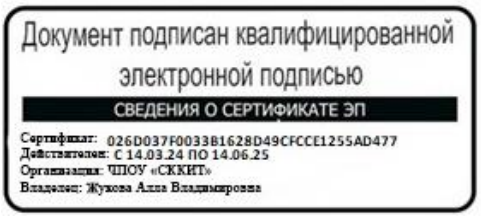
Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрена и утверждена
на Педагогическом совете
от 27.03.2025 Протокол № 03



УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Согласовано:
Заместитель директора по учебно - методической работе С.В. Марченко

Проверено:
Руководитель объединения инноваций и сетевого и системного администрирования В.М. Жукова

Составитель:
Преподаватель А.М. Жуков

2025 г.

Рабочая программа учебной дисциплины Безопасность компьютерных сетей разработана в соответствии с
- Приказом Минпросвещения Российской Федерации от 10 июля 2023 года № 519 «Об утверждении федерального государственного образовательного стандарта среднего профессионального образования по специальности 09.02.06 «Сетевое и системное администрирование»

Укрупненная группа специальности: 09.00.00 Информатика и вычислительная техника

Организация-разработчик: Частное профессиональное образовательное учреждение «Северо-Кавказский колледж инновационных технологий»

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

1.1. Область применения программы

Рабочая программа учебной дисциплины ОП.16 Безопасность компьютерных сетей является частью основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование, квалификация – Системный администратор.

1.2 Место программы учебной дисциплины в структуре основной образовательной программы:

Дисциплина входит в общепрофессиональный цикл дисциплин (ОП.016) основной образовательной программы в соответствии с ФГОС СПО по специальности 09.02.06 Сетевое и системное администрирование.

1.3. Результаты освоения программы учебной дисциплины:

В рамках программы учебной дисциплины формируются следующие компетенции:

Код и название компетенции	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать	номенклатура информационных источников, применяемых в профессиональной деятельности; приемы

информационные технологии для выполнения задач профессиональной деятельности	получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	структурирования информации; формат оформления результатов поиска информации
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятельности	психологические основы деятельности коллектива, психологические особенности личности; основы проектной деятельности
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных

		систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.
ПК 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и комплектующие информационно-коммуникационной системы	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем управления ремонтом и обслуживанием Типовые сроки проведения профилактического ремонта Правила и процедуры проведения

		инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

2. СТРУКТУРА И СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1 Объем программы учебной дисциплины и виды работы

Вид учебной работы	Объем в академических часах очная форма обучения	Объем в академических часах заочная форма обучения
Объем учебной дисциплины	126	126
в том числе реализуемый в форме практической подготовки	100	10
в том числе из объема учебной дисциплины:		
Теоретическое обучение	20	4
Практические занятия (если предусмотрено)	100	10
Самостоятельная работа (если предусмотрена)	6	112
Промежуточная аттестация/ Форма контроля	Дифференцированный зачет (7 семестр)	Дифференцированный зачет (10 семестр)

2.2. Тематический план и содержание программы учебной дисциплины

Наименование разделов и тем	Формы организации учебной деятельности обучающихся	Содержание форм организации учебной деятельности обучающихся	Объем часов (очная форма)	Объем часов (заочная форма)	Наименование синхронизированных образовательных результатов (только коды)	Уровень освоения
1	**2**	**3**	**4**	**5**	**6**	**7**
Тема 1.1. Безопасность компьютерных сетей	Теоретическое обучение	1. Фундаментальные принципы безопасной сети Современные угрозы сетевой безопасности. Вирусы, черви и троянские кони. Методы атак. 2. Безопасность Сетевых устройств OSI Безопасный доступ к устройствам. Назначение административных ролей. Мониторинг и управление устройствами. Использование функция автоматизированной настройки безопасности. 3. Авторизация, аутентификация и учет доступа (AAA) Свойства AAA. Локальная AAA аутентификация. Server-based AAA 4. Реализация технологий брандмауэра ACL. Технология брандмауэра. Контекстный контроль доступа (CBAC). Политики брандмауэра основанные на зонах. 5. Реализация технологий предотвращения вторжения	20	4	ОК 01,02,04,09 ПК 1.2,1.3,1.7	1

		IPS технологии. IPS сигнатуры. Реализация IPS. Проверка и мониторинг IPS 6. Безопасность локальной сети Обеспечение безопасности пользовательских компьютеров. Соображения по безопасности второго уровня (Layer-2). Конфигурация безопасности второго уровня. Безопасность беспроводных сетей, VoIP и SAN 7. Криптографические системы Криптографические сервисы. Базовая целостность и аутентичность. Конфиденциальность. Криптография открытых ключей. 8Реализация технологий VPN VPN. GRE VPN. Компоненты и функционирование IPSec VPN. Реализация Site-to-site IPSec VPN с использованием CLI. Реализация Site-to-site IPSec VPN с использованием CCP. Реализация Remote-access VPN 9. Управление безопасной сетью Принципы безопасности сетевого дизайна. Безопасная архитектура. Управление процессами и безопасность. Тестирование сети на уязвимости. Непрерывность бизнеса, планирование восстановления аварийных ситуаций. Жизненный цикл сети и планирование. Разработка регламентов компании и политик безопасности. 10. Cisco ASA Введение в Адаптивное устройство				

		безопасности ASA. Конфигурация фаирвола на базе ASA с использованием графического интерфейса ASDM. Конфигурация VPN на базе ASA с использованием графического интерфейса ASDM.				
	Практическое занятие	**Практические задания:** 1. Социальная инженерия 2. Исследование сетевых атак и инструментов проверки защиты сети 3. Настройка безопасного доступа к маршрутизатору 4. Обеспечение административного доступа AAA и сервера Radius 5. Настройка политики безопасности брандмауэров 6. Настройка системы предотвращения вторжений (IPS) 7. Настройка безопасности на втором уровне на коммутаторах 8. Исследование методов шифрования 9. Настройка Site-to-SiteVPN используя интерфейс командной строки 10. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки 11. Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM 12. Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM	100	10		2

		13. НастройкаClientless Remote Access SSL VPNs используя ASDM 14. Настройка AnyConnect Remote Access SSL VPN, используя ASDM 15. Финальная комплексная лабораторная работа по безопасности. Тестовые задания				
	Самостоятельная работа	Поиск информации в сети Интернет, работа с книгой, лекционным материалом	**6**	112		3
Промежуточная аттестация (или указать формы контроля) – Дифференцированный зачет очная форма (7 семестр); заочная форма Дифференцированный зачет (10 семестр). -						
		ИТОГО:	**126**	**126**		

Для характеристики уровня освоения учебного материала используются следующие обозначения:
1. – Ознакомительный (узнавание ранее изученных объектов, свойств);
2. – Репродуктивный (выполнение деятельности по образцу, инструкции или под руководством);
3.– Продуктивный (планирование и самостоятельное выполнение деятельности, решение проблемных задач).

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Материально-техническое обеспечение

Реализация дисциплины требует:

- оснащение лаборатории

№	Наименование оборудования	Техническое описание
I. Специализированная мебель и системы хранения		
	Основное оборудование:	
	Стол ученический	регулируемый по высоте
	Стул ученический	регулируемый по высоте
	Дополнительное оборудование:	
	Магнитно-маркерная доска / флипчарт	модель подходит для письма (рисования) маркерами и для размещения бумажных материалов с помощью магнитов
II. Технические средства		
	Основное оборудование:	
	Сетевой фильтр	с предохранителем
	Интерактивный программно-аппаратный комплекс мобильный или стационарный, программное обеспечение	диагональ интерактивной доски должна составлять не менее 65” дюймов (165,1 см); для монитора персонального компьютера и ноутбука – не менее 15,6” (39,6 см), планшета – 10,5” (26,6 см)[1]
	Лаборатория «Организация и принципы построения компьютерных систем»	- Компьютеров обучающихся – 12 шт - Компьютер преподавателя - 1 шт - Аппаратное обеспечение: 2 сетевые платы, процессор Core i3, оперативная память объемом 8 Гб; HD 500 Gb - Операционная система: Windows - Пакет офисных программ, общего и профессионального назначения: FreeCAD, KiCad, EDA, FidoCadJ, Мой оффис EclipseIDEforJavaEEDevelopers, MicrosoftVisualStudio, AndroidStudio, Web – Appach, Ninja IDE, Gimp, Eclipse, Python, Web Browser – Chrome, Sublime Text 3, Notepad ++ windows и RedOS, Blender, SketchUp. Сервер в лаборатории (аппаратное обеспечение: 2 сетевые платы, 8-х ядерный процессор с частотой 3 ГГц, оперативная память объемом 16 Гб, жесткие диски общим объемом 2 Тб, программное обеспечение: Windows Server 2019, лицензионная антивирусная программа (Kaspersky antivirus) , лицензионная программа восстановления данных (Hetman Partition Recovery), лицензионная программы по виртуализации (Java 32-64

[1] Постановление Главного санитарного врача Российской Федерации от 28 сентября 2020 года N 28 «Об утверждении санитарных правил СП 2.4.3648-20 "Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи"

		bits). - Технические средства обучения: Интерактивная доска (IQ BOARD с передвижной подставкой) , Проектор (Epson) - Типовой состав для монтажа и наладки компьютерной сети: кабели различного типа (Cablexpert PP12-0.25M, DEXP), обжимной инструмент, коннекторы RJ-45, тестеры для кабеля, кросс-нож, кросс-панель. - Пример проектной документации (обеспечения компьютерных сетей, программирования и баз данных) Лицензионное программное обеспечение для администрирования сетей и обеспечения ее безопасности - Wireshark - 6 маршрутизаторов (WiFi роутер) -1 Коммутатор с 24 портами Ethernet со скоростью не менее 100 Мб/с и 2 портами Ethernet со скоростью не менее 1000Мб/с - телекоммуникационная стойка (сетевой фильтр на 6 гнезд, источник бесперебойного питания); - 2 беспроводных маршрутизатора Linksys E1200-EE - IP телефоны - 3 шт. - Программно-аппаратные шлюзы безопасности - 2шт. (ПО VipNet Clirnt For Windows 4.x (КС2), VipNet PCI Client 1.x) Интерактивная камера – 1 шт Рециркулятор – 1 шт
	Дополнительное оборудование:	
	Колонки	для воспроизведения звука любой модификации
	Web-камера	любой модификации
III. Демонстрационные учебно-наглядные пособия		
	Основные:	
	нет	нет
	Дополнительные:	
	настенный стенд	отражающий специфику дисциплины

- оснащение помещений, задействованных при организации самостоятельной и воспитательной работы:

помещения для организации самостоятельной и воспитательной работы должны быть оснащены компьютерной техникой с возможностью подключения к информационно-телекоммуникационной сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду образовательной организации.

3.2. Требования к учебно-методическому обеспечению

Учебно-методический материал по дисциплине включает: лекции; перечень практических занятий, практические задания, тестовые задания, упражнения, перечень вопросов к текущему контролю и промежуточной аттестации.

3.3. Интернет-ресурсы

https://rkn.gov.ru/?ysclid=kzax21zwwl Роскомнадзор РФ
https://digital.gov.ru/ru/?utm_referrer=https%3a%2f%2fyandex.ru%2f Министерство цифрового развития связи и массовых коммуникаций Российской Федерации
http://www.ras.ru/ Российская академия наук

3.4. Программное обеспечение, цифровые инструменты

Колледж обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства. Используются программы, входящие в Единый реестр российских программ для электронных вычислительных машин и баз данных, а также реестр социальных соцсетей:«Яндекс.Диск (для Windows)», Яндекс.Почта, Telegram, Power Point, ВКонтакте (vk.com), Вебинар.ру

3.5. Основная печатная или электронная литература

1.Мэйволд, Э. Безопасность сетей: учебное пособие для СПО / Э. Мэйволд. — Саратов: Профобразование, 2021. — 571 с. — ISBN 978-5-4488-0990-3. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/102183.html
2.Технологии защиты информации в компьютерных сетях: учебное пособие для СПО / Н. А. Руденков, А. В. Пролетарский, Е. В. Смирнова, А. М. Суровов. — Саратов: Профобразование, 2021. — 368 с. — ISBN 978-5-4488-1014-5. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/102207.html

3.6. Дополнительная печатная или электронная литература

1.Самойлова, Е. М. Информационная безопасность: учебное пособие для СПО / Е. М. Самойлова, М. В. Виноградов. — Саратов, Москва: Профобразование, Ай Пи Ар Медиа, 2023. — 135 с. — ISBN 978-5-4488-1662-8, 978-5-4497-2244-7. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/131646.html
2.Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие для СПО / Б. А. Фороузан; под редакцией А. Н. Берлина. — Саратов: Профобразование, 2021. — 776 с. — ISBN 978-5-4488-0999-6. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/102192.html

3.7. Словари, справочники, энциклопедии, периодические материалы (журналы и газеты)

1.Терминологический словарь по предметам кафедры «Бизнес- информатика» / составители Я. А. Донченко [и др.]. — Симферополь: Университет экономики и управления, 2020. —240 с. — Текст: электронный// Электронно-библиотечная система IPR BOOKS: [сайт]. —URL: https://www.iprbookshop.ru/108 063.html
2.Шитова, Л. Ф. Digital Idioms = Словарь цифровых идиом / Л. Ф. Шитова. — Санкт-Петербург: Антология, 2021. — 158 с. — ISBN 978-5-94962-216-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: https://www.iprbookshop.ru/104021.html
3.Журнал Директор информационной службы https://www.iprbookshop.ru/76373.html
4.Журнал Прикладная информатика https://www.iprbookshop.ru/11770.html

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения учебной дисциплины осуществляется преподавателем в процессе проведения практических занятий, выполнения практических заданий, написании докладов.

Содержание обучения	**Характеристика основных видов учебной деятельности студентов (на уровне учебных действий)**
Тема 1.1. Безопасность компьютерных сетей	Выполнение практических заданий. тестовые задания.

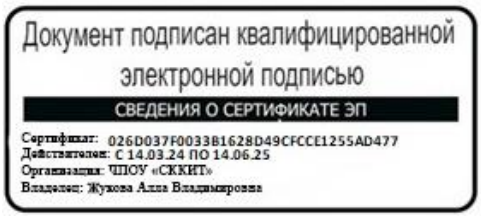
Результаты подготовки обучающихся при освоении рабочей программы учебной дисциплины определяются оценками:

Оценка	**Содержание**	**Проявления**
Неудовлетворительно	Студент не обладает необходимой системой знаний и умений	Обнаруживаются пробелы в знаниях основного программного материала, допускаются принципиальные ошибки в выполнении предусмотренных программой заданий
Удовлетворитель	Уровень оценки результатов обучения показывает, что студенты обладают необходимой системой знаний и владеют некоторыми умениями по дисциплине. Студенты способны понимать и интерпретировать освоенную информацию, что является основой успешного формирования умений и навыков для решения практикоориентированных задач	Обнаруживаются знания основного программного материала в объеме, необходимом для дальнейшей учебы и предстоящей работы по специальности (профессии); студент справляется с выполнением заданий, предусмотренных программой, знаком с основной литературой, рекомендованной программой. Как правило, оценка "удовлетворительно" выставляется студентам, допустившим погрешности в ответе и при выполнении заданий, но обладающим необходимыми знаниями для их устранения под руководством преподавателя
Хорошо	Уровень осознанного владения учебным материалом и учебными умениями, навыками и способами деятельности по дисциплине; способны анализировать, проводить сравнение и обоснование	Обнаруживается полное знание программного материала; студент, успешно выполняющий предусмотренные в программе задания, усвоивший основную литературу, рекомендованную в программе. Как правило, оценка "хорошо" выставляется студентам, показавшим систематический

	выбора методов решения заданий в практико-ориентированных ситуациях	характер знаний по дисциплине и способным к их самостоятельному пополнению и обновлению в ходе дальнейшей учебной работы и профессиональной деятельности
Отлично	Уровень оценки результатов обучения студентов по дисциплине является основой для формирования общих и профессиональных компетенций, соответствующих требованиям ФГОС СПО. Студенты способны использовать сведения из различных источников для успешного исследования и поиска решения в нестандартных практико-ориентированных ситуациях	Обнаруживается всестороннее, систематическое и глубокое знание программного материала, умение свободно выполнять задания, предусмотренные программой; студент, усвоивший основную и знакомый с дополнительной литературой, рекомендованной программой. Как правило, оценка "отлично" выставляется студентам, усвоившим взаимосвязь основных понятий дисциплины в их значении для приобретаемой профессии, проявившим творческие способности в понимании, изложении и использовании программного материала

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрен и утвержден
на Педагогическом совете
от 27.03.2025 Протокол № 03



УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

2025

ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

После освоения дисциплины студент должен обладать следующими компетенциями:

Код и название компетенции	Умения	Знания
ОК 01. Выбирать способы решения задач профессиональной деятельности применительно к различным контекстам	распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника)	актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте; алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структура плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности
ОК 02 Использовать современные средства поиска, анализа и интерпретации информации и информационные технологии для выполнения задач профессиональной деятельности	определять задачи для поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска	номенклатура информационных источников, применяемых в профессиональной деятельно-сти; приемы структурирования информации; формат оформления результатов поиска информации
ОК 04 Эффективно взаимодействовать и работать в коллективе и команде	организовывать работу коллектива и команды; взаимодействовать с коллегами, руководством, клиентами в ходе профессиональной деятель-ности	психологические основы деятельности кол-лектива, психологические особенности лично-сти; основы проектной деятельности
ОК 09 Пользоваться профессиональной документацией на государственном и иностранном языках	понимать общий смысл четко произнесенных высказываний на известные темы (профессиональные и бытовые), понимать тексты на базовые профессиональные темы; участвовать в диалогах на знакомые общие и профессиональные темы; строить простые высказывания о себе и о своей профессиональной деятельности; кратко обосновывать и	правила построения простых и сложных предложений на профессиональные темы; основные общеупотребительные глаголы (бытовая и профессиональная лексика); лексический минимум, относящийся к описанию предметов, средств и процессов

	объяснить свои действия (текущие и планируемые); писать простые связные сообщения на знакомые или интересующие профессиональные темы	профессиональной деятельности; особенности произношения; правила чтения текстов профессиональной направленности
ПК 1.2 Поддерживать работоспособность аппаратно-программных средств устройств инфокоммуникационных систем	применять инструкции по установке и эксплуатации периферийного оборудования; выполнять замену расходных материалов и комплектующих периферийного оборудования; использовать контрольно-измерительное оборудование для проверки электрических соединений устройств инфокоммуникационных систем; выявлять и устранять механические повреждения и дефекты устройств инфокоммуникационных систем	основ архитектуры аппаратных средств; принципов функционирования аппаратных средств вычислительной техники; типовых регламентов обслуживания аппаратных средств; способов обнаружения механических неполадок в работе устройств инфокоммуникационных систем, причин их возникновения и приемов устранения; требований охраны труда при работе с программно-аппаратными средствами инфокоммуникационных систем.
ПК 1.3 Устранять неисправности в работе инфокоммуникационных систем	идентифицировать инциденты, возникающие при установке программного обеспечения, и принимать решение об изменении процедуры установки; оценивать степень критичности инцидентов при работе прикладного программного обеспечения; устранять возникающие инциденты; производить мониторинг администрируемой информационно-коммуникационной системы; документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику.	лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения; основы архитектуры, устройства и функционирования вычислительных систем; требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.
ПК 1.7 Осуществлять регламентное обслуживание и замену расходных материалов периферийного, сетевого и серверного оборудования инфокоммуникационных систем	Работать с договорной и отчетной документацией на обслуживаемую информационно-коммуникационную систему Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Работать с информационной системой управления запасами и ремонтом Оформлять заявки на материалы и	Типовые сроки заключения и действия договоров на обслуживание информационно-коммуникационной системы Действующие в организации локальные акты на оформление заявок на материалы и комплектующие Принципы организации информационных систем

	комплектующие информационно-коммуникационной системы	управления ремонтом и обслуживанием Типовые сроки проведения профилактического ремонта Правила и процедуры проведения инвентаризации Правила маркировки устройств и элементов информационно-коммуникационной системы Основы делопроизводства Процедура списания технических средств Отраслевые нормативные правовые акты

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ ТЕКУЩЕГО КОНТРОЛЯ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

1. ПАСПОРТ ОЦЕНОЧНЫХ СРЕДСТВ
Матрица учебных заданий

№	Наименование темы	Вид контрольного задания
	МДК.03.02. БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ	
1.	Тема 2.1. Безопасность компьютерных сетей	Поиск информации в сети Интернет, работа с книгой, лекционным материалом. Выполнение практических заданий. Тестовые задания

Тема 2.1. Безопасность компьютерных сетей

Практическое задание: *Социальная инженерия*

Вопросы для проверки знаний

1. Каковы главные предпосылки смены традиционной управленческой парадигмы?
2. Назовите основные референты изменения роли и места человека в экономике и общественном развитии.
3. Назовите этапы появления субъективных индикаторов в управлении экономикой и обществом.
4. Чем обусловлена необходимость научного социологического и психологического сопровождения совершенствования современного управления?
5. Назовите основные этапы развития отечественной социологии и психологии управления.
6. Почему движение ПОТ нельзя считать в полной мере разделом социологии и психологии управления?
7. В чем заключаются основные отличия развития западной и отечественной социологии и психологии управления?
8. Назовите основные задачи социальной инженерии.
9. Назовите ограничения в использовании социальной инженерии на современном этапе.

Практическое задание:*Исследование сетевых атак и инструментов проверки защиты сети*

Лабораторная работа

Задачи

Часть 1 Изучение веб-сайта SANS

•Откройте веб-сайт SANS и определите имеющиеся ресурсы.

Часть 2 Определение новых угроз сетевой безопасности

•Определите несколько потенциальных угроз сетевой безопасности с помощью веб-сайта SANS.

•Определите, какие сайты, помимо SANS, содержат информацию о сетевых угрозах.

Часть 3 Подробное описание отдельной угрозы сетевой безопасности

Выберите и подробно опишите какую-либо новую угрозу сетевой безопасности.

•Расскажите об этой угрозе.

Исходные данные/сценарий

Чтобы защитить сеть от атак, администратор должен определить, какие внешние угрозы представляютопасность для сети. Для определения возникающих угроз и способов их устранения можнопользоваться специализированными веб-сайтами.Одним из наиболее известных и проверенных ресурсов для защиты компьютера и сети является веб-сайт SANS (системное администрирование, проверка, сеть, безопасность). На веб-сайте SANS

доступны несколько разных ресурсов, включая список 20 основных средств контроля безопасностидля эффективной киберзащиты и еженедельную новостную рассылку по вопросам безопасности@Risk: Консенсус-Предупреждение Безопасности. В рассылке подробно рассказывается о новых сетевых атакахи уязвимостях.В ходе лабораторной работы вам необходимо открыть и изучить веб-сайт SANS, определить новыеугрозы сетевой безопасности с его помощью, посетить другие аналогичные веб-ресурсы и подготовить подробное описание отдельной сетевой атаки.

Необходимые ресурсы

•Устройство с выходом в Интернет

•Компьютер для презентации с установленной программой PowerPoint или другой программой дляпрезентаций.Часть 1: Изучение веб-сайта SANS

В части 1 вам нужно открыть веб-сайт SANS и изучить предлагаемые ресурсы.

Шаг 1:

Найдите ресурсы SANS.

Откройте веб-сайт www.sans.org в браузере. На главной странице наведите указатель мыши на менюResources (Ресурсы).

Назовите три доступных ресурса.

_____

Выберите пункт меню Top 20 Critical Controls (20 основных средств контроля безопасности).

Список 20 основных средств контроля безопасности на веб-сайте SANS был составлен в результате совместной работы государственных и частных компаний при участии Министерстваобороны, Ассоциации национальной безопасности, Центра интернет-безопасности и Института SANS.Его задачей было определение приоритетности средств контроля кибербезопасности и связанныхс ними расходов для Министерства обороны. На основе этого списка правительство США разработалоэффективные программы обеспечения безопасности. В меню Resources (Ресурсы) выберите пунктTop 20 Critical Controls (20 основных средств контроля безопасности).Выберите одно из 20 средств и назовите три предложения по его реализации.

Шаг 3:

Выберите меню «Newsletters» (Новостные рассылки).

Откройте меню Resources (Ресурсы) и выберите пункт Newsletters (Новостные рассылки). Кратко опишите каждую из трёх предлагаемых рассылок.

_____

Часть 2: Определение новых угроз сетевой безопасности

В части 2 вам нужно изучить новые угрозы сетевой безопасности, пользуясь веб-сайтом SANS, и узнать, на каких других сайтах можно найти информацию по этой теме.

Шаг 1:

Выберите раздел «Archive» (Архив) новостной рассылки @Risk: Consensus Предупреждение Службы Безопасности.

Откройте страницу Newsletters (Новостные рассылки) и выберите раздел Archive (Архив) рядомс названием @Risk: ConsensusSecurityAlert. Прокрутите страницу вниз до раздела Archives Volumes(Тома архива) и выберите последний выпуск еженедельной новостной рассылки. Ознакомьтесьс информацией в разделах Notable Recent Security Issues (Последние важные проблемыбезопасности) и Most Popular Malware Files (Наиболее распространённые файлы вредоносныхпрограмм).

Назовите некоторые из новых атак. При необходимости просмотрите несколько последних выпусковрассылки.

Шаг 2:

Найдите веб-сайты, которые содержат информацию о новых угрозахбезопасности.

Выясните, на каких ещё сайтах, помимо SANS, можно ознакомиться с информацией о новых угрозахсетевой безопасности.

_____

Назовите некоторые новые угрозы безопасности, подробно описанные на этих веб-сайтах.

_____

Часть 3: Подробное описание отдельной угрозы сетевой безопасности

В части 3 вы займётесь изучением отдельной сетевой атаки, а затем на основе полученной информации

подготовите презентацию. Используя полученные результаты, заполните приведённую ниже форму.

Шаг 1:

Заполните приведённую ниже форму данными выбранной сетевой атаки.

Имя атаки:

Тип атаки:

Даты атак:

Пострадавшие компьютеры илиорганизации:

Механизм атаки и её последствия:

Способы устранения:

Источники и ссылки на информационные ресурсы:

Шаг 2:

Для завершения презентации следуйте инструкциям инструктора.

Вопросы на закрепление

1 Какие меры можно предпринять для защиты собственного компьютера?

_____

_____

_____

_____

2 Какие важные меры могут предпринимать компании для защиты своих ресурсов?

Практическое задание: *Настройка безопасного доступа к маршрутизатору*

Практическое задание:*Обеспечение административного доступа AAA и сервера Radius*

Лабораторная работа

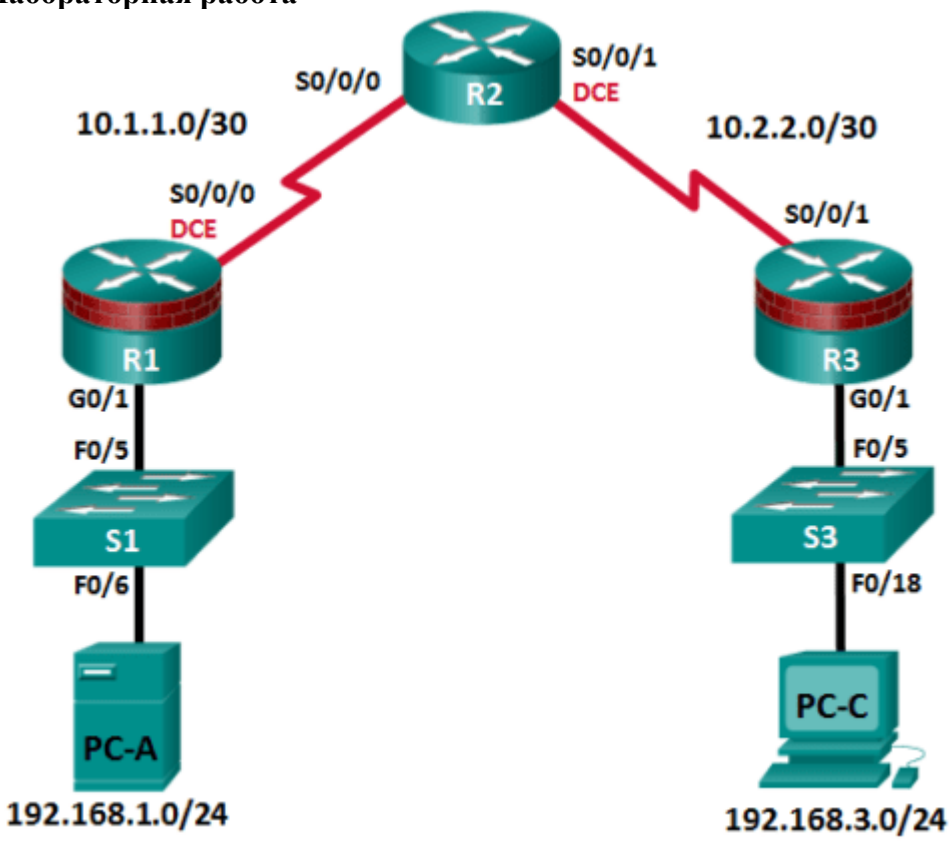


Таблица адресации
Устройство Интерфейс IP-адрес Маска подсети Шлюз по умолчанию Порт коммутатора
R1
G0/1 192.168.1.1 255.255.255.0 Н/П S1 F0/5
S0/0/0 (DCE) 10.1.1.1 255.255.255.252 Н/П Н/П
R2
S0/0/0 10.1.1.2 255.255.255.252 Н/П Н/П
S0/0/1 (DCE) 10.2.2.2 255.255.255.252 Н/П Н/П
R3
G0/1 192.168.3.1 255.255.255.0 Н/П S3 F0/5
S0/0/1 10.2.2.1 255.255.255.252 Н/ПН/П
PC-A NIC 192.168.1.3 255.255.255.0 192.168.1.1 S1 F0/6
PC-C NIC 192.168.3.3 255.255.255.0 192.168.3.1 S3 F0/18

Задачи

Часть 1. Настройка основных параметров устройства

 Настройте основные параметры, такие как имена хостов, IP-адреса интерфейсов и пароли для доступа.

 Настройте статическую маршрутизацию.

Часть 2. Настройка локальной аутентификации

 Настройте локального пользователя базы данных и локальный доступ для линий консоли, vty и aux.

 Проверьте конфигурацию.

Часть 3. Настройка локальной аутентификации с помощью AAA

 Настройте локальную базу данных пользователей с помощью Cisco IOS.

 Настройте локальную аутентификацию AAA с помощью Cisco IOS.

 Проверьте конфигурацию.

Часть 4. Настройка централизованной аутентификации с помощью AAA и RADIUS

 Установите на компьютер сервер RADIUS.

 Настройте пользователей на сервере RADIUS.

 На маршрутизаторе настройте сервисы AAA с помощью Cisco IOS, чтобы получить доступ к серверу RADIUS
для аутентификации.

 Проверьте конфигурацию AAA и RADIUS.

Исходные данные/сценарий

Самым распространенным способом обеспечения безопасного доступа к аршрутизатору является созданиепаролей для линий консоли, vty и aux. При попытке доступа к маршрутизатору у пользователя будетзапрашиваться только пароль. Настройка секретного пароля в привилегированном режиме повышает уровеньбезопасности, но в любом случае для каждого уровня доступа требуется только основной пароль.Помимо основных паролей, в локальной базе данных маршрутизатора можно настроитьотдельные именаили учетные записи пользователей с разными уровнями привилегий, которые могут применяться ко всемумаршрутизатору. Когда для линий консоли, vty или aux настроено обращение к этой локальной базе данных,то при использовании любой из этих линий для доступа к маршрутизатору пользователю предлагается ввестиимя и пароль.

Для дополнительного контроля над процессом входа может применяться методаутентификации, авторизациии учета (AAA). Для обеспечения базовой аутентификации функцию AAA можно настроить на доступ к локальнойбазе данных при вводе имен пользователей. Кроме того, могут быть определены запасные процедуры. Однакоданный подход не обладает хорошей масштабируемостью, так как его нужно настраивать на каждом маршрутизаторе. Для обеспечения максимальной масштабируемости и максимально эффективного применения AAA,данную функцию нужно использовать совместно с базой данных внешнего сервера TACACS+ или RADIUS.

При попытке пользователя войти в систему маршрутизатор обращается к внешнему серверу базы данных дляпроверки действительности имени пользователя и пароля.
В данной лабораторной работе вы построите сеть из нескольких маршрутизаторов и настроите маршрутизаторыи хосты. Затем вам будет необходимо использовать команды CLI для настройки на маршрутизаторах базовой
локальной аутентификации с помощью AAA. Вы установите на внешнем компьютере программное обеспечение
RADIUS и будете использовать AAA для аутентификации пользователей с помощью сервера RADIUS.
Часть 1: Настройка основных параметров устройства
В части 1 этой лабораторной работы вы создадите топологию сети и настроите основные параметры, такие как
IP-адреса интерфейсов, статическая маршрутизация, доступ к устройствам и пароли.
Все операции должны быть выполнены на маршрутизаторах R1 и R3. На маршрутизаторе R2 необходимовыполнить только шаги 1, 2, 3 и 6. В качестве примера здесь показана процедура для маршрутизатора R1.
Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.
Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельныесоединения.
Шаг 2: Настройте основные параметры для каждого маршрутизатора.
a. Задайте имена хостов согласно топологической схеме.
b. Настройте IP-адреса, как показано в таблице IP-адресов.
c. Настройте тактовую частоту маршрутизаторов с помощью DCE-кабеля, подключенного к последовательномуинтерфейсу каждого из них.
R1(config)# interface S0/0/0
R1(config-if)# clock rate 64000
d. Чтобы маршрутизатор не пытался неправильно интерпретировать введенные команды как имена хостов,отключите функцию DNS-поиска.
R1(config)# noipdomain-lookup
Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.
a. Настройте статический маршрут по умолчанию из маршрутизатора R1 в R2 и из маршрутизатора R3 в R2.
b. Настройте статический маршрут из маршрутизатора R2 к LAN маршрутизатора R1 и статический маршрутиз маршрутизатора R2 к LAN маршрутизатора R3.
Шаг 4: Настройте параметры IP для хостов.Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показанов таблице IP-адресов.
Шаг 5: Проверьте связь между компьютером PC-A и маршрутизатором R3.
a. Отправьте эхо-запрос с маршрутизатора R1 на маршрутизатор R3.
Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем,
как продолжить.
b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-Св локальной сети маршрутизатора R3.Если запрос был выполнен с ошибкой, проведите диагностику основных параметров устройства перед тем,как продолжить.Примечание. Если эхо-запрос с компьютера PC-A на компьютер PC-C выполнен успешно, то это означает,что статическая маршрутизация настроена верно и работает исправно. Если эхо-запрос был выполненс ошибкой, но интерфейсы устройств активны и IP-адреса заданы верно, воспользуйтесь командамishowrun и showiproute, чтобы определить проблемы, связанные с протоколом маршрутизации.
Шаг 6: Сохраните основную текущую конфигурацию для каждого маршрутизатора.
Шаг 7: Сконфигурируйте и зашифруйте пароли на маршрутизаторах R1 и R3.

Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегченияпроцесса выполнения лабораторной работы пароли были относительно упрощены. В производственной сетирекомендуется использовать более сложные пароли.На данном шаге настройте параметры одинаковым образом на маршрутизаторах R1 и R3. В качестве примераздесь показан маршрутизатор R1.

a. Задайте минимальную длину пароля.

Используйте команду securitypasswords, чтобы задать минимальную длину пароля в 10 символов.R1(config)# security passwords min-length 10

b. Настройтепароль enable secret наобоихмаршрутизаторах. Используйте алгоритм хеширования type 9 (SCRYPT).R1(config)# enablealgorithm-typescryptsecretcisco12345

Шаг 8: Настройте основную консоль, вспомогательный порт и линии vty.

a. Настройте пароль консоли и активируйте вход в систему для маршрутизатора 1. Для дополнительнойбезопасности команда exec-timeout обеспечивает выход из системы линии, если в течение 5 минутотсутствует активность. Команда loggingsynchronous предотвращает прерывание ввода командсообщениями консоли.

Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во времялабораторной работы, вы можете ввести команду exec-timeout с параметрами 0 0, чтобы отключить проверкуистечения времени ожидания. Однако такой подход не считается безопасным.

R1(config)# lineconsole 0
R1(config-line)# password ciscoconpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login
R1(config-line)# logging synchronous

Настройте пароль для порта AUX для маршрутизатора R1.

R1(config)# line aux 0
R1(config-line)# password ciscoauxpass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login

c. Настройте пароль на линиях vty для маршрутизатора R1.

R1(config)# line vty 0 4
R1(config-line)# password ciscovtypass
R1(config-line)# exec-timeout 5 0
R1(config-line)# login

d. Зашифруйте пароли для консоли, aux и vty.

R1(config)# service password-encryption

e. Введите команду show run. Можете ли вы прочитать пароли для консоли, aux и vty? Поясните ответ.

_____
_____
_____
_____

Шаг 9: Настройте предупреждающий баннер при входе в систему на маршрутизаторах R1 и R3.

a. Настройте предупреждение для неавторизованных пользователей в виде баннера с ежедневнымсообщением (MOTD) с помощью команды bannermotd. При подключении пользователя к маршрутизатору

до запроса на ввод авторизационных данных отображается баннер MOTD. В данном примере в началеи конце сообщения используется знак доллара ($).

R1(config)# banner motd $Unauthorized access strictly prohibited!$
R1(config)# exit

b. Выйдите из привилегированного режима с помощью команды disable или exit, а затем нажмите Enter дляначала работы.
Если баннер отображается некорректно, создайте его заново с помощью команды banner-motd.
Шаг 10: Сохраните базовые конфигурации на всех маршрутизаторах.
Сохраните текущую конфигурацию в конфигурацию запуска через командную строку в привилегированномрежиме.
R1# copy running-config startup-config
Часть 2: Настройка локальной аутентификации
В части 2 данной лабораторной работы необходимо создать локальное имя пользователя и пароль, а такженастроить способ доступа к линиям консоли, aux и vty через локальную базу данных маршрутизатора, гденаходятся действительные имена пользователей и пароли. Выполните все шаги на маршрутизаторах R1 и R3.
Ниже показана процедура для маршрутизатора R1.
Шаг 1: Настройте локальную базу данных пользователей.
a. Создайте локальную учетную запись пользователя с паролем, зашифрованным по алгоритму хешированияMD5. Используйтеалгоритмхеширования type 9 (SCRYPT).
R1(config)# username user01 algorithm-type scrypt secret user01pass
b. Выйдите из режима глобальной настройки и отобразите текущую конфигурацию. Можете ли вы прочитать
пароль пользователя?

_____

Шаг 2: Настройте локальную аутентификацию для линии консоли и входа в систему.
a. Настройте линию консоли на использование локально определенных имен пользователей и паролей.
R1(config)# line console 0
R1(config-line)# login local
b. Перейдите к начальному экрану маршрутизатора, на котором будет отображаться:
R1 con0 is now available. Press RETURN to get started.
c. Войдите в систему с помощью ранее настроенной учетной записи user01 и пароля.
Чем сейчас отличается вход через консоль от того, что было раньше?

_____

d. После входа введите команду showrun. Вам удалось отправить команду? Поясните ответ.

_____

Войдите в привилегированный режим, используя команду enable. У вас был запрошен пароль? Поясните ответ
Шаг 3: Проверьте новую учетную запись путем входа в рамках сеанса Telnet.
a. Установите сеанс Telnet с маршрутизатором R1 с компьютера PC-A.
PC-A>telnet 192.168.1.1
b. Система запросила у вас учетные данные? Поясните ответ.

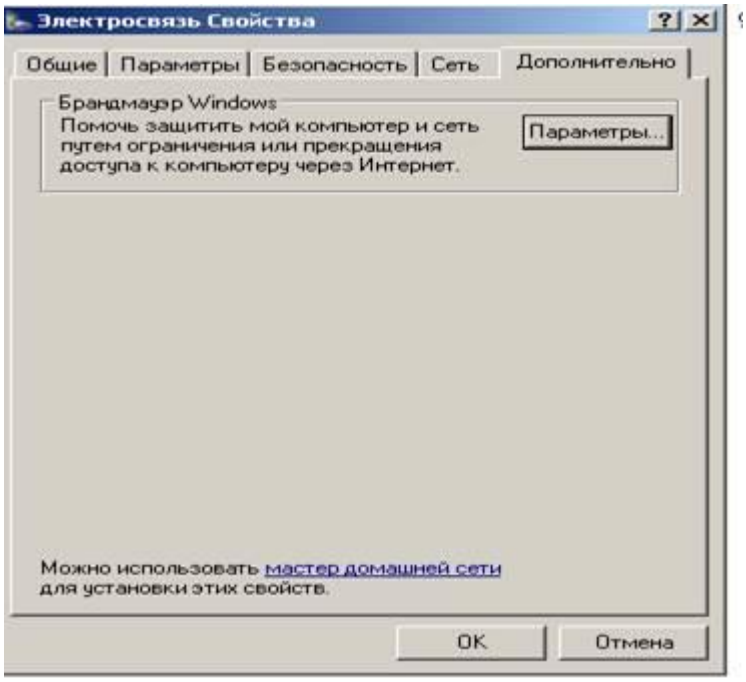
_____

c. Настройте линию vty на использование ранее локально определенных учетных записей и паролей
и сконфигурируйте команду transportinput, чтобы разрешить Telnet.
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input telnet
R1(config-line)# exit
d. Повторно свяжитесь с маршрутизатором R1 с компьютера PC-A с помощью Telnet.
PC-A>telnet 192.168.1.1
Система запросила у вас учетные данные? Поясните ответ.

e. Войдите в систему как пользователь user01 с паролем user01pass.
f. Во время сеанса Telnet с маршрутизатором R1 войдите в привилегированный режим с помощью команды enable.
Какой пароль вы использовали?

_____

Практическое задание:*Настройка политики безопасности брандмауэров*
Цель работы: Настройка встроенного межсетевого экрана (брандмауэра).
Краткие теоретические сведения:
Межсетевое экранирование повышает безопасность объектов внутренней сети за счет игнорирования неавторизованных запросов из внешней сети, тем самым обеспечивая все составляющие информационной безопасности. Кроме функций разграничения доступа, экранирование обеспечивает регистрацию информационных обменов.
Функции экранированиявыполняет **межсетевой экран или брандмауэр (firewall),** под которым понимают программную или программно-аппаратную систему, которая выполняет контроль информационных потоков, поступающих в систему и/или выходящих из неё, и обеспечивает защиту информационной системы посредством фильтрации информации. Фильтрация информации состоит в анализе информации по совокупности критериев и принятии решений о её приеме и/или передаче.
Брандмауэр в ОС Windows XP – это система защиты подключения к Интернет (Internet Connection Firewall, ICF), представляет собой программу настроек ограничений, регулирующих обмен данными между Интернетом и небольшой локальной сетью или локальным компьютером. Брандмауэр ICF необходимо установить для любого компьютера, подключенного к Интернету с помощью модема удаленного доступа, брандмауэр ICF обеспечивает защиту подключения.
Задание: активизировать встроенный брандмауэр операционной системы Windows XP и настроить его параметры.
Алгоритм выполнения работы:
А. Активизация встроенного сетевого экрана.
1. Откройте компонент Сетевые подключения.
2. Для этого наберите последовательно Пуск-Панель Управления- Сетевые подключения.
3. Выделите подключение удаленного доступа, подключение по локальной сети или высокоскоростное подключение к Интернету, которое требуется защитить брандмауэром, и затем выберите в контекстном меню (при выделенном подключении нажать правую клавишу мыши) команду Свойства.
4. На вкладке Дополнительно в группе Брандмауэр подключение к Интернету отметьте пункт Защитить моё подключение к Интернету. (рис 1.), отметьте пункт Включить.
Примечание: *Для отключения брандмауэра достаточно поставить флажок Выключить*.
В. **Настройка параметров брандмауэра.**
1. Выполните пункты 1-3 предыдущего задания.
2. Выберите кнопку Параметры в верхней части окна (рис.2).



2. В результате откроется окно Дополнительные параметры (рис. 3) с четырьмя закладками (параметры сетевого подключения, параметры по умолчанию, ведение журнала безопасности, протокол ICMP).

4. Выберите закладку Службы (рис. 4).

Примечание: На закладке службы Вы можете в явном виде указать службы Интернета, прохождение трафика, которых разрешено. Например, чтобы обеспечить прохождение web страниц из Интернета на компьютер, необходимо включить службу «Веб-сервер HTTP».

5. Отметьте все службы.

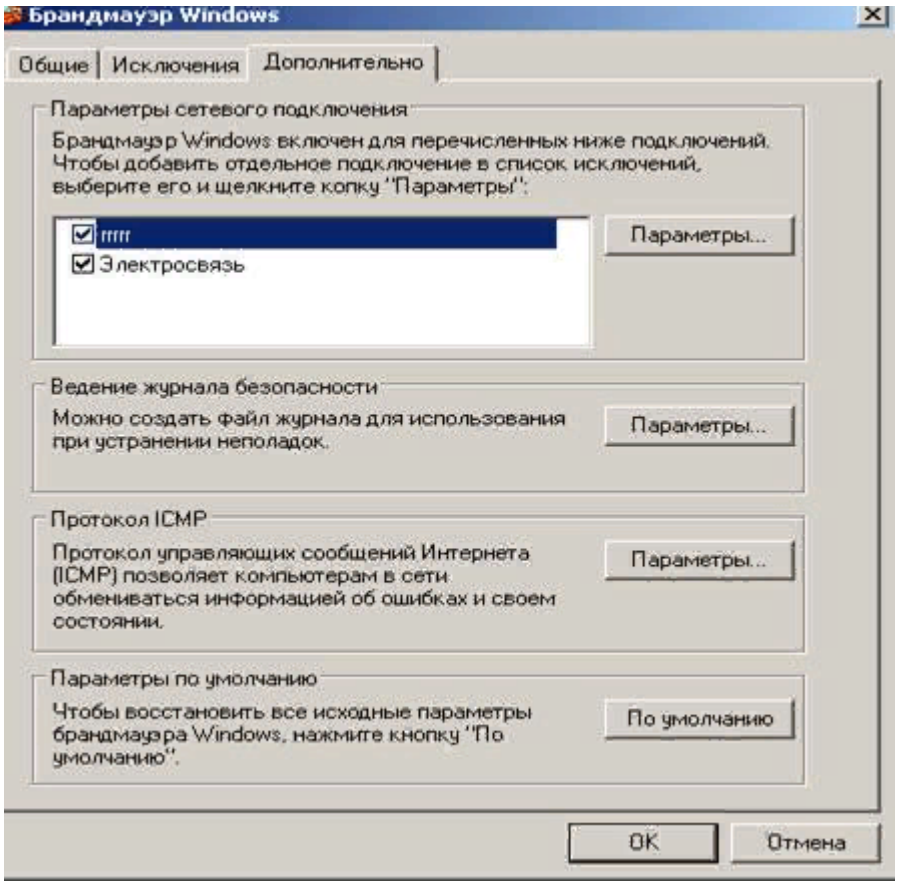
6. Выберите закладку Ведение журнала безопасности (рис. 5).

Примечание: Для брандмауэра подключение к Интернету предусмотрен журнал безопасности для записи событий, связанных с его работой. Журнал безопасности ICF поддерживает следующие возможности.

Запись пропущенных пакетов. Этот параметр задает запись в журнал сведений обо всех потерянных пакетах, исходящих из сети (компьютера) или из Интернета. Если установить флажок Записывать пропущенные пакеты, будут собираться сведения о каждом пакете, который пытается пройти через ICF, но был обнаружен и отвергнут брандмауэром.

Запись успешных подключений . Этот параметр задает запись в журнал сведений обо всех успешных подключениях, инициированных из сети (компьютера) или из Интернета.

7. Отметьте пункты Записывать пропущенные пакеты и Записывать успешные подключения. Обратите внимание на местоположение журнала безопасности.



Примечание: *Журнал безопасности брандмауэра состоит из двух разделов. В заголовке журнала содержатся сведения о версии журнала и полях, в которые можно записывать данные. Содержимое заголовка имеет вид статического списка. Содержимое журнала безопасности представляет собой откомпилированные данные, которые вводятся при обнаружении трафика, пытающегося пройти через брандмауэр. Поля журнала заполняются слева на право, как они расположены на странице. Для того чтобы в журнал вводились данные, необходимо выбрать хотя бы один параметр ведения журнала или оба параметра.*

8. Теперь Ваш брандмауэр настроен и готов к защите Вашего компьютера от внешних угроз.

Задание для самостоятельной работы:

1. Настройте брандмауэр для работы с Веб — сервером (HTTP), FTP-сервером и зафиксируйте соответствующее окно для отчета.
2. Включите журнал безопасности.
3. После выполнения задания 1 и 2 подключитесь и просмотрите какой либо ресурс на внутреннем FTP-сервере.
4. Завершите работу и просмотрите журнал безопасности.

Практическое задание:*Настройка системы предотвращения вторжений (IPS)*

Лабораторная работа

Задачи

Часть 1. Настройка базовых параметров маршрутизатора

 Настройте имена хостов, IP-адреса интерфейсов и пароли для доступа.

 Настройте статическую маршрутизацию.

Часть 2. Настройка IOS IPS с помощью CLI

 Настройте IOS IPS с помощью CLI.

 Измените сигнатуры IPS.

 Рассмотрите итоговую конфигурацию IPS.

 Проверьте работоспособность IPS.

 Запишите сообщения журнала IPS на сервер syslog.
Часть 3. Имитация атаки
 Используйте инструмент сканирования для моделирования атаки
Исходные данные/сценарий
В данной лабораторной работе необходимо настроить Cisco IOS IPS, которая является частью набора функционала
межсетевого экрана Cisco IOS. Система предотвращения вторжений (IPS) изучает конкретные шаблоны атак
и оповещает или противостоит подобным атакам, когда они случаются. Одной лишь системы IPS недостаточно
для того, чтобы превратить маршрутизатор в надежный межсетевой экран для Интернета, но совместно с другими
средствами безопасности организовать эффективную защиту можно.
Необходимо настроить IPS с помощью Cisco IOS CLI, а затем проверить работоспособность IPS. Вы загрузите
пакет сигнатур IPS с сервера TFTP и сконфигурируете открытый криптографический ключ с помощью Cisco IOS.
Примечание. В данной лабораторной работе используются команды и выходные данные для маршрутизатораCisco 1941 с ПО Cisco IOS версии 15.4(3)M2. Допускается использование других маршрутизаторов и версий
Cisco IOS. См. сводную таблицу по интерфейсам маршрутизаторов в конце этой лабораторной работы дляопределения идентификаторов интерфейсов с учетом оборудования в лаборатории. Доступные командыи выходные данные зависят от используемых моделей маршрутизаторов и версии Cisco IOS. Таким образом,
они могут отличаться от того, что представлено в данной лабораторной работе.
Примечание. Убедитесь, что маршрутизаторы и коммутаторы сброшены и не имеют конфигурацию запуска.
Необходимые ресурсы
 3 маршрутизатора (Cisco 1941 с образом Cisco IOS Release 15.4(3)M2)
 2 коммутатора (Cisco 2960 или аналогичный)
 2 ПК (Windows Vista или 7), сервер Tftpd32, Nmap/Zenmap, последняя версия Java, Internet Explorer и Flash Player)
 Последовательные кабели и кабели Ethernet, как показано на топологической схеме
 Консольные кабели для настройки сетевых устройств Cisco
 Пакет сигнатур IPS и файлы открытых криптографических ключей на компьютерах PC-A и PC-C
(предоставляются инструктором)
В части 1 вы создадите топологию сети и настроите основные параметры, такие как имена хостов, IP-адресаинтерфейсов, статическая маршрутизация, доступ к устройствам и пароли.Примечание. Выполните шаги, указанные в части 1, на всех трех маршрутизаторах. Ниже указана процедура
только для маршрутизатора R1.
Шаг 1: Подключите сетевые кабели, как показано на топологической схеме.
Присоедините устройства, как показано на топологической схеме, и установите необходимые кабельные соединения.
Шаг 2: Настройте основные параметры для каждого маршрутизатора.
a. Задайте имена хостов, как показано на топологической схеме.
b. Настройте IP-адреса интерфейсов, как показано в таблице IP-адресов.
c. Настройте тактовую частоту последовательных интерфейсов маршрутизатора с помощью последовательного
DCE-кабеля.
R1(config)# interface S0/0/0

R1(config-if)# clock rate 64000
d. Чтобы предотвратить попытки маршрутизатора неправильно интерпретировать введенные команды,
отключитефункцию DNS-поиска.
R1(config)# no ip domain-lookup
Шаг 3: Настройте статическую маршрутизацию на маршрутизаторах.
a. Настройте статический маршрут по умолчанию от маршрутизатора R1 к R2 и от маршрутизатора R3 к R2,используя адрес IPv4 следующего узла.
b. Настройте статический маршрут от маршрутизатора R2 к LAN R1 (192.168.1.0) и статический маршрутот маршрутизатора R2 к LAN R3 (192.168.3.0) с помощью подходящих адресов IPv4 следующего узла.
Шаг 4: Настройте параметры IP для хостов.
Настройте статический IP-адрес, маску подсети и шлюз по умолчанию для компьютеров PC-A и PC-C, как показанов таблице IP-адресов.
Шаг 5: Проверьте базовую связь по сети.
a. Отправьте эхо-запрос с маршрутизатора R1 на маршрутизатор R3.
Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем,как продолжить работу.
b. Отправьте эхо-запрос с компьютера PC-A в локальной сети маршрутизатора R1 на компьютер PC-Cв локальной сети маршрутизатора R3.
Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем,как продолжить работу
Шаг 6: Настройте учетную запись пользователя, шифрованные пароли и криптографическиеключи для SSH.
Примечание. В данной задаче установлена минимальная длина пароля в 10 символов, однако для облегченияпроцесса выполнения лабораторной работы пароли были относительно упрощены. В рабочих сетяхрекомендуется использовать более сложные пароли.
a. Используйте команду security passwords, чтобы задать минимальную длину пароля в 10 символов.
R1(config)# security passwords min-length 10
b. Настройтедоменноеимя.
R1(config)# ip domain-name ccnasecurity.com
c. Настройте криптографические ключи для SSH.
R1(config)# crypto key generate rsa general-keys modulus 1024
d. Создайте учетную запись пользователя admin01, используя algorithm-type scrypt для шифрования и парольcisco12345.
R1(config)# username admin01 algorithm-type scrypt secret cisco12345
e. Настройте линию 0 консоли на использование локальной базы данных пользователей для входа в систему.Для дополнительной безопасности команда exec-timeout обеспечивает выход из системы линии, еслив течение 5 минут отсутствует активность. Команда logging synchronous предотвращает прерывание вводакоманд сообщениями консоли.
Примечание. Чтобы исключить необходимость постоянного повторного входа в систему во времялабораторной работы, вы можете ввести команду exec-timeout с параметрами 0 0, чтобы отключить проверкуистечения времени ожидания. Однако такой подход не считается безопасным
R1(config)# lineconsole 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
R1(config-line)# logging synchronous
f. Настройте линию aux 0 на использование локальной базы данных пользователей для входа в систему.

R1(config)# line aux 0
R1(config-line)# login local
R1(config-line)# exec-timeout 5 0
g. Настройте линию vty 0 4 на использование локальной базы данных пользователей для входа в систему
и разрешите доступ только для соединений по SSH.
R1(config)# line vty 0 4
R1(config-line)# login local
R1(config-line)# transport input ssh
R1(config-line)# exec-timeout 5 0
h. Настройте пароль привилегированного доступа с надежным шифрованием.
R1(config)# enable algorithm-type scrypt secret class12345
Шаг 7: Сохраните основную текущую конфигурацию для каждого маршрутизатора.
Сохраните текущую конфигурацию в конфигурацию запуска в привилегированном режиме.
R1# copy running-config startup-config
Часть 2: Настройка IPS с помощью CiscoIOSCLI
В части 2 данной лабораторной работы вы настроите IPS на маршрутизаторе R1 с помощью CiscoIOSCLI. Затем
вы проверите итоговую конфигурацию.
Задача 1: Проверка доступа к сети LAN маршрутизатора R1 из R2
В этой задаче вы убедитесь, что без настройки IPS внешний маршрутизатор R2 может отправить эхо-запросна интерфейс S0/0/0 маршрутизатора R1 и компьютер PC-A во внутренней сети LAN маршрутизатора R1.
Шаг 1: Отправьте эхо-запрос с маршрутизатора R2 на R1.
С маршрутизатора R2 отправьте эхо-запрос на интерфейс S0/0/0 маршрутизатора R1 по IP-адресу 10.1.1.1.
R2# ping 10.1.1.1
Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем,как продолжить работу.
Шаг 2: Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A в локальной сети маршрутизатора R1.Отправьте эхо-запрос с маршрутизатора R2 на компьютер PC-A в локальной сети маршрутизатора R1
по IP-адресу 192.168.1.3.
R2# ping 192.168.1.3
Если запрос завершается с ошибкой, измените значения основных параметров устройства перед тем, какпродолжить работу.
Шаг 3: Отобразите текущую конфигурацию маршрутизатора R1 до настройки IPS.
Введите команду showrun для проверки текущей базовой конфигурации маршрутизатора R1.
Есть ли какие-то команды безопасности, относящиеся к IPS?

Задача 2: Подготовка маршрутизатора и сервера TFTP
Шаг 1: Убедитесь в наличии файлов CiscoIOSIPS
Для настройки Cisco IPS 5.x необходимо, чтобы на компьютере PC-A были доступны файл пакета сигнатур IOS IPSи файл открытых криптографических ключей. Если данных файлов нет на компьютере, обратитесь к инструктору.Файлы можно скачать с сайта www.cisco.com, используя действительную учетную запись пользователя после
успешной авторизации.
a. Убедитесь, что файл IOS-Sxxx-CLI.pkg находится в папке TFTP. Это пакет сигнатур. Буквами xxx в именифайла обозначается номер версии, который зависит от загруженного файла.

b. Убедитесь, что имеется файл realm-cisco.pub.key.txt, запомните его расположение на компьютере PC-A.
Это открытый криптографический ключ, используемый в IOS IPS.
Шаг 2: Проверьте или создайте каталог IPS во флеш-памяти маршрутизатора R1.
a. На данном шаге вы проверите наличие каталога или создадите каталог во флеш-памяти маршрутизатора,в котором будут храниться требуемые файлы сигнатур и конфигурации.
Примечание. Вы также можете использовать USB-накопитель, подключенный к USB-порту маршрутизатора,для хранения файлов сигнатур и конфигураций. USB-накопитель должен быть постоянно подключен к указанному порту маршрутизатора, если он используется в качестве хранилища для конфигурации IOS IPS. IOS IPS
также поддерживает любую файловую систему Cisco IOS в качестве места хранения конфигурациис соответствующим доступом на запись.
Из командной строки маршрутизатора R1 отобразите содержимое флеш-памяти с помощью командыshow flash и проверьте наличие каталога ipsdir.
R1# show flash
c. Если каталог ipsdir отсутствует, создайте его в привилегированном режиме.
R1# mkdir ipsdir
Create directory filename [ipsdir]? <Enter>
Created dir flash:ipsdir
d. Если каталог уже существует, появится следующее сообщение:
%Error Creating dir flash:ipsdir (Can't create a file that exists)
Используйте команду delete для удаления содержимого каталога ipsdir.
R1# delete flash:ipsdir/*
Delete filename [/ipsdir/*]?
Delete flash:/ipsdir/R1-sigdef-default.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-delta.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-typedef.xml? [confirm]
Delete flash:/ipsdir/R1-sigdef-category.xml? [confirm]
Delete flash:/ipsdir/R1-seap-delta.xml? [confirm]
Delete flash:/ipsdir/R1-seap-typedef.xml? [confirm]
Примечание. Используйте данную команду с осторожностью. Если каталог ipsdir пуст, появится следующеесообщение:
R1# delete flash:ipsdir/*
Delete filename [/ipsdir/*]?
No such file
e. СпомощьюCLI маршрутизатора R1 убедитесь, что каталог существует. Используйте команду dir flash: или
dir flash:ipsdir.
R1# dir flash:
Directory of flash:/
1 -rw- 75551300 Feb 16 2015 01:53:10 +00:00 c1900-univeralk9-mz.SPA.154-3.M2.bin
2 drw- 0 Mar 8 2015 12:38:14 +00:00 ipsdir
или
R1# dir flash:ipsdir
Directory of flash:/ipsdir/
No files in directory
Примечание. Каталог существует, но в нем на данный момент отсутствуют файлы.
Задача 3: Настройка криптографического ключа IPSКриптографический ключ проверяет цифровую подпись для главного файла сигнатур (sigdef-default.xml).
Содержимое подписывается с помощью закрытого ключа Cisco, чтобы гарантировать подлинность и целостностьпри каждом выпуске.
Шаг 1: Скопируйте файл криптографических ключей на маршрутизатор R1.

В режиме глобальной настройки выберите и скопируйте файл криптографического ключа с именем
realm-cisco.pub.key.txt.
crypto key pubkey-chain rsa
named-key realm-cisco.pub signature
 key-string
 30820122 300D0609 2A864886 F70D0101 01050003 82010F00 3082010A 02820101
 00C19E93 A8AF124A D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
 17E630D5 C02AC252 912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
 B199ABCB D34ED0F9 085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
 5B2146A9 D7A5EDE3 0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
 FE3F0C87 89BCB7BB 994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
 50437722 FFBE85B9 5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
 006CF498 079F88F8 A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
 2F56D826 8918EF3C 80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
F3020301 0001
 quit
Шаг 2: Примените содержимое текстового файла на маршрутизаторе.
a. В привилегированном режиме на маршрутизаторе R1 войдите в режим глобальной настройки с помощью
команды conf t.
b. Вставьте содержимое криптографического ключа в запросе режима глобальной настройки.
R1(config)#
R1(config)# crypto key pubkey-chain rsa
R1(config-pubkey-chain)# named-key realm-cisco.pub signature
R1(config-pubkey-key)# key-string
Enter a public key as a hexidecimal number ....
R1(config-pubkey)#$2A864886 F70D0101 01050003 82010F00 3082010A 02820101
R1(config-pubkey)#$D6CC7A24 5097A975 206BE3A2 06FBA13F 6F12CB5B 4E441F16
R1(config-pubkey)#$912BE27F 37FDD9C8 11FC7AF7 DCDD81D9 43CDABC3 6007D128
R1(config-pubkey)#$085FADC1 359C189E F30AF10A C0EFB624 7E0764BF 3E53053E
R1(config-pubkey)#$0298AF03 DED7A5B8 9479039D 20F30663 9AC64B93 C0112A35
R1(config-pubkey)#$994AE74C FA9E481D F65875D6 85EAF974 6D9CC8E3 F0B08B85
R1(config-pubkey)#$5E4189FF CC189CB9 69C46F9C A84DFBA5 7A0AF99E AD768C36
R1(config-pubkey)#$A3B3FB1F 9FB7B3CB 5539E1D1 9693CCBB 551F78D2 892356AE
R1(config-pubkey)#$80CA4F4D 87BFCA3B BFF668E9 689782A5 CF31CB6E B4B094D3
R1(config-pubkey)# F3020301 0001
R1(config-pubkey)# quit
R1(config-pubkey-key)#
c. Выйдите из режима глобальной настройки и введите команду show run, чтобы убедиться, что криптографический
ключ настроен
Задача 4: Настройка IPS
Шаг 1: Создайте правило IPS.
a. На маршрутизаторе R1 создайте имя правила IPS с помощью команды ip ips name name в режиме глобальной
настройки. Присвойте правилу IPS имя iosips. Оно будет использовано в дальнейшем на интерфейсе для
включения IPS.
R1(config)# ip ips name iosips

b. Вы можете по выбору указать либо расширенный, либо стандартный список контроля доступа (ACL) для
фильтрации трафика, который будет сканироваться правилом с этим именем. Весь трафик, разрешенный
списком ACL, будет инспектироваться системой IPS. Трафик, отклоняемый списком ACL, системой IPS
инспектироваться не будет.
c. Чтобы посмотреть варианты указания списка ACL с помощью имени правила, используйте команду ip ips name
ифункциюсправки CLI (?).
R1(config)# ip ips name ips list ?
<1-199> Numbered access list
WORD Named access list
Шаг 2: Укажите местоположение хранилища сигнатур IPS во флеш-памяти маршрутизатора.
Файлы IPS будут храниться в каталоге ipsdir, созданном в задаче 2, часть 2. Укажите его местоположение
с помощью команды ip ips config location.
R1(config)# ip ips config location flash:ipsdir
Шаг 3: Включите уведомление о событиях IPS SDEE.
Сервер Cisco Security Device Event Exchange (SDEE) построеннаосновепротокола Simple Object Access Protocol
(SOAP), спецификации формата оповещений IDS и транспортных протоколов. SDEE заменяет Cisco RDEP.
Для использования SDEE необходимо включить HTTP-сервер с помощью команды ip http server. Если HTTP-сервер
не включен, маршрутизатор не сможет отвечать клиентам SDEE, так как он не увидит запросы. Уведомления SDEE
по умолчанию отключены и должны быть явно включены.
R1(config)# ip http server
Для включения SDEE используйте следующую команду:
R1(config)# ip ips notify sdee
Шаг 4: Включите поддержку Syslog для IPS.
Система IOS IPS также поддерживает использование Syslog для отправки уведомлений. SDEE и Syslog могут
использоваться независимо друг от друга или работать одновременно для отправки уведомлений о событиях IOS
IPS. Функция уведомлений Syslog включена по умолчанию.
a. Если ведение журнала для консоли включено, отображаются сообщения журнала IPS Syslog. Если Syslog
не включен, включите его.
R1(config)# ip ips notify log
b. С помощью команды show clock проверьте текущее время и дату для маршрутизатора. При необходимости
сбросьте часы с помощью команды clock set в привилегированном режиме. В следующем примере показано,как установить время.
R1# clock set 01:20:00 8 march 2015
c. Убедитесь, что на маршрутизаторе включен сервис временных меток для ведения журналов с помощьюкоманды show run. Если сервис временных меток не включен, включите его.
R1(config)# servicetimestampslogdatetimemsec

Для отправки журнальных сообщений на сервер Syslog на компьютере PC-A используйте следующую команду:
R1(config)# logging 192.168.1.3
e. С помощью команды showlogging определите тип и уровень ведения журнала на маршрутизаторе R1.
R1# showlogging
Примечание. Проверьте наличие связи между маршрутизатором R1 и компьютером PC-A с помощью эхо-запроса
с PC-A на IP-адрес 192.168.1.1 интерфейса Fa0/1 на R1. Если это сделать не удается, устраните проблему передтем, как продолжить.
Ниже показано, как скачать один из бесплатных серверов syslog, если он не установлен на компьютере PC-A.
Шаг 5: (Необязательно) Скачайте и запустите сервер syslog.
Если сервер syslog в данный момент на компьютере PC-A отсутствует, вы можете скачать Tftpd32 с сайтаhttp://tftpd32.jounin.net. Если сервер syslog имеется на ПК, перейдите к шагу 6.
Запустите ПО сервера syslog на компьютере PC-A, чтобы отправлять на него журнальные сообщения.
Шаг 6: Настройка IOSIPS на использование одной из предварительно заданных категорий сигнатур.
IOSIPS с сигнатурами в формате Cisco 5.x работает с категориями сигнатур так же, как это выполняют другиеустройства CiscoIPS. Все сигнатуры предварительно разбиты по категориям, а сами категории имеют иерархическую структуру. Это позволяет классифицировать сигнатуры для более простой настройки и группирования.Предупреждение. Категория сигнатур all содержит все сигнатуры в выпуске сигнатур. Не возвращайтев использование категорию all, так как IOSIPS не сможет одновременно компилировать и использовать всесигнатуры в выпуске. Маршрутизатору не хватит на это памяти.
Примечание. При настройке IOSIPS необходимо сначала вывести из использования все сигнатуры в категории
all, а затем вернуть в использование выбранные категории сигнатур.
В следующем примере все сигнатуры категории all выведены из использования, а затем введена в использованиекатегория ios_ipsbasic.
R1(config)# ip ips signature-category
R1(config-ips-category)# category all
R1(config-ips-category-action)# retired true
R1(config-ips-category-action)# exit
R1(config-ips-category)# category ios_ips basic
R1(config-ips-category-action)# retired false
R1(config-ips-category-action)# exit
R1(config-ips-category)# exit
Do you want to accept these changes? [confirm] <Enter>
Jan 6 01:32:37.983: Applying Category configuration to signatures ...
Шаг 7: Примените к интерфейсу правило IPS.
a. Примените к интерфейсу правило IPS с помощью команды ipipsnamedirection в режиме настройки
интерфейса. Примените только что созданное правило для входящего трафика на интерфейсе S0/0/0.
После включения IPS некоторые журнальные сообщения будут отправлены на линию консоли. Этоозначает, что в механизмах IPS выполняется инициализация.
Примечание. Направление in означает, что система IPS проверяет только трафик, входящий на интерфейс.Аналогичным образом, направление out означает только трафик,

исходящий из интерфейса. Чтобы IPSпроверял входящий и исходящий трафик, введите имя правила IPS отдельно для направлений in и outна интерфейсе.
R1(config)# interface serial0/0/0
R1(config-if)# ip ips iosips in
Jan 6 03:03:30.495: %IPS-6-ENGINE_BUILDS_STARTED: 03:03:30 UTC Jan 6 2008
Jan 6 03:03:30.495: %IPS-6-ENGINE_BUILDING: atomic-ip - 3 signatures - 1 of 13 engines
Jan 6 03:03:30.511: %IPS-6-ENGINE_READY: atomic-ip - build time 16 ms – packets for this enginewill be scanned
Jan 6 03:03:30.511: %IPS-6-ALL_ENGINE_BUILDS_COMPLETE: elapsed time 16 ms
Это сообщение также появится на сервере syslog, если он включен. Ниже показаны сообщения сервера
syslog Tftpd32.
Примечание. Это сообщение может появиться только в том случае, если на маршрутизаторе нет встроенного
файласигнатур IOS.
****
The signature package is missing or was saved by a previous version
IPS Please load a new signature package
****
Jan 6 01:22:17.383: %IPS-3-SIG_UPDATE_REQUIRED: IOS IPS requires a signature update package
to be loaded

Практическое задание:*Настройка безопасности на втором уровне на коммутаторах*

Практическое задание:*Исследование методов шифрования*

Тестовые задания

1. Обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней:
а) шифрование +
б) зашифровка
в) закрытость

2. Сколько лет назад появилось шифрование:
а) три тысячи лет назад
б) четыре тысячи лет назад +
в) шесть тысяч лет назад

3. Первое известное применение шифра:
а) индийский текст
б) русский текст
в) египетский текст +
4. Какое ещё определение можно дать шифрованию:
а) преобразовательный процесс исходного текста в зашифрованный +
б) упорядоченный набор из элементов алфавита
в) неупорядоченный набор из элементов алфавита

5. Что такое дешифрование:
а) пароли для доступа к сетевым ресурсам
б) сертификаты для доступа к сетевым ресурсам и зашифрованным данным на самом

компьютере
в) на основе ключа шифрованный текст преобразуется в исходный +

6. Пользователи являются авторизованными, если они обладают определённым:
а) математическим ключом
б) аутентичным ключом +
в) паролем

7. Одно из составляющих шифрования:
а) перешифровка
б) запечатывание
в) зашифровывание +

8. Одно из составляющих шифрования:
а) расшифровывание +
б) распечатывание
в) перешифрование

9. Одно из состояний безопасности информации:
а) доступность
б) открытость
в) конфиденциальность +

10. Одно из состояний безопасности информации:
а) раздробленность
б) целостность +
в) частичность

11. Одно из состояний безопасности информации:
а) идентифицируемость +
б) инкогнито
в) доступность

12. Шифрование, которое используется для скрытия информации от неавторизованных пользователей при передаче или при хранении:
а) идентифицируемость
б) конфиденциальность +
в) целостность

13. Шифрование, которое используется для предотвращения изменения информации при передаче или хранении:
а) целостность +
б) конфиденциальность
в) идентифицируемость
14. Шифрование используется для аутентификации источника информации и предотвращения отказа отправителя информации от того факта, что данные были отправлены именно им:
а) конфиденциальность
б) целостность
в) идентифицируемость +

15. Для того чтобы прочитать зашифрованную информацию, принимающей стороне необходим:
а) ключ +
б) замок
в) подсказки

16. Для того чтобы прочитать зашифрованную информацию, принимающей стороне необходим:
а) подсказки
б) дешифратор +
в) расшифрователь

17. Перед отправлением данных по линии связи или перед помещением на хранение они подвергаются:
а) идентифицируемости
б) расшифровыванию
в) зашифровыванию +

18. Пара алгоритмов, реализующих каждое из указанных преобразований:
а) код
б) шифр +
в) загадка

19. Свойство криптографического шифра противостоять криптоанализу, то есть анализу, направленному на изучение шифра с целью его дешифрования:
а) криптографическая доступность
б) криптографическая мягкость
в) криптографическая стойкость +

20. Что такое пространство ключей k:
а) длина ключа
б) набор возможных значений ключа +
в) размер ключа

21. Количество используемых ключей в симметричных криптосистемах для шифрования и дешифрования:
а) 1 +
б) 2
в) 3

Практическое задание:*Настройка Site-to-SiteVPN используя интерфейс командной строки*

Практическое задание:*Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя интерфейс командной строки*

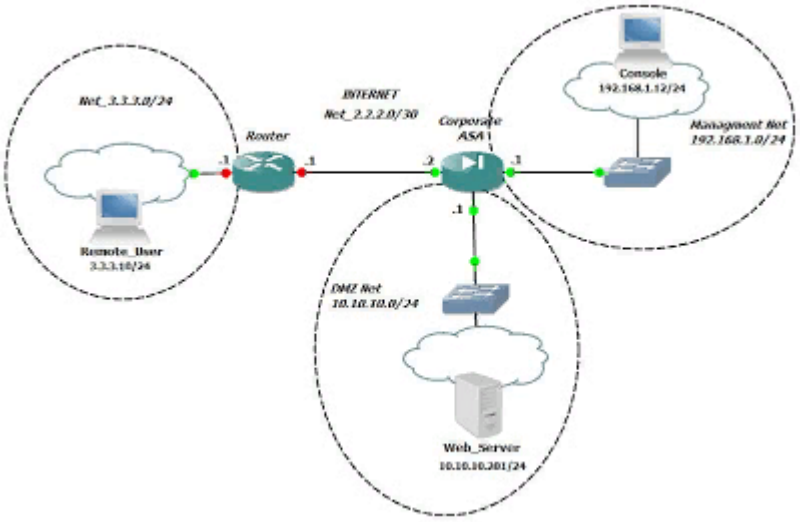
Практическое задание:*Базовая настройка шлюза безопасности ASA и настройка брандмауэров используя ASDM*

Практическое задание:*Настройка Site-to-SiteVPN с одной стороны на маршрутизаторе используя интерфейс командной строки и с другой стороны используя шлюз безопасности ASA посредством ASDM*

Практическое задание: *НастройкаClientlessRemoteAccessSSLVPNs используя ASDM*
Лабораторная работа
Цель: НастройкаClientlessRemoteAccessSSLVPNs используя ASDM
Существует 3 (три) способа организации SSL VPN:

- 1. **Clientless SSL VPN** – удаленному клиенту требуется всего лишь наличие Web – браузера с включенной поддержкой SSL. Обеспечивается доступ к внутреннему Web – серверу (http, https), просмотр файлов посредством Common Internet File System (CIFS), доступ через Outlook Web Access (OWA) client, подключение к ftp – серверу.
- 2. **Thin-Client SSL VPN (Port Forwarding)** – удаленный клиент должен скачать специальный Java-апплет для доступа определенных TCP приложений которые используют статические порты (UDP не поддерживается). Примером могут быть POP3, SMTP, IMAP, SSH, и Telnet. Стоит отметить, что данный метод не подойдет для приложений, которые используют динамическое определение порта.
- 3. **SSL VPN Client (SVC-Tunnel Mode)** – удаленный клиент должен скачать специальное клиентское приложение на свой PC. Данный метод обеспечивает полный доступ к внутренним корпоративным ресурсам.

Пойдем по порядку и рассмотрим первый вариант. Если пост будет получаться объемный, то я разобью его на части. В общем, будет видно по ходу :).
Для ориентировки, будем собирать вот такую схему:



Небольшие пояснения к схеме. Существует сеть для администраторов (192.168.1.0/24) и сеть для серверов (10.10.10.0/24) на границе которых находится cisco ASA. В сети DMZ стоит Web – сервер (Web_Server), консоль (Console) для конфигурирования cisco ASA находится в сети Menegment. Имеется сеть INTERNET (2.2.2.0/30) и удаленный клиент (Remote_User 3.3.3.10/24), который выходит «в свет» через NAT (как обычно и бывает :)).
От нас требуется настроить SSL VPN (Web VPN) между удаленным клиентом и cisco ASA, для организации доступа к корпоративному Web – серверу по HTTP.
Для начала давайте настроим базовую сетевую доступность между всеми устройствами.
Итак, начнем с роутера (Router).

- R1>en

R1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#hostname ROUTER
ROUTER(config)#int fa 0/0

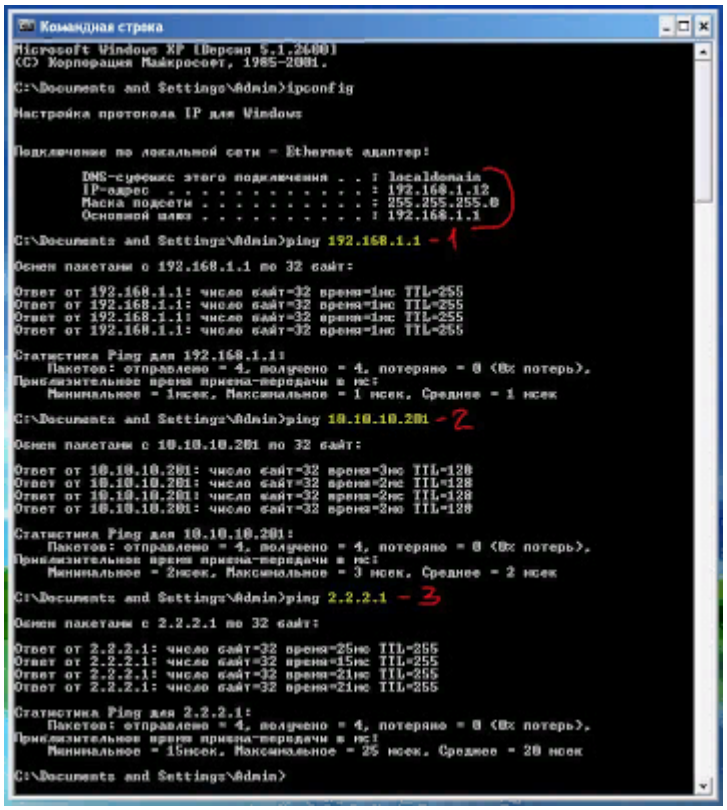
```
ROUTER(config-if)#ip address 2.2.2.1 255.255.255.252
ROUTER(config-if)#ip nat outside
ROUTER(config-if)#no shutdown
ROUTER(config-if)#exit
ROUTER(config)#int fa 0/0
ROUTER(config)#int fa 0/1
ROUTER(config-if)#ip address 3.3.3.1 255.255.255.252
ROUTER(config-if)#ip nat inside
ROUTER(config-if)#no shutdown
ROUTER(config-if)#exit
ROUTER(config)#ip access-list extended FOR_NAT
ROUTER(config-ext-nacl)#permit ip 3.3.3.0 0.0.0.255 any
ROUTER(config-ext-nacl)#exit
ROUTER(config)#ip nat inside source list FOR_NAT interface fa 0/0
ROUTER(config)#exit
ROUTER#wr
ROUTER#
```

Теперь перейдем на ASA и сделаем настройки на ней:

- ASA> en

```
Password:
ASA#conf t
ASA(config)# command-alias exec wr copy run disk0:/.private/startup-config
ASA(config)# hostname ASA
ASA(config)# enable password cisco
ASA(config)# username admin password ciscocisco privilege 15
ASA(config)# int ethernet 0/0
ASA(config-if)# ip address 2.2.2.2 255.255.255.252
ASA(config-if)# nameif outside
ASA(config-if)# no shutdown
INFO: Security level for "outside" set to 0 by default.
ASA(config-if)# exit
ASA(config)# int ethernet 0/1
ASA(config-if)# ip address 192.168.1.1 255.255.255.0
ASA(config-if)# nameif inside
INFO: Security level for "inside" set to 100 by default.
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# int ethernet 0/2
ASA(config-if)# nameif dmz
ASA(config-if)# security-level 50
ASA(config-if)# ip address 10.10.10.1 255.255.255.0
ASA(config-if)# no shutdown
ASA(config-if)# exit
ASA(config)# http server enable
ASA(config)# http 192.168.1.0 255.255.255.0 inside
ASA(config)# route outside 0.0.0.0 0.0.0.0 2.2.2.1
ASA(config)# access-list ADMIN extended permit ip 192.168.1.0 255.255.255.0 any
ASA(config)# access-group ADMIN in interface inside
ASA(config)#wr
ASA(config)# access-list FOR_NAT extended permit ip 192.168.1.0 255.255.255.0 any
ASA(config)# access-list NO_NAT extended permit ip 192.168.1.0 255.255.255.0 10.10.10.0
```

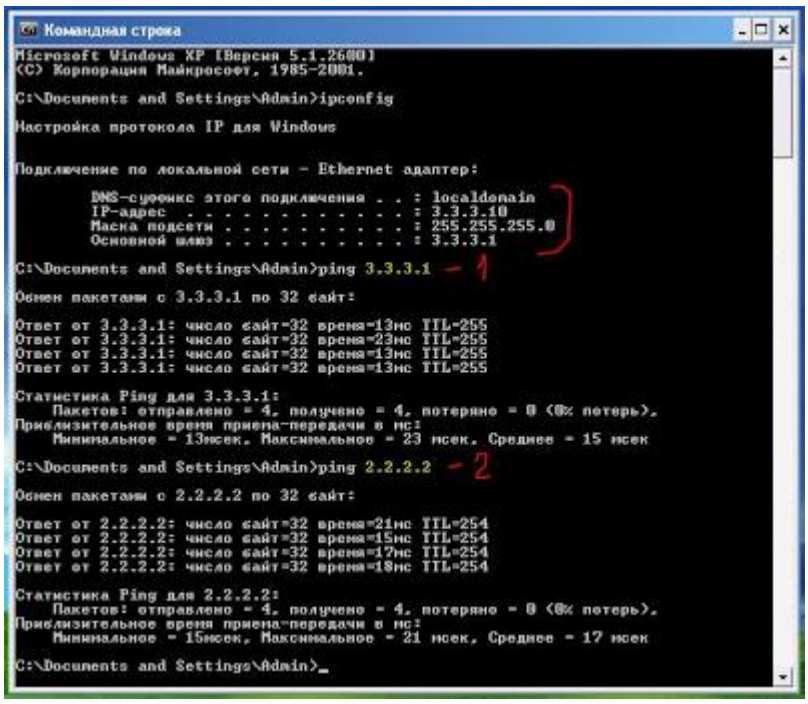
255.255.255.0
ASA(config)# nat (inside) 0 access-list NO_NAT
ASA(config)# nat (inside) 1 access-list FOR_NAT
ASA(config)# global (outside) 1 interface
INFO: outside interface address added to PAT pool
ASA(config)#wr
ASA(config)#exit
ASA#
Для начала нам хватит. Проверим сетевую доступность.
Console:



где:

- 1 – inside интерфейс ASA;
- 2 – внутренний Web-server;
- 3 – «интернет» IP – адрес роутера.

Remote_User:

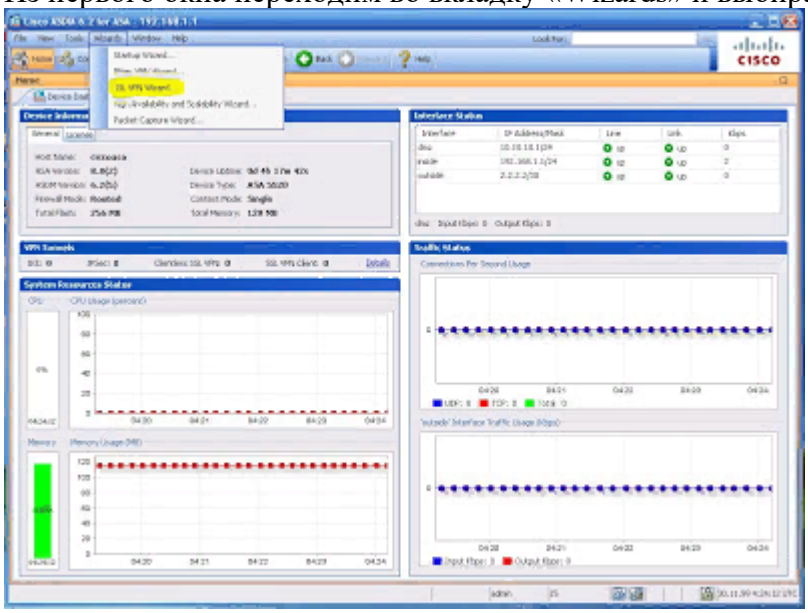


где:

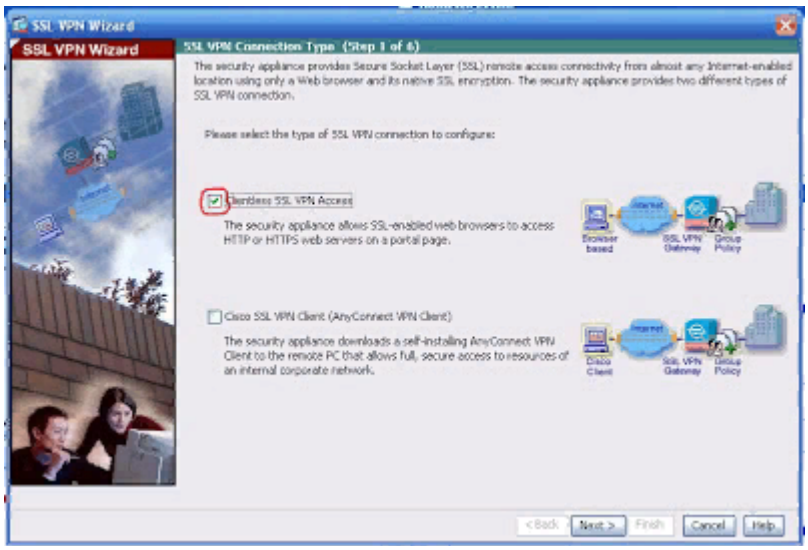
- 1 – шлюз по умолчанию (Router);
- 2 – outside интерфейс ASA.

Теперь загружаем asdm на cisco ASA и затем запускаем его. Кто не знает, как это сделать, можно посмотреть вот тут.

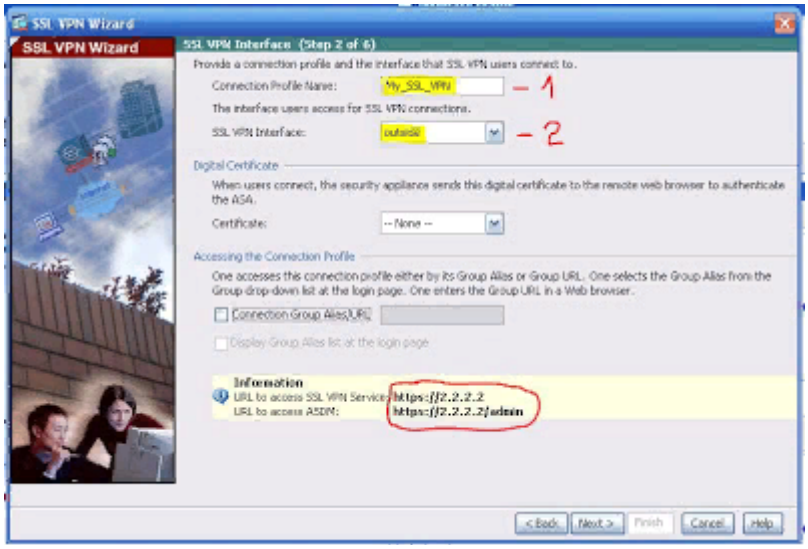
Из первого окна переходим во вкладку «Wizards» и выбираем «SSL VPN Wizard»:



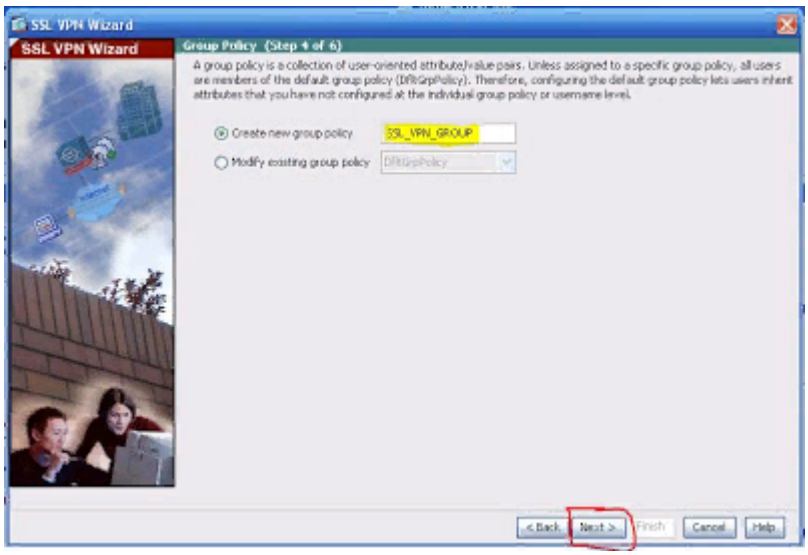
Откроется окно «Wizard»-а:



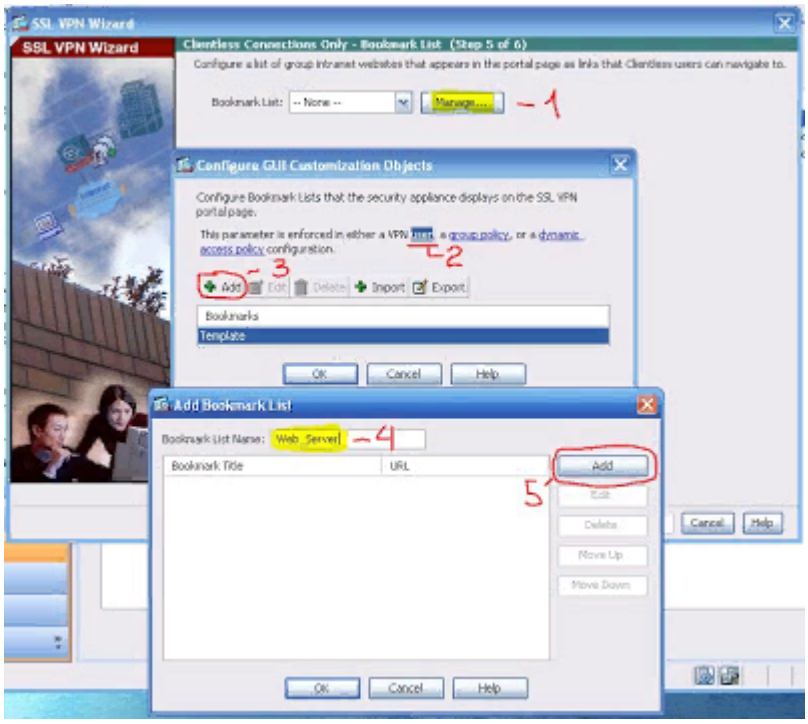
Выбираем первый пункт («Clientless SSL VPN Access») и нажимаем далее:



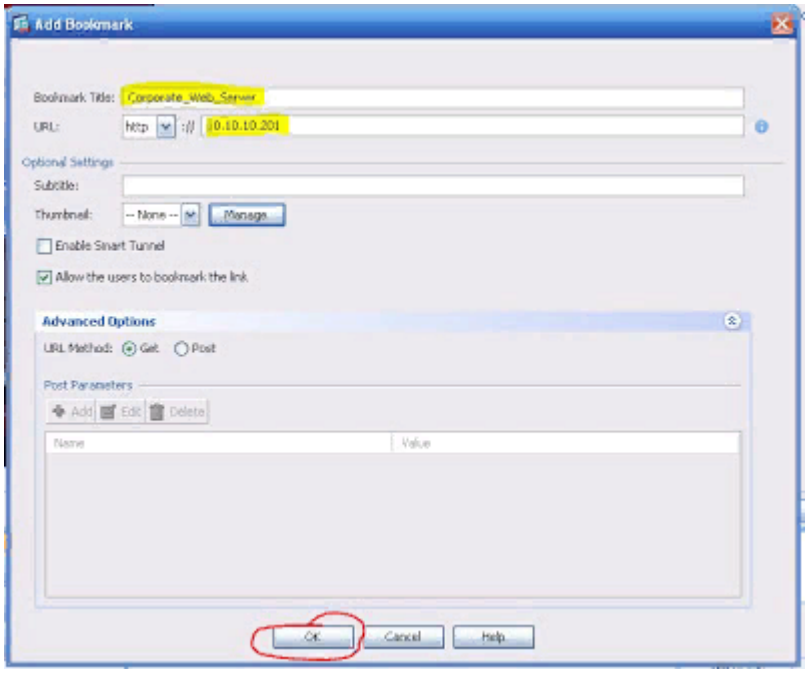
Здесь создаем новый Profile для нашего соединения. Задаем ему имя (1) и указываем, на какой интерфейс будут приходить запросы на установление SSL VPN от пользователей (2). Цифровые сертификаты мы не используем пока, так что оставляем поле пустым. Внизу видно, на какие адреса должны приходить пользователи для SSL VPN сервисов и для доступа к ASDM. Нажимаем «Next»:



Здесь создадим новую групповую политику для наших SSL VPN пользователей. Нажимаем «Next»:

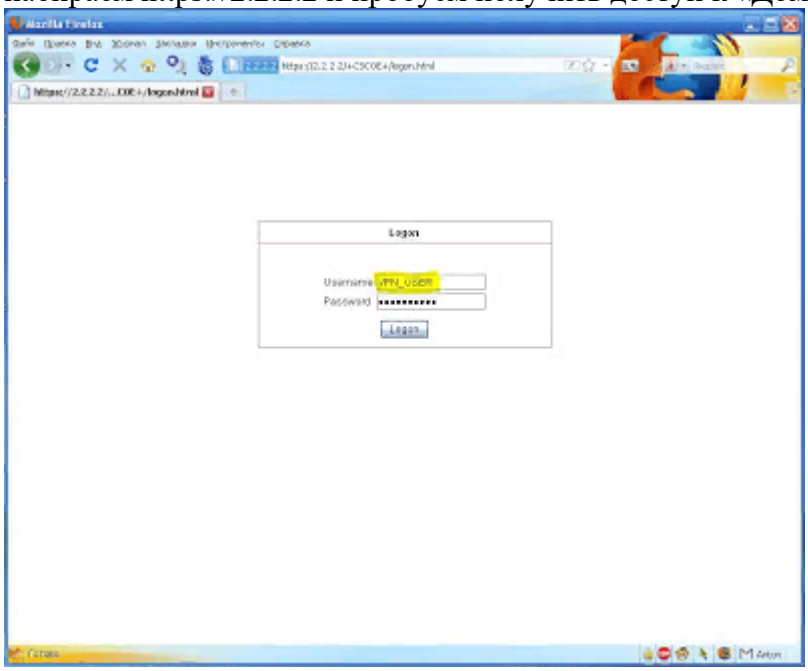


Итак, здесь нам нужно указать список серверов, которые будут показаны на странице web-браузера клиента в виде ссылок, и к которым он будет иметь доступ. Нажимаем «Manage» (1). Откроется небольшое окошко (по центру). В нем мы можем назначить, кому показывать этот список. Либо чисто конкретному юзеру, либо всей группе и так далее. Оставляем юзера (2) и нажимаем «Add» (3). Появится следующее окно. Тут задаем имя (4) и нажимаем «Add» (5). Появится следующее окно:

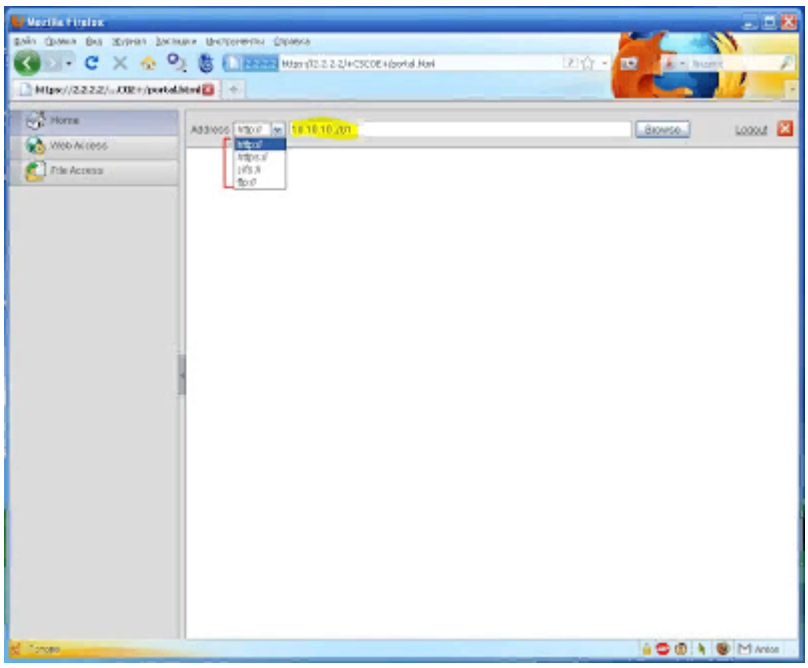


Здесь снова пишем название сервера и указываем его IP – адрес. Далее все время нажимаем «OK». На последнем окне нажимаем «Next»:

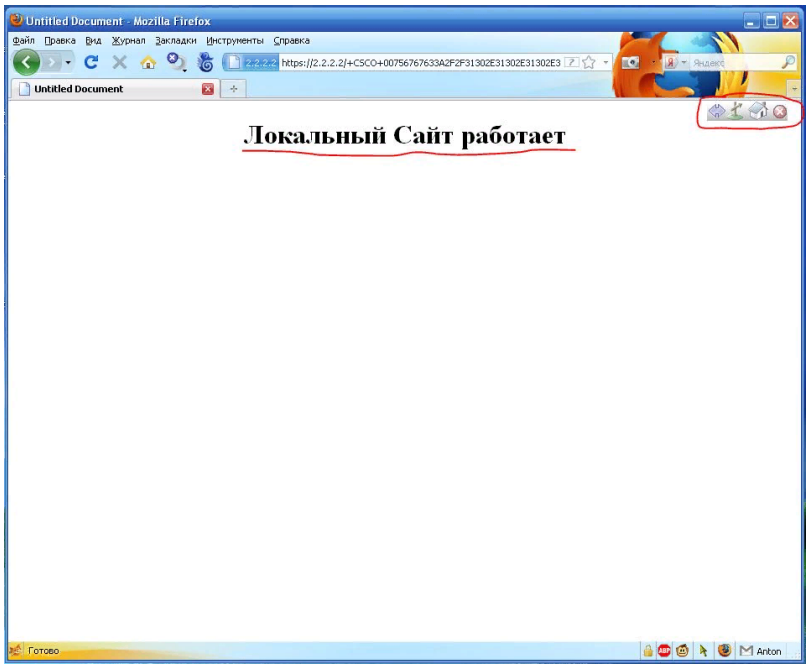
Нажимаем «Finish». Если вы используете GNS3 и у вас появились ошибки, то не пугайтесь. Это связано с тем, что созданный ранее список ссылок на сервер (Bookmark List) не может записаться в память. На реальном оборудовании этого не должно быть. Итак, переходим на нашего Remote_User-a (3.3.3.10/24), открываем Web-браузер, набираем https://2.2.2.2 и пробуем получить доступ к «Домашней страничке ASA»:



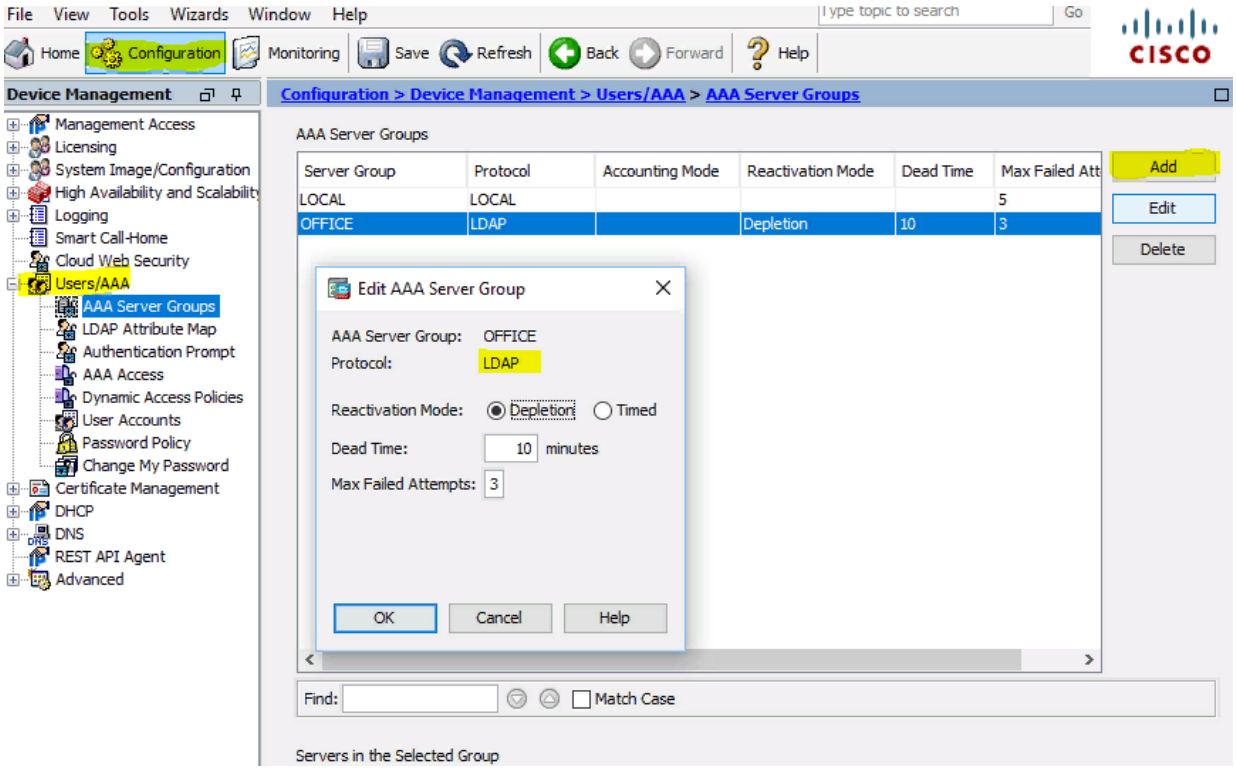
После добавления сайта в доверенные и получения сертификата (https) выскочит окно для ввода логина и пароля. Вводим наш username и password, который мы создавали ранее. Нажимаем «Login»:



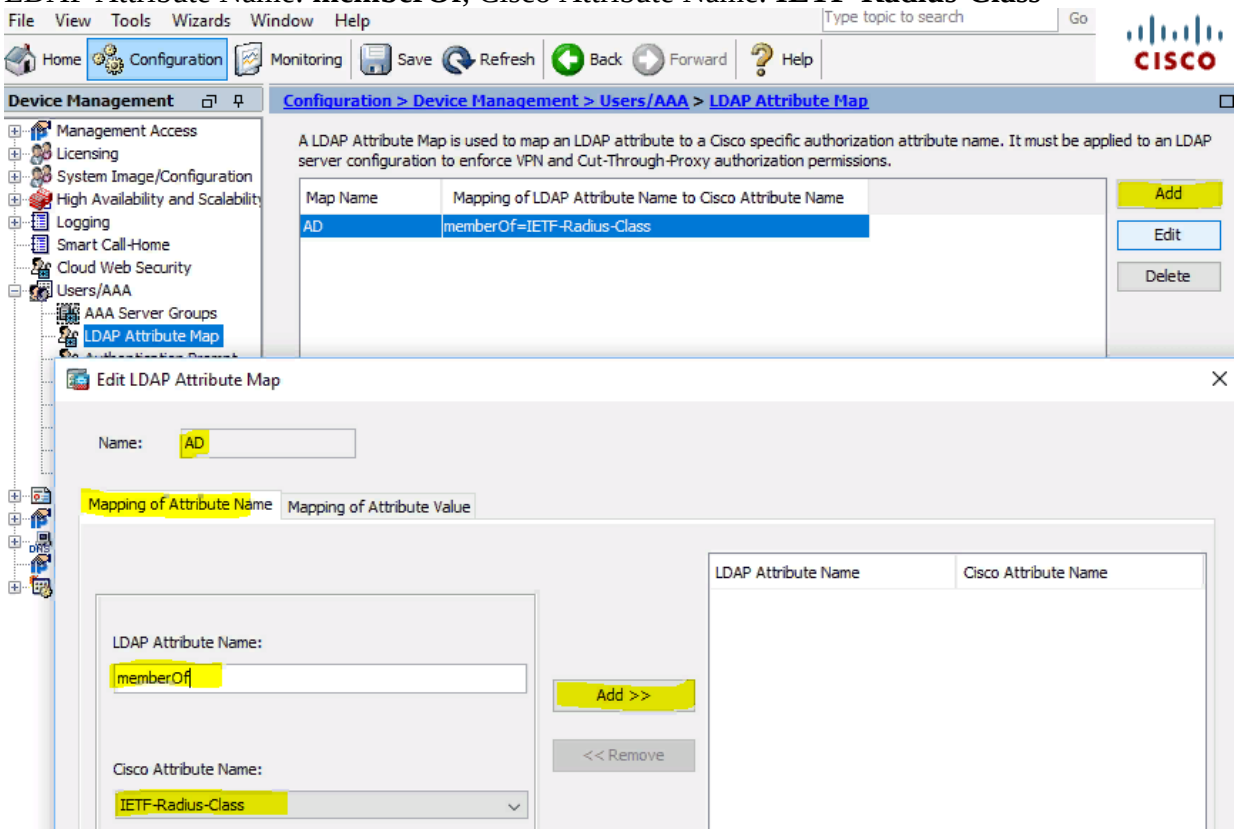
Появится главное окно (так называемый Portal). Слева не хитрое меню. Чуть правее мы можем выбрать то, что и каким образом нам делать. Либо открыть страницу по http, либо по https, либо залезть на ftp сервер. Так как у меня есть и http – сервер и ftp – сервер, то посмотрим и то и другое. Выбираем http из выпадающего меню и указываем IP-адрес сервера. Нажимаем «Browse». Вот, что мы получаем:



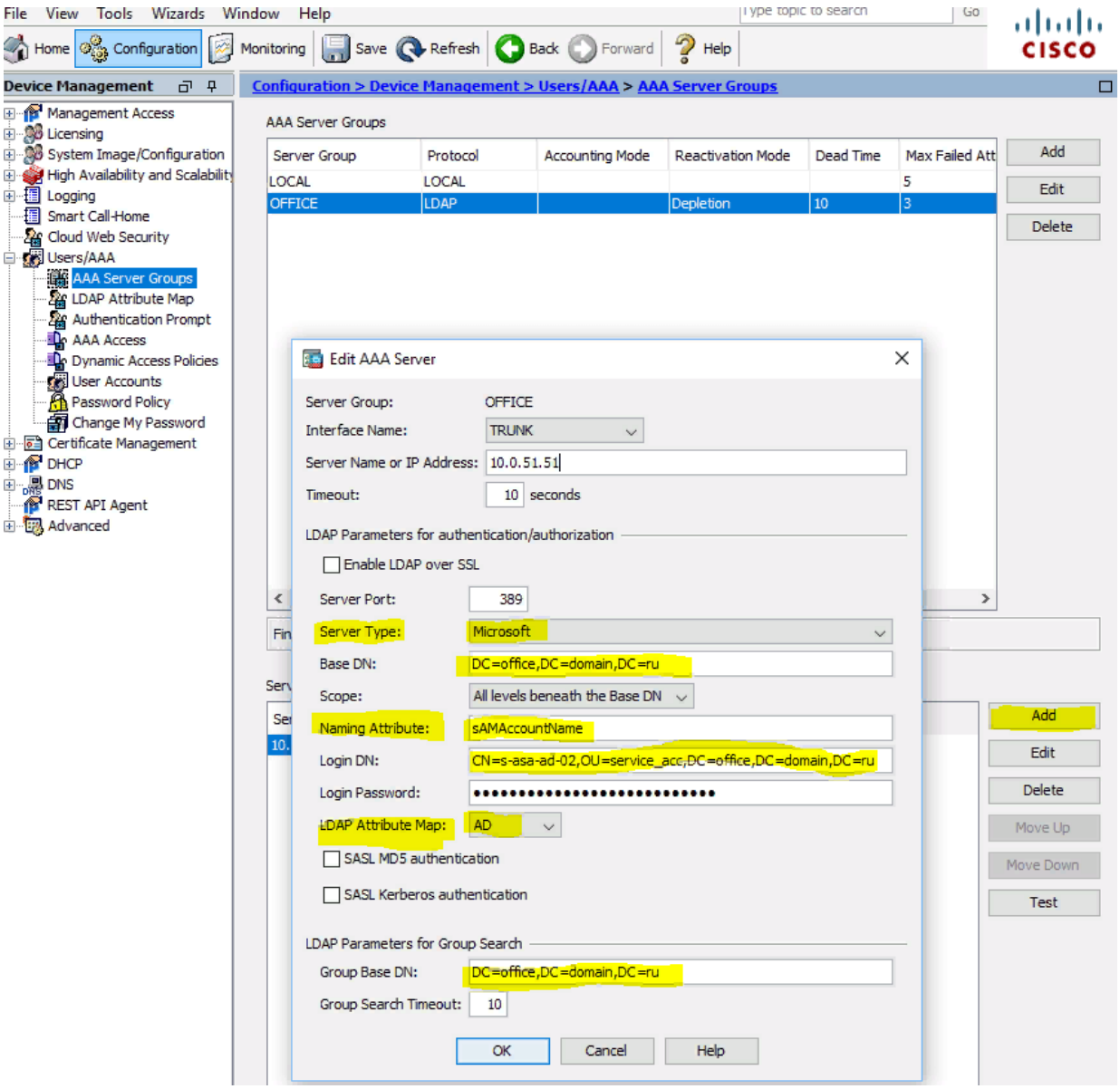
Практическое задание:*Настройка AnyConnectRemoteAccessSSLVPN используя ASDM*
Лабораторная работа
Цель: изучение настройки AnyConnectRemoteAccessSSLVPN используя ASDM
Начнем с настройки **LDAP** сервера (в нашем случае это DCActiveDirectory), для этого переходим в **Configuration>DeviceManagement>Users/AAA>AAAServerGroups** и создаем группу, назовем ее **OFFICE**, Protocol указываем **LDAP**



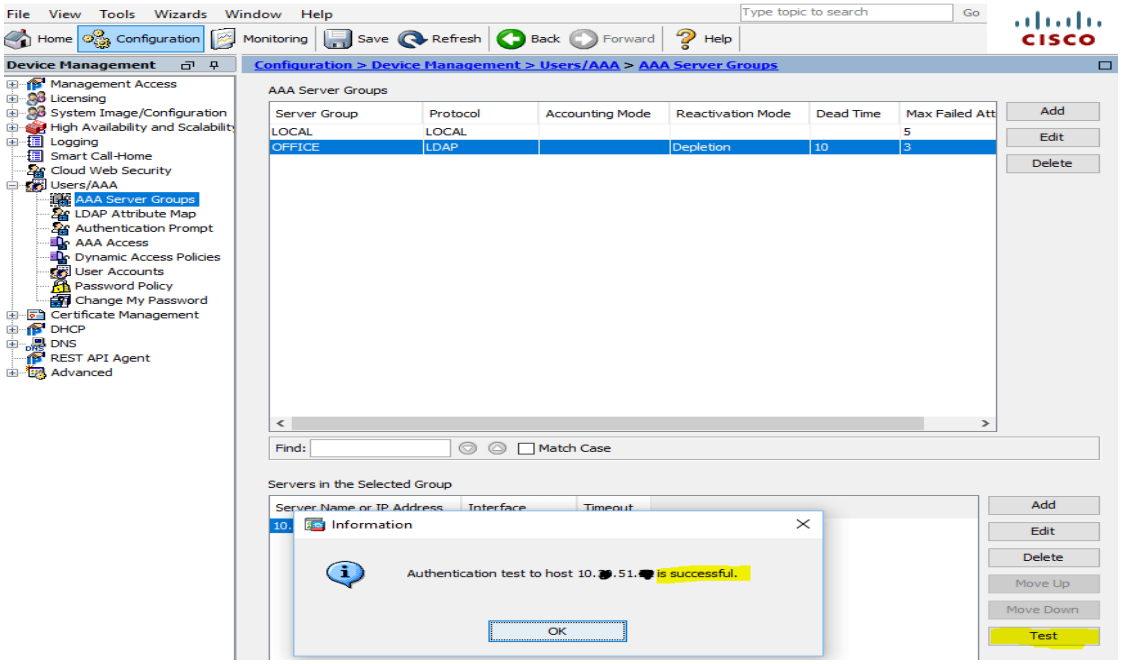
Для того, чтобы добавить сервер в созданную группу, нам необходимо предварительно создать **LDAP Atribute Map**. Для этого переходим в соответствующий раздел: **Configuration > DeviceManagement > Users/AAA >LDAP Attribute Map** и создаем новую карту: в нашем случае это Map Name: **AD**, Mapping of Attribute Name > LDAP Attribute Name: **memberOf**, Cisco Attribute Name: **IETF-Radius-Class**



Теперь можно добавить сервер (настроить подключение к контроллеру домена), указываем интерфейс, через который будем подключаться, IP адрес DC, Server Type: Microsoft, Base DN, Naming Attribute: sAMAccountName, Login DN, Login Password, только что созданную карту LDAP Attribute Map: AD, Group Base DN:

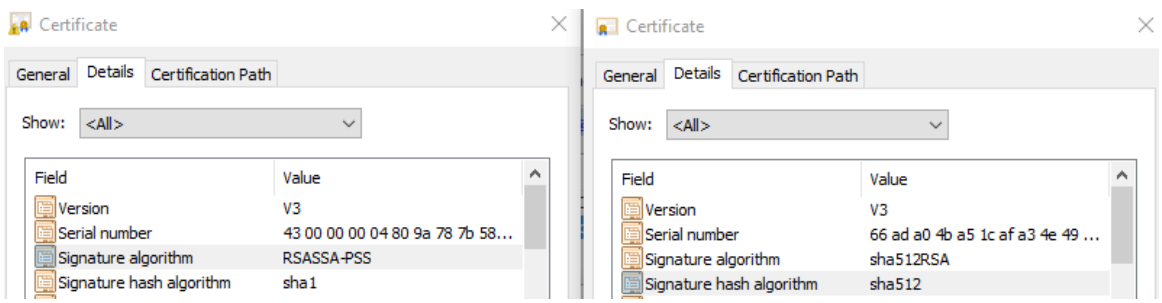


После добавления сервера делаем проверку, проходим аутентификацию учетной записью AD:



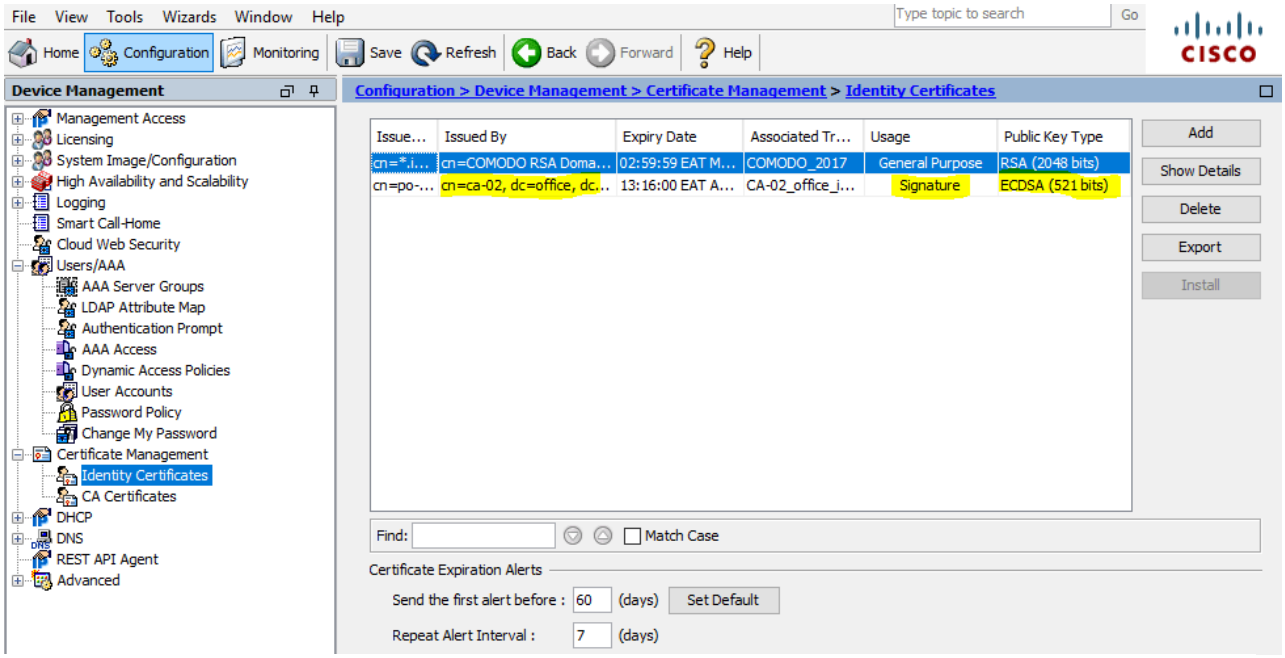
Test AAA Server — Authentication

Теперь можно добавить сертификат удостоверяющего центра (используется Microsoft CA, в рамках статьи о его настройке рассказывать не буду, единственное о чем следует обязательно помнить: Cisco ASA не воспринимает сертификаты с Signature algorithm **RSASSA-PSS**, который Microsoft предлагает использовать по умолчанию. мы меняли на **sha512RSA**):



Identity Certificates Signature algorithm RSASSA-PSS — sha512

Переходим **Configuration > DeviceManagement >Certificate Management > Identity Certificates** и импортируем в формате PKCS12 (*.pfx сертификат + private key):

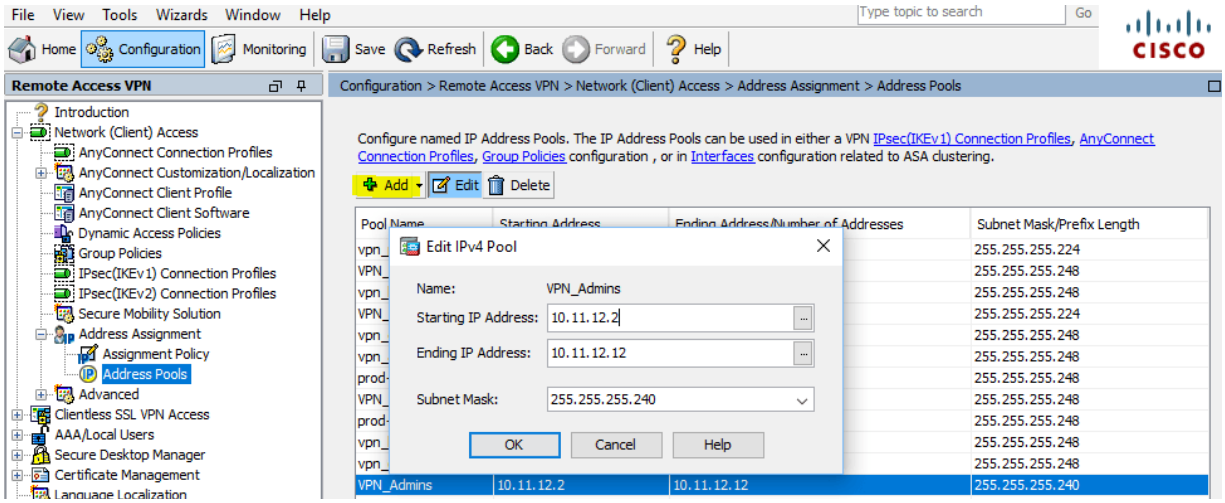


Identity Certificates Signature algorithm sha512RSA (ECDSA 521 bits)

С подготовительными действиями закончили, можно переходить к настройке профилей для AnyConnect VPN. Для примера, будем использовать 2 профиля, у которых будут разные IP Address Pools и соотв. ACL, Dynamic Access Policies, Group Policies исоответственно 2 группы ActiveDirectory. При подключении пользователей по ВПН используем политику «Туннелирование только указанных сетей», так называемый **Split Tunneling**, чтобы не гнать весь пользовательский траффик через впн. Но это «на любителя», может кому-то, наоборот, такое потребуется — последнее время это очень актуально ;)

Начнем с **IP Address Pools**, для этого переходим в **Configuration > Remote Access VPN > Network (Client) Access > Address Assignment > Address Pools**

Создадим пул адресов (сегмент) для администраторов (назовем, например VPN_Admins):

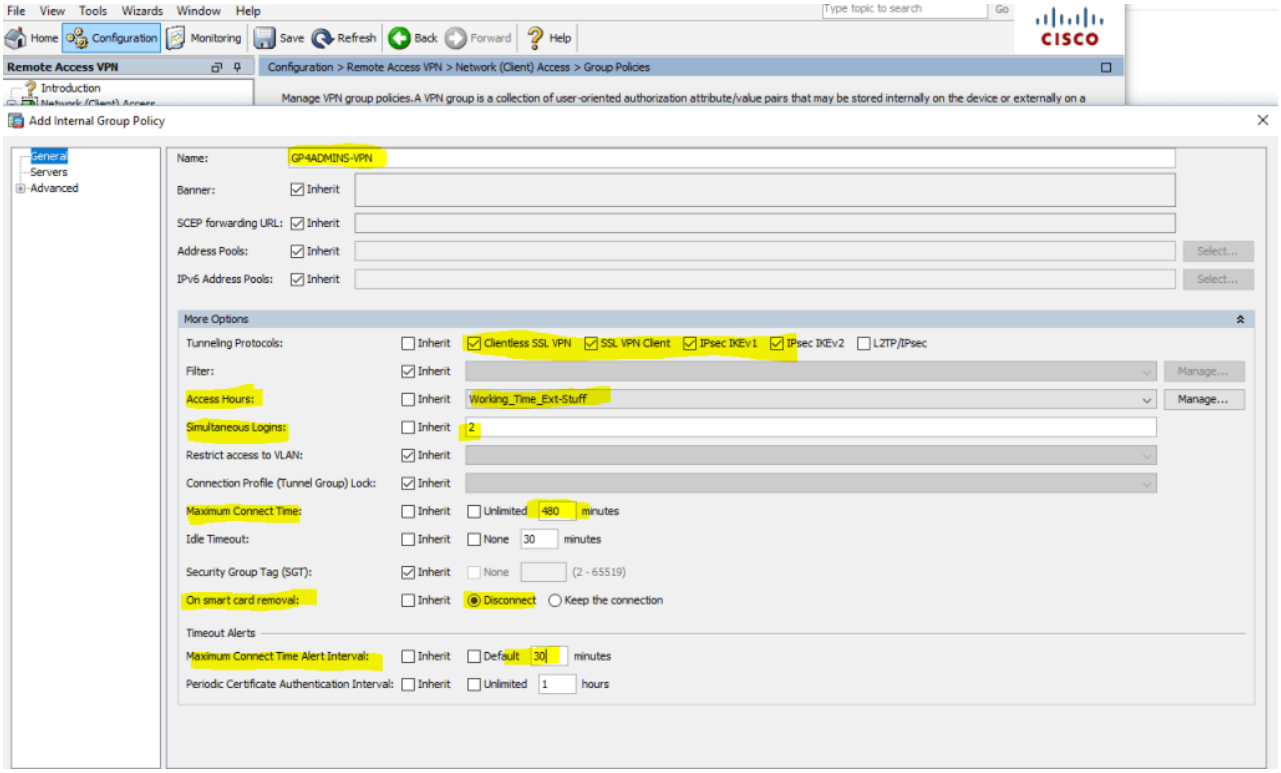


Address Assignment — Address Pools

Далее создадим политику (это основная часть настроеек профиля, в которой можно задат: протоколы, которые будут использоваться для туннелей, время доступа, количество одновременных логинов, закрыть доступы к определенным VLAN, выставить таймауты, задать DNS серверы, настроить **Split Tunneling**, клиентский файерволл и тд и тп) — в

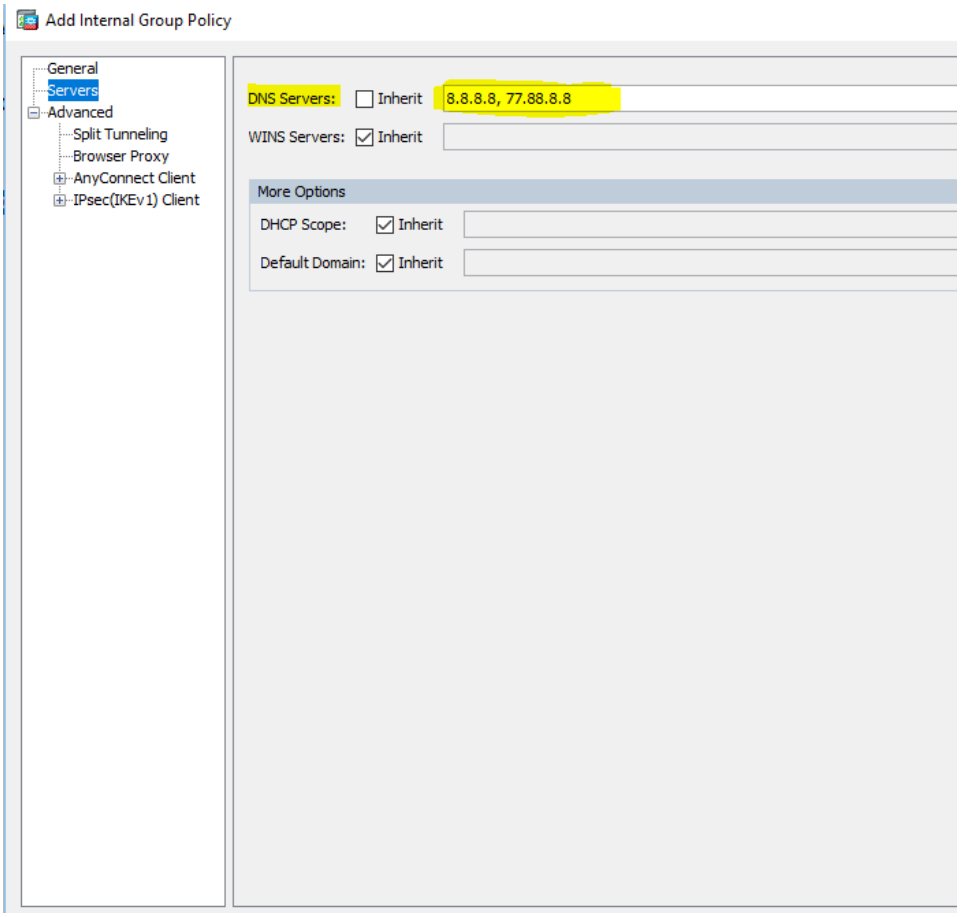
общем этой настройке следует уделить особое внимание! Итак, начнем: **Configuration > Remote Access VPN > Network (Client) Access > Group Policies, Add Internal Group Policy**

Все выставленные параметры сугубо индивидуальны — в нашем случае немного параноидальны Указаны протоколы, которые допускаются для создания туннеля (Tunneling Protocols), временной период для доступа по ВПН (Access Hours), количество одновременных подключений с одной учетной записью (Simultaneous Logins), максимальное время для сеанса и пр.:



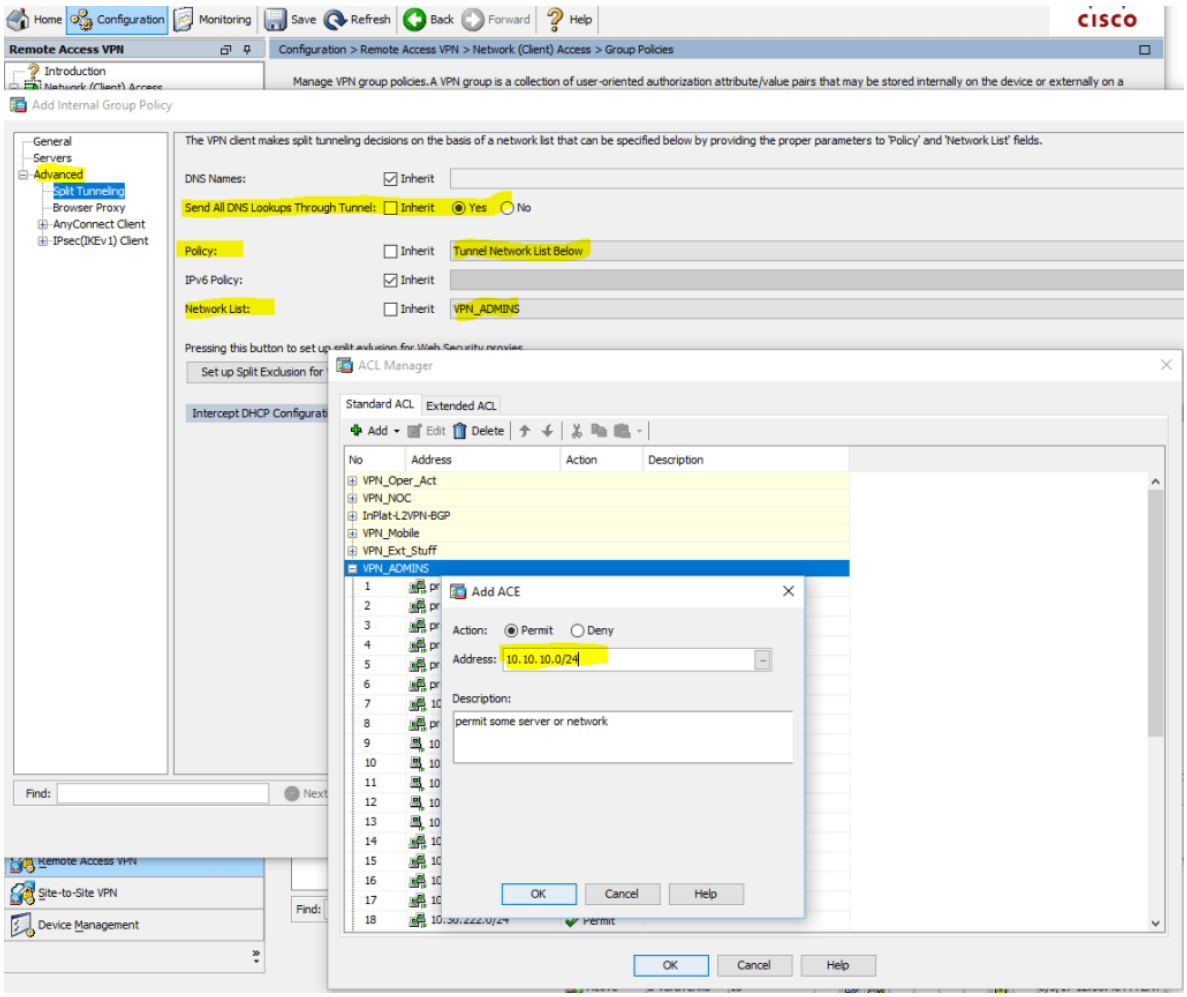
Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add Internal Group Policy

Следующая полезная настройка — вкладка Servers, в которой мы можем указать внутр. ДНС серверы, для пользователей ВПН AnyConnect, чтобы они могли обращаться к внутренним ресурсам по имени:



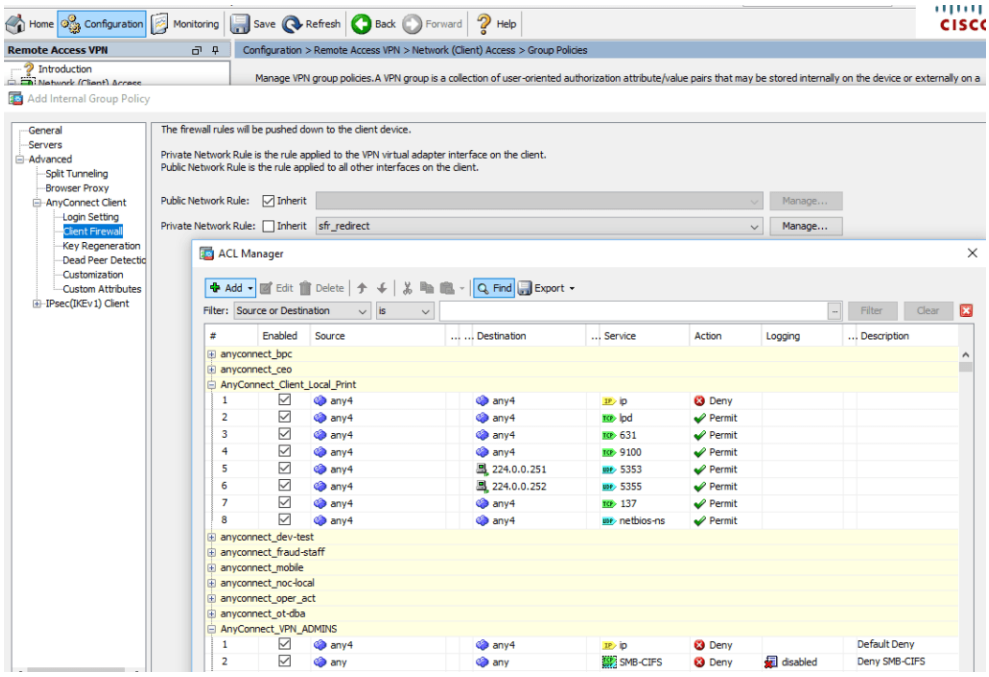
Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit Internal Group Policy — Servers

Теперь перейдем к еще одной интересной опции — настройке **Split Tunneling**. Как я уже писал ранее — будем использовать политику «туннелирование только указанных сетей» (мы не заворачиваем в туннель весь траффик пользователей и разрешаем доступ к локальным ресурсам — опция «**Local Lan Access**» далее будет отдельно рассмотрена):



Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit Internal Group Policy > Advanced > Split Tunneling >

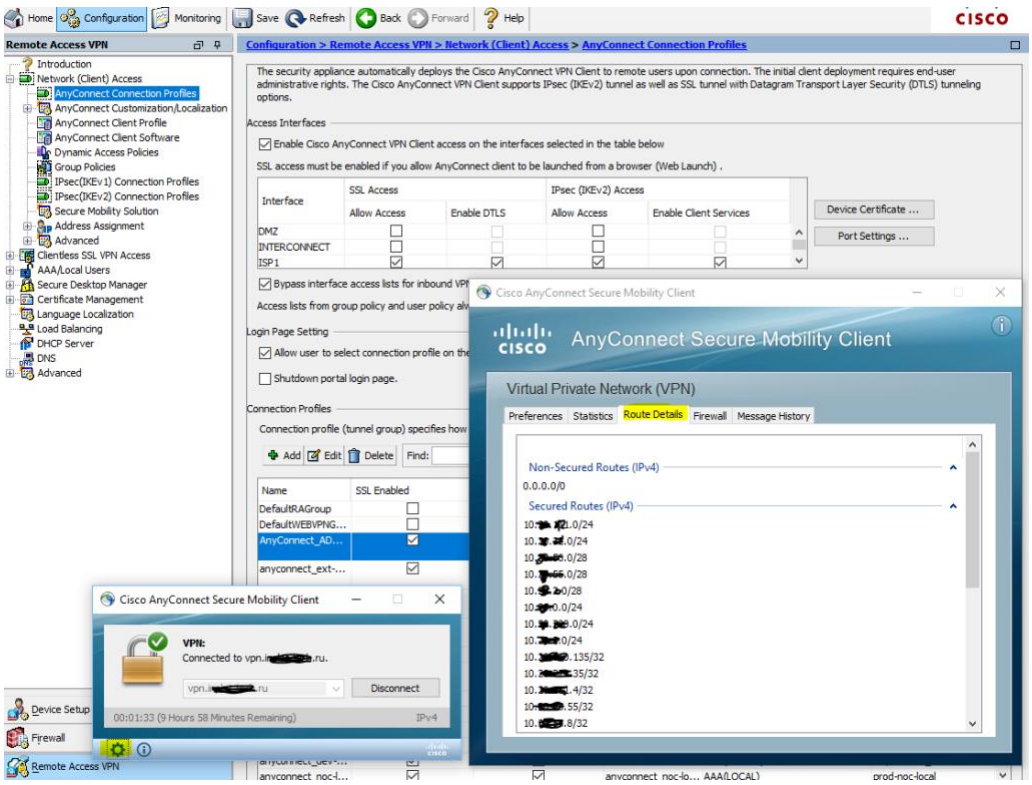
Ранее мы указали к каким сетям\хостам мы разрешили доступ, теперь ограничим доступ к ним по протоколам\портам (еще один **ACL**):



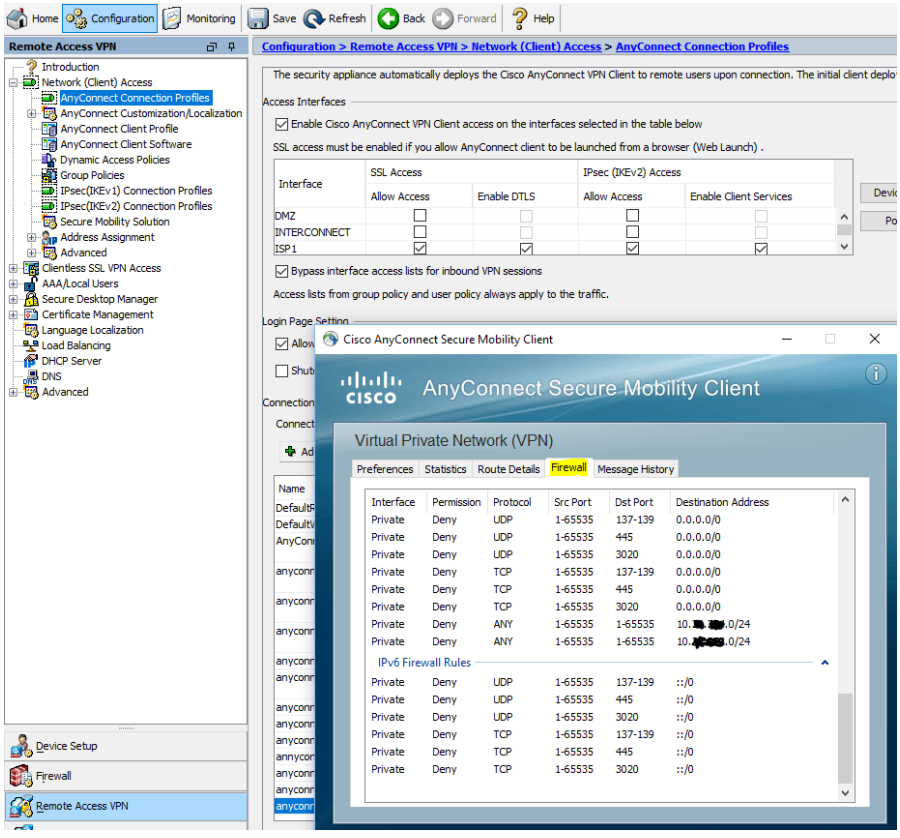
Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Edit Internal Group Policy > Advanced > AnyConnect Client > Client Firewall > Private

Network Rule

В итоге, после подключения к впн AnyConnect клиентом, можно увидеть маршруты в сторону туннеля и правила файерволла:

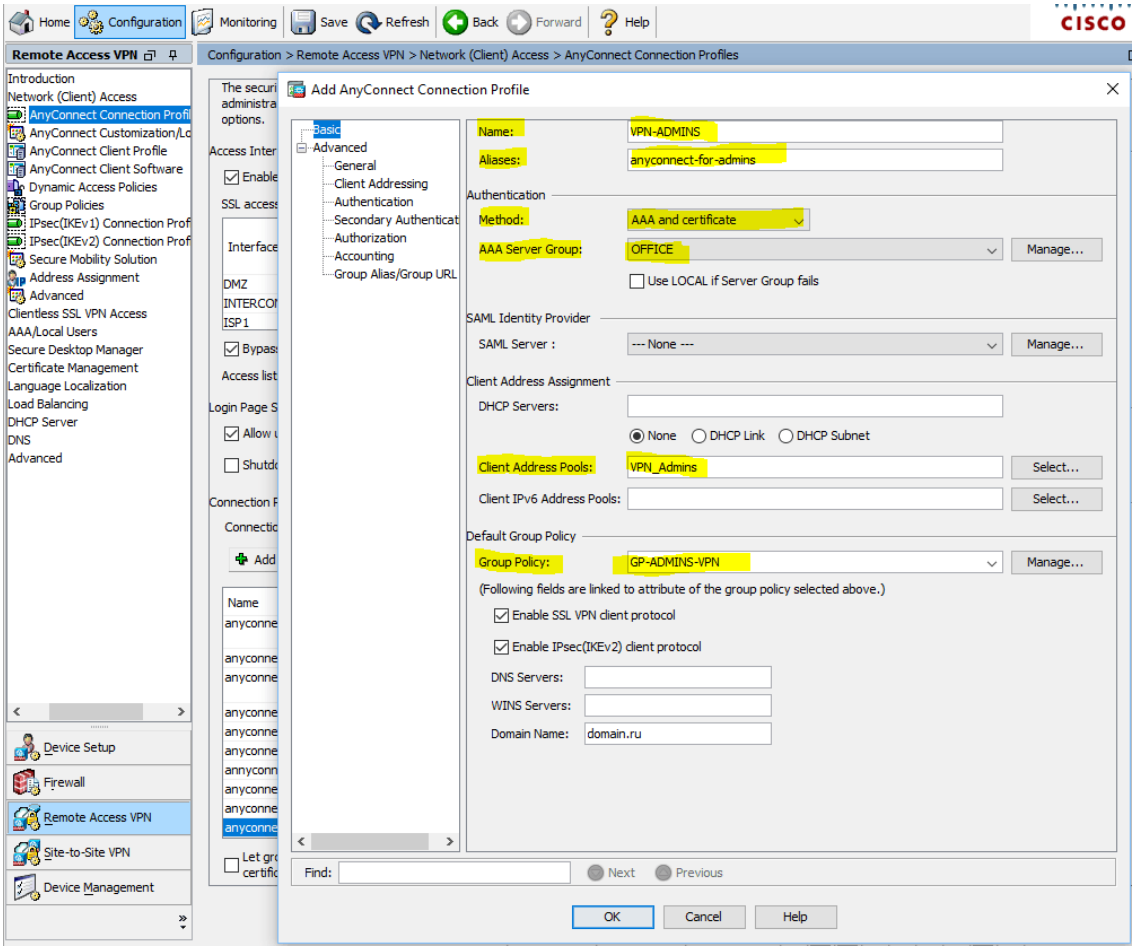


AnyConnect Client > Route Details



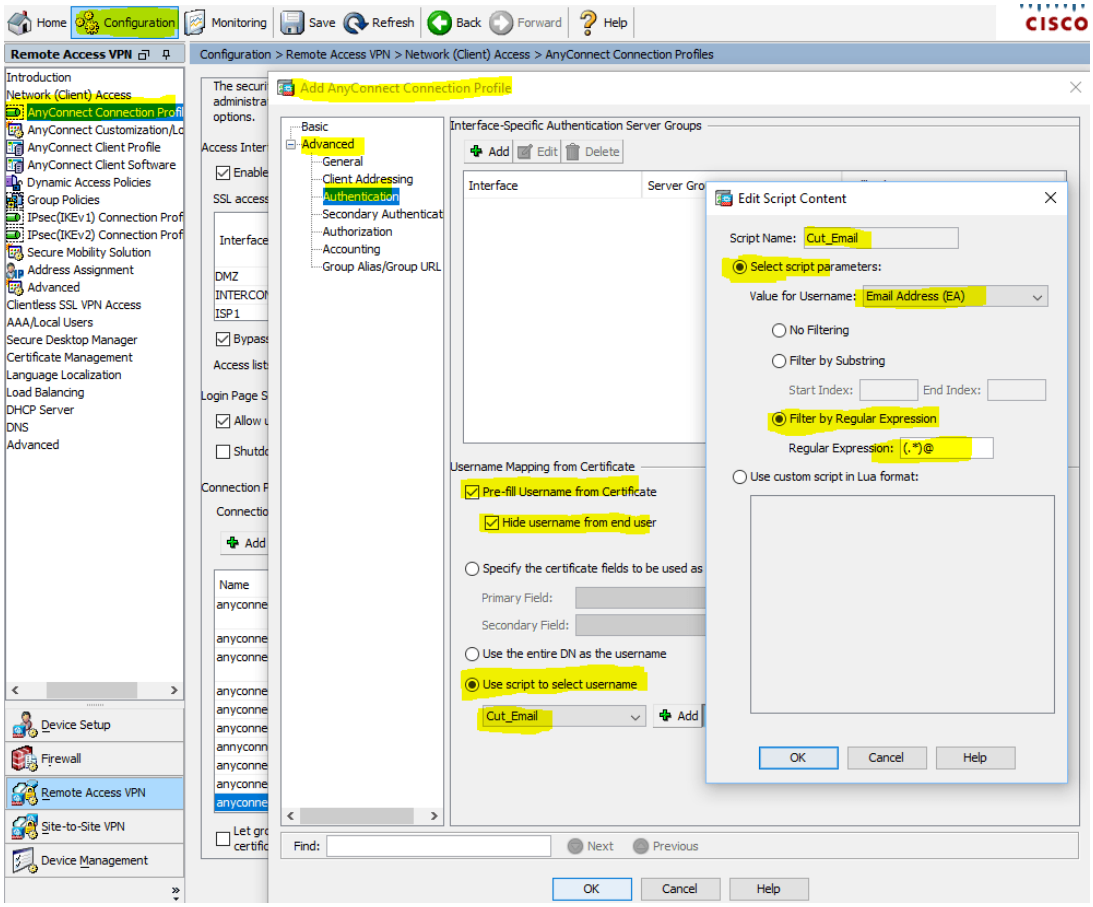
AnyConnect Client > Firewall

Теперь можно перейти непосредственно к созданию профиля AnyConnect, переходим **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles >, Add AnyConnect Connection Profile**
и указываем: *Name*, *Aliases*, далее *Authentication Method (AAA and certificate)*, *AAA Server Group*, *Client Address Pools*, *Group Policy* — все созданное ранее!



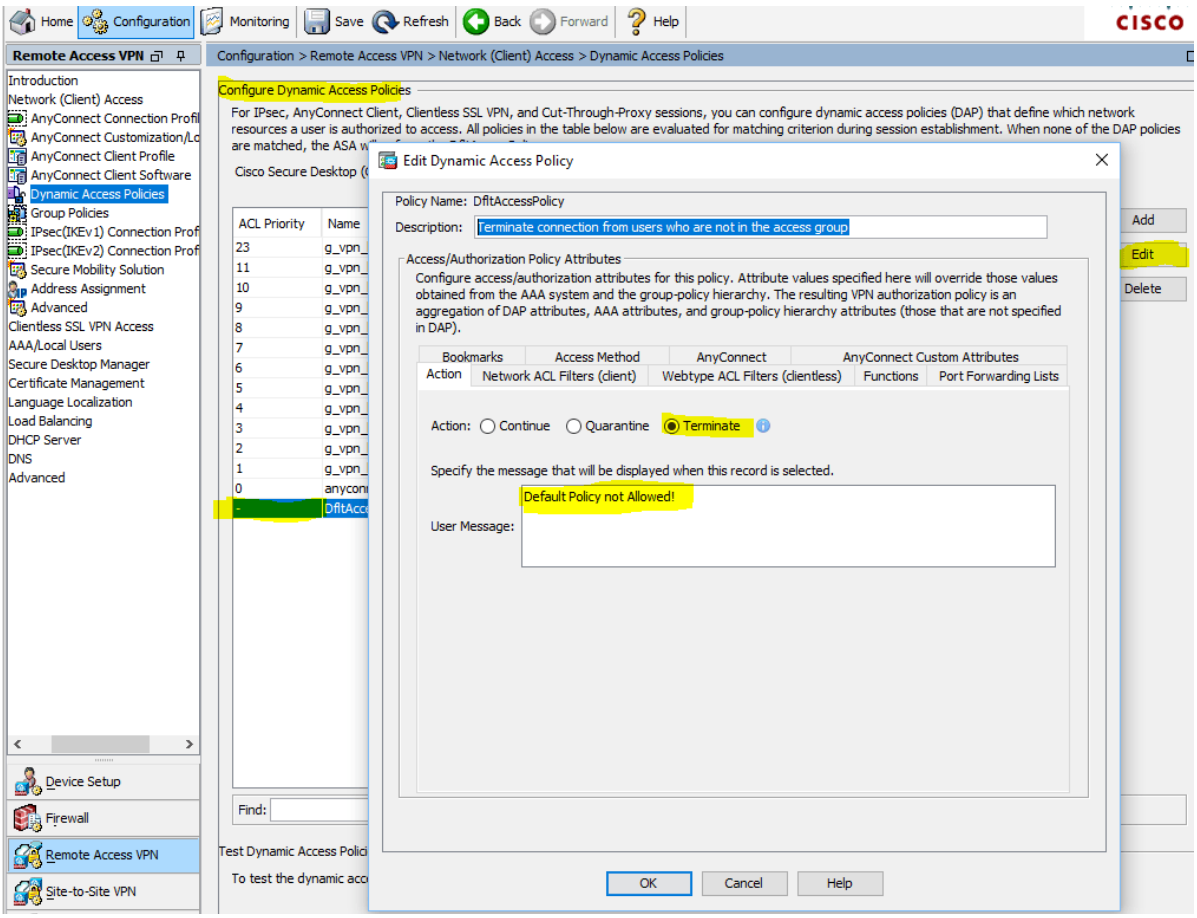
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add AnyConnect Connection Profile > Basic

И теперь небольшой «лайфхак» — мы из пользовательского сертификата вытащим значение E-mail и с помощью регулярки (.*)@ отрежем от него @domain.ru (значение **E-mail** должно быть %AD username%@somedomain.ru) и подставим его в поле **Username** при подключении.



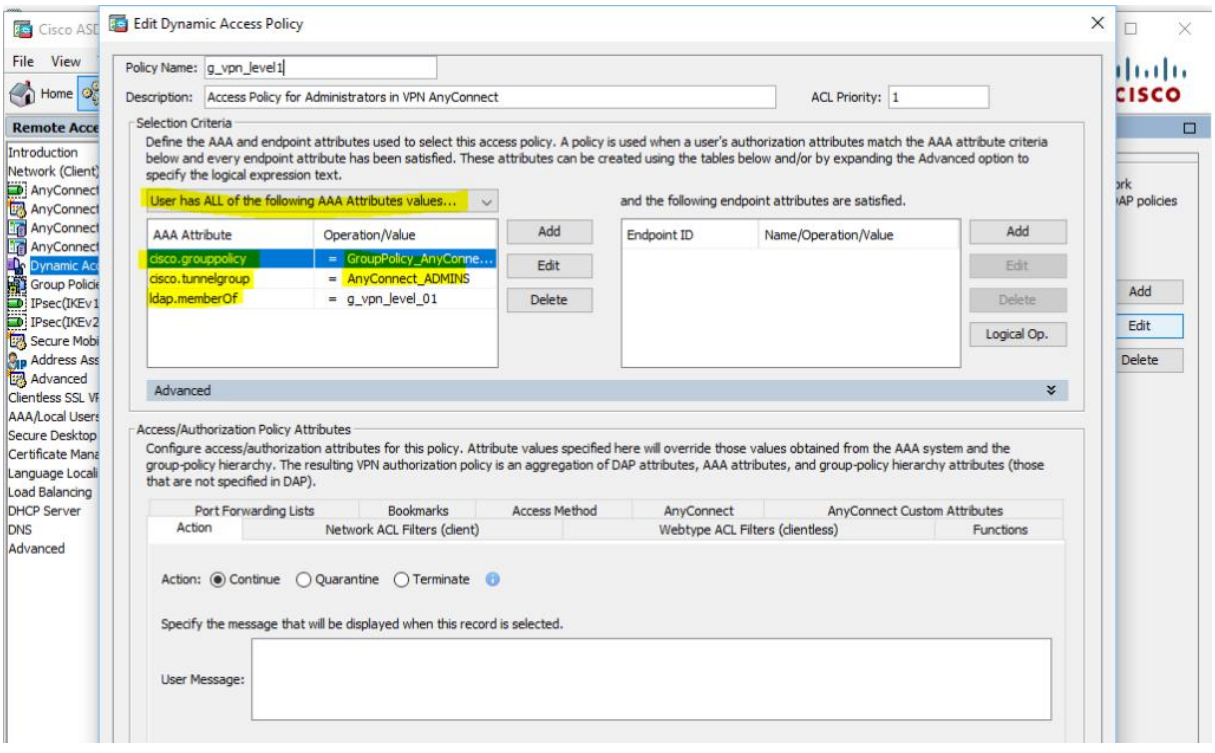
Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add AnyConnect Connection Profile > Advanced > Authentication > Username Mapping from Certificate

Когдапрофилинастроили — мыужеможемподключаться, потомукакбудетотрабатыватьполитикапоумолчанию **DfltAccessPolicy** для всех пользователей, прошедших аутентификацию (у нее самый высокий приоритет). Мы же хотим, чтобы для разных групп ActiveDirectory использовался свой профиль и отрабатывала своя групповая политика \ политика доступа. Поэтому, переходим: **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies** и запрещаем **DfltAccessPolicy** (на самом деле не запрещаем, а делаем Terminate с уведомлением пользователя — хорошая диагностика того, что пользователь не включен в требую группу ActiveDirectory):

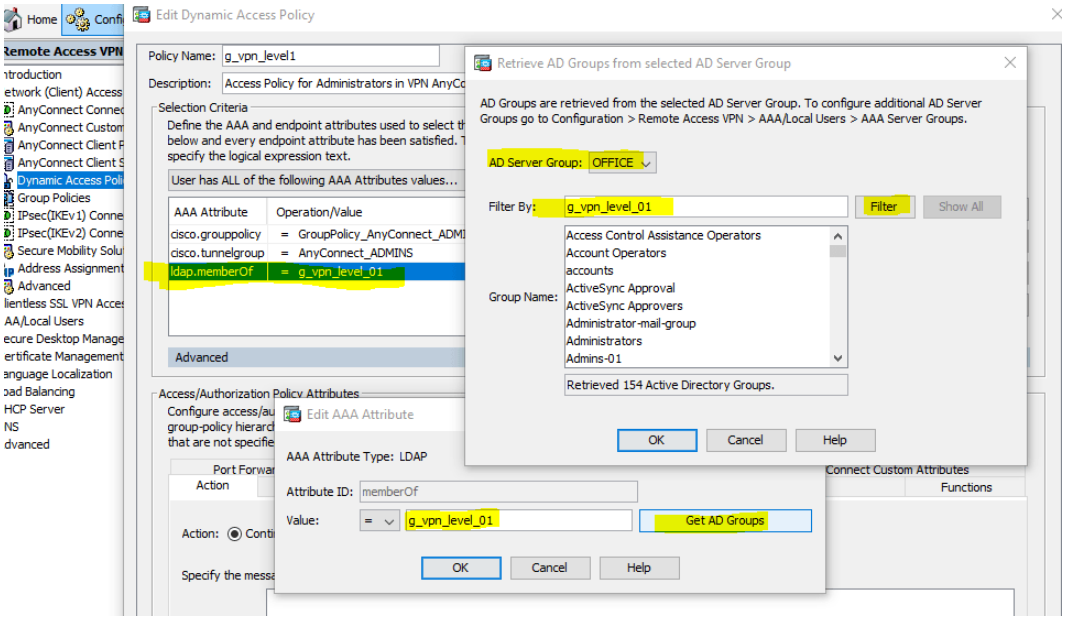


Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies
Terminate connection from users who are not in the access group

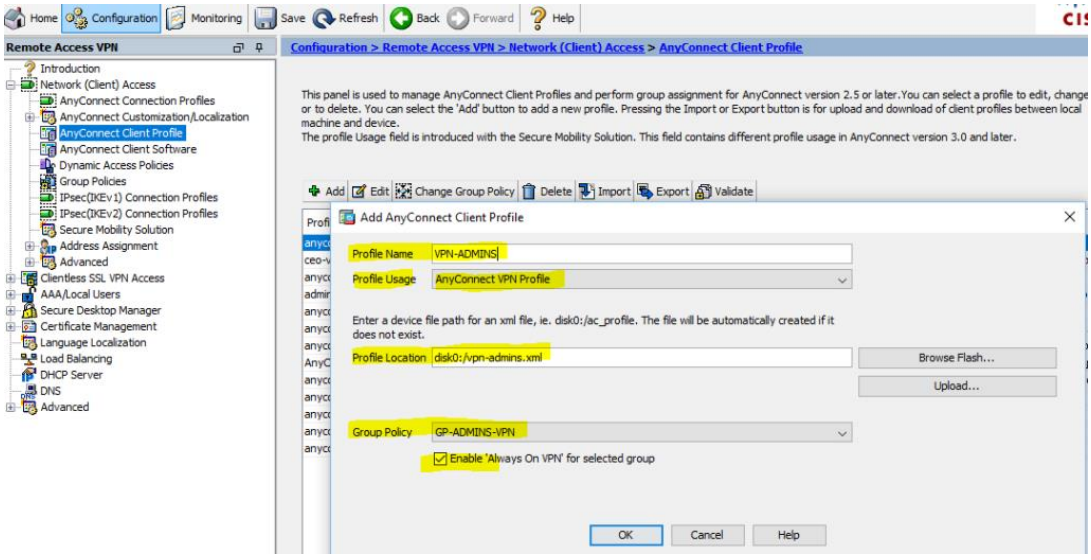
После того, как политику по умолчанию запретили, — создадим новую:
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add Dynamic Access Policy



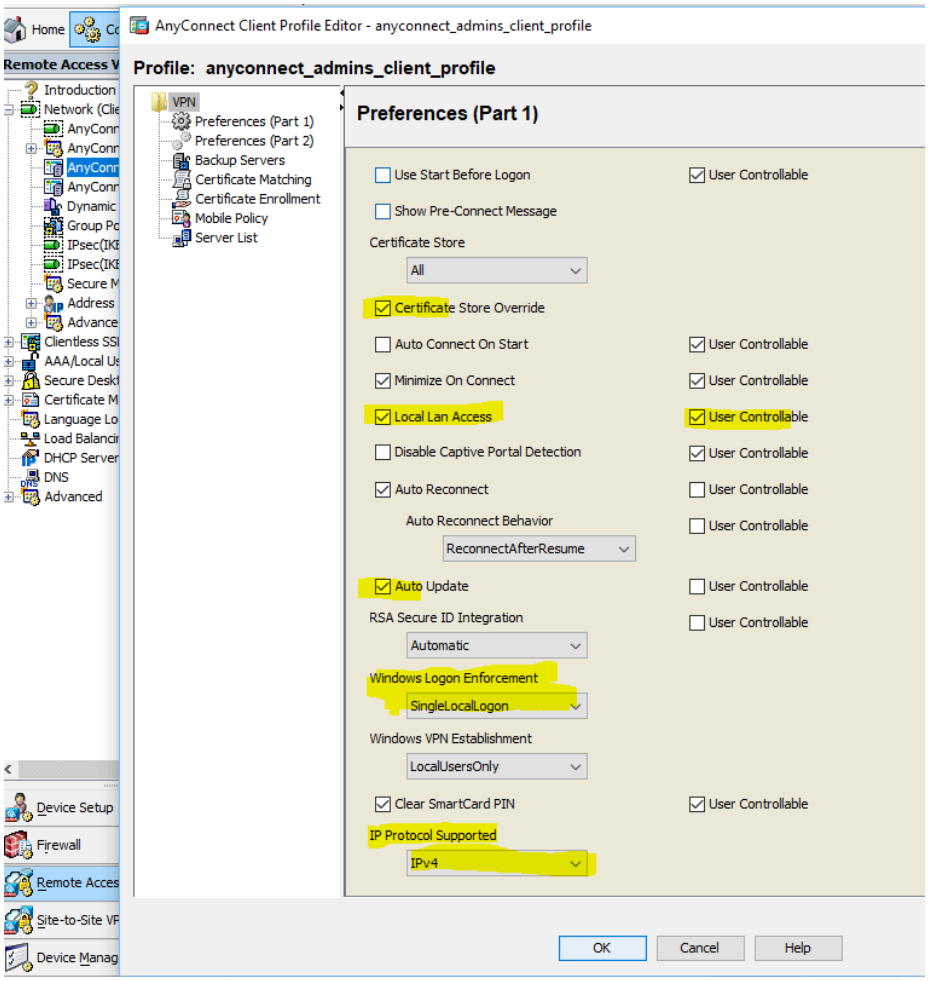
Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add Dynamic Access Policy with AAA Attributes
где **g_vpn_level_01** — созданная в ActiveDirectory группа безопасности, куда мы включаем необходимые админские учетки, для подключения по ВПН AnyConnect с профилем **VPN-ADMINS**:



Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add Dynamic Access Policy with AAA Attributes > Get AD Groups
ну и заключительный «штрих» — рекомендую сохранить созданный профиль в файл (полезно, например, для синхронизации профилей для StandBy unit при Failover конфигурации):



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile



Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile > Edit

Тестовые задания

1) К правовым методам, обеспечивающим информационную безопасность, относятся:

- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:

- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:

+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций
5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы
6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных

тест_20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением Содержание лекционного материалая информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети

- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:

- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск-ситуаций

Критерии оценки результата тестирования

Оценка (стандартная)	Оценка (тестовые нормы: % правильных ответов)
«отлично»	80-100 %
«хорошо»	70-79%
«удовлетворительно»	50-69%
«неудовлетворительно»	Меньше 50 %

ОЦЕНОЧНЫХ СРЕДСТВ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Вопросы для подготовки к дифференцированному зачету

1. Классификацияугрозинформационнойбезопасностиавтоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угрозаотказаслужб(угрозаотказавдоступе).
4. Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности ипримеры реализации угрозы.
6. Понятие политики безопасности информационных систем.
7. Назначение политики безопасности.
8. Основные типы политики безопасности доступа к данным.
9. Дискреционные и мандатные политики.
10. Требованияксистемамкриптографическойзащиты:криптографические требования, требования надежности, требованияпо защите от НСД, требования к средствам разработки.
11. Законодательный уровень обеспечения информационнойбезопасности.
12. Основные законодательные акты РФ в области защитыинформации.
13. Функцииназначениестандартовинформационнойбезопасности. Примеры стандартов, их роль при проектировании иразработке информационных систем.
14. Критерии оценки безопасности компьютерных систем(«Оранжевая книга»).
15. Структура требований безопасности. Классызащищенности.
16. ОсновныеположенияруководящихдокументовГостехкомиссии России.
17. Классификация автоматизированных системпоклассамзащищенности.
18. Показателизащищенностисредстввычислительной техники от несанкционированного доступа.
19. Единыекритериибезопасностиинформационныхтехнологий. Понятие профиля защиты. Структура профиля защиты.
20. Требованиябезопасности(функциональные требования и требования адекватности).
21. Административный уровень защиты информации. Задачиразличных уровней управления в решении задачи обеспеченияинформационной безопасности.
22. Процедурныйуровеньобеспечениябезопасности.Авторизация пользователей в информационной системе.
23. Идентификацияиаутентификацияпривходевинформационнуюсистему.
24. Использованиепарольныхсхем.Недостатки парольных схем.
25. Идентификацияиаутентификацияпользователей.Применениепрограммно-аппаратныхсредстваутентификации(смарт-карты, токены).
26. Аутентификация субъектов в распределенных системах,проблемы и решения. Схема Kerberos.
27. Аудит в информационных системах. Функции и назначениеаудита, его роль в обеспечении информационной безопасности.
28. Местоинформационнойбезопасностиэкономическихсистемвнациональнойбезопасностистраны.
29. Концепцияинформационной безопасности.
30. Средства обеспечения информационной безопасности в OCWindows’2000.Разграничениедоступакданным.Групповаяполитика.
31. Применение файловой системы NTFS для обеспечения
32. информационной безопасности в Windows NT/2000/XP. Списыкиконтроля доступа к данным (ACL) их роль в разграничении доступа кданным.

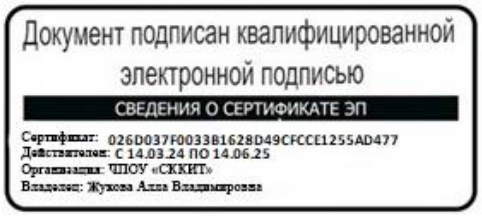
Практические задания

1. Анализ бизнес-требований к информационной безопасности

2. Разработка концептуального плана защиты.
3. Анализ технических ограничений плана защиты
4. Применение сертификатов для аутентификации и авторизации
5. Проектирование иерархии ЦС.
6. Проектирование административных ролей ЦС
7. Проектирование политики подачи заявок на сертификаты.
8. Проектирование размещения CRL и интервала публикации.
9. Проектирование защиты границ сети.
10. Зашита DNS. Проектирование политики IPSec.
11. Выполнить сканирование локальной сети с программой LanSurfer по
12. заданным параметрам
13. Создайте профиль для сканирования Моё сканирование
14. Укажите диапазон адресов от 192.168.3.1 до 192.168.3.254
15. ПросканируйтесетьИспользуявозможностипрограммынайдитефайлMyTestX-Setup.exe
16. Перейдите в папку содержащий данный файл.
17. Используя оснастку Event Viewer, продемонстрируйте возможностиработы с системными журналами.
18. Выполните установку сетевого монитора
19. Запишите данные средствами сетевого монитора
20. Сохраните кадры в текстовый файл средствами утилиты Netsh.
21. Выполните трассировку сети средствами утилиты Netsh
22. Продемонстрируйте устранение неполадок с использованием NetworkDiagnostics Framework
23. Продемонстрируйте устранение неполадок с помощью Ping
24. Продемонстрируйте устранение неполадок с помощью PathPing
25. Настройте сетевую карту, имя компьютера, рабочую группу позаданным параметрам
26. Настройте сетевой интерфейс для введения компьютера в domain.

Частное профессиональное образовательное учреждение
«СЕВЕРО-КАВКАЗСКИЙ КОЛЛЕДЖ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ»

Рассмотрены и утверждены
на Педагогическом совете
от 27.03.2025 Протокол № 03



УТВЕРЖДАЮ
Директор ЧПОУ «СККИТ»
А.В. Жукова
«27» марта 2025

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ

РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СЕТЕЙ

09.02.06 СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ

СИСТЕМНЫЙ АДМИНИСТРАТОР

Пятигорск - 2025

РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ ВИДОВ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

Рекомендации по подготовке к лекциям

Главное в период подготовки к лекционным занятиям – научиться методам самостоятельного умственного труда, сознательно развивать свои творческие способности и овладевать навыками творческой работы. Для этого необходимо строго соблюдать дисциплину учебы и поведения. Четкое планирование своего рабочего времени и отдыха является необходимым условием для успешной самостоятельной работы.

Каждому студенту следует составлять еженедельный и семестровый планы работы, а также план на каждый рабочий день. С вечера всегда надо распределять работу на завтрашний день. В конце каждого дня целесообразно подводить итог работы: тщательно проверить, все ли выполнено по намеченному плану, не было ли каких-либо отступлений, а если были, по какой причине это произошло. Нужно осуществлять самоконтроль, который является необходимым условием успешной учебы. Если что-то осталось невыполненным, необходимо изыскать время для завершения этой части работы, не уменьшая объема недельного плана.

Рекомендации по подготовке к практическим занятиям

При подготовке к практическому занятию студент должен ознакомиться с планом, выполнить все инструкции, предложенные преподавателем.

Результатом работы является свободное владение теоретическим материалом, полные ответы на поставленные вопросы, коллективное обсуждение проблемных тем.

Методические рекомендации по подготовке докладов

Доклад – публичное сообщение, представляющее собой развернутое изложение на определенную тему.

Различают следующие виды докладов: научный доклад и учебный доклад. Научные доклады готовятся научными работниками для представления своих результатов на научной конференции, научном семинаре и др. К учебным докладам относятся студенческие доклады и любые другие доклады, подготавливаемые обучающимися средних образовательных учреждений.

Для того, чтобы облегчить работу над докладом, предлагаем разбить процесс на несколько последовательных этапов. Надеемся, что знакомство с ними поможет вам овладеть необходимым инструментарием и разобраться в принципах построения письменной работы.

Этапы подготовки доклада

1. Подготовка и планирование.
2. Выбор и осознание темы доклада
3. Подбор источников и литературы.
4. Работа с выбранными источниками и литературой.
5. Систематизация и анализ материала.
6. Составление рабочего плана доклада.
7. Письменное изложение материала по параграфам.
8. Редактирование, переработка текста.
9. Оформление доклада.
10. Выступление с докладом.

При подготовке доклада рекомендуется придерживаться следующих правил:

Во-первых, необходимо четко соблюдать регламент.

Для того чтобы уложиться в отведенное время необходимо:

а) тщательно отобрать факты и примеры, исключить из текста выступления все, не относящееся напрямую к теме;

б) исключить все повторы;

в) весь иллюстративный материал (графики, диаграммы, таблицы, схемы) должен быть подготовлен заранее;

г) необходимо заранее проговорить вслух текст выступления, зафиксировав время и сделав поправку на волнение, которое неизбежно увеличивает время выступления перед аудиторией.

Во-вторых, доклад должен хорошо восприниматься на слух.

Это предполагает:

а) краткость, т.е. исключение из текста слов и словосочетаний, не несущих смысловой нагрузки;

б) смысловую точность, т.е. отсутствие возможности двоякого толкования тех или иных фраз;

в) отказ от неоправданного использования иностранных слов и сложных грамматических конструкций.

Доклады оцениваются по следующим критериям:

- соблюдение требований к его оформлению;
- необходимость и достаточность информации для раскрытия темы;
- умение обучающегося свободно излагать основные идеи, отраженные в докладе;
- способность учащегося понять суть задаваемых ему вопросов и сформулировать точные ответы на них.

Методические рекомендации по подготовке конспектов

При подготовке конспекта рекомендуется придерживаться такой последовательности:

1.Прочтите текст.

2.Определите цель изучения темы (какие знания должны приобрести и какими умениями обладать).

3.Выделите основные положения.

4.Проанализируйте основные положения.

5.Сделайте выводы.

6.Составьте краткую запись.

Работа с литературными источниками

В процессе обучения студенту необходимо самостоятельно изучать учебно-методическую литературу. Самостоятельно работать с учебниками, учебными пособиями, Интернет-ресурсами. Это позволяет активизировать процесс овладения информацией, способствует глубокому усвоению изучаемого материала.

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Различают два вида чтения; первичное и вторичное. Первичное - эти внимательное, неторопливое чтение, при котором можно остановиться на трудных местах. После него не должно остаться ни одного непонятного слова. Содержание не всегда может быть понятно после первичного чтения.

Задача вторичного чтения полное усвоение смысла целого (по счету это чтение может быть и не вторым, а третьим или четвертым).

Как уже отмечалось, самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие формирования у себя научного способа познания.

При работе с литературой рекомендуется вести записи.

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Промежуточная аттестация

Каждый семестр заканчивается сдачей зачетов (экзаменов). Подготовка к сдаче зачетов (экзаменов) является также самостоятельной работой студентов. Студенту необходимо к зачету (экзамену) повторить весь пройденный материал по дисциплине в рамках лекций и рекомендуемой литературы.

Методические рекомендации по работе с Интернет-ресурсами

Среди Интернет-ресурсов, наиболее часто используемых студентами в самостоятельной работе, следует отметить электронные библиотеки, образовательные порталы, тематические сайты, библиографические базы данных, сайты периодических изданий. Для эффективного поиска в WWW студент должен уметь и знать:

- чётко определять свои информационные потребности, необходимую ретроспективу информации, круг поисковых серверов, более качественно индексирующих нужную информацию,
- правильно формулировать критерии поиска;
- определять и разделять размещённую в сети Интернет информацию на три основные группы: справочная (электронные библиотеки и энциклопедии), научная (тексты книг, материалы газет и журналов) и учебная (методические разработки, рефераты);
-давать оценку качества представленной информации, отделить действительно важные сведения от информационного шума;
- давать оценки достоверности информации на основе различных признаков, по внешнему виду сайта, характеру подачи информации, её организации;
- студентам необходимо уметь её анализировать, определять её внутреннюю непротиворечивость.

Запрещена передача другим пользователям информации, представляющей коммерческую или государственную тайну, распространять информацию, порочащую честь и достоинство граждан. Правовые отношения регулируются Законом «Об информации, информатизации и защите информации», Законом «О государственной тайне», Законом «Об авторском праве и смежных правах», статьями Конституции об охране личной тайны, статьями Гражданского кодекса и статьями Уголовного кодекса о преступлениях в сфере компьютерной информации.

При работе с Интернет-ресурсами обращайте внимание на источник: оригинальный авторский материал, реферативное сообщение по материалам других публикаций, студенческая учебная работа (реферат, курсовая, дипломная и др.). Оригинальные авторские материалы, как правило, публикуются на специализированных тематических сайтах или в библиотеках, у них указывается автор, его данные. Выполнены такие работы последовательно в научном или научно-популярном стиле. Это могут быть научные статьи, тезисы, учебники, монографии, диссертации, тексты лекций. На основе таких работ на некоторых сайтах размещаются рефераты или обзоры. Обычно они не имеют автора, редко указываются источники реферирования. Сами сайты посвящены разнообразной тематике. К таким работам стоит относиться критически, как и к сайтам, где размещаются учебные студенческие работы. Качество этих работ очень низкое, поэтому, сначала подумайте, оцените ресурс, а уже потом им пользуйтесь. В остальном с Интернет-ресурсами можно работать как с обычной печатной литературой. Интернет – это ещё и огромная библиотека, где вы можете найти практически любой художественный текст. В интернете огромное количество словарей и энциклопедий, использование которых приветствуется.