Санкт-Петербургское государственное бюджетное
профессиональное образовательное учреждение
«Академия управления городской средой, градостроительства и печати»

УТВЕРЖДАЮ
Заместитель директора
по учебно-производственной работе
_____ О.В. Фомичева
«22» 12 2023 г.

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ
по выполнению практических работ
по МДК.01.03 Безопасность компьютерных сетей
ПМ.01 НАСТРОЙКА СЕТЕВОЙ ИНФРАСТРУКТУРЫ

для специальности

09.02.06 Сетевое и системное администрирование

Санкт-Петербург
2023 г.

Методические рекомендации рассмотрены на заседании методического совета СПб ГБПОУ «АУГСГиП»
Протокол № 2 от «29» 11 202 3 г.

Методические рекомендации одобрены на заседании цикловой комиссии информационных технологий
Протокол № 4 от «2» 11 202 3 г.

Председатель цикловой комиссии: Караченцева М.С. _____

Разработчики: преподаватели СПб ГБПОУ «АУГСГиП»

С О Д Е Р Ж А Н И Е

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Методические рекомендации по выполнению практических работ предназначены для организации работы на практических занятиях по МДК.01.03 «Безопасность компьютерных сетей», которая является важной составной частью в системе подготовки специалистов среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование».

Практические занятия являются неотъемлемым этапом изучения учебной дисциплины и проводятся с целью:

- формирования практических умений в соответствии с требованиями к уровню подготовки обучающихся, установленными рабочей программой учебной дисциплины;
- обобщения, систематизации, углубления, закрепления полученных теоретических знаний;
- готовности использовать теоретические знания на практике.

Практические занятия по МДК.01.03 «Безопасность компьютерных сетей» способствуют формированию в дальнейшем при изучении профессиональных модулей, следующих общих и профессиональных компетенций:

ОК 1. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам;

ОК 2. Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности;

ОК 3. Планировать и реализовывать собственное профессиональное и личностное развитие, предпринимательскую деятельность в профессиональной сфере, использовать знания по правовой и финансовой грамотности в различных жизненных ситуациях;

ОК 4. Эффективно взаимодействовать и работать в коллективе и команде;

ОК 5. Осуществлять устную и письменную коммуникацию на государственном языке Российской Федерации с учетом особенностей социального и культурного контекста;

ОК 6. Проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных российских духовно-нравственных ценностей, в том числе с учетом гармонизации межнациональных и межрелигиозных отношений, применять стандарты антикоррупционного поведения;

ОК 7. Содействовать сохранению окружающей среды, ресурсосбережению, применять знания об изменении климата, принципы бережливого производства, эффективно действовать в чрезвычайных ситуациях;

ОК 8. Использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности;

ОК 9. Пользоваться профессиональной документацией на государственном и иностранном языках.

ПК 1.1. Документировать состояния инфокоммуникационных систем и их составляющих в процессе наладки и эксплуатации

ПК 1.2. Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем.

ПК 1.3. Устранять неисправности в работе инфокоммуникационных систем.

ПК 1.4. Проводить приемо-сдаточные испытания компьютерных сетей и сетевого оборудования различного уровня и оценку качества сетевой топологии в рамках своей ответственности.

ПК 1.5. Осуществлять резервное копирование и восстановление конфигурации сетевого оборудования информационно-коммуникационных систем.

ПК 1.6. Осуществлять инвентаризацию технических средств сетевой инфраструктуры, контроль оборудования после проведенного ремонта.

ПК 1.7. Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем.

В методических рекомендациях предлагаются к выполнению практические работы, предусмотренные рабочей программой МДК.01.03 «Безопасность компьютерных сетей».

При разработке содержания практических работ учитывался уровень сложности освоения студентами соответствующей темы, общих и профессиональных компетенций, на формирование которых направлена дисциплина.

Выполнение практических работ в рамках МДК.01.03 «Безопасность компьютерных сетей» позволяет освоить комплекс работ по выполнению практических заданий по всем темам МДК.01.03 «Безопасность компьютерных сетей».

Методические рекомендации по МДК.01.03 «Безопасность компьютерных сетей» имеют практическую направленность и значимость. Формируемые в процессе практических занятий умения могут быть использованы студентами в будущей профессиональной деятельности.

Оценки за выполнение практических работ выставляются по пятибалльной системе. Оценки за практические работы являются обязательными текущими оценками по учебной дисциплине и выставляются в журнале теоретического обучения.

1. Перечень практических работ по МДК.01.03 «Безопасность компьютерных сетей»

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
Тема 3.1. Обеспечение безопасности компьютерных сетей	использовать многофункциональные приборы мониторинга, программно-аппаратные средства технического контроля локальной сети	ПК 1.1-ПК 1.7 ОК 01-02, ОК 05-07, ОК 09	**Практическое занятие № 1** Социальная инженерия	2
			Практическое занятие № 2 Исследование сетевых атак и инструментов проверки защиты сети	2
			Практическое занятие № 3 Безопасность ресурсов и контроль доступа	2
			Практическое занятие № 4 Сканирование уязвимостей	2
			Практическое занятие № 5 Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.	2
			Практическое занятие № 6 Допуск к ресурсам сети	2
			Практическое занятие № 7 Применение различных способов разграничения доступа к компьютерным ресурсам	2
			Практическое занятие № 8 Настройка безопасного доступа к маршрутизатору	2
			Практическое занятие № 9 Настройка Site-to-Site VPN используя интерфейс командной строки	2
			Практическое занятие № 10 Автоматическое шифрование логических дисков ПК.	2
			Практическое занятие № 11 Базовая настройка шлюза безопасности ASA	2
			Практическое занятие № 12 Создание правил Modular Policy Framework (MPF) в шлюзе безопасности ASA	2
			Практическое занятие № 13 Настройка безопасности на втором уровне на коммутаторах	2
			Практическое занятие № 14 Настройка политики безопасности брандмауэров	2

№ раздела, темы	Освоение умений в процессе занятия	Формируемые ОК и ПК	Тема практического занятия	Кол-во часов
			Практическое занятие № 15 Установка и настройка SSL VPN	2
			Практическое занятие № 16 Установка и настройка IPSec VPN	2
			Практическое занятие № 17 Обеспечение информационной безопасности сети	2

2. Описание порядка выполнения практических работ

Практическая работа № 1
Социальная инженерия

Задание:

Приняты ли в вашей компании или школе процедуры, призванные предотвращать применение социальной инженерии?
Если да, в чем заключаются эти процедуры?
Найдите в Интернете процедуры, принятые в организациях для того, чтобы предотвратить получение доступа к конфиденциальной информации при помощи социальной инженерии. Перечислите найденное.

Практическая работа № 2
Исследование сетевых атак и инструментов проверки защиты сети

Исходные данные/сценарий
За многие годы злоумышленники разработали множество инструментов для проведения атак и компрометации сетей. Эти атаки имеют множество форм, но чаще всего они направлены на получение конфиденциальной информации, уничтожение ресурсов или блокирование доступа легальных пользователей к ресурсам. Когда сетевые ресурсы оказываются недоступны, может страдать продуктивность работника, приводя к упущенной выгоде для всего бизнеса.
Чтобы понять, как защитить сеть от атак, администратор должен определить уязвимости сети. Специальные программы аудита безопасности, разработанные производителями оборудования и программного обеспечения, помогают определить потенциальные уязвимости. Инструменты, которые применяются для атак на сеть, могут быть использованы и сетевыми специалистами для тестирования способности сети противостоять этим атакам. После определения уязвимостей можно предпринимать меры для защиты сети.
Эта лабораторная работа представляет собой структурированный исследовательский проект, разделенный на две части: изучение сетевых атак и инструментов аудита безопасности. Сообщите инструктору, какие сетевые атаки и инструменты для аудита безопасности вы выбрали для изучения. Таким образом, участники группы расскажут о целом наборе сетевых атак и инструментов для определения уязвимостей.
В части 1 изучите реально произошедшие сетевые атаки. Выберите одну из этих атак и опишите, каким образом она была совершена, объем урона, нанесенного сети, и время простоя. Затем проанализируйте, каким образом данная атака могла бы быть нейтрализована и какие техники нейтрализации можно реализовать для предотвращения будущих атак. В конце подготовьте отчет по форме, описанной в этой лабораторной работе.
В части 2 изучите инструменты аудита безопасности и проведения атак. Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Составьте отчет на одну страницу по этому инструменту по форме, описанной в этой лабораторной работе. Подготовьте короткую (на 5-10 минут) презентацию для группы.
Вы можете работать в парах, где один человек рассказывает о сетевой атаке, а другой – об инструментах. Каждый участник группы составляет короткий рассказ о результатах своего анализа. Можно использовать презентации Powerpoint или просто продемонстрировать полученные результаты.

Задание:

Изучите различные сетевые атаки.
Перечислите несколько атак, которые вы обнаружили в ходе изучения.

Заполните следующую форму по выбранной сетевой атаке.

Название атаки	
Тип атаки	
Даты проведения атак	
Пострадавшие компьютеры/организации	
Принцип действия и результаты	
Варианты нейтрализации	
Справочные данные и ссылки	
Графики и иллюстрации (включают ссылки на файл PowerPoint или веб-сайты)	

Изучение инструментов аудита безопасности и проведения атак
Изучите различные инструменты аудита безопасности и проведения атак.
Перечислите несколько инструментов, которые вы обнаружили в ходе изучения.

Заполните следующую форму для выбранного инструмента аудита безопасности/проведения атак.

Наименование инструмента	
Разработчик	
Тип инструмента (с интерфейсом или символьно-ориентированный)	
Место использования (сетевое устройство или компьютер)	
Стоимость	
Описание ключевых особенностей и возможностей продукта или инструмента	
Справочные данные и ссылки	

Практическая работа № 3
Безопасность ресурсов и контроль доступа

Задание

1. Создайте папку, в которую поместите текстовый файл и приложение в виде файла с расширением exe. Например, одну из стандартных программ Windows, такую какnotepad.exe(Блокнот).
2. Установите для этой папки разрешения полного доступа для одного из пользователей группы администраторы, и ограниченные разрешения для пользователя с ограниченной учетной записью.
3. Выполните различные действия с папкой и файлами для обеих учетных записей и установите, как действуют ограничения, связанные с назначением уровня доступа ниже, чем полный доступ.
4. Установите общий доступ к папке и подключитесь к ней через сеть с другого виртуального компьютера.
5. Установите разрешения общего доступа так, чтобы администратор не имел ограничений, а пользователь имел ограниченный уровень доступа.
6. Экспериментально убедитесь в правилах объединения разрешений NTFS и разрешений общего доступа.
7. Составьте отчет о проведенных экспериментах.
8. Разработайте стратегию регулирования безопасности при коллективном доступе к общим папкам для различных групп пользователей.

Практическая работа № 4
Сканирование уязвимостей

Задание 1. Загрузите из Интернета и установите на компьютер программу Microsoft Baseline Security Analyzer.

1. Запустите Интернет-обозреватель и задайте адрес web-страницы официального сайта Microsoft www.microsoft.com/technet/ security/tools/mbsahome.asp. Загрузите с этой страницы файл MBSASetup-EN.msi.

2. Для инсталляции Microsoft Baseline Security Analyzer 2.1 после сохранения файла MBSASetup-EN.msi запустите этот файл, затем подтвердите согласие с условиями использования и следуйте указаниям мастера инсталляции.

Задание 2. Тестирование безопасности с помощью MS Baseline Security Analyzer 2.1.

1.Для запуска программы щелкните соответствующий ярлык или выберите в меню **Программы** команду **Microsoft Baseline Security Analyzer 2.1.**

2.Для изучения справки программы щелкните в левой части окна на ссылке **Microsoft Baseline Security Analyzer Help.** После изучения справочного материала закройте окно справки.

3.Для сканирования компьютера на предмет наличия уязвимостей щелкните в правой части окна программы на ссылке **Scan a computer.** Затем в окне *Pick a computer to scan* (Выберите компьютер для сканирования) включите варианты проверки:

Check for Windows vulnerabilities Проверить уязвимость Windows
Check for weak passwords Проверить надежность паролей
Check for IIS vulnerabilities Проверить уязвимость IIS
Check for SQL vulnerabilities Проверить уязвимость SQL
Check for security updates Проверить модификации защиты
Щелкните ссылку Start scan.

После выполнения сканирования компьютера в правой части окна программы **Microsoft Baseline Security Analyzer 2.1** будет показан отчет о наличии уязвимостей, как показано на *рис. 2*.
Значок в виде красного креста указывает на критическую уязвимость данного компонента системы, желтый крест указывает на угрозу, зеленая метка указывает на соответствие требованиям по уязвимости. Для просмотра подробного отчета по каждому пункту можно щелкнуть на ссылке **What was scanned** (Что отсканировано), **Result details** (Подробности) или **How to correct this** (Как это исправить).
4. Для вывода на печать или копирования отчета в буфер обмена щелкните на соответствующей ссылке на панели Actions. Завершите работу программы.
Число факторов, способных привести к нестабильной работе компьютерной системы и потере пользовательских данных, весьма велико - это и попытки заставить старые драйверы специфических устройств работать в Windows, и установка нового ПО, несовместимого с используемой ОС, и некорректное выключение компьютера, и множество других рискованных действий.
Разработчики Windows XP постарались предусмотреть все возможные воздействия внешних факторов на стабильность ее работы, предложив пользователю широкий выбор средств для решения связанных с этих проблем.
Перечисленные методы необходимо сочетать с другими средствами восстановления данных, такими, как Driver Rollback и загрузочная конфигурация LastKnownGood, - в зависимости от характера и причины сбоя.

Практическая работа № 5
Идентификация пользователей и установление их подлинности при доступе к компьютерным ресурсам.

Задание

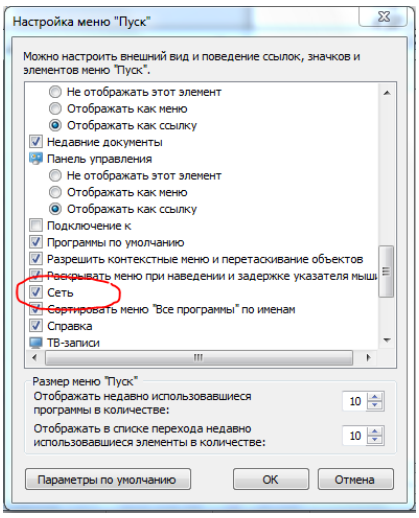
Задание	Алгоритм
1	2
Пусть на экран выведены следующие три слова: «Sony», «Hewlett» и «Packard». Составить программу, которая записывает пароль следующим образом	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 2. В качестве второго символа записать букву, которая в алфавите предшествует букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся средним символом третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся первым символом первого слова на экране; если это буква «z», записать «a». 5. Вывести полученную строку.

Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?
Пусть на экран выведены следующие три слова: «scleroses», «scoliosis», «paradantoz». Составить программу, которая записывает пароль следующим образом	Исходные данные — строковые константы 1. В строку <*результат*> в качестве первого символа записать букву, которая в алфавите следует за буквой, являющейся вторым символом первого слова на экране; если это буква «z», записать «a». 2. В качестве второго символа записать букву, которая в алфавите предшествует предпоследней букве, являющейся последним символом второго слова на экране; если это буква «a», записать «z». 3. Если третье слово содержит нечетное количество букв, то в качестве третьего символа записать букву, которая в алфавите следует за буквой, являющейся предшественником среднего символа третьего слова; если это буква «z», записать «a». Если же третье слово содержит четное количество символов, то в качестве третьего символа записать букву, которая в алфавите предшествует букве, являющейся первым из двух средних символов третьего слова; если это буква «a», записать «z». 4. В качестве четвертого символа записать букву, которая в алфавите стоит на месте, соответствующем сумме количеств символов в первом и третьем словах плюс 1 символ; если эта сумма больше 26, найти и использовать в качестве номера позиции искомой буквы в алфавите остаток от деления указанной суммы на 26. 5. Вывести полученную строку.
Дополнить полученную программу средствами аутентификации	1. Ввести пароль пользователя. При вводе пароля пользователя обеспечить ввод пароля с отображением вместо каждого символа знаков «*». 2. Сравнить пароль пользователя с паролем, вычисленным ЭВМ. 3. Вывести результат аутентификации: пароль верен или неверен?

Практическая работа № 6
Допуск к ресурсам сети

Задание:

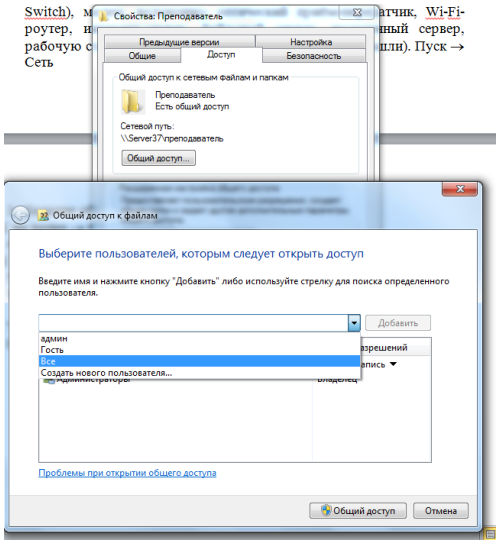
1. Отобразить ярлык Сеть в Главном меню (ПК на кнопке Пуск → Настроить → Сеть)



2. Ознакомиться с содержимым локальной компьютерной сети (открыть папку Сеть). Найдите в вашей сети сетевой адаптер, концентратор (HUB или Switch), модем, волоконно- оптический приёмопередатчик, Wi-Fi-роутер, интернет-сервер, файловый сервер, выделенный сервер, рабочую станцию (покажите преподавателю, что вы нашли). Скриншот окна разместить в документе Word
3. На диске D: создать папку с вашей фамилией и поместить в неё 2 любых файла.
4. На диске D: задать общий доступ для вашей папки

4.1. Задание общего доступа папке:

ПК на папке → Свойства → Доступ → Общий доступ → из списка пользователей выбрать Все → Добавить



настроить доступ Чтение и запись → Общий доступ

5. Проверить доступ к папке. Для этого открыть папку D:\ ваша папка на любом другом компьютере, входящем в вашу рабочую группу. Поместить скриншот содержимого вашей папки в документ Word.
6. Прерывание общего доступа папке:

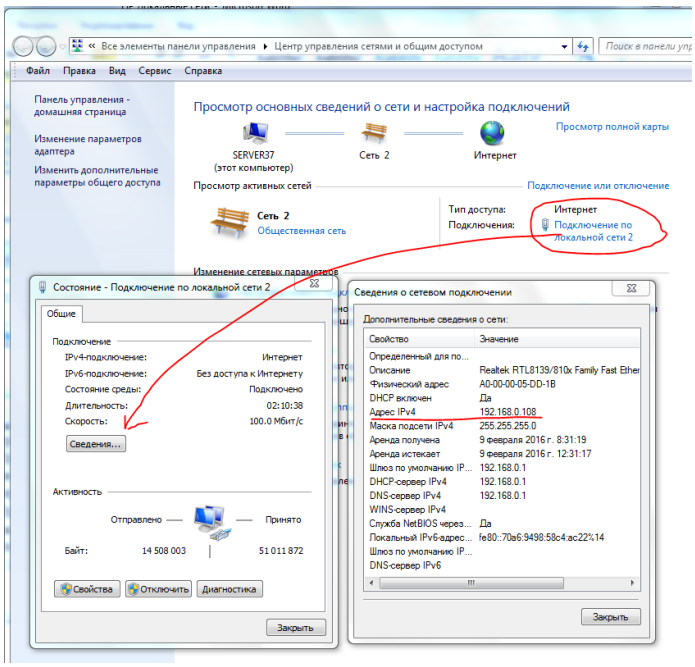
ПК на папке → Общий доступ → Никому из пользователей

7. Определите IP адрес вашего персонального компьютера.

7.1. Для определения IP адреса воспользуемся командной строкой. Для этого ЛК на кнопке Пуск и в поле Поиск ввести в поле команду cmd. Далее ввести команду ipconfig и найти свой IP адрес.

7.2. Скрин разместить в отчёте

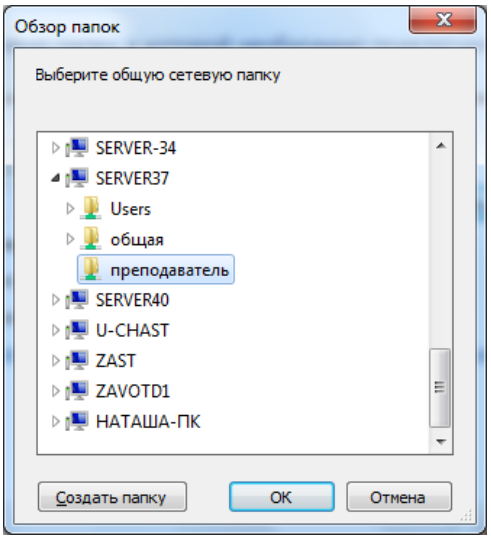
7.3. ЛК на индикаторе Сеть → Центр управления сетями и общим доступом →



7.4. Скрин окон (как в методичке) разместить в отчёте. Вырезать часть экрана с помощью инструмента Ножницы и пером отметить IP адрес.

8. Создать сетевой диск из папки Преподаватель, расположенной на ПК SERVER37.

8.1. Пуск → ПК на ярлыке Сеть → Подключить сетевой диск → Обзор → выбрать ПК и выбрать папку → ОК .



8.2. Просмотреть как отображается сетевой диск в папке Мой компьютер

8.3. Скопировать скриншот окна Мой компьютер в отчёт.

8.4. Отправить отчёт по локальной сети в папку Преподаватель.

8.5. Найдите в сети Интернет информацию о назначении сетевого диска и выпишите в тетрадь.

9. Отключите сетевой диск Преподаватель.

Практическая работа № 7
Применение различных способов разграничения доступа к компьютерным ресурсам.

Задание № 1. Определение общих ресурсов компьютера.

Для этого: В операционной системе Windows найти на рабочем столе значок Сеть. Открыть папку, где будут видны все компьютеры, которые подключены в одну сеть. В данном окне появятся все компьютеры, которые подключены к сети. Открыть один из них. Посмот-

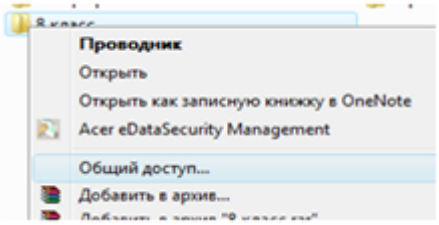
реть ресурсы компьютера, которыми можно воспользоваться. Такие ресурсы называются общими.

Задание № 2.

Предоставить доступ для пользователей локальной сети к папке на своем компьютере, подключенном к локальной сети.

Для этого:

- В операционной системе Windows открыть окно папки Компьютер и на одном из дисков C: или D: создать свою папку. Назвать ее номером своей группы.
- Щелкнуть правой кнопкой мыши по значку папки и в контекстном меню папки выберите команду Общий доступ.



- В появившемся диалоговом окне Дополнительный общий доступ установить флажок Открыть общий доступ к этой папке.
- Если все правильно сделано, то на диске (у вашей папки) появится значок, который показывает, что папка является общей.

Задание №3. Осуществить проверку возможности доступа к ресурсам компьютеров, подключенных к локальной сети.

Для этого:

- Щелкнуть по значку Сеть, в окне появится список компьютеров, подключенных к локальной сети (смотри задание 1.)
- Открыть свой компьютер и внимательно посмотреть, какие из ресурсов доступны пользователям. Если название Вашей папки есть в перечне, то все сделано правильно.

Практическая работа № 8
Настройка безопасного доступа к маршрутизатору

Задание:

Топология

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	192.168.1.1	255.255.255.0	Недоступно
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
ПК-А	Сетевой адаптер	192.168.1.3	255.255.255.0	192.168.1.1

Задачи

Часть 1. Настройка основных параметров устройства

Часть 2. Настройка маршрутизатора для доступа по протоколу SSH

Часть 3. Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

Часть 4. Проверка сеанса связи по протоколу SSH с помощью программы Wireshark
Часть 5. Настройка коммутатора для доступа по протоколу SSH
Часть 6. Настройка протокола SSH в интерфейсе командной строки коммутатора
Исходные данные/сценарий
Раньше для удалённой настройки сетевых устройств в основном применялся протокол Telnet. При этом протоколы типа Telnet не включают проверку подлинности и шифрование информации, передаваемой между клиентом и сервером, что позволяет сетевым средствам слежения перехватывать пароли и данные конфигурации.
Secure Shell(SSH)— это сетевой протокол, устанавливающий безопасное подключение эмулятора терминала к маршрутизатору или иному сетевому устройству. Протокол SSH шифрует все сведения, которые поступают по сетевому каналу, и предусматривает аутентификацию удалённого компьютера. Протокол SSH всё больше заменяет Telnet — именно его выбирают сетевые специалисты в качестве средства удалённого входа в систему. Чаще всего протокол SSH применяется для входа на удалённое устройство и выполнения команд, но может также передавать файлы по связанным протоколам SFTP или SCP.
Чтобы протокол SSH работал, на взаимодействующих сетевых устройствах должна быть настроена его поддержка. В ходе лабораторной работы вы активируете на маршрутизаторе SSH-сервер и подключитесь к маршрутизатору, используя ПК с клиентом SSH. В локальной сети подключение обычно устанавливается с помощью Ethernet и IP-адреса.
Кроме того, в ходе лабораторной работы вы настроите маршрутизатор для приёма подключений по протоколу SSH и воспользуетесь программой Wireshark для перехвата и просмотра сеансов Telnet и SSH. Это покажет, какую важную роль играет шифрование данных, осуществляемое протоколом SSH. И, наконец, вам придётся самостоятельно настроить коммутатор для подключения по протоколу SSH.
Примечание. Маршрутизаторы, используемые на практических занятиях CCNA: маршрутизаторы с интеграцией сервисов серии Cisco 1941 (ISR) установленной версии Cisco IOS 15.2(4) M3 (образ universalk9). Используемые коммутаторы: семейство коммутаторов Cisco Catalyst 2960 версии CISCO IOS 15.0(2) (образ lanbasek9). Можно использовать другие маршрутизаторы, коммутаторы и версии CISCO IOS. В зависимости от модели и версии Cisco IOS выполняемые доступные команды и выводы могут отличаться от данных, полученных в ходе лабораторных работ. Точные идентификаторы интерфейса см. в таблице сводной информации об интерфейсах маршрутизаторов в конце данной лабораторной работы.
Примечание. Убедитесь, что информация, имеющаяся на маршрутизаторе и коммутаторе, удалена и они не содержат файлов загрузочной конфигурации. Если вы не уверены, что сможете это сделать, обратитесь к инструктору.
Необходимые ресурсы

- 1 маршрутизатор (Cisco 1941 с универсальным образом M3 версии CISCO IOS 15.2(4) или аналогичным)
- 1 коммутатор (серия Cisco 2960, с программным обеспечением Cisco IOS версии 15.0(2), образ lanbasek9 или аналогичный)
- Один ПК (Windows 7, Vista или XP с эмулятором терминала, например Tera Term, и установленной программой Wireshark)
- Консольные кабели для настройки устройств CISCO IOS через консольные порты
- Кабели Ethernet в соответствии с топологией

Часть 1: Основные настройки устройства
В части 1 потребуется настройка топологии сети и основных параметров, таких как IP-адреса интерфейсов, доступ к устройствам и пароли на маршрутизаторе.
Шаг 1: Создайте сеть в соответствии с изображенной на схеме топологией.
Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.
Шаг 3: Настройте маршрутизатор.

a. Подключите консоль к маршрутизатору и активируйте привилегированный режим.

b. Войдите в режим конфигурации.

c. Отключите поиск в DNS, чтобы предотвратить попытки маршрутизатора преобразовывать неверно введённые команды таким образом, как будто они являются именами узлов.

d. Назначьте **class** в качестве пароля привилегированного режима.

e. Назначьте **cisco** в качестве пароля консоли и включите вход по паролю.

f. Назначьте **cisco** в качестве пароля виртуального терминала и включите вход по паролю. g. Зашифруйте пароли.

h. Создайте баннер, который предупреждает о запрете несанкционированного доступа.

i. Настройте и активируйте интерфейс маршрутизатора G0/1 с помощью сведений, содержащихся в таблице адресации.

j. Сохраните текущую конфигурацию в файл загрузочной конфигурации.

Шаг 4: Настройте ПК-А.

a. Настройте на ПК-А IP-адрес и маску подсети.

b. Настройте на ПК-А шлюз по умолчанию.

Шаг 5: Проверьте подключение к сети.

Отправьте эхо-запрос с помощью команды ping с ПК-А на маршрутизатор R1. Если эхо-запрос с помощью команды ping не проходит, найдите и устраните неполадки подключения.

Часть 2: Настройка маршрутизатора для доступа по протоколу SSH

Подключение к сетевым устройствам по протоколу Telnet сопряжено с риском для безопасности, поскольку вся информация передаётся в виде открытого текста. Протокол SSH шифрует данные сессии и требует аутентификации устройств, поэтому для удалённых подключений рекомендуется использовать именно его. В части 2 вам нужно настроить маршрутизатор для приёма соединений по протоколу SSH по линиям VTY.

Шаг 1: Настройте аутентификацию устройств.

При генерации ключа шифрования используются имя устройства и домен. Это значит, что эти имена необходимо указать перед вводом команды **crypto key**.

a. Укажите имя устройства.

Router(config)# **hostname R1**

b. Укажите домен для устройства.

R1(config)# **ip domain-name ccna-lab.com**

Шаг 2: Создайте ключ шифрования с указанием его длины.

R1(config)# **crypto key generate rsa modulus 1024**

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 1 seconds)

R1(config)#

*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled

Шаг 3: Создайте имя пользователя в локальной базе учётных записей.

R1(config)# **username admin privilege 15 secret adminpass**

R1(config)#

*Feb 6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc

R1(config)#

Примечание. Пятнадцатый уровень привилегий предоставляет пользователю права администратора.

Шаг 4: Активируйте протокол SSH на линиях VTY.

a. Активируйте протоколы Telnet и SSH на входящих линиях VTY с помощью команды **transport input**.

R1(config)# **line vty 0 4**
R1(config-line)# **transport input telnet ssh**

b. Измените способ входа в систему — выберите проверку пользователей по локальной базе учётных записей.

R1(config-line)# **login local**
R1(config-line)# **end** R1#

Шаг 5: Сохраните текущую конфигурацию в файл загрузочной конфигурации.

R1# **copy running-config startup-config**
Destination filename [startup-config]?
Building configuration...
[OK]
R1#

Часть 3: Проверка сеанса связи по протоколу Telnet с помощью программы Wireshark

В части 3 вы воспользуетесь программой Wireshark для перехвата и просмотра данных, передаваемых во время сеанса связи маршрутизатора по протоколу Telnet. С помощью программы Tera Term вы подключитесь к маршрутизатору R1 по протоколу Telnet, войдёте в систему и запустите на маршрутизаторе команду show run.

Примечание. Если на вашем компьютере нет программного обеспечения клиента Telnet/SSH, его необходимо установить. Чаще всего для работы с протоколами Telnet и SSH используются программы Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) и PuTTy (www.putty.org).

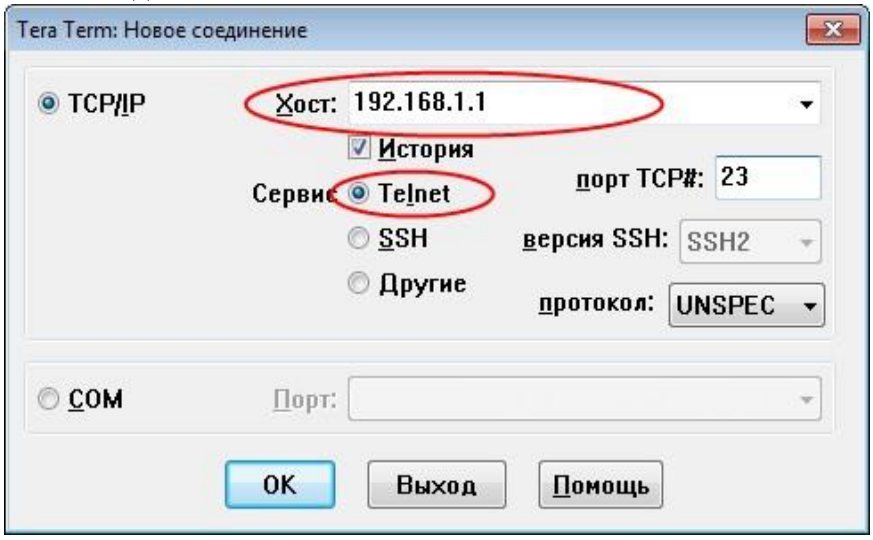
Примечание. По умолчанию доступ к Telnet из командной строки вWindows 7 отключён. Чтобы
активировать подключение по протоколу Telnet из окна командной строки, нажмите кнопку **Пуск >Панель управления>Программы>Программы и компоненты>Включение или отключение компонентов Windows**. Установите флажок рядом с компонентом **Клиент Telnet** и нажмите кнопку **OK**.

Шаг 1: Откройте Wireshark и начните сбор данных в интерфейсе локальной сети.

Примечание. Если перехват данных в интерфейсе локальной сети запустить не удаётся, попробуйте открыть программу Wireshark с помощью параметра **Запуск от имени администратора**.

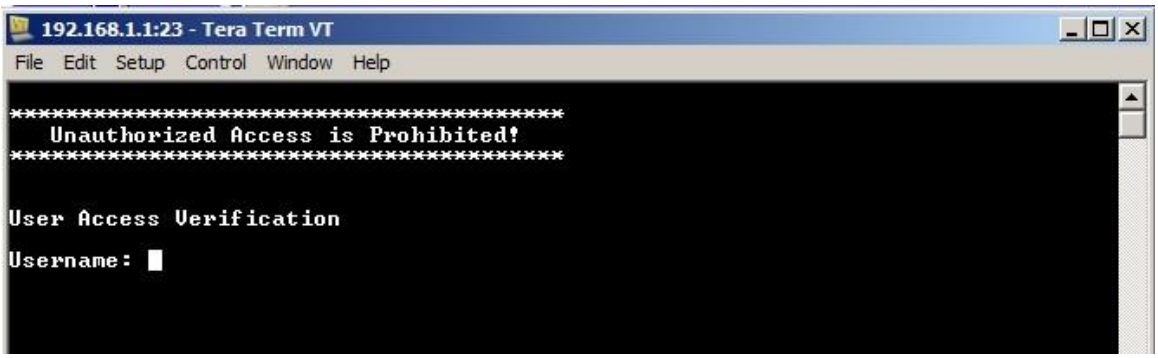
Шаг 2: Начните сеанс подключения к маршрутизатору по протоколу Telnet.

a. Запустите программу Tera Term, установите переключатель сервиса **Telnet**, а в поле «Host» введите **192.168.1.1**.



Какой порт TCP используется для сеансов Telnet по умолчанию? _____

a. В окне командной строки после приглашения Username: (Имя пользователя) введите **admin**, а после Password: (Пароль) — **adminpass**. Эти запросы появляются потому, что командой **login local** вы настроили линии VTY на использование локальной базы учётных записей.



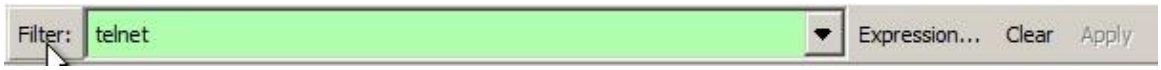
c. Введите команду **show run**.

R1# **show run**

d. Введите команду **exit**, чтобы завершить сеанс работы с протоколом Telnet и выйти из программы Tera Term.
R1# **exit**

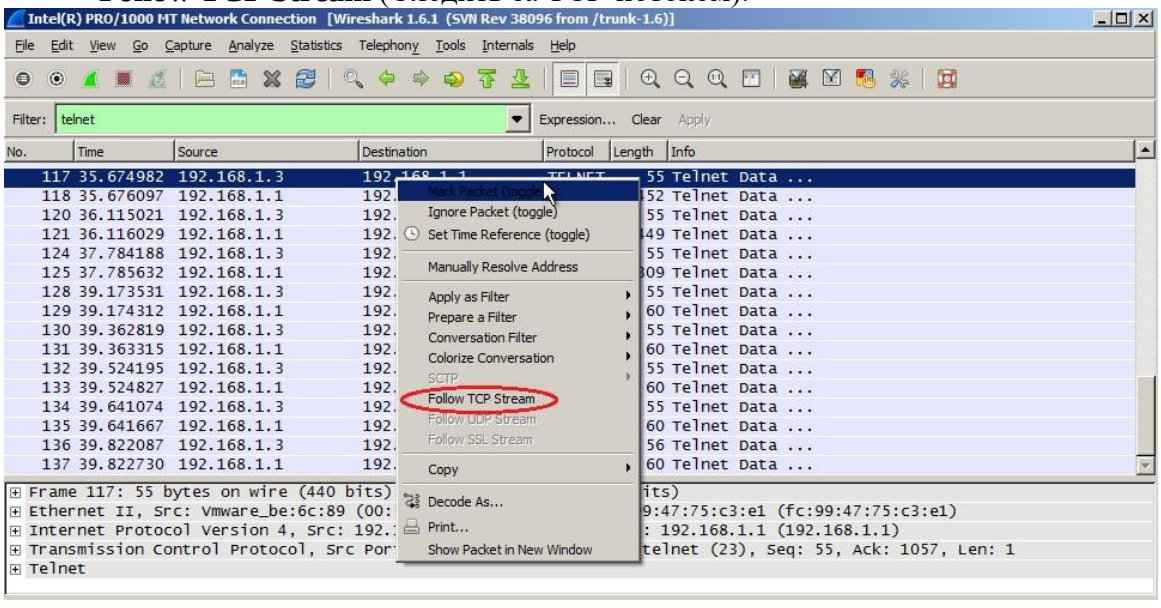
Шаг 3: Остановите сбор данных программой Wireshark.

Шаг 4: Примените один из фильтров Telnet для данных, собираемых программой Wireshark.



Шаг 5: Используйте функцию TCP в Wireshark для просмотра сеанса Telnet.

a. Нажмите правой кнопкой мыши на одну из строк **Telnet** в разделе **Packet list** (Список пакетов) программы Wireshark и выберите в раскрывающемся списке пункт **Follow TCP Stream** (Следить за TCP-потоком).



b. В окне Follow TCP Stream (Следить за TCP-потоком) отображаются данные о текущем сеансе подключения к маршрутизатору по протоколу Telnet. Весь сеанс связи (включая пароль) отображается открытым текстом. Обратите внимание на то, что введённые имя пользователя и команда **show run** отображаются с повторяющимися символами. Это связано с настройкой отображения в Telnet, которая позволяет выводить на экран символы, набираемые на клавиатуре.

Практическая работа № 9
Настройка Site-to-Site VPN используя интерфейс командной строки

Исходные данные:

Рассмотрим построение VPN-соединения «точка-точка» для связи нескольких локаций с целью расширения ИТ-инфраструктуры.
Участвуют две площадки: Россия и Франция.
(В примере используются реальные IP-адреса провайдеров для большей наглядности.)
FR.SW.DEVSERVERS.NETWORK - **45.32.144.83**
RU.SW.DEVSERVERS.NETWORK - **195.209.51.5**
Local subnet: **10.0.5.0/24**
Remote subnet: **10.0.1.0/24**

Задание:

Шаг 1. Установка VyOS
Прежде всего установим **VyOS** на оборудование или виртуальные мощности, которые планируются использовать для сетевого маршрутизатора и выполним базовую настройку.
Шаг 2. Базовая настройка
Выполняем настройку удаленного маршрутизатора (*FR.SW.DEVSERVERS.NETWORK*)
В интерфейсе командной строки **VyOS** переходим в режим конфигурации configure и выполняем базовую настройку *(все доступы временные и созданы исключительно для статьи)*:

```
set system host-name fr.sw.devservers.network
set system time-zone Europe/Moscow
set service ssh port 55555

set system ntp server 0.fr.pool.ntp.org
set system ntp server 1.fr.pool.ntp.org
set system ntp server 2.fr.pool.ntp.org
set system ntp server 3.fr.pool.ntp.org

set interfaces ethernet eth0 address 45.32.144.83/22
set interfaces ethernet eth0 description PublicNetwork
set protocols static route 0.0.0.0/0 next-hop 45.32.144.1 distance 1

set interfaces ethernet eth1 address 10.0.1.1/24
set interfaces ethernet eth1 description PrivateNetwork

set system login user rbogachev full-name "Roman Bogachev"
set system login user rbogachev authentication plaintext-password
wuQeXZcLt7GVHxnAqoMW9NjHrhtjFP8N
set system login user rbogachev level admin
```

Выполняем настройку локального маршрутизатора (*RU.SW.DEVSERVERS.NETWORK*)
По аналогии с предыдущим пунктом выполняем базовую настройку локального маршрутизатора:

```
set system host-name ru.sw.devservers.network
set system time-zone Europe/Moscow
set service ssh port 55555

set system ntp server 0.ru.pool.ntp.org
set system ntp server 1.ru.pool.ntp.org
set system ntp server 2.ru.pool.ntp.org
set system ntp server 3.ru.pool.ntp.org

set interfaces ethernet eth0 address 195.209.51.5/24
set interfaces ethernet eth0 description PublicNetwork
set protocols static route 0.0.0.0/0 next-hop 195.209.51.1 distance 1

set interfaces ethernet eth1 address 10.0.5.1/24
set interfaces ethernet eth1 description PrivateNetwork

set system login user rbogachev full-name "roman"
set system login user rbogachev authentication plaintext-password
wuQeXZcLt7GVHxnAqoMW9NjHrhtjFP8N
set system login user rbogachev level admin
```

Шаг 3. Настройка IPSec, ESP и IKE групп
Группа **IKE** (*Internet Key Exchange*) позволяет предварительно определить набор из одного или нескольких предложений, которые будут использоваться в согласовании **IKE Phase 1**, после чего может быть настроена «ассоциация безопасности» **ISAKMP** (*SA*).
Для каждого предложения в группе определяется следующая информация:

- Шифр, который зашифровывает пакеты во время **IKE Phase**;
- Хеш-функция, которая аутентифицирует пакеты во время **IKE Phase 1**;
- Срок жизни ассоциации;

Протокол **ESP** (*Encapsulating Security Payload*) обеспечивает конфиденциальность данных. Кроме того, он позволяет идентифицировать отправителя данных, а также обеспечить целостность данных и защиту от воспроизведения информации. При работе с **ESP** для шифрования и расшифровки данных обе конечные системы применяют общий ключ.
Если одновременно применяются средства шифрования и идентификации данных, то отвечающая система вначале идентифицирует пакет, а если идентификация выполнена успешно, то расшифровывает пакет. Такой способ обработки пакетов снижает нагрузку на систему и уменьшает риск взлома защиты с помощью атаки типа DDoS.
Выполняем настройку ESP и IKE групп на обоих устройствах (*FR.SW.DEVSERVERS.NETWORK && RU.SW.DEVSERVERS.NETWORK*)

```
set vpn ipsec esp-group DevServerESP lifetime 1800
set vpn ipsec esp-group DevServerESP mode tunnel
set vpn ipsec esp-group DevServerESP pfs enable
set vpn ipsec esp-group DevServerESP proposal 1 encryption aes256
set vpn ipsec esp-group DevServerESP proposal 1 hash sha1
set vpn ipsec ike-group DevServerESP lifetime 3600
set vpn ipsec ike-group DevServerESP proposal 1 encryption aes256
set vpn ipsec ike-group DevServerESP proposal 1 hash sha1
set vpn ipsec ipsec-interfaces interface eth0
```

Шаг 4. Поднимаем VPN-соединение «точка-точка»
Для настройки соединения потребуется указать параметры:

- IP-адрес удаленного узла.
- Режим проверки подлинности, который будет использоваться для аутентификации друг друга (**PSK**).
- Группа **ESP**, которая будет использоваться в соединении.
- Группа **IKE**, которая будет использоваться в соединении.
- IP-адрес локального устройства для использования в туннеле.
- Связывающая сеть (**CIDR**) или хост для каждого конца туннеля (*изолированная сеть на оборудовании*).

Выполняем настройку удаленного устройства (*FR.SW.DEVSERVERS.NETWORK*)

```
set vpn ipsec site-to-site peer 195.209.51.5 local-address 45.32.144.83
set vpn ipsec site-to-site peer 195.209.51.5 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 195.209.51.5 authentication pre-shared-secret MyS3cR3T
set vpn ipsec site-to-site peer 195.209.51.5 connection-type initiate
set vpn ipsec site-to-site peer 195.209.51.5 default-esp-group DevServerESP
set vpn ipsec site-to-site peer 195.209.51.5 ike-group DevServerESP
set vpn ipsec site-to-site peer 195.209.51.5 tunnel 0 local prefix 10.0.1.0/24
set vpn ipsec site-to-site peer 195.209.51.5 tunnel 0 remote prefix 10.0.5.0/24
```

Выполняем настройку локального устройства (*RU.SW.DEVSERVERS.NETWORK*)

Обратите внимание, что параметры зеркально отражены по сравнению с предыдущей настройкой.

```
set vpn ipsec site-to-site peer 45.32.144.83 local-address 195.209.51.5
set vpn ipsec site-to-site peer 45.32.144.83 authentication mode pre-shared-secret
set vpn ipsec site-to-site peer 45.32.144.83 authentication pre-shared-secret MyS3cR3T
set vpn ipsec site-to-site peer 45.32.144.83 connection-type initiate
set vpn ipsec site-to-site peer 45.32.144.83 default-esp-group DevServerESP
set vpn ipsec site-to-site peer 45.32.144.83 ike-group DevServerESP
set vpn ipsec site-to-site peer 45.32.144.83 tunnel 0 local prefix 10.0.5.0/24
set vpn ipsec site-to-site peer 45.32.144.83 tunnel 0 remote prefix 10.0.1.0/24
```

Шаг 5. Настройка политики маршрутизации

VyOS поддерживает политику маршрутизации (*Policy Routing*), позволяя назначать трафик другой таблице маршрутизации. Трафик можно сопоставить с использованием стандартного соответствия (*адрес источника, адрес назначения, протокол, порт источника, порт назначения*).

MSS Clamping обычно используется для трафика на основе **IPSec**, чтобы гарантировать, что трафик не превышает **MTU** пути, из-за дополнительных накладных расходов, которые представляет **IPSec**.

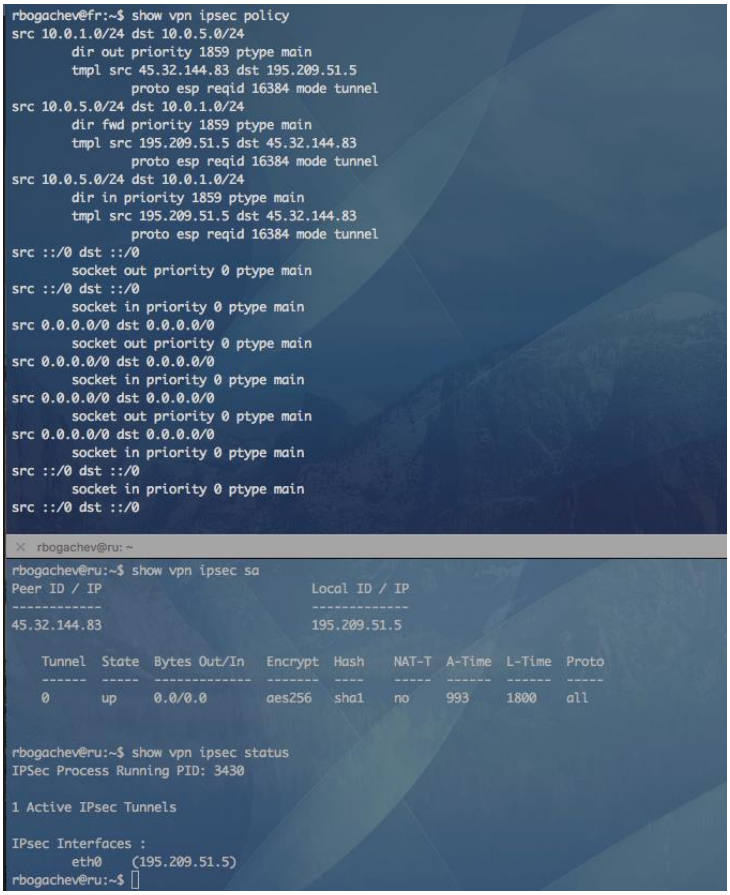
Выполняем настройку удаленного устройства (*FR.SW.DEVSERVERS.NETWORK*)

```
set policy route TCP-MSS1386-ETH0 rule 1 destination address 10.0.5.0/24
set policy route TCP-MSS1386-ETH0 rule 1 protocol tcp
set policy route TCP-MSS1386-ETH0 rule 1 set tcp-mss 1386
set policy route TCP-MSS1386-ETH0 rule 1 tcp flags SYN
set interfaces ethernet eth0 policy route TCP-MSS1386-ETH0
```

Выполняем настройку локального устройства (*RU.SW.DEVSERVERS.NETWORK*)

```
set policy route TCP-MSS1386-ETH0 rule 1 destination address 10.0.1.0/24
set policy route TCP-MSS1386-ETH0 rule 1 protocol tcp
set policy route TCP-MSS1386-ETH0 rule 1 set tcp-mss 1386
set policy route TCP-MSS1386-ETH0 rule 1 tcp flags SYN
set interfaces ethernet eth0 policy route TCP-MSS1386-ETH0
```

Подтверждаем все внесенные изменения commit и сохраняем настройки save.
И проверяем статус настроенного туннеля.



Шаг 6. Настройка VPN для клиентов

Подробная инструкция с видеоуроком по настройке L2TP/IPSec доступна на моём блоге.

Выполняем настройку VPN на удаленном устройстве (*FR.SW.DEVSERVERS.NETWORK*)

set vpn ipsec nat-traversal enable
set vpn ipsec nat-networks allowed-network 0.0.0.0/0
set vpn l2tp remote-access outside-address 45.32.144.83
set vpn l2tp remote-access client-ip-pool start 10.0.1.100
set vpn l2tp remote-access client-ip-pool stop 10.0.1.150
set vpn l2tp remote-access ipsec-settings authentication mode pre-shared-secret
set vpn l2tp remote-access ipsec-settings authentication pre-shared-secret MySecretPSKkey
set vpn l2tp remote-access authentication mode local
set vpn l2tp remote-access authentication local-users username TestUser password MyCryptPass
set vpn l2tp remote-access dns-servers server-1 8.8.8.8

Подтверждаем внесенные изменения commit и сохраняем настройки save

Troubleshooting

Сеть 10.0.5.0/24 без доступа в интернет

Для того, чтобы дать доступ в интернет для устройств из сети 10.0.5.0/24 необходимо немного изменить конфигурацию VPN-туннеля.

Выполняем настройку удаленного устройства (*FR.SW.DEVSERVERS.NETWORK*)

set nat source rule 5 outbound-interface eth0
set nat source rule 5 source address 10.0.5.0/24
set nat source rule 5 translation address masquerade

Выполняем настройку удаленного устройства (*FR.SW.DEVSERVERS.NETWORK*)

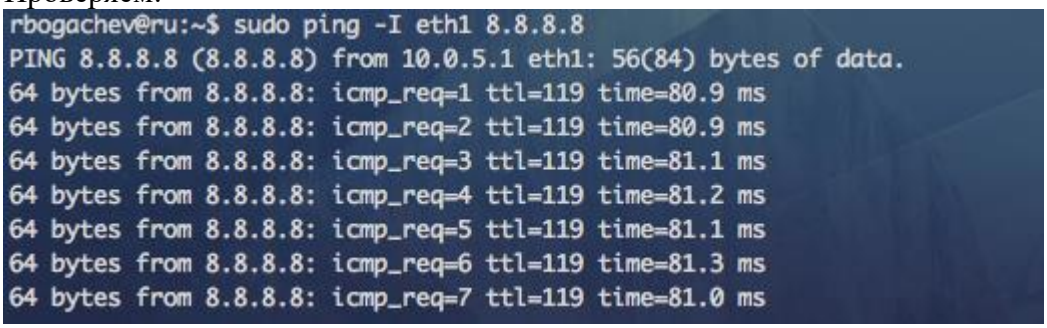
set vpn ipsec site-to-site peer 195.209.51.5 tunnel 0 local prefix 0.0.0.0/0
set vpn ipsec site-to-site peer 195.209.51.5 tunnel 0 remote prefix 10.0.5.0/24

Выполняем настройку локального устройства (*RU.SW.DEVSERVERS.NETWORK*)

set vpn ipsec site-to-site peer 45.32.144.83 tunnel 0 local prefix 10.0.5.0/24

set vpn ipsec site-to-site peer 45.32.144.83 tunnel 0 remote prefix 0.0.0.0/0

Проверяем:



$ monitor interfaces ethernet eth0 traffic filter "host 8.8.8.8"
Capturing traffic on eth0 ...

0.000000	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
1.001370	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
2.002658	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
3.004103	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
4.005408	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
5.006465	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
6.007675	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply
7.009037	8.8.8.8 -> 10.0.5.1	ICMP Echo (ping) reply

Практическая работа № 10
Автоматическое шифрование логических дисков ПК.

Задание

1. Применить технологию BitLocker к локальному диску с пошаговым описанием всех действий. Указать в отчете заданный пароль.
2. Применить технологию BitLocker To Go к Flash – диску с пошаговым описанием всех действий. Указать в отчете заданный пароль.
3. Дать сравнительную характеристику шифрования жесткого и съемного дисков.

Практическая работа № 11
Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки

Задание:

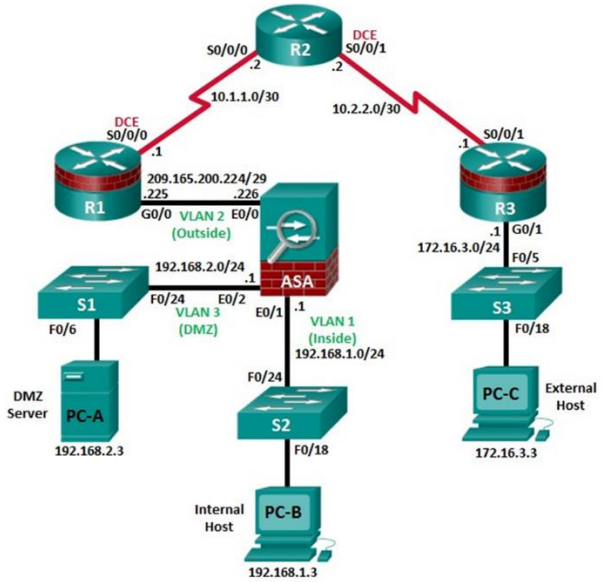


Таблица IP-адресов

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/0	209.165.200.225	255.255.255.248	Н/П	ASA E0/0
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П	S2 F0/24
	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П	R1 G0/0
	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П	S1 F0/24
PC-A	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S1 F0/6
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1	S3 F0/18

- Подключите сетевые кабели и сбросьте предыдущие настройки на устройствах.
- Сконфигурируйте основные параметры для маршрутизаторов и коммутаторов.
- Настройте статическую маршрутизацию, включая маршруты по умолчанию, между маршрутизаторами R1, R2 и R3.
- Включите HTTP-сервер на маршрутизаторе R1, настройте пароли привилегированного доступа и пароли VTY.
- Сконфигурируйте параметры IP для хоста.
- Проверьте связь.

Порядок выполнения:

Шаг 1: Подключение сетевых кабелей и сброс предыдущих настроек на устройствах.

Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.

Шаг 2: Конфигурирование основных параметров для маршрутизаторов и коммутаторов.

a. Задайте имена хостов для каждого маршрутизатора, как показано на топологической схеме.

b. Настройте IP-адреса интерфейсов маршрутизаторов, как показано в таблице IP-адресов.

c. Настройте тактовую частоту маршрутизаторов с помощью последовательного кабеля DCE, подключенного к последовательному интерфейсу. В качестве примера показан маршрутизатор R1.

R1(config)# **interface S0/0/0**
R1(config-if)# **clock rate 64000**

d. Настройте имена хостов для коммутаторов. Остальные параметры коммутаторов можно оставить по умолчанию. IP-адрес для управления сетью VLAN для коммутаторов задавать необязательно.

Шаг 3: Настройка статической маршрутизации на маршрутизаторах.

a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из R3 в R2.

R1(config)# **ip route 0.0.0.0 0.0.0.0 10.1.1.2**

R3(config)# **ip route 0.0.0.0 0.0.0.0 10.2.2.2**

b. Настройте статический маршрут из маршрутизатора R2 к подсети Fa0/0 на R1 (подключенной к интерфейсу ASA E0/0) и статический маршрут из маршрутизатора R2 к LAN R3.

R2(config)# **ip route 209.165.200.224 255.255.255.248 10.1.1.1**
R2(config)# **ip route 172.16.3.0 255.255.255.0 10.2.2.1**

Шаг 4: Конфигурирование и шифрование паролей на маршрутизаторе R1.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, а сами пароли были упрощены для облегчения выполнения лабораторной работы. В производственной сети рекомендуется использовать более сложные пароли.

a. Задайте минимальную длину пароля. Используйте команду **security passwords**, чтобы задать минимальную длину пароля в 10 символов.

b. Установите на обоих маршрутизаторах пароль привилегированного доступа **cisco12345**. Используйте алгоритм хеширования type 9 (SCRYPT).

c. Создайте локальную учетную запись **admin01,** установите для нее пароль **admin01pass.** Используйте алгоритм хеширования type 9 (SCRYPT) и установите уровень привилегий 15.

d. Настройте линии консоли и VTY на использование локальной базы данных для входа. В целях дополнительной безопасности настройте эти линии на выход из системы через 5 минут при отсутствии активности. Используйте команду **logging synchronous** для предотвращения прерывания ввода команд сообщениями консоли.

e. Включите доступ к HTTP-серверу на маршрутизаторе R1. Используйте локальную базу данных для аутентификации HTTP.

Примечание. Доступ к серверу HTTP будет использован для демонстрации инструментов ASDM в части 3.

Шаг 5: Конфигурирование параметров IP для хостов.

Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A, PC-B и PC-C, как показано в таблице IP-адресов.

Шаг 6: Проверка связи.

Между устройствами, подключенными к ASA, не будет связи, так как ASA является центральным узлом для сетевых зон и оно не было сконфигурировано. Однако у компьютера PC-C должна быть возможность отправить эхо-запрос на интерфейс G0/0 маршрутизатора R1. С компьютера PC-C отправьте эхо-запрос на IP-адрес интерфейса G0/0 маршрутизатора R1 (**209.165.200.225**). Если запросы завершаются с ошибкой, измените значения основных параметров устройства перед тем, как продолжить работу.

Примечание. Если эхо-запросы с компьютера PC-C на интерфейсы G0/0 и S0/0/0 маршрутизатора R1 выполнены успешно, это означает, что адресация настроена верно и статическая маршрутизация настроена и работает исправно.

Шаг 7: Сохранение основной текущей конфигурации для каждого маршрутизатора и коммутатора.

Практическая работа № 12
Создание правил Modular Policy Framework (MPF) в шлюзе безопасности ASA

Всего существует несколько способов блокировки страниц в интернете:

- Регулярные выражения с **MPF** (Modular Policy Framework);
- Блокировка по сетевому адресу с помощью листов контроля доступа (**ACL**);
- Используя **FQDN** (Fully Qualified Domain Name) в листе контроля доступа (ACL);

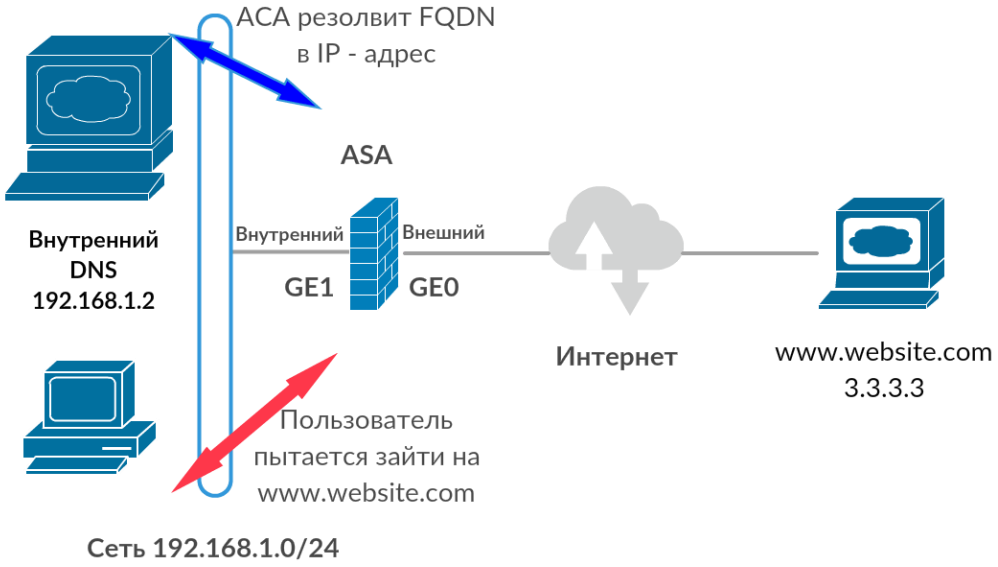
Первый метод работает довольно хорошо с HTTP сайтами, но он не будет работать от слова совсем с **HTTPS** сайтами. Второй метод будет работать только для простых сайтов, у которых статический IP – адрес, то есть будет очень трудоемко настроить его для работы с такими сайтами как Facebook, VK, Twitter и т.д.

ОПИСАНИЕ НАСТРОЙКИ

При использовании версии ПО выше или равной 8.4(2), появилась возможность добавлять в ACL такие объекты как FQDN (полные доменные имена). Таким образом, вы можете разрешить или запретить доступ к хостам используя их доменные имена вместо IP – адресов. То есть можно будет запретить доступ к Фейсбуку просто запретив доступ к FQDN объекту «www.facebook.com» внутри ACL.

Важное преимущество данного метода состоит в том, что это не скажется на производительности вашего МСЭ – т.к DNS лукап будет совершен до этого и все ассоциированные с этим FQDN будут храниться в памяти устройства. В зависимости от TTL на DNS лукапе, МСЭ может продолжать совершать DNS запросы для определенного доменного имени (каждые несколько часов, к примеру) и обновлять IP – адреса в памяти.

На примере сети ниже, мы хотим заблокировать доступ к www.website.com, который имеет IP-адрес 3.3.3.3. Наша ASA будет использовать внутренний DNS — сервер (или любой другой DNS – сервер) для получения адреса и запрета доступа к нему во входящем ACL на внутреннем интерфейсе.



КОМАНДЫ

Теперь настало время написать сам конфиг (точнее только его часть, которая касается блокировки страниц). Он указан ниже, с комментариями:

domain-name xakinfo.ru
interface GigabitEthernet0
nameif outside
security-level 0
ip address 1.2.3.0 255.255.255.0
interface GigabitEthernet1
nameif inside
security-level 100
ip address 192.168.1.1
!другие команды настройки интерфейса скрыты
!Указываем, какой DNS сервер использовать для определения IP – адресов
dns domain-lookup inside
dns server-group DefaultDNS
name-server 192.168.1.2
domain-name mycompany.com
!Созда-
ем FQDN объекты для тех сайтов, которые хотим заблокировать. Указываем как с www т ак и без
object network obj-www.website.com
fqdn www.website.com
object network obj-website.com
fqdn website.com
!Добавляем FQDN объекты во входящий ACL на внутреннем интерфейсе
access-list INSIDE-IN extended deny ip any object obj-www.website.com
access-list INSIDE-IN extended deny ip any object obj-website.com
access-list INSIDE-IN extended permit ip any any
!Применяем ACL выше для внутреннего интерфейса
access-group INSIDE-IN in interface inside

Практическая работа № 13
Настройка безопасности на втором уровне на коммутаторах

Задание:

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/1	172.16.99.1	255.255.255.0	N/A
S1	VLAN 99	172.16.99.11	255.255.255.0	172.16.99.1
PC-A	NIC	172.16.99.3	255.255.255.0	172.16.99.1

Задачи
Часть 1. Настройка топологии и установка исходного состояния устройства
Часть 2. Настройка базовых параметров устройств и проверка подключения Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1
Настройте доступ по протоколу SSH.
Измените параметры SSH.
Проверьте конфигурацию SSH.
Часть 4. Настройка и проверка параметров безопасности для S1
Настройте и проверьте общие функции безопасности.
Настройте и проверьте функцию безопасности порта.
Исходные данные/Сценарий
На компьютерах и серверах следует ограничивать доступ, устанавливая качественную систему безопасности. На ваших устройствах сетевой инфраструктуры, например коммутаторах и маршрутизаторах, тоже важно настраивать функции безопасности.
В ходе данной лабораторной работе вам нужно настроить функции безопасности на коммутаторах LAN в соответствии с практическими рекомендациями. Вам следует разрешить только сеансы протокола SSH и безопасного протокола HTTPS. Кроме того, вам предстоит настроить и проверить работу функции безопасности порта, направленную на блокировку любого устройства с MAC-адресом, который неизвестен коммутатору.
Примечание. В лабораторных работах CCNA используются маршрутизаторы с интегрированными службами серии Cisco 1941 под управлением Cisco IOS 15.2(4) M3 (образ universalk9). В лабораторных работах используется коммутатор Cisco Catalyst 2960 под управлением ОС Cisco IOS 15.0(2) (образ lanbasek9). Допускается использование коммутаторов и маршрутизаторов других моделей, под

управлением других версий ОС Cisco IOS. В зависимости от модели устройства и версии Cisco IOS доступные команды и выходные данные могут отличаться от данных, полученных при выполнении лабораторных работ. Точные идентификаторы интерфейса указаны в таблице сводной информации об интерфейсах маршрутизаторов в конце лабораторной работы.
Примечание. Убедитесь, что информация из маршрутизаторов и коммутаторов удалена, и они не содержат файлов загрузочной конфигурации. Если вы не уверены, обратитесь к пре-

подавателю или вернитесь к процедурам инициализации и перезагрузки устройств, описанных в предыдущей лабораторной работе.
Необходимые ресурсы:
1 маршрутизатор (Cisco 1941 с универсальным образом M3 под управлением ОС Cisco IOS 15.2(4) или аналогичная модель);
1 коммутатор (Cisco 2960 под управлением ОС Cisco IOS 15.0(2), образ lanbasek9 или аналогичная модель);
1 ПК (под управлением Windows 7, Vista или XP с программой эмуляции терминала, например Tera Term);
консольные кабели для настройки устройств Cisco IOS через консольные порты;
кабели Ethernet, расположенные в соответствии с топологией.
Часть 1. Настройка топологии и инициализация устройств
В первой части вам предстоит создать топологию сети и при необходимости удалить все конфигурации.
Шаг 1: Подключите кабели в сети в соответствии с топологией.
Шаг 2: Выполните инициализацию и перезагрузку маршрутизатора и коммутатора.
Если ранее на маршрутизаторе или коммутаторе были сохранены конфигурационные файлы, выполните инициализацию и перезагрузку устройств, чтобы восстановить базовые настройки.
Часть 2. Настройка базовых параметров устройств и проверка подключения
Во второй части лабораторной работы вам предстоит настроить базовые параметры маршрутизатора, коммутатора и ПК. Имена и адреса устройств можно найти в топологии и таблице адресации в начале этой лабораторной работы.
Шаг 1: Настройте IP-адрес на PC-A.
Шаг 2: Настройте базовые параметры на маршрутизаторе R1.
Задайте имя устройства.
Отключите поиск DNS.
Настройте IP-адрес интерфейса в соответствии с таблицей адресации.
Назначьте class в качестве пароля привилегированного режима EXEC.
Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.
Зашифруйте все незашифрованные пароли.
Сохраните текущую конфигурацию в загрузочную конфигурацию.
Шаг 3: Выполните базовую настройку коммутатора S1.
Не рекомендуется назначать административный IP-адрес коммутатора для сети VLAN 1 (или любой другой VLAN с конечными пользователями). На данном этапе вам предстоит создать VLAN 99 на коммутаторе и назначить этой сети IP-адрес.
Задайте имя устройства.
Отключите поиск DNS.
Назначьте class в качестве пароля привилегированного режима EXEC.
Назначьте cisco в качестве пароля консоли и виртуального терминала VTY и активируйте вход.
Настройте шлюз по умолчанию для коммутатора S1 с помощью IP-адреса маршрутизатора R1.
Зашифруйте все незашифрованные пароли.
Сохраните текущую конфигурацию в загрузочную конфигурацию.
Создайте на коммутаторе сеть VLAN 99 и назовите её Management.
S1(config)# vlan 99 S1(config-vlan)# name Management S1(config-vlan)# exit S1(config)#
i. Настройте IP-адрес интерфейса административной сети VLAN 99 в соответствии с таблицей адресации и включите интерфейс.
S1(config)# interface vlan 99
S1(config-if)# ip address 172.16.99.11 255.255.255.0

S1(config-if)# no shutdown S1(config-if)# end S1#
Выполните команду show vlan на коммутаторе S1. В каком состоянии находится сеть VLAN 99?
Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол?
Почему протокол выключен несмотря на то, что вы выполнили команду no shutdown для интерфейса VLAN 99?
Назначьте порты F0/5 и F0/6 для сети VLAN 99 на коммутаторе.
S1# config t
S1(config)# interface f0/5
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# interface f0/6
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 99
S1(config-if)# end
m. Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии интерфейс VLAN 99 и протокол? _____
Примечание. При сходимости состояний портов может произойти небольшая задержка.
Шаг 4: Проверьте наличие подключения между всеми устройствами.
От компьютера PC-A отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1.
Успешно ли выполнены эхо-запросы? _____
От компьютера PC-A отправьте эхо-запрос на адрес управления коммутатора S1. Успешно ли выполнены эхо-запросы? _____
От коммутатора S1 отправьте эхо-запрос на шлюз по умолчанию маршрутизатора R1.
Успешно ли выполнены эхо-запросы? _____
В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Если появится запрос на ввод имени пользователя пароля, оставьте имя пользователя пустым, а в качестве пароля введите class. Если появится запрос о защищённом подключении, ответьте No.
Удалось ли вам получить доступ к веб-интерфейсу на коммутаторе S1?
Закройте сеанс браузера на компьютере PC-A.
Примечание. Незащищённый веб-интерфейс (сервер HTTP) коммутатора Cisco 2960 включён по умолчанию. Для обеспечения безопасности рекомендуется отключить данную службу, как описано в части 4.
Часть 3. Настройка и проверка доступа с помощью протокола SSH к коммутатору S1
Шаг 1: Настройте доступ к протоколу SSH на коммутаторе S1.
Включите SSH на S1. В режиме глобальной конфигурации создайте имя домена CCNA-Lab.com.
S1(config)# ip domain-name CCNA-Lab.com
Создайте запись локальной базы данных пользователей, которую вы будете использовать для подключения к коммутатору через SSH. Пользователь должен обладать правами доступа администратора.
Примечание. Используемый пароль не является надёжным. Он используется исключительно в рамках лабораторной работы.
S1(config)# username admin privilege 15 secret sshadmin
Настройте вход транспортировки таким образом, чтобы в каналах VTY были разрешены только подключения по протоколу SSH. Для аутентификации используйте локальную базу данных.
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
S1(config-line)# login local S1(config-line)# exit
d. Создайте ключ шифрования RSA с использованием модуля 1024 бит.

S1(config)# crypto key generate rsa modulus 1024
The name for the keys will be: S1.CCNA-Lab.com

% The key modulus size is 1024 bits % Generating 1024 bit RSA keys, keys will be non-exportable... [OK] (elapsed time was 3 seconds)
e. Проверьте конфигурацию протокола SSH и ответьте на следующие вопросы.
S1# show ip ssh
Какую версию SSH использует коммутатор? _____
Сколько попыток аутентификации разрешает SSH? _____
На какое значение настроен лимит времени по умолчанию для SSH? _____
Шаг 2: Измените конфигурацию SSH на коммутаторе S1.
Измените конфигурацию SSH по умолчанию.
S1# config t
S1(config)# ip ssh time-out 75
S1(config)# ip ssh authentication-retries 2
Сколько попыток аутентификации разрешает SSH? _____
На какое значение настроен лимит времени для протокола SSH? _____
Шаг 3: Проверьте конфигурацию SSH на коммутаторе S1.
С помощью клиентского программного обеспечения SSH на компьютере PC-A (например Tera Term), настройте SSH-подключение к коммутатору S1. Если в вашей клиентской программе SSH появилось сообщение о ключе узла, примите его. Войдите в систему, используя admin в качестве имени пользователя, и cisco в качестве пароля.
Удалось ли настроить связь? _____ Какой запрос был отображён на коммутаторе S1? Почему?
Чтобы завершить сеанс SSH на коммутаторе S1, введите exit.
Часть 4. Настройка и проверка параметров безопасности для S1
В четвёртой части лабораторной работы вам предстоит закрыть неиспользуемые порты, выключить определённые сервисы, работающие на коммутаторе, и настроить функцию безопасности порта на основе MAC-адресов. Коммутаторы могут быть подвержены переполнению таблицы MAC-адресов, спуфинг-атакам и попыткам неавторизованных подключений к портам коммутатора. Вам нужно будет настроить функцию порта безопасности, чтобы ограничить количество MAC-адресов, которые могут быть получены портом коммутатора, а также отключить порт при превышении этого количества.
Шаг 1: Настройка общих функций безопасности на коммутаторе S1.
Настройте баннер MOTD (сообщение дня) для коммутатора S1 в виде соответствующего предупреждения.
Выполните команду show ip interface brief на коммутаторе S1. Какие физические порты включены?
Выключите все неиспользуемые физические порты коммутатора. Используйте команду interface range.
S1(config)# interface range f0/1 – 4
S1(config-if-range)# shutdown
S1(config-if-range)# interface range f0/7 – 24
S1(config-if-range)# shutdown
S1(config-if-range)# interface range g0/1 – 2
S1(config-if-range)# shutdown S1(config-if-range)# end S1#
d. Выполните команду show ip interface brief на коммутаторе S1. В каком состоянии находятся порты от F0/1 до F0/4?
e. Введите команду show ip http server status.
В каком состоянии находится сервер HTTP? _____
Какой порт сервера он использует? _____
В каком состоянии находится защищённый сервер HTTP? _____

Какой порт сервера он использует? _____
Сеансы HTTP отправляют все данные в незашифрованном виде. Вам нужно отключить сервис HTTP, который работает на коммутаторе S1.
S1(config)# no ip http server
В компьютере PC-A откройте веб-браузер и перейдите по адресу http://172.16.99.11. Что у вас получилось?
В компьютере PC-A откройте защищённый сеанс веб-браузера по адресу https://172.16.99.11. Примите сертификат. Войдите в систему без имени пользователя, используйте пароль class. Что у вас получилось?
Закройте сеанс браузера на компьютере PC-A.
Шаг 2: Настройка и проверка работы функции безопасности порта на коммутаторе S1.
a. Запишите MAC-адрес интерфейса G0/1 маршрутизатора R1. В интерфейсе командной строки маршрутизатора R1 выполните команду show interface g0/1 и запишите MAC-адрес интерфейса.
R1# show interface g0/1
Каков MAC-адрес интерфейса G0/1 маршрутизатора R1?
В интерфейсе командной строки S1 выполните команду show mac address-table в привилегированном режиме. Найдите динамические записи для портов F0/5 и F0/6. Запишите их ниже.
MAC-адрес интерфейса F0/5: _____
MAC-адрес интерфейса F0/6: _____
Настройка базовой безопасности порта.
Примечание. Как правило, эту процедуру выполняют на всех портах доступа коммутатора. Интерфейс F0/5 представлен в качестве примера.
1) Из интерфейса командной строки коммутатора S1 войдите в режим конфигурации интерфейса для порта, который подключается к R1.
S1(config)# interface f0/5 2) Выключите порт.
S1(config-if)# shutdown
Включите функцию безопасности порта на интерфейсе F0/5.
S1(config-if)# switchport port-security
Примечание. Выполнение команды switchport port-security позволит установить максимальное количество MAC-адресов на значение 1. При попытке нарушения безопасности порт будет выключен. Команды switchport port-security maximum и switchport port-security violation можно использовать для того, чтобы изменить настройки по умолчанию.
Настройте статическую запись для MAC-адреса интерфейса G0/1 маршрутизатора R1, записанного на шаге 2a.
S1(config-if)# switchport port-security mac-address xxxx.xxxx.xxxx
(Настоящий MAC-адрес интерфейса G0/1 маршрутизатора имеет формат xxxx.xxxx.xxxx).
Примечание. При желании вы можете использовать команду switchport port-security macaddress, чтобы добавить в текущую конфигурацию коммутатора защищённые MAC-адреса, которые были динамически получены на порте (до заданного максимального значения).
Включите порт коммутатора.
S1(config-if)# no shutdown S1(config-if)# end
d. Проверьте функцию безопасности порта на интерфейсе F0/5 коммутатора S1 с помощью команды show port-security interface.
S1# show port-security interface f0/5
Port Security : Enabled
Port Status : Secure-up
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled

Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : 0000.0000.0000:0
Security Violation Count : 0
В каком состоянии находится порт F0/5?
Из командной строки маршрутизатора R1 отправьте эхо-запрос на компьютер PC-A, чтобы проверить подключение.
R1# ping 172.16.99.3
Далее, изменив MAC-адрес интерфейса маршрутизатора, вы нарушите систему безопасности. Войдите в режим конфигурации интерфейса для G0/1 и выключите его.
R1# config t
R1(config)# interface g0/1
R1(config-if)# shutdown
Настройте новый MAC-адрес для интерфейса, используя aaaa.bbbb.cccc в качестве адреса.
R1(config-if)# mac-address aaaa.bbbb.cccc
По возможности, одновременно с этим шагом установите консольное подключение на коммутаторе S1. В консольном подключении к коммутатору S1 вы увидите различные сообщения о нарушении системы безопасности. Включите интерфейс G0/1 маршрутизатора R1.
R1(config-if)# no shutdown
Из привилегированного режима коммутатора R1 отправьте эхо-запрос на компьютер PC-A.
Успешно ли выполнен эхо-запрос? Поясните свой ответ.
На коммутаторе проверьте функцию безопасности порта с помощью команд, указанных ниже.
S1# show port-security
Secure Port MaxSecureAddr CurrentAddr SecurityViolation Security Action
(Count) (Count) (Count)

Fa0/5 1 1 1 Shutdown

Total Addresses in System (excluding one mac per port) :0 Max Addresses limit in System (excluding one mac per port) :8192

S1# show port-security interface f0/5
Port Security : Enabled
Port Status : Secure-shutdown
Violation Mode : Shutdown
Aging Time : 0 mins
Aging Type : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Configured MAC Addresses : 1
Sticky MAC Addresses : 0
Last Source Address:Vlan : aaaa.bbbb.cccc:99
Security Violation Count : 1

S1# show interface f0/5
Hardware is Fast Ethernet, address is 0cd9.96e2.3d05 (bia 0cd9.96e2.3d05) MTU 1500 bytes, BW 10000 Kbit/sec, DLY 1000 usec, reliability 255/255, txload 1/255, rxload 1/255
<output omitted>

S1# show port-security address
Secure Mac Address Table

Vlan Mac Address Type Ports Remaining Age (mins)
---- ---------- ---- ----- -------------
99 30f7.0da3.1821 SecureConfigured Fa0/5 -

Total Addresses in System (excluding one mac per port) :0
Max Addresses limit in System (excluding one mac per port) :8192
k. На маршрутизаторе выключите интерфейс G0/1, удалите жёстко запрограммированный MACадрес из маршрутизатора и повторно включите интерфейс G0/1.
R1(config-if)# shutdown
R1(config-if)# no mac-address aaaa.bbbb.cccc
R1(config-if)# no shutdown R1(config-if)# end
Из маршрутизатора R1 повторите эхо-запрос на компьютер PC-A по адресу 172.16.99.3.
Успешно ли выполнен эхо-запрос? _____
Чтобы определить причину неудачи эхо-запроса, выполните команду show interface f0/5. Запишите полученные результаты.
Очистите состояние выключения порта F0/5 в результате сбоя S1.
S1# config t
S1(config)# interface f0/5
S1(config-if)# shutdown S1(config-if)# no shutdown
Примечание. При сходимости состояний портов может произойти небольшая задержка.
Чтобы убедиться, что порт F0/5 вышел из состояния выключения в результате сбоя, на коммутаторе S1 выполните команду show interface f0/5.
S1# show interface f0/5
Hardware is Fast Ethernet, address is 0023.5d59.9185 (bia 0023.5d59.9185) MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec, reliability 255/255, txload 1/255, rxload 1/255
Из командной строки маршрутизатора R1 повторите эхо-запрос на компьютер PC-A. Эхо-запрос должен пройти успешно.

Практическая работа № 14
Настройка политики безопасности брандмауэров

Задание:

Активизация встроенного межсетевого экрана
1. Откройте компоненту *Брандмауэр Windows.* Для этого выберите последовательно *Пуск —» Панель управления —> Система и безопасность* и выберите соответствующий компонент в списке.
Другой способ поиска данной компоненты осуществляется с помощью последовательного выбора *Пуск —> Панель управления —> Сеть и Интернет —> Центр управления сетями и общим доступом,* в котором в списке *См. также* находится ссылка на компоненту *Брандмауэр Windows* (рис. 6.2).
2. На вкладке *Включение и отключение брандмауэра Windows* в группе *Брандмауэр Windows* (рис. 6.3) выберите параметры размещения сети и включите брандмауэр для нужной сети.
Для выполнения этого действия требуются *права администратора* (см. материал тем 2—5).
Запуск программ или компонентов через брандмауэр Windows

Для того чтобы разрешить, удалить или изменить разрешенные программы и порты, сделаем следующее: на вкладке *Разрешить запуск программы или компонента через брандмауэр Windows* в группе

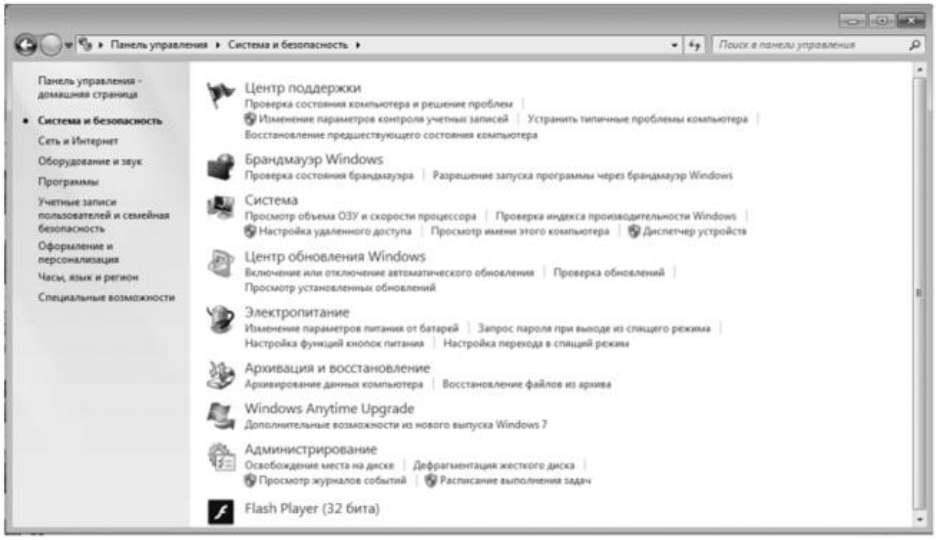


Рис. 6.2. Брандмауэр Windows

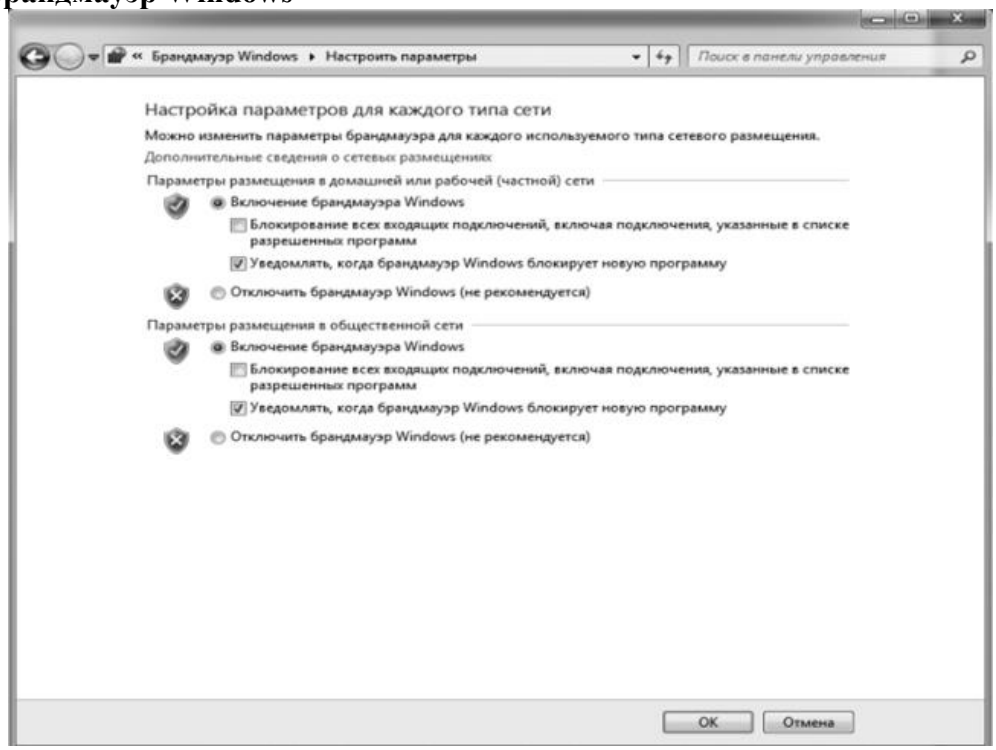
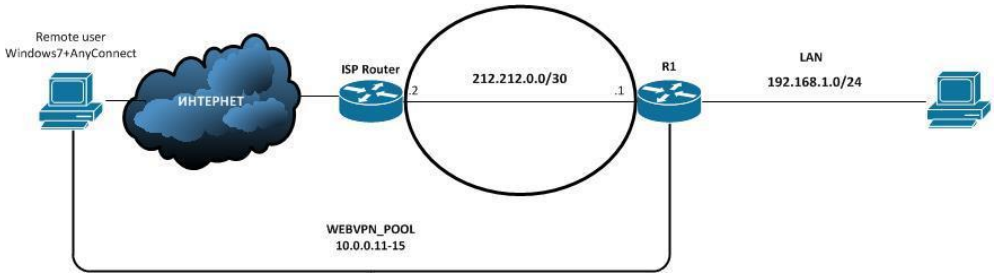


Рис. 6.3. Настройка параметров типов подключения

Брандмауэр Windows (рис. 6.4) выбираем и отмечаем галочками программы, которым мы хотим дать доступ к сети.

Практическая работа № 15
Установка и настройка SSL VPN



Для начала, что такое SSL VPN (или WEBVPN) от Cisco. Это своего рода наследник easy vpn или ipsec vpn, который позволяет по протоколу ssl (443 порт) удаленно подключиться к вашей корпоративной или домашней сети. Кроме простоты настройки и относительно «легкого» конфига, самым большим доводом за использование ssl является то, что он использует практически повсеместно «открытый» 443 порт для подключения, т.е. если бы вы, например, использовали ipsec, то необходимо было бы на межсетевом экране или же на граничном роутере открывать isakmp (500) порты, наверняка разрешить nat-t (4500), и еще вдобавок разрешить трафик esp, тогда как в случае с ssl подключение проходит по 443 порту, который в большинстве своем разрешен для хостов. Кроме этого не надо на стороне клиента производить каких либо настроек, удаленному пользователю достаточно знать всего лишь внешний ip или dns имя роутера, а также логин и пароль для входа (при использовании easyvpn помимо вышеперечисленного нужен pre-share ключ, а также наименование client configuration group).

Задание:

1. Для начала необходимо активировать лицензию на роутере, в нашем случае используется cisco 881 с ios 15.2(4), для ознакомительной активации на 60 дней вводим след. команду в privilege режиме:
license modify priority SSL_VPN high

После чего соглашаемся с лицензионным соглашением.

2. Далее копируем дистрибутив any connect на роутер любым удобным способом(копирование лучше производить в заранее созданную директорию webvpn, так как если просто скопировать в корень flash, то при установке создастся копия файла установки в той же директории, соответственно займет больше места на flash) и устанавливаем его:
mkdir flash:/webvpn
copy tftp: flash:/webvpn/
crypto vpn anyconnect flash:/webvpn/anyconnect-win-4.4.00243-k9.pkg

3. Включаем aaa (необходим, чтобы указать authentication list на нашем Web шлюзе (webvpn gateway)), заводим локальных пользователей (логин и пароль, которые здесь указываем необходимы для подключения к порталу из интернета, по типу внешнийадресроутера) и активируем https сервер:
aaa new-model
aaa authentication login SSL_USERS local
username admin secret **********
ip http secure-server

4. Генерируем RSA ключи, создаем trustpoint и затем генерируем самоподписанный сертификат:
crypto key generate rsa label SSLKEY modulus 1024
crypto pki trustpoint SALAM_TRUSTPOINT

```
 enrollment selfsigned
 serial-number
 subject-name CN=firewallcx-certificate
 revocation-check crl
 rsakeypair SSLKEY
crypto pki enroll SALAM_TRUSTPOINT
```

5. Настраиваем пул адресов, который будет выдаваться клиентам и создаем WebVPN Gateway, для команды ip interface вместо интерфейса можно указать непосредственно ip адрес командой ip address **** port 443:

```
ip local pool WEBVPN_POOL 10.0.0.11 10.0.0.15
webvpn gateway WEBVPN_GW
 ip interface Dialer1 port 443
 ssl trustpoint SALAM_TRUSTPOINT
 inservice
```

6. Далее создаем и привязываем к нашему gateway так называемый webvpn context, в котором указаваем ранее созданный auth list, максимальное кол-во подключаемых пользователей, а также приветствие отображаемое при входе на портал через браузер(команда inservice в этом и предыдущем шаге активирует webvpn gateway и context):

```
webvpn context WEBVPN_CON
 title "Assalyamu alyaikum"
 login-message "Salyam"
 aaa authentication list SSL_USERS
 gateway WEBVPN_GW
 max-users 5
inservice
```

7. Там же в конфигурации webvpn context создаем policy group, в которой задаем наш пул адресов, указываем какой трафик от клиентов будет заворачиваться в туннель (в нашем случае, когда destination у клиентов будут сети 192.168.1.0 /24 или 172.16.1.0/24 в таблице маршрутизации на клиентах появятся соответствующие записи только для этих двух сетей, указывающие на то, что этот трафик будет уходить в шифрованный туннель), команда functions svc-enabled указывает, что удаленный пользователь может подключаться с помощью самостоятельно установленного клиента anyconnect, т.е. не надо заходить через браузер:

```
policy group WEBVPN_POLICY
   functions svc-enabled
   svc address-pool "WEBVPN_POOL" netmask 255.255.255.0
   svc split include 192.168.1.0 255.255.255.0
   svc split include 172.16.1.0 255.255.255.0
default-group-policy WEBVPN_POLICY
```

8. Если у нас на внешнем интерфейсе висит ACL, то необходимо дописать правило:
permit tcp any host «внешний адрес роутера» eq 443

В итоге запускаем на нашем клиенте браузер, вводим внешний адрес нашего роутера 212.212.0.1 и видим приглашение:

Осталось ввести логин пароль и установить соединение, на этом бы все, но есть один нюанс. Если обратиться к нашей схеме, то сеть 192.168.1.0/24, та самая к которой мы подключаемся, находится за NATом, настройка NAT для роутера R1 следующая:
ip nat inside source list NAT_POOL interface Dialer1 overload

где NAT_POOL:
ip access-list extended NAT_POOL
 permit ip 192.168.1.0 0.0.0.255 any

что произойдет если мы будем пинговать сеть 192.168.1.0 с подключившегося по vpn клиента(клиент получил адрес 10.0.0.12)? Пакеты от него зашифрованными будут уходить на R1, тот в свою очередь создает ответ с destination 10.0.0.12 и смотрит в таблицу маршрутизации:
R1#sh ip route 10.0.0.12
Routing entry for 10.0.0.12/32
  Known via "static", distance 0, metric 0
  Routing Descriptor Blocks:
  * directly connected, via Virtual-Access3
      Route metric is 0, traffic share count is 1
R1#sh interfaces virtual-access 3
Virtual-Access3 is up, line protocol is up
  Hardware is Virtual Access interface
  Description: ***Internally created by SSLVPN context WEBVPN_CON***
  Interface is unnumbered. Using address of Dialer1 (212.212.0.1)
  MTU 1406 bytes, BW 100000 Kbit/sec, DLY 100000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation SSL
  SSL vaccess

Т.е. пакеты уходят с интерфейса dialer 1, а согласно вот этой замечательной таблице порядка операций над трафиком

Inside-to-Outside	Outside-to-Inside
• If IPSec then check input access list • decryption - for CET (Cisco Encryption Technology) or IPSec • check input access list • check input rate limits • input accounting • redirect to web cache • policy routing • routing • **NAT inside to outside (local to global translation)** • crypto (check map and mark for encryption) • check output access list • inspect (Context-based Access Control (CBAC)) • TCP intercept • encryption • Queueing	• If IPSec then check input access list • decryption - for CET or IPSec • check input access list • check input rate limits • input accounting • redirect to web cache • **NAT outside to inside (global to local translation)** • policy routing • routing • crypto (check map and mark for encryption) • check output access list • inspect CBAC • TCP intercept • encryption • Queueing

после routing у нас идет NAT, а наше правило nat говорит нам, что наш source заменится на публичный адрес и в таком виде уйдет на клиента, который понятия не имеет о нашем внешнем адресе, следовательно пинг не пройдет и ничего работать не будет, исправляем добавлением следующей команды в acl NAT_POOL:
ip access-list extended NAT_POOL
 1 deny ip 192.168.1.0 0.0.0.255 10.0.0.0 0.0.0.255

Практическая работа № 16
Установка и настройка IPSec VPN

Задание:

Конфигурация для Router A
Создаем политику безопасности и настраиваем ее
RouterA(config)#crypto isakmp policy 1
Указываем метод шифрования (симметричный блочный шифр)
RouterA(config)#encryption 3des
Указываем метод хеширования MD5
RouterA(config)#hash md5
Указываем метод аутентификации (с предварительным ключом)
RouterA(config)#authentication pre-share
Выходим из режима редактирования политики безопасности
RouterA(config)#exit
Ключ для аутентификации (должен совпадать для обеих точек)
RouterA(config)#crypto isakmp key PASS address 33.33.33.33
Применение набора преобразований
RouterA(config)#crypto ipsec transform-set LAN1 esp-3des esp-md5-hmac
Указываем режим работы IPSec (туннельный режим)
RouterA(cfg-crypto-trans)#mode tunnel

RouterA(cfg-crypto-trans)#exit
Создаем крипто-карту (детали туннелирования)
RouterA(config)#crypto map MAP1 10 ipsec-isakmp
Указываем Ip-адрес маршрутизатора, с которым устанавливаем VPN
RouterA(config-crypto-map)#set peer 33.33.33.33
Указываем набор политик безопасности
RouterA(config-crypto-map)#set transform-set LAN1
Шифровать данные, которые будут проходить через список доступа под номером 100
RouterA(config-crypto-map)#match address 100
Выходим из режима настройки крипто-карты
RouterA(config-crypto-map)#exit
GRE-трафик с хоста 11.11.11.11 на хост 33.33.33.33 подлежит шифрованию
RouterA(config)#access-list 100 permit gre host 11.11.11.11 host 33.33.33.33
Переходим в режим настройки внешнего интерфейса
RouterA(config)#interface fa 0/1
Привязка карты шифрования MAP1 к внешнему интерфейсу
RouterA(config-if)#crypto map MAP1
Аналогично настраивается Router B:
RouterB(config)#crypto isakmp policy 1
RouterB(config)#encryption 3des
RouterB(config)#hash md5
RouterB(config)#authentication pre-share
RouterB(config)#exit
RouterB(config)#crypto isakmp key PASS address 11.11.11.11
RouterB(config)#crypto ipsec transform-set LAN2 esp-3des esp-md5-hmac
RouterB(cfg-crypto-trans)#mode tunnel
RouterB(cfg-crypto-trans)#exit
RouterB(config)#crypto map MAP2 10 ipsec-isakmp
RouterB(config-crypto-map)#set peer 11.11.11.11
RouterB(config-crypto-map)#set transform-set LAN2
RouterB(config-crypto-map)#match address 100
RouterB(config-crypto-map)#exit
RouterB(config)#access-list 100 permit gre host 33.33.33.33 host 11.11.11.11
RouterB(config)#interface fa 0/1
RouterB(config-if)#crypto map MAP2

Практическая работа № 17
Обеспечение информационной безопасности

Настроить полный доступ к внутренним корпоративным ресурсам используя **SSL VPN (using Cisco AnyConnect Client) на cisco ASA**

Задание:

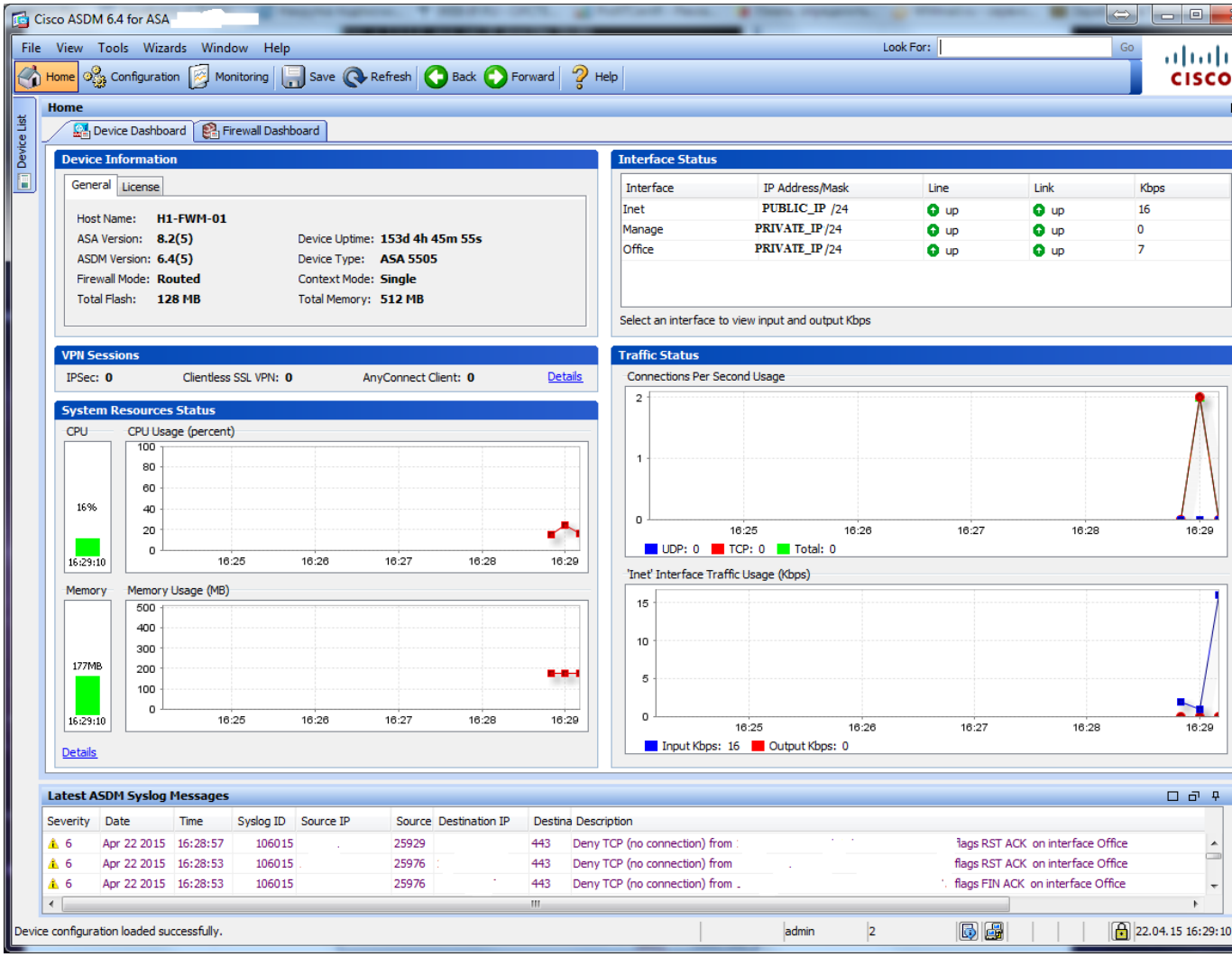
Удаленный клиент при подключении через браузер непосредственно к cisco, скачивает специальное клиентское приложение Cisco AnyConnect Client на свой компьютер.

Будем рассматривать настройку SSL VPN параллельно 2-мя способами через графический интерфейс Cisco ASDM и через консоль CLI.

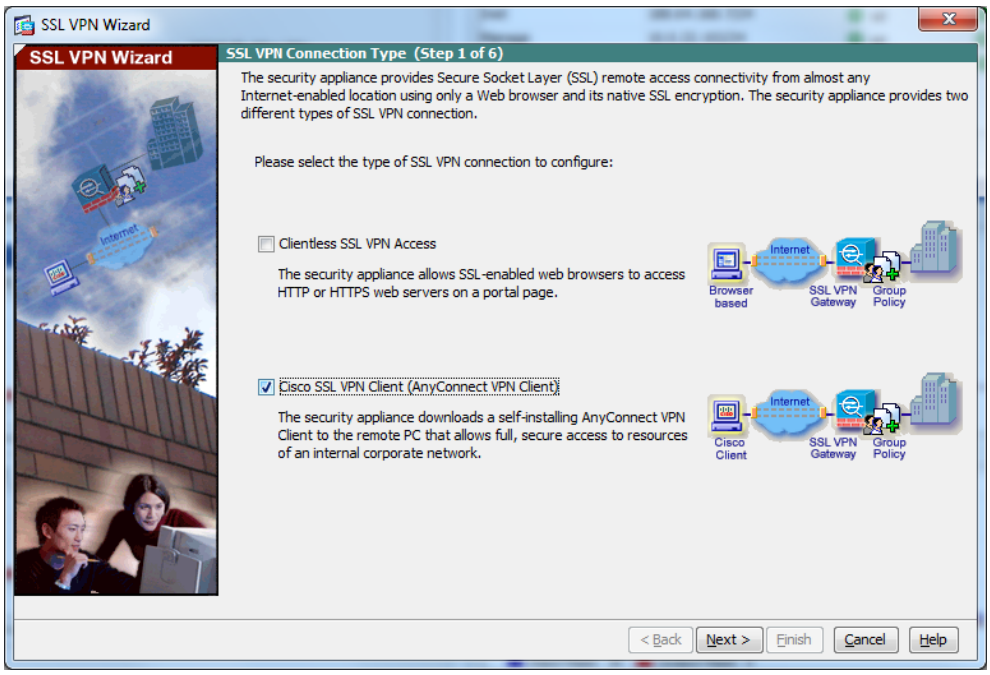
Используемое оборудование Cisco ASA-5505 (Security Appliance Software Version 9.1(6)6)

Настройка с помощью ASDM

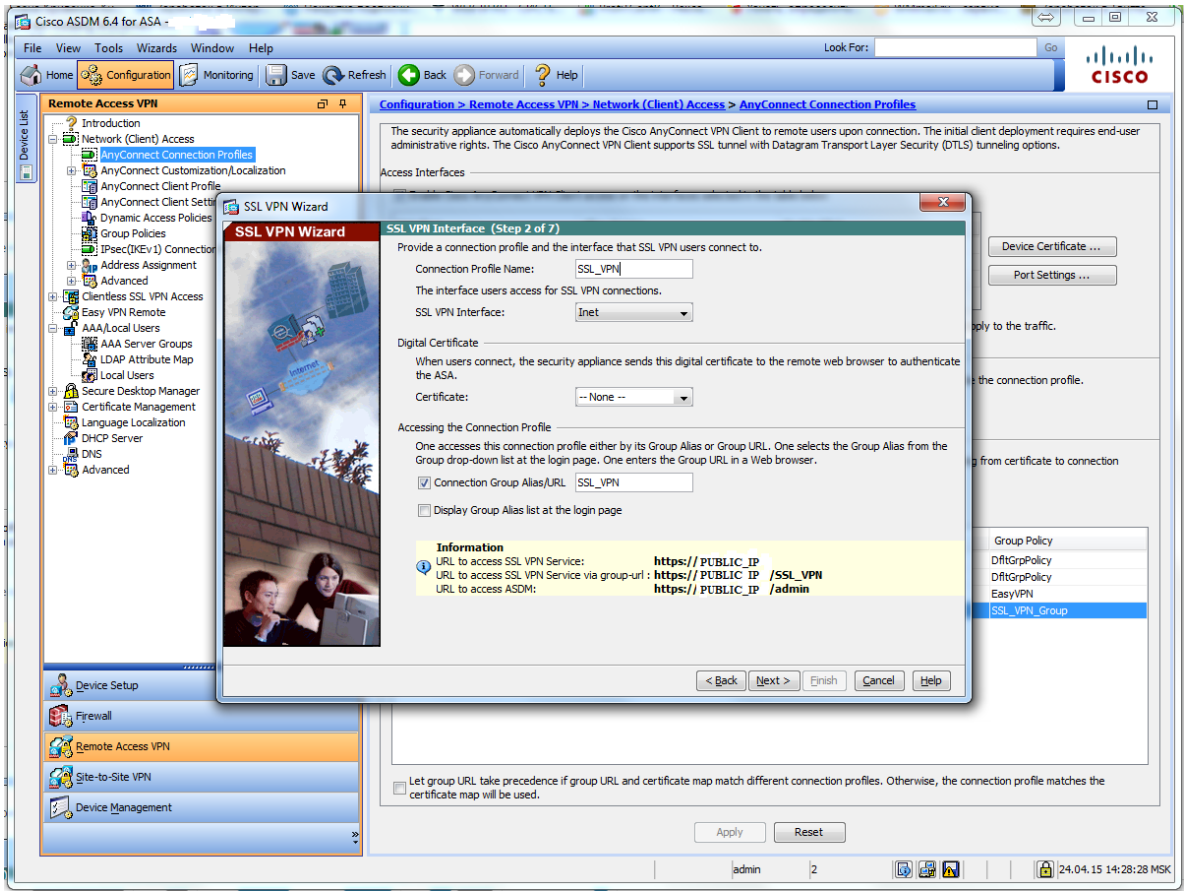
Запускаем Cisco ASDM, откроется основной экран



Здесь выбираем «Wizard»---«SSL VPN Wizard».



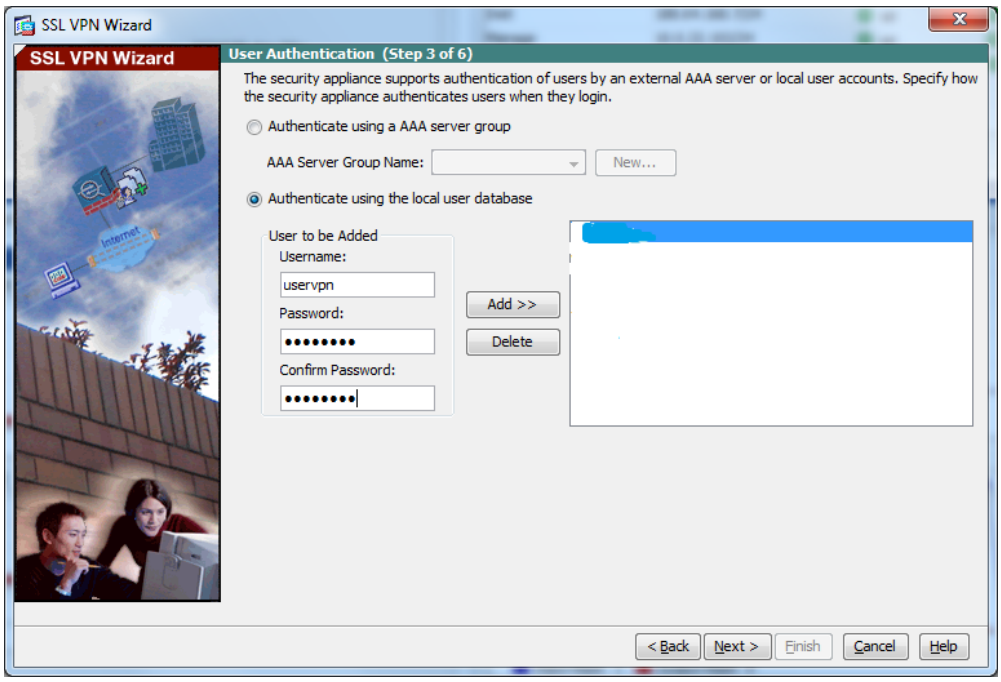
В открывшемся окне выбираем пункт «Cisco SSL VPN Client (AnyConnect VPN Client)» и нажимаем «Next»:



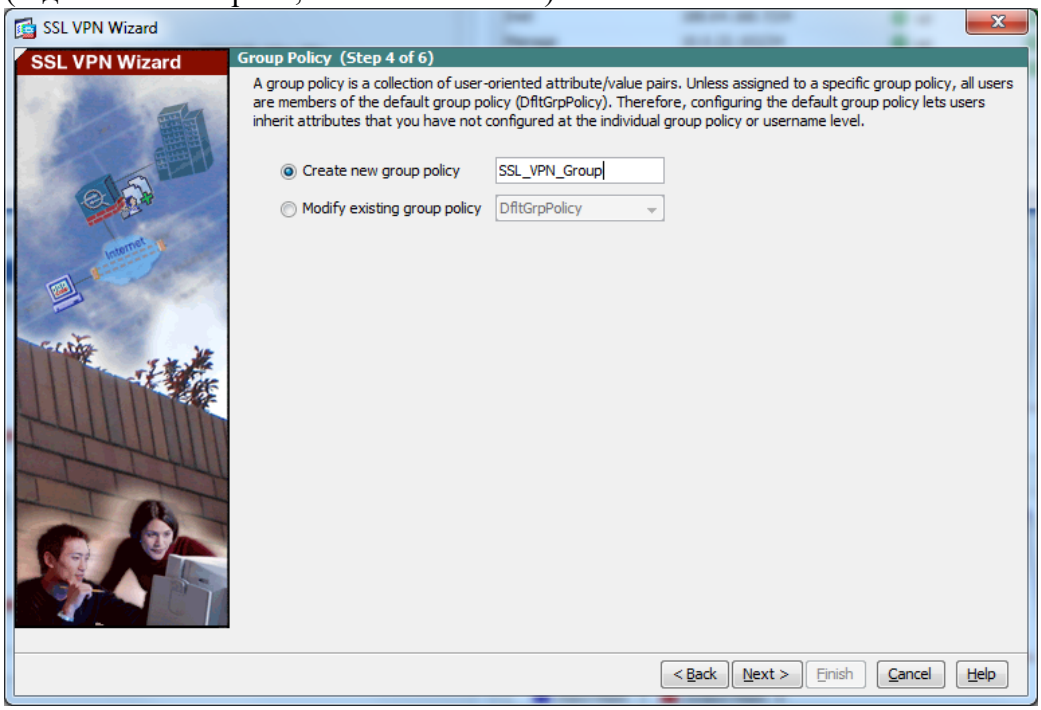
Здесь вводим имя нашего профайла, проверяем, что стоит имя нашего внешнего интерфейса (в данном случае Inet).

Если на cisco настроено несколько vpn подключений, то также указываем имя алиаса. Запоминаем доступы к SSL VPN Service и ASDM.

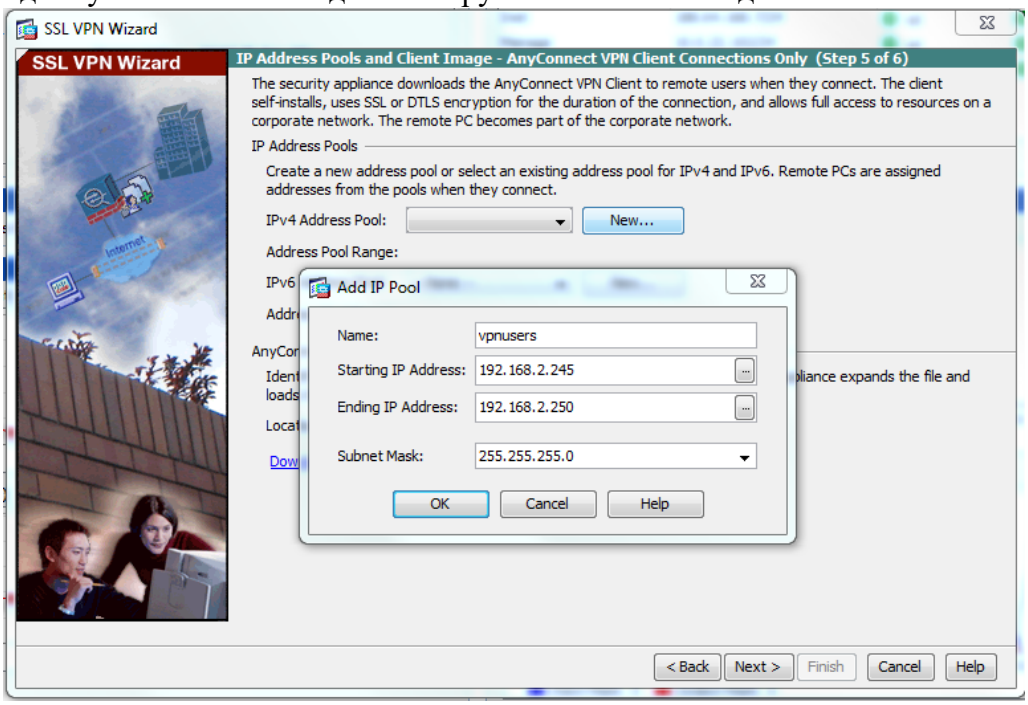
Затем нажимаем «Next»:



Ставим аутентификацию с использованием локальной базы и создаем нового пользователя (задаем имя и пароль, нажимаем «Add»). Затем нажимаем «Next»:

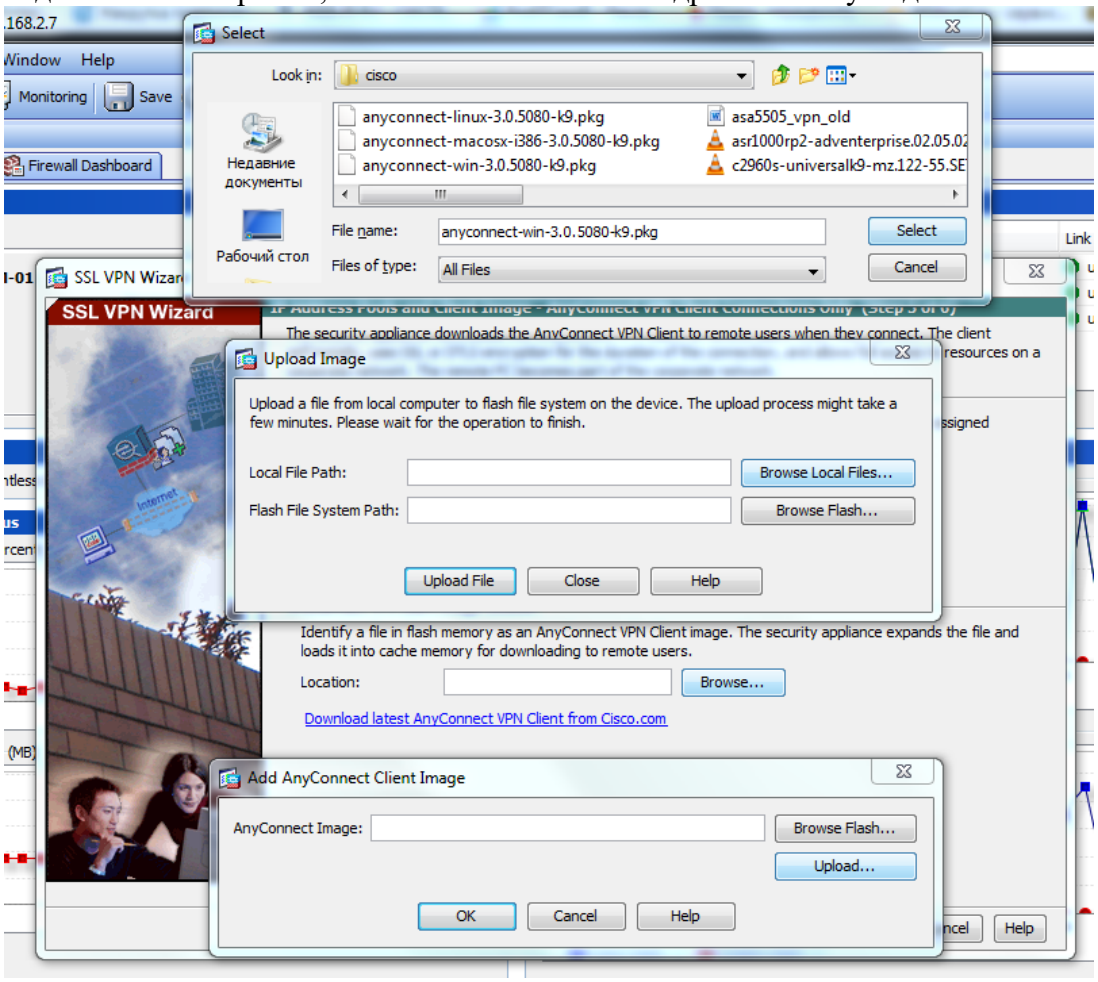


Здесь указываем имя отдельной групповой политики для SSL клиентов и нажимаем «Next»:



Здесь сначала создаем пул ip адресов, из которого будут выдаваться ip адреса для SSL VPN клиентов.

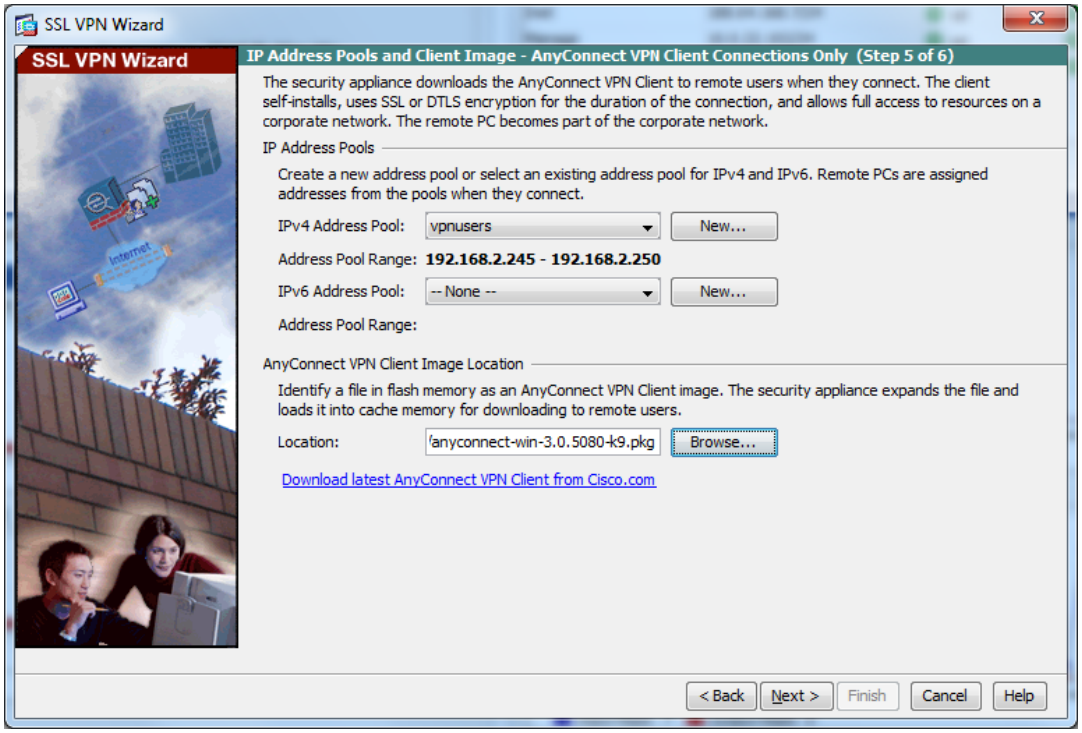
Задаем название pool-а, начальный и конечный адреса и маску подсети. Нажимаем «OK».



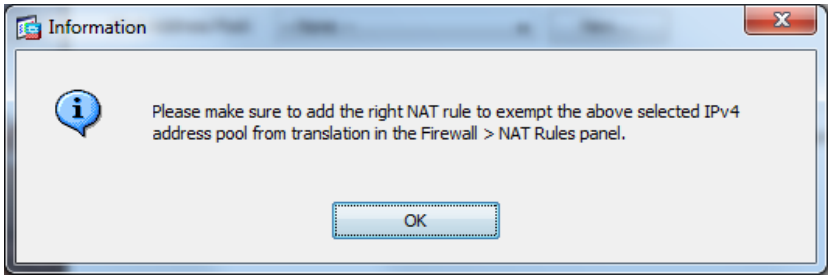
На этой же странице загружаем образ клиента Cisco AnyConnect под Windows.

Для того чтобы его загрузить во flash cisco ASA, необходимо нажать в соответствующем

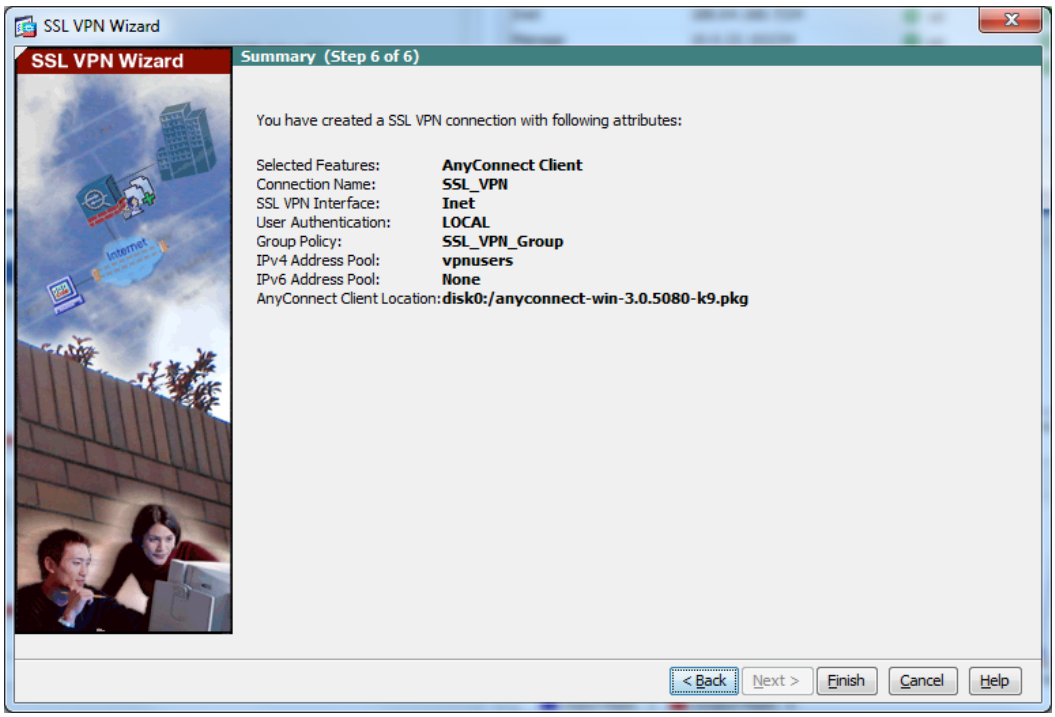
пункте «Browse», в следующем появившемся окошке «Upload»,
затем в следующем окошке «Browse local files» и указать нужный файл из списка. Далее нажимаем по порядку «Select»---«Upload File»---«OK»
(после нажатий будут всплывать информационные окошки об успешном выполнении). В итоге, получиться вот такое окно:



Нажимаем «Next»:

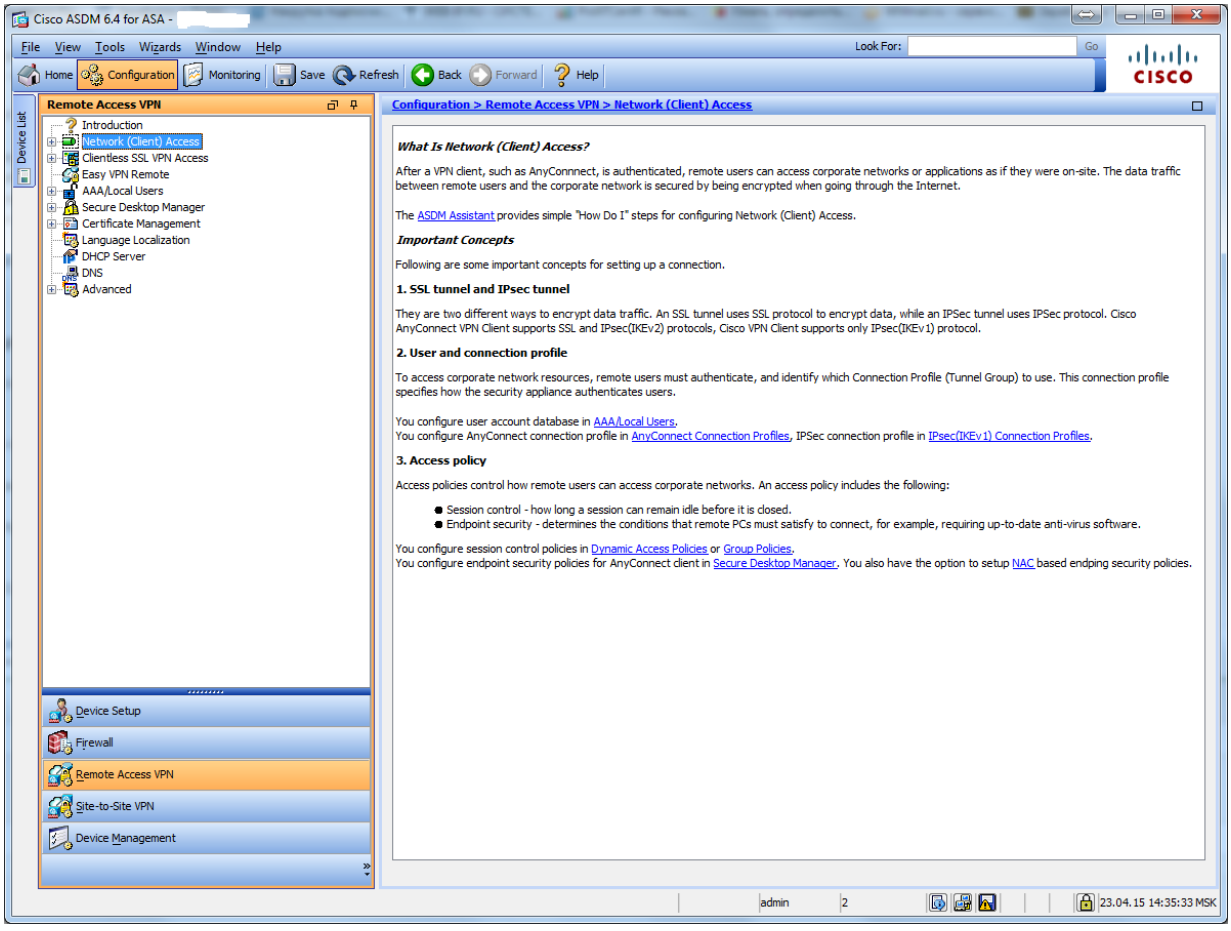


Это окно напоминает, что адреса, которые используются в пуле не должны попадать под политики NAT, если он настроен на cisco.
Нажимаем «OK».



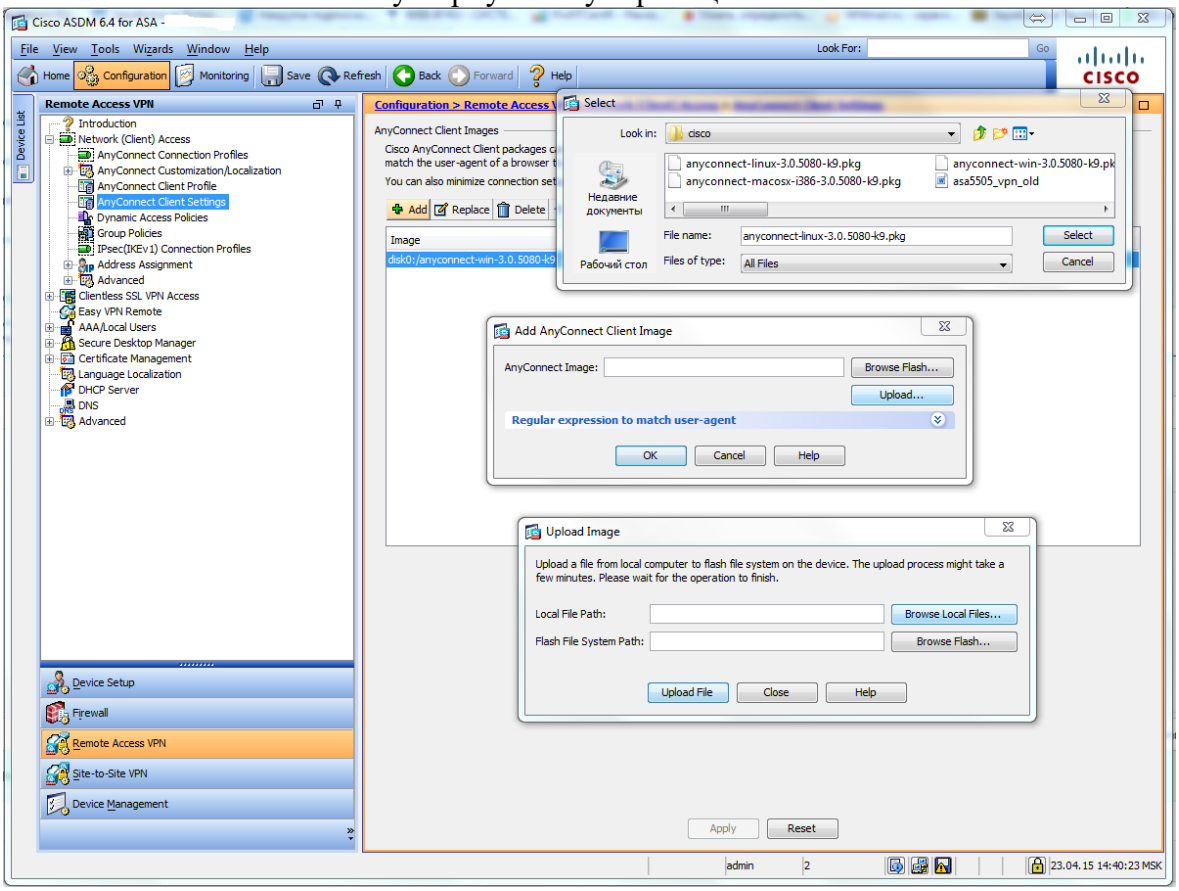
Здесь показаны все наши настройки, которые будут сконфигурированы. Нажимаем «Finish».

Более точные настройки (не через Wizard) можно посмотреть в разделе Configuration - Remote Access VPN

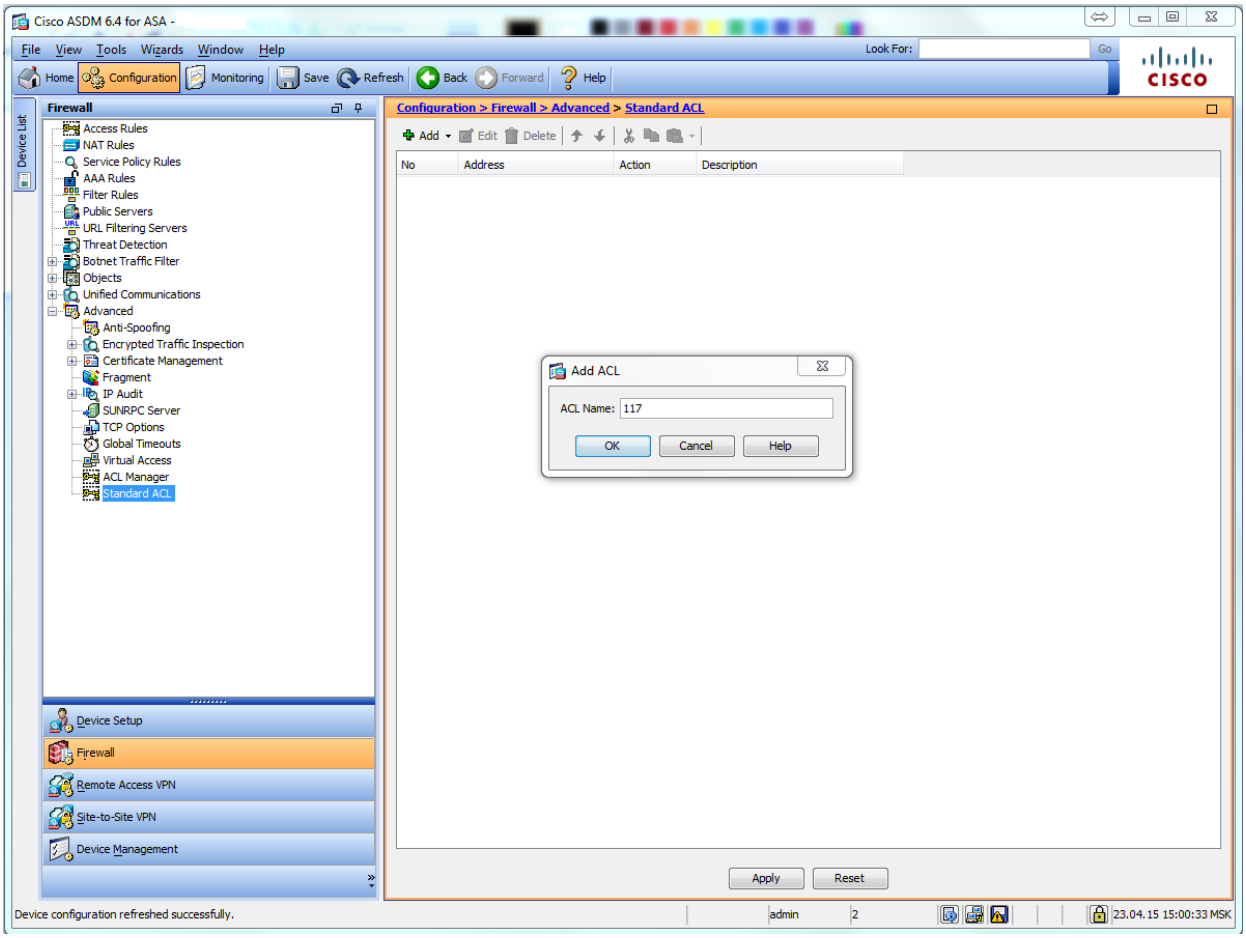


Нам необходимо добавить образы клиента под Mac и Linux, для этого заходим в раздел Network (Client) Access - AnyConnect Client Settings,

Здесь мы увидим уже загруженный образ клиента под Windows, нажимаем кнопку с зеленым плюсиком Add, и по аналогии как в Wizard добавляем образы под Linux и Mac.
После чего нажимаем кнопку "Aplly" внизу страницы.

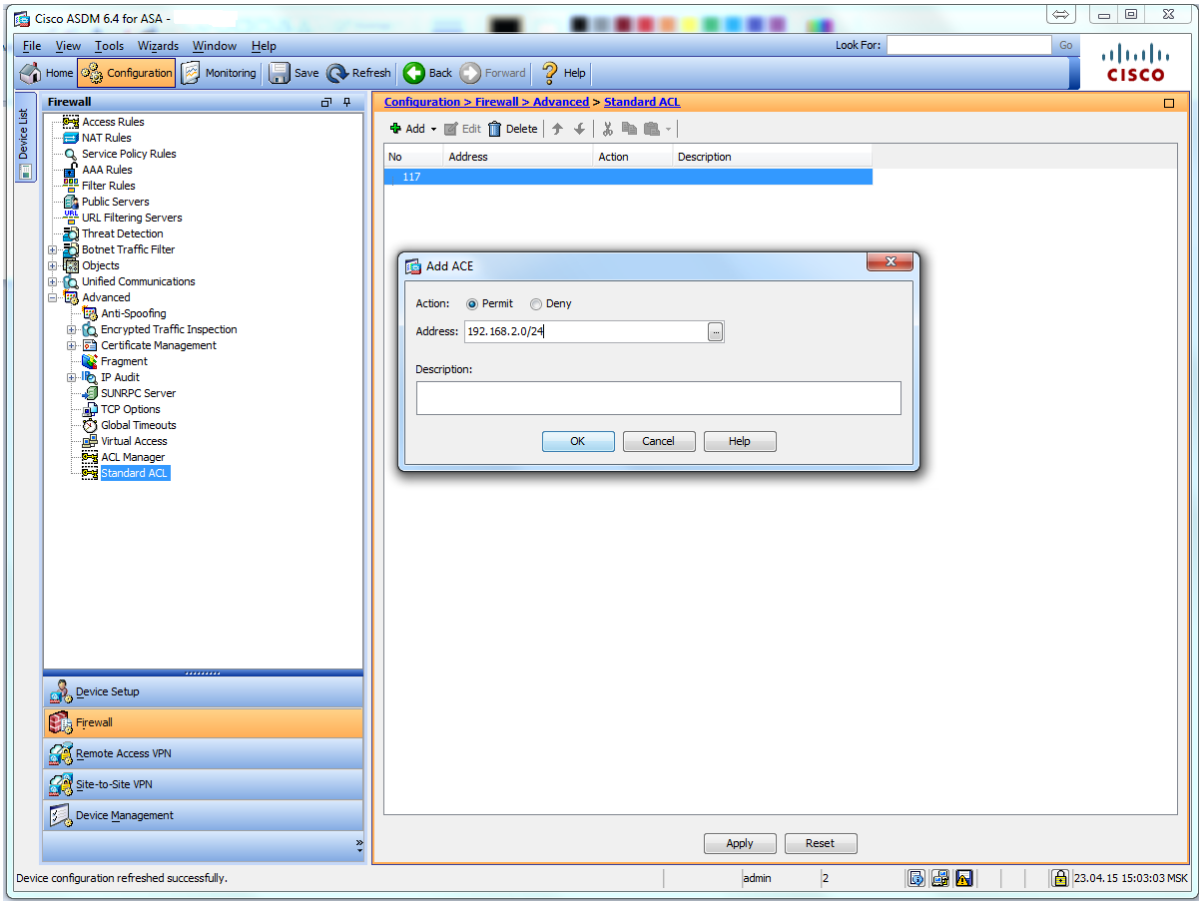


По умолчанию весь трафик клиента попадает в туннель, так как эта настройка наследуется из политики по умолчанию.
Для того чтобы указать какой трафик должен попадать в туннель, необходимо создать ACL, который будет его описывать и изменить политику туннелирования.
Эта функция называется split tunneling.
Для групповой политики SSL_VPN в туннель будет попадать только трафик, который идет в сеть 192.168.2.0/24.
Сначала создадим access-list, под который будет попадать трафик 192.168.2.0/24.
Для этого заходим в раздел Configuration - Firewall - Advanced - Standart ACL, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.
В появившемся окне вводим номер ACL и нажимаем OK.



Теперь нужно добавить содержимое для этого листа, это будет одна строка, встаем на наш аксесс лист 117, нажимаем кнопку с зеленым плюсиком Add, в выпадающем списке выбираем Add ACL.
Появится окно для ввода содержимого, Action оставляем Permit, в строку address вводим 192.168.2.0/24. Нажимаем OK и Aplly внизу страницы.

Аксесс-лист готов.



Теперь настраиваем split tunneling. Для этого нужно зайти в настройки самой групповой политики.

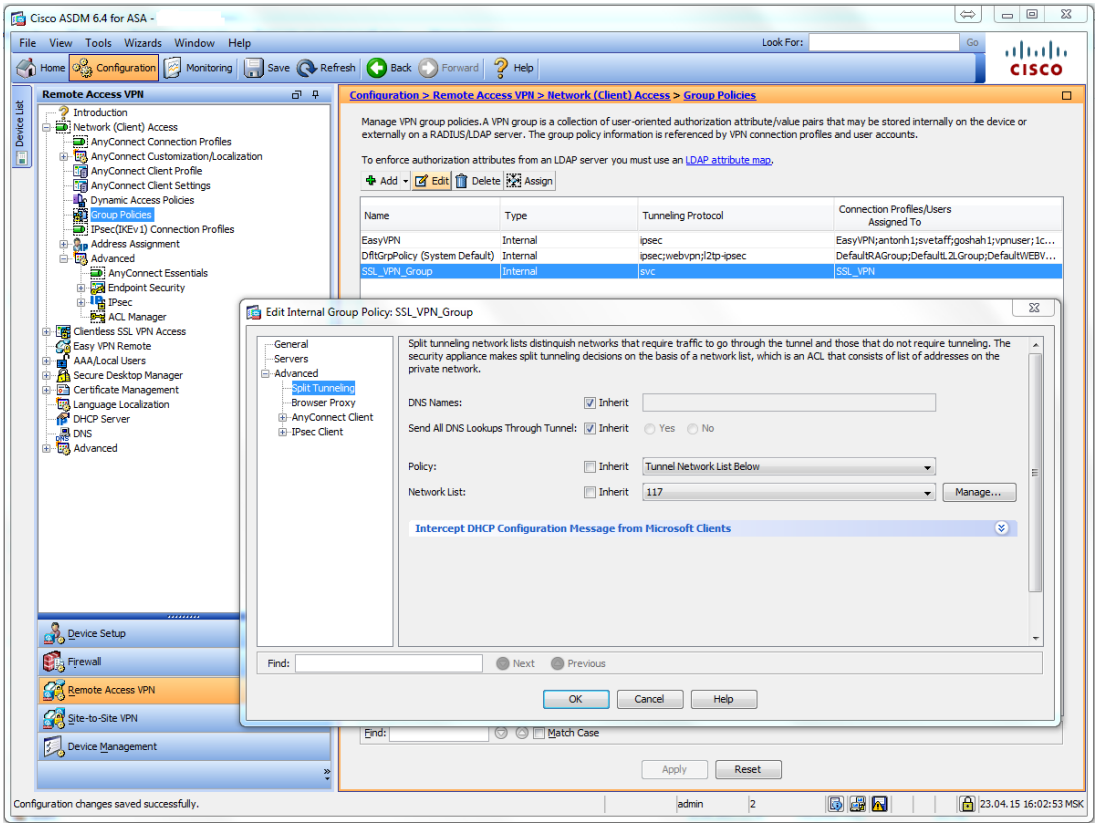
Идем Configuration - Remote Access VPN - Network (Client) Access - Group Policies.

В открывшемся окне в списке политик находим нашу SSL_VPN_Group. Встаем на нее, нажимаем кнопку Edit.

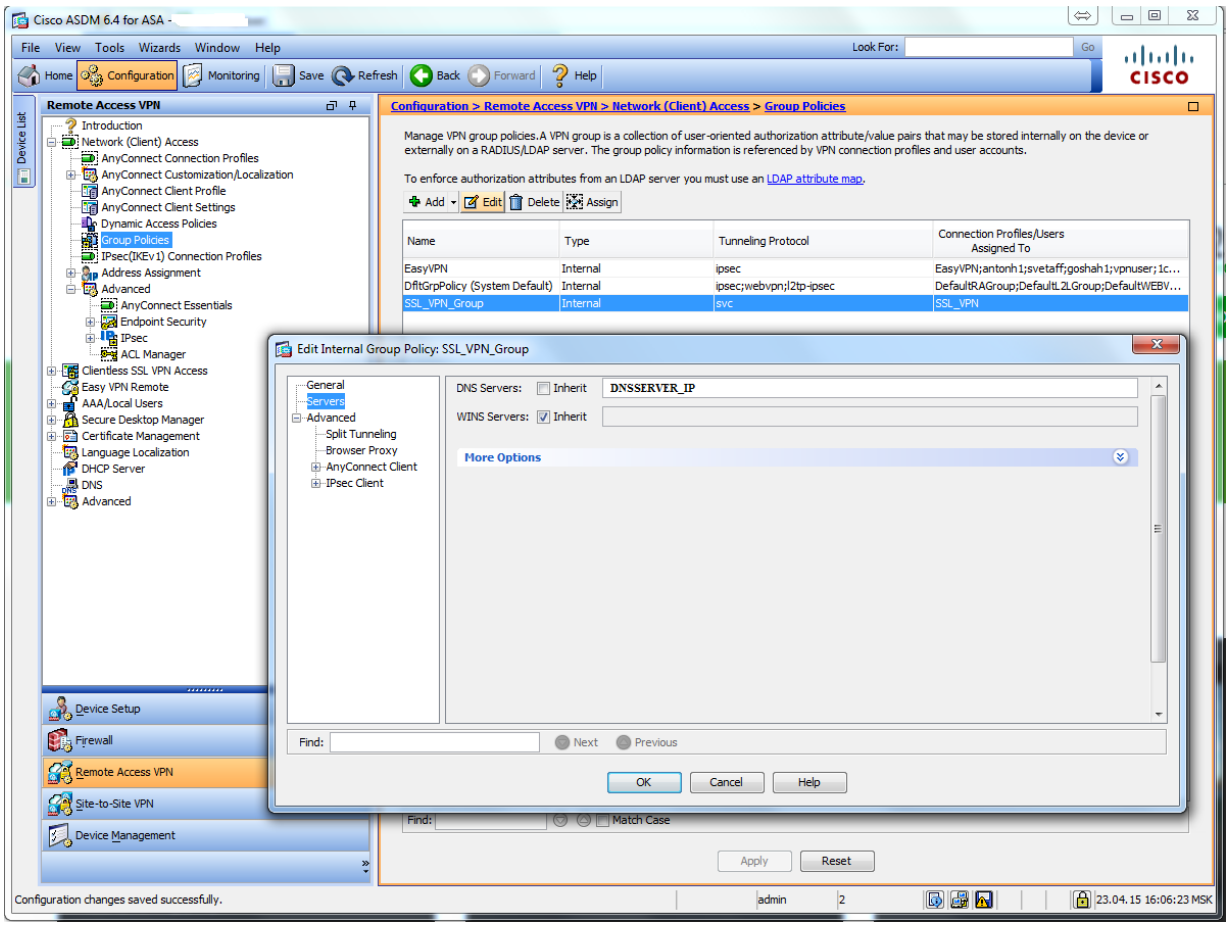
Откроется окно настроек групповой политики. Слева разворачиваем вкладку Advanced, выбираем Split Tunneling.

Напротив записи Policy убираем галку Inherit, и в выпадающем списке выбираем Tunnel Network List Bellow.

Напротив записи Network List убираем галку Inherit, и в выпадающем списке выбираем аксесс-лист 117. Нажимаем ОК и Aplly внизу страницы.



Если имеется локальный DNS сервер также нужно прописать его в групповой политике. Идем туда же в настройки групповой политики. Слева выбираем Servers. Напротив строки DNS servers убираем галку Inherit и вписываем адрес локального DNS сервера. Нажимаем OK и Aplly внизу страницы.



Настройка с помощью CLI

Теперь посмотрим какие настройки появились у нас в CLI.

Акксесс-лист для опции Split Tunneling.

access-list 117 standard permit 192.168.2.0 255.255.255.0
Пул для ip адресов

ip local pool vpnusers 192.168.2.245-192.168.2.250 mask 255.255.255.0

Настройки webvpn. Включение svc. Интерфейс Inet. Пути к образам клиентов.
webvpn
 enable Inet
 anyconnect-essentials
 svc image disk0:/anyconnect-win-3.0.5080-k9.pkg 1
 svc image disk0:/anyconnect-linux-3.0.5080-k9.pkg 2
 svc image disk0:/anyconnect-macosx-i386-3.0.5080-k9.pkg 3
 svc enable
 tunnel-group-list enable

Настройки профайла.
tunnel-group SSL_VPN type remote-access
tunnel-group SSL_VPN general-attributes
 address-pool vpnusers
 default-group-policy SSL_VPN_Group

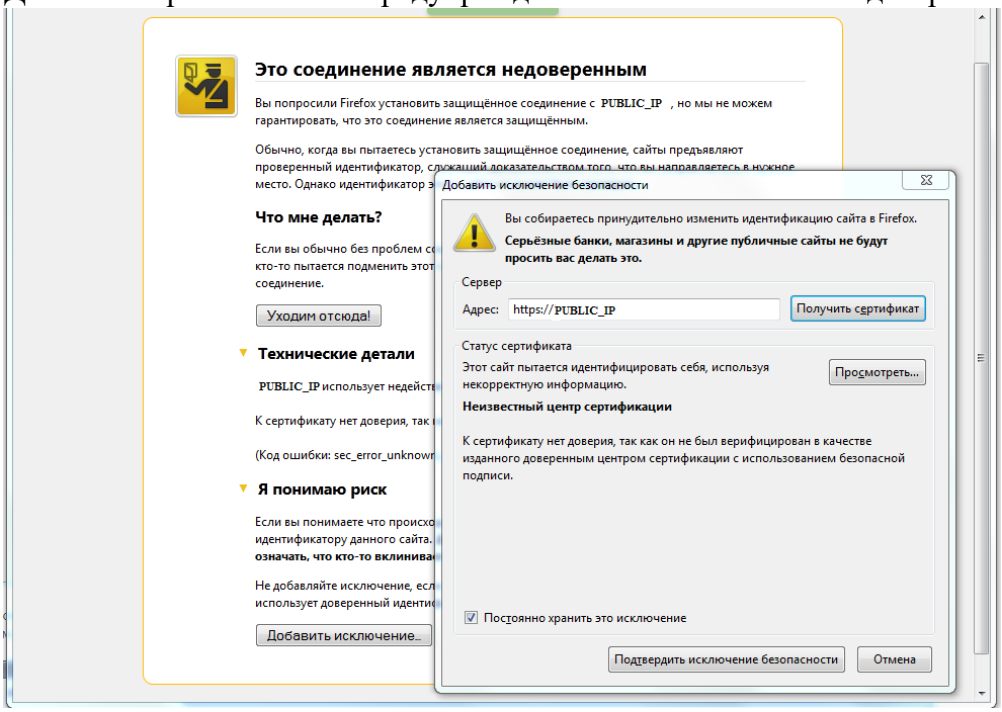
```
tunnel-group SSL_VPN webvpn-attributes
 group-alias SSL_VPN enable
```

Настройки групповой политики. DNS сервер. Опция split-tunnel.

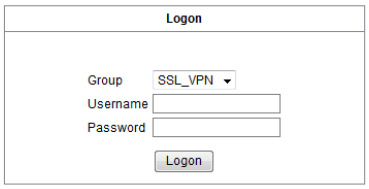
```
group-policy SSL_VPN_Group internal
group-policy SSL_VPN_Group attributes
 dns-server value DNSSERVER_IP
 vpn-tunnel-protocol svc
 split-tunnel-policy tunnelspecified
 split-tunnel-network-list value 117
 default-domain none
```

Установка клиента

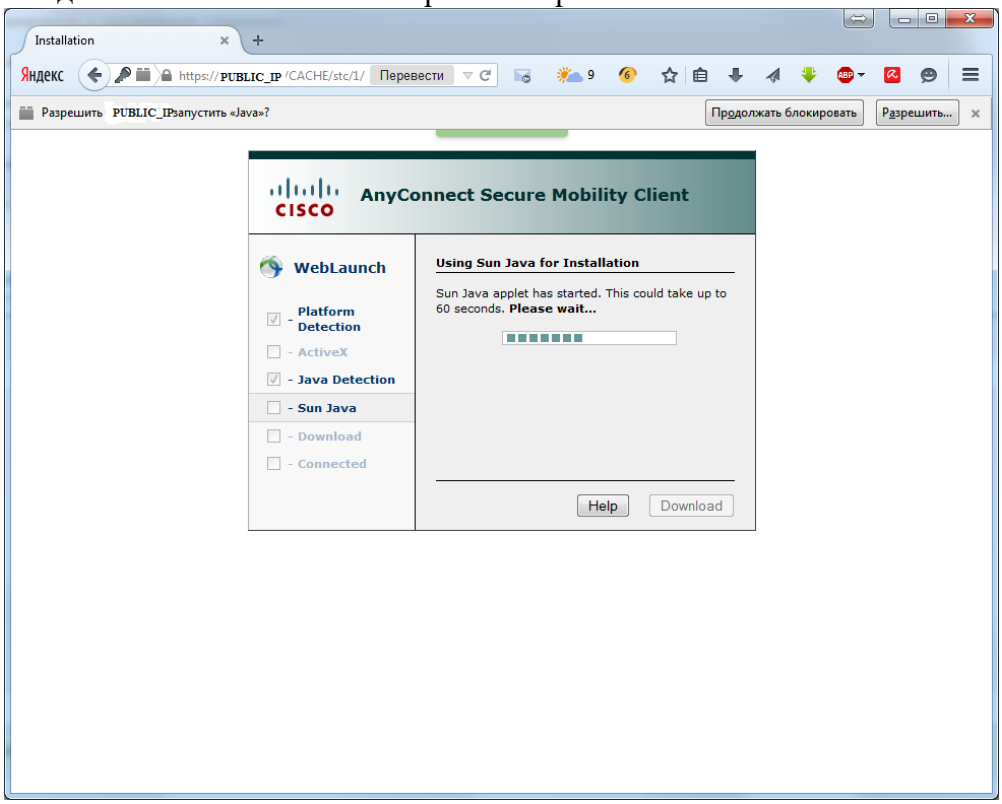
Заходим в браузер. В адресной строке набираем https://PUBLIC_IP
Должно открыться окно с предупреждением безопасности о недоверенном соединении.



Со всем соглашаемся (устанавливаем (получаем) сертификат и добавляем источник в исключения).
Нажимаем на «Подтвердить исключение безопасности» и у вас откроется следующее окно:

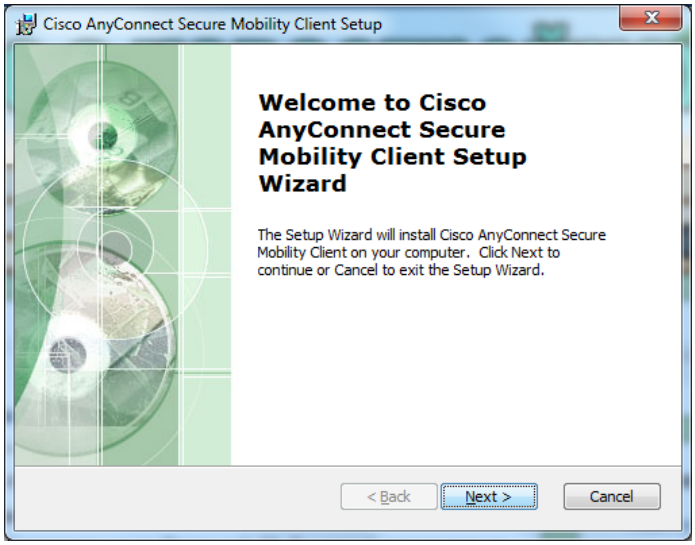


Вводим имя пользователя и пароль. Откроется такое окно:



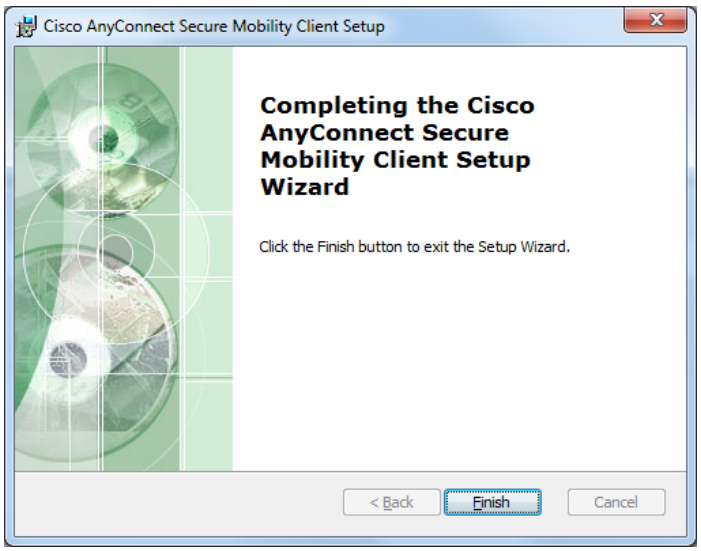
Программа установки пытается определить установленную ОС, для того чтобы запустить установку Cisco AnyConnect Client.
В результате программа предложить скачать подходящий под ОС образ:

Скачиваем образ и запускаем программу установки:



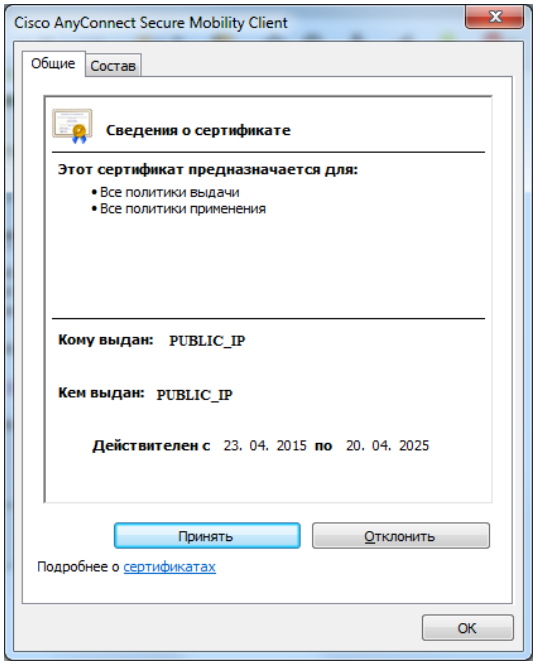
Нажимаем Next, принимаем лицензионное соглашение, Next, Install. Начнется установка.

Нажимаем Finish. Установка завершена.



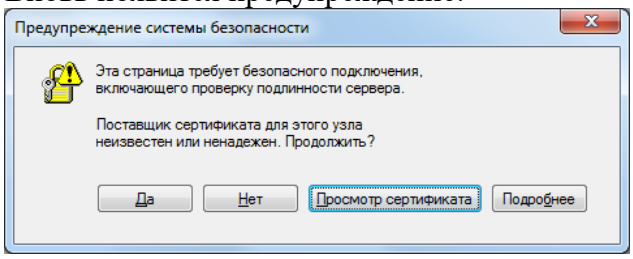
Запускаем программу. Справа внизу появится окошко.

Вводим ip-адрес для подключения, нажимаем Connect.
Появится окно с информацией о сертификате.



Нажимаем "Принять". Появится окно с запросом логина и пароля.

Вновь появится предупреждение:



Нажимаем Принять, начнется подключение. В результате окно справа внизу примет вид. VPN подключен.