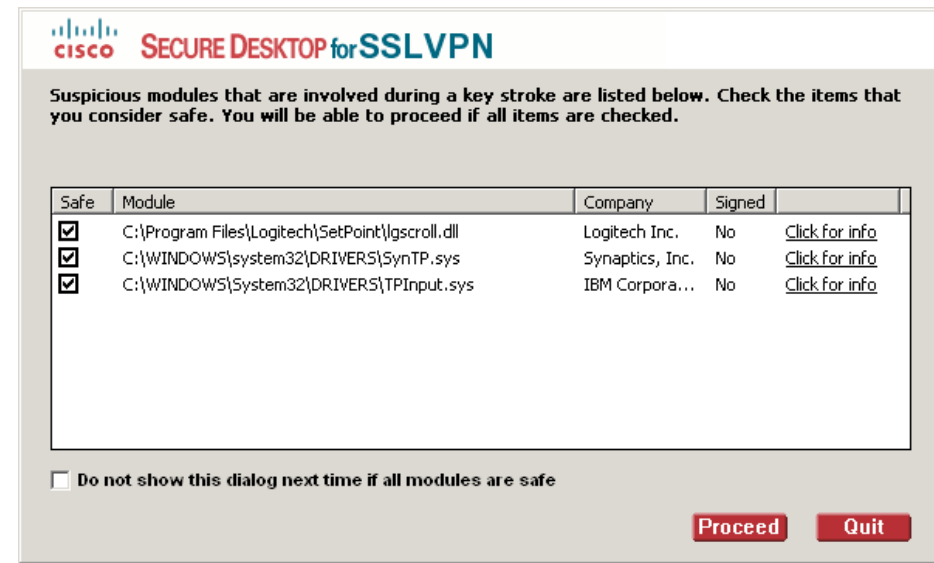
# Cisco Secure Desktop



Приводится  
для справки

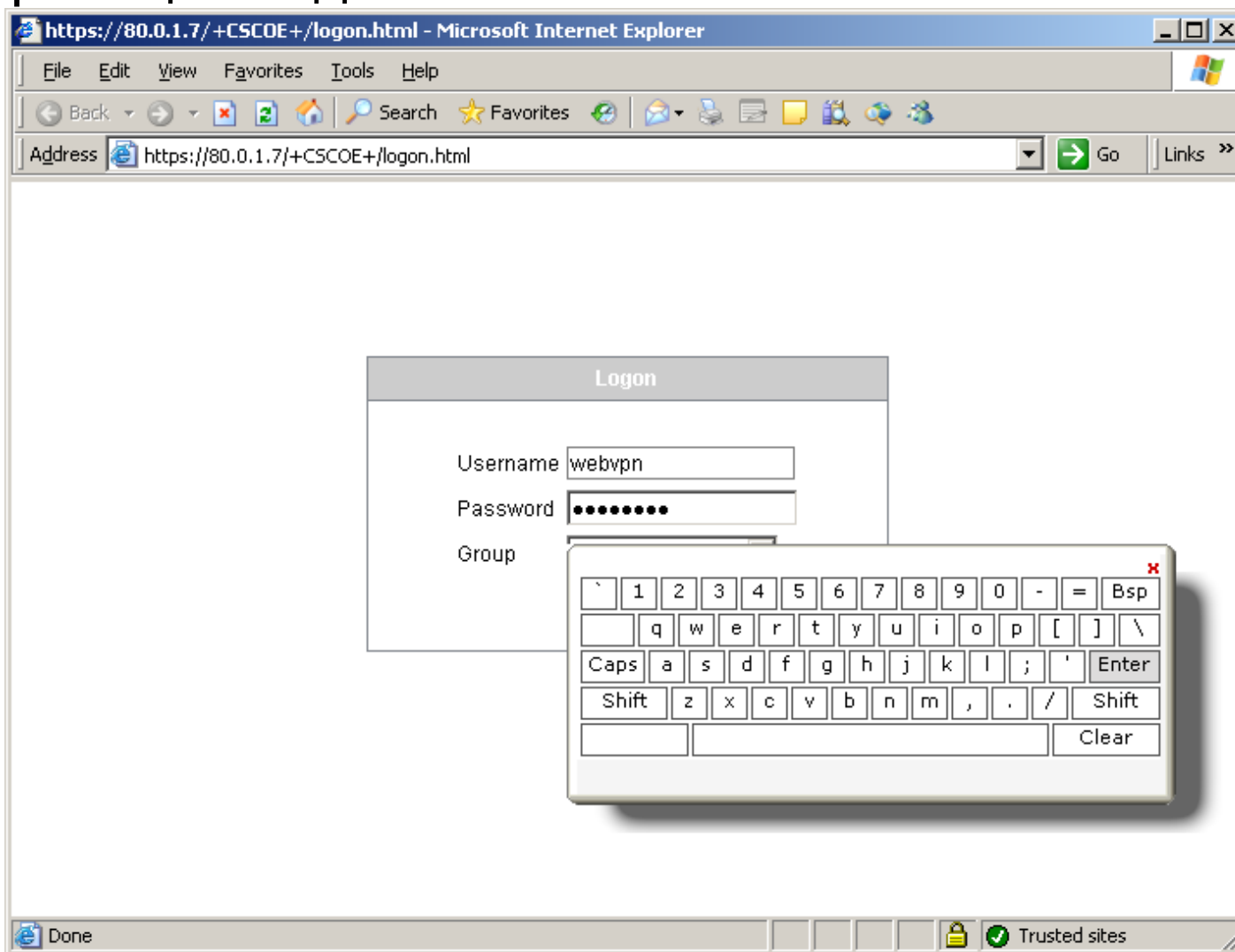
## Обнаружение средств регистрации нажатий клавиш

- При установке сеанса CSD проверяет систему хоста на предмет аномальных драйверов, свидетельствующих о работе программ, которые регистрируют нажатия клавиш.
- CSD предлагает пользователю выбрать подозрительные модули и завершить их работу перед загрузкой Secure Desktop.
- Пока пользователь не подтвердит, что все обнаруженные модули являются безопасными, соединение не будет установлено.
- Если в процессе работы с Secure Desktop будет обнаружена попытка установки средства регистрации нажатий клавиш, пользователь получит соответствующее уведомление.



# Виртуальная клавиатура и средство обнаружения программ, регистрирующих нажатия клавиш

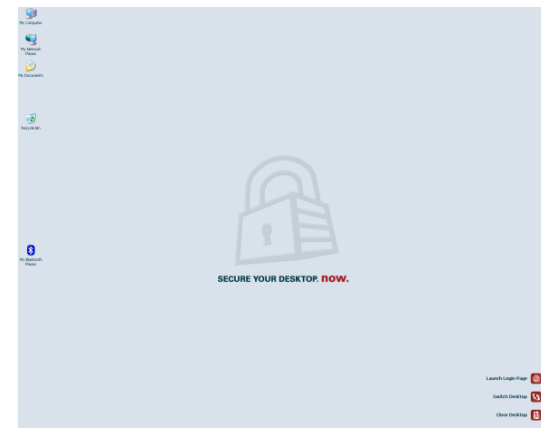
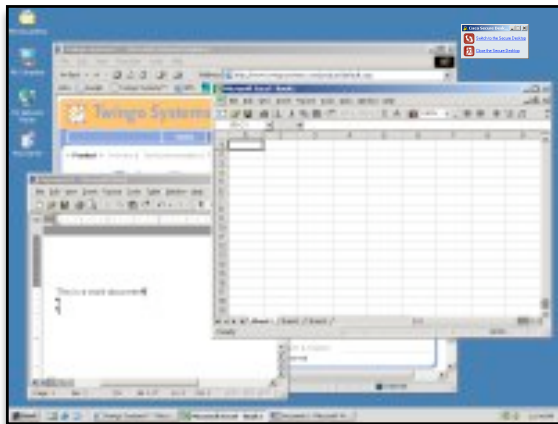
## Страница входа в WebVPN



# Cisco Secure Desktop

## Схема работы (этап входа)

- **Шаг 5.** Поиск средств регистрации нажатий клавиш и сред эмуляции.
- **Шаг 6.** Создание безопасной среды и переключение на работу со средой Secure Desktop.
- **Шаг 7.** Отображение окна входа.
- **Шаг 8.** Пользователь выполняет вход и инициирует установление VPN-подключения.
- **Шаг 9.** Выполняется анализ состояния ПК для назначения DAP.



# Cisco Secure Desktop

## Схема работы (после входа)

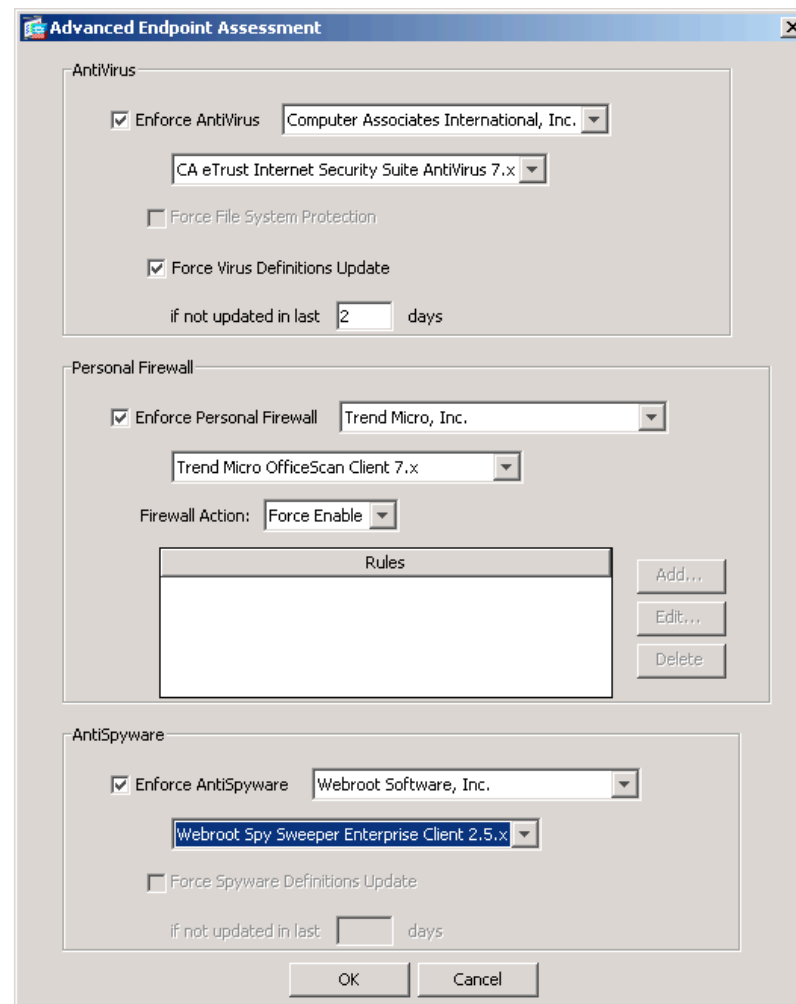
- **Шаг 10.** Применяется DAP (по результатам проверки).
- **Шаг 11.** Устанавливается VPN-подключение.
- **Шаг 12.** Пользователь может получать доступ к ресурсам.
- **Шаг 13.** После завершения сеанса (или истечения тайм-аута) VPN-подключение разрывается, выполняется очистка после работы со средой Secure Desktop.



# Расширенная оценка состояния оконечного устройства

## Встроенные средства повышения защищенности

- Поддерживаемые компоненты
  - Антивирус
  - Персональный МСЭ
  - Средства борьбы со шпионскими программами
- Предоставляются регулярные обновления
- Не требуется использовать динамические политики доступа



# Динамическая политика доступа (DAP)

## Авторизация

- Новый метод обеспечения выполнения (с версии ASA 8.0)
- Дополняет или переопределяет существующие атрибуты авторизации
- Использует совокупность результатов оценки и данных об авторизации
- Поддерживает агрегацию **нескольких** записей DAP

# Принципы DAP

- Критерии выбора

- Определяет соответствующие атрибуты AAA и (необязательно)

- Определяет соответствующие атрибуты результатов оценки оконечного устройства (несколько)

- Результат1 = применение политики DAP

- Результат2 = применение нескольких соответствующих политик DAP

# Пример DAP в ASDM(1)

Policy Name: Second-Policy  
Description: Second-DAP  
Priority: 1

**Selection Criteria**

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes and endpoint attributes criteria below, and every endpoint attribute has been satisfied. These attributes can be created using the tables below. Use the logical expression text to specify the logical expression text.

User has ANY of the following AAA Attributes values...

AAA Attribute	Operation/Value
ldap.memberOf	= Users
cisco.memberof	= Radius

**AAA gives this**

and the following endpoint attributes are...

Endpoint ID	Name/Operation/Value
av.McAfeeAV	exists = true
	description = McAfee VirusScan Enterpri.
os	version = Windows XP
os	version = Windows Vista

**Assessment requires these**

**Advanced**

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action | Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists | **URL Lists** | Access Method

Enable URL lists

Bookmarks

Manage... Add>> Delete

**Policy Results are here**

OK Cancel Help

# Пример DAP в ASDM(2)

Policy Name: Default-Policy  
Description: First-DAP  
Priority: 0

Selection Criteria

Define the AAA and endpoint attributes used to select this access policy. A policy is used when a user's authorization attributes match the AAA attribute criteria below and every endpoint attribute has been satisfied. These attributes can be created using the tables below and/or by expanding the Advanced option to specify the logical expression text.

User has ALL of the following AAA Attributes values... and the following endpoint attributes are satisfied.

AAA Attribute	Operation/Value	Add
cisco.memberof	= Radius	Add

**AAA Results**

Endpoint ID	Name/Operation/Value	Add
application	clienttype = AnyConnect	Add

**AnyConnect in Use**

Advanced

Access Policy Attributes

Configure access policy attributes for this policy. Attributes values specified here will override those values obtained from the AAA system.

Action | Network ACL Filters | Web-Type ACL Filters | Functions | Port Forwarding Lists | URL Lists | Access Method

Network ACL (only all-permit and all-deny entries allowed)

Block-SMTP-Port-25

Available ACLs

Network ACLs

Block-SMTP-Port-25

Resulting ACLs

OK Cancel Help

# Правила агрегации DAP



Приводится  
для справки

- Атрибут Action (Terminate или Continue)

DAP-1	DAP-2	DAP-3	Результирующая DAP
Continue	Terminate	Continue	Terminate
Continue	Continue	Continue	Continue

- Списки URL (список1, список2, список3, ...)

DAP-1	DAP-2	DAP-3	Результирующая DAP
Список1	Список2, список3	Список2	Список1,2,3

- Функции для сети без использования клиента (file-browse, file-entry, url-entry, ...)

Функция	DAP-1	DAP-2	Результирующая DAP
File-entry	enable	disable	enable
Url-enty		disable	disable

# Простая проверка агрегации DAP

DAP1	memberOf = Sales		<b>URL-List 1</b>
DAP2	memberOf = Marketing		<b>URL-List 2</b>
DAP3	memberOf = Sales/Marketing	Доверенный ПК	<b>Все функции</b>

USER-1	memberOf = Sales		<b>URL-List 1</b>
USER-2	memberOf = Sales&Marketing		<b>URL-List 1+2</b>
USER-2	memberOf = Sales&Marketing	Доверенный ПК	<b>URL-List 1+2</b> <b>Все функции</b>

# Результаты авторизации (некоторые)

- Terminate/Continue
- Сетевые списки ACL
- Списки ACL для интернет-ресурсов
- Функции (работа с файловыми серверами, URL, приложениями)
- Списки перенаправления портов
- Списки URL (нет, определенные URL)
- Метод доступа (AnyConnect, web-портал)
- Настройка портала
- и многое другое...

# УПРАВЛЕНИЕ VPRN УДАЛЕННОГО ДОСТУПА

# Методы управления

## Вариант I: интерфейс командной строки

- Можно выполнить БОЛЬШУЮ ЧАСТЬ настройки, настройка SSL VPN может вызвать затруднения
- Настройка CSD с помощью командной строки НЕВОЗМОЖНА

```
3: Ext: Ethernet0/2      : address is 001d.a25c.5222, irq 255
4: Ext: Ethernet0/3      : address is 001d.a25c.5223, irq 255
5: Ext: Ethernet0/4      : address is 001d.a25c.5224, irq 255
6: Ext: Ethernet0/5      : address is 001d.a25c.5225, irq 255
ASA5505#
ASA5505#
ASA5505# sh run
: Saved
:
ASA Version 8.0(4)
!
hostname ASA5505
enable password 2KFQnbNIdI.2KYOU encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
names
!
interface Vlan1
no nameif
no security-level
no ip address
!
interface Vlan10
nameif VLAN10
security-level 100
ip address 192.168.1.20 255.255.255.0
!
interface Vlan20
nameif VLAN20
security-level 0
ip address 192.168.2.20 255.255.255.0
!
```

# Методы управления

## Вариант II: ASDM

- Вся настройка SSL VPN может быть выполнена с помощью ASDM. Необходимо изменить порт по умолчанию ASDM (443) на другой порт.
- ASDM позволяет выполнять мониторинг VPN-подключений и просматривать журналы VPN
- Не разрешайте доступ к ASDM с того интерфейса, который используется для SSL VPN!

The screenshot displays the Cisco ASDM 6.1 for ASA interface. The left pane shows the configuration tree with 'Prelogin Policy' selected under 'Secure Desktop Manager'. The right pane shows the 'Prelogin Policy' configuration page, which includes a decision tree diagram. The decision tree starts with 'Start' and branches based on the operating system (OS): Win 2K/XP/Vista leads to 'subsequence: Windows Start', Win 9x leads to 'subsequence: Windows Start', Mac and Linux lead to 'Mac/Linux Default', and Failure leads to 'Login Denied'. Below this, a 'Windows Start' subsequence leads to a 'File Check?' step, which branches to 'Kiosk' on Success and 'Default' on Failure.

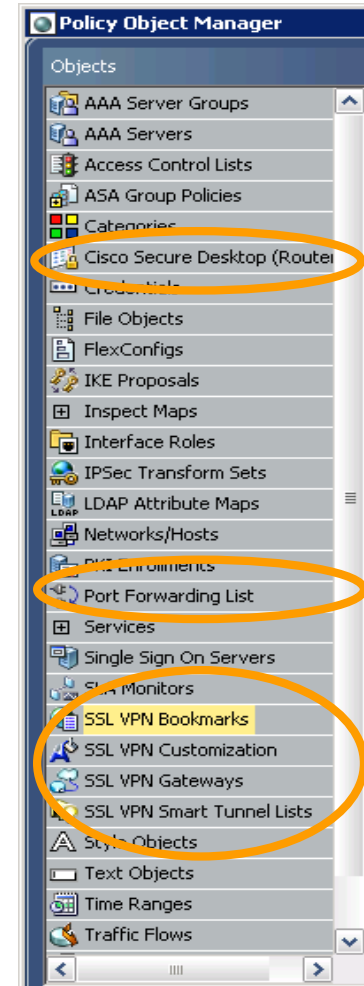
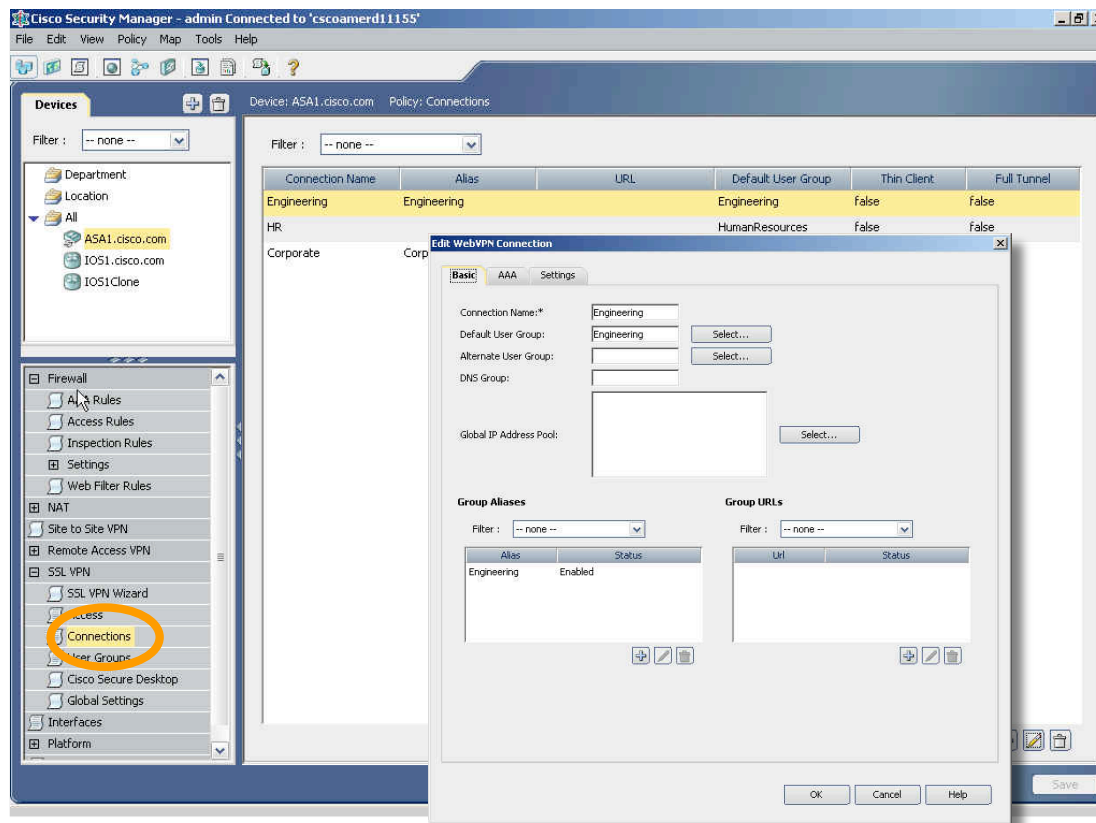
Client Type: SSL VPN Client  
Client Ver: Cisco AnyConnect VPN Agent for Wind.  
Packets Tx: 1  
Packets Rx: 0  
Packets Tx Dropped: 0  
Packets Rx Dropped: 0

DTLS-Tunnel	AES-128	Tunnel ID: 8.3 Assigned IP 10.1.80.10 Public IP: 10.1.55.2 Hashing: SHA1 Encapsulation: DTLSv1.0 UDP Source Port 1861 UDP Destination Port 443 Authentication Mode: userPassword Ttl: Time Out: 20 Minutes	616 1067
-------------	---------	--	-------------

# Методы управления

## Вариант III: Cisco Security Manager

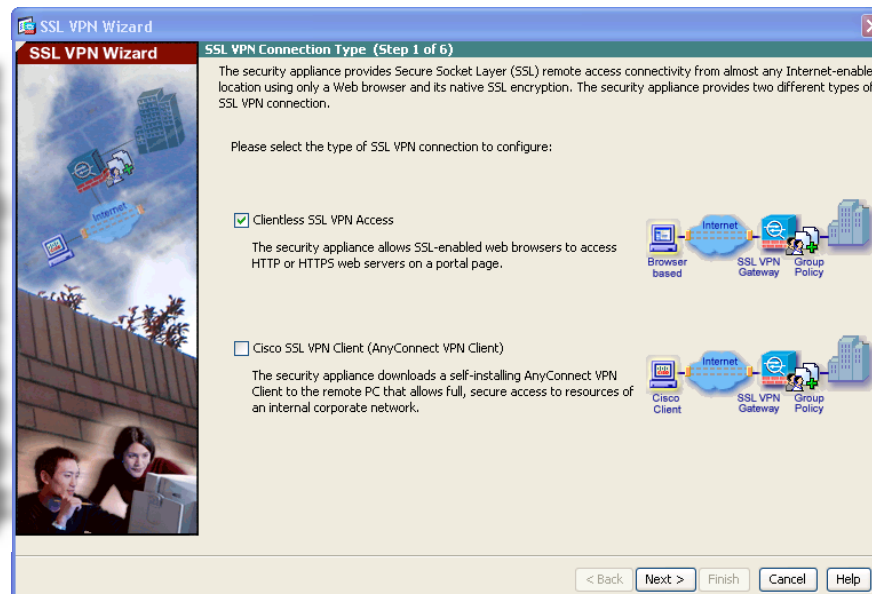
- CSM позволяет задать большую часть настроек SSL VPN



# РЕЗЮМЕ

# Как эффективно выполнить начальное развертывание?

- Используйте мастер SSL-VPN в ASDM
  - Помогает создать хорошую начальную конфигурацию
- Используйте XML-Editor (загружается с [www.cisco.com](http://www.cisco.com)) для редактирования профилей AnyConnect (Cisco VPN Client Tools ...или ASA 8.3)



# Основные результаты

## Выбор наиболее подходящего решения

- Если пользователи не расстаются с ноутбуками и установка клиента не представляет проблем, ориентируйтесь на AnyConnect
  - AnyConnect — клиент нового поколения
- Если пользователи нерегулярно обращаются к корпоративным ресурсам или необходимо предоставить доступ внешним пользователям, создайте SSL VPN без использования клиента
  - Подходит для доступа партнеров и гостевого доступа
  - Удовлетворяет базовые потребности сотрудников
- Для домашних работников оптимальной является установка специализированного устройства
  - Интеграция средств организации беспроводной сети и поддержки IP-телефонии
  - Члены семьи могут пользоваться интернет-ресурсами, не создавая рисков безопасности (разделение трафика)

Ваши вопросы?



[Security-request@cisco.com](mailto:Security-request@cisco.com)



**CISCO**