Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Выборнова Любовь Алексеевна
Должность: Ректор
Дата подписания: 29.10.2024 11:00:29
Уникальный программный ключ:
c3b3b9c625f6c113afa2a2c42baff9e05a38b76e

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования
«Поволжский государственный университет сервиса» (ФГБОУ ВО «ПВГУС»)

Высшая школа интеллектуальных систем и кибертехнологий

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«ЗАЩИТА ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ»

Направление подготовки:
10.03.01 «Информационная безопасность»

Направленность (профиль):
«Организация и технологии защиты информации
(по отрасли или в сфере профессиональной деятельности)»

Квалификация выпускника: **бакалавр**

Тольятти 2024

Рабочая программа дисциплины «*Защита информации в компьютерных сетях*» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования - *бакалавриат* по направлению подготовки *10.03.01 «Информационная безопасность»*, утверждённым приказом Министерства науки и высшего образования Российской Федерации от 17.11.2020 № 1427.

Составители:

к.т.н., доцент	Т.С. Яницкая
(учёная степень, учёное звание)	(ФИО)

РПД утверждена на заседании Высшей школы интеллектуальных систем и кибертехнологий *(ВШИСиКТ)*

06.09.2024 г. протокол №2

директор *ВШИСиКТ*	к.э.н., доцент	О.А. Филиппова
	(уч. степень, уч. звание)	(ФИО)

1. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫХ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

1.1. Цель освоения дисциплины

Целью освоения дисциплины является:

- формирование у обучающихся общепрофессиональных компетенций в области использования информационно-коммуникационных технологий и информационной безопасности.
- формирование у обучающихся профессиональных компетенций, необходимых для решения задач профессиональной деятельности

1.2. Перечень планируемых результатов обучения по дисциплине

Код и наименование компетенции	**Код и наименование индикатора достижения компетенции**	**Планируемые результаты обучения по дисциплине**	**Основание (ПС)** *для профессиональных компетенций
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты.	ИОПК-10.3. Осуществляет управление процессом обеспечения информационной безопасности	**Знает** принципы сетевой безопасности, методы защиты устройств, механизмы аутентификации, авторизации и учёта, работу межсетевых экранов, IPS, VPN и криптографических систем. **Умеет** настраивать средства защиты сети, конфигурировать AAA, ACL, IPS, VPN и межсетевые экраны, анализировать угрозы и тестировать безопасность. **Владеет** методами выявления угроз, средствами контроля доступа, инструментами мониторинга, технологиями шифрования и практиками защиты сетевой инфраструктуры.	
ПК-6 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	ИПК-6.2. Работает с программным обеспечением с соблюдением действующих требований по защите информации		06.032 «Специалист по безопасности компьютерных систем и сетей» 06.033 «Специалист по защите информации в автоматизированных системах»

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина относится к обязательной *части, формируемой участниками образовательных отношений*, Блока 1. Дисциплины (модули) образовательной программы бакалавриата (Профессиональный модуль).

3. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

3.1. Объем и структура дисциплины

Общая трудоёмкость дисциплины составляет **3 з.е. (108 час.)**, их распределение по видам работ и семестрам представлено в таблице.

Виды учебных занятий и работы обучающихся	Трудоёмкость, час
Общая трудоёмкость дисциплины, час	**108**
Контактная работа обучающихся с преподавателем по видам учебных занятий (всего), в т.ч.:	**102/62**
Занятия лекционного типа (лекции)	44/20
Занятия семинарского типа (семинары, практические занятия, практикумы, коллоквиумы и иные аналогичные занятия)	48/32
Лабораторные работы	10/10
Самостоятельная работа всего, в т.ч.:	**6/42**
Самоподготовка по темам (разделам) дисциплины	**-**
Выполнение курсового проекта /курсовой работы	**-**
Контроль (часы на экзамен, зачёт)	**0/4**
Промежуточная аттестация	**Зачёт**

Примечание: *-/- объем часов соответственно для очной, очно-заочной формы обучения*

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

В процессе освоения дисциплины может применяться электронное обучение и дистанционные образовательные технологии.

В процессе освоения дисциплины обучающиеся обеспечены доступом к электронной информационно-образовательной среде и электронно-библиотечным системам.

3.2. Содержание дисциплины, структурированное по темам

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные занятия, час	Практические занятия, час		
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 1. Современные угрозы сетевой безопасности** 1.1 Защита сетей 1.2 Сетевые угрозы 1.3 Нейтрализация угроз	4/1				Внеаудиторное тестирование (тест)
	Лабораторная работа №1 Социальная инженерия		2/2			Отчёт по работе
	Лабораторная работа №2 Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак		4/4			Отчёт по работе
	Самостоятельная работа.				0/2	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 2. Обеспечение безопасности сетевых устройств** 2.1 Защита доступа к устройствам 2.2 Назначение административных ролей 2.3 Мониторинг устройств и управление ими 2.4 Использование автоматических функций обеспечения безопасности	4/1				Внеаудиторное тестирование (тест)
	Практическая работа №1 Packet Tracer - Настройка маршрутизаторов Cisco для операций Syslog, NTP и SSH			4/2		Отчёт по работе
	Лабораторная работа №3 Защита маршрутизатора для административного доступа		4/4			Отчёт по работе
	Самостоятельная работа				0/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 3. Аутентификация, авторизация и учёт** 3.1 Назначение AAA 3.2 Локальная аутентификация AAA 3.3 Серверное решение AAA 3.4 Серверная аутентификация AAA 3.5 Серверная авторизация и учит AAA	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №2. Packet Tracer - Настройка аутентификации AAA на маршрутизаторах Cisco Routers			4/2		Отчёт по работе
	Самостоятельная работа				0/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 4. Внедрение технологий межсетевого экрана** 4.1 Списки контроля доступа 4.2 Технологии межсетевых экранов 4.3 Зональные межсетевые экраны	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №3. Packet Tracer - Настройка расширенных списков ACL			2/2		Отчёт по практической рабо-

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные занятия, час	Практические занятия, час		
	Сценарий 1					те
	Практическая работа №4. Packet Tracer - Настройка сценария расширенных списков ACL 2			2/2		Отчёт по практической работе
	Практическая работа №5. Packet Tracer - Настройка списков управления доступом IP для смягчения атак			4/2		Отчёт по практической работе
	Практическая работа №6. Packet Tracer - Настройка IPv6 ACLS			4/2		Отчёт по практической работе
	Практическая работа №7. Packet Tracer - Настройка межзонного межсетевого экрана (ZPF).			4/2		Отчёт по практической работе
	Самостоятельная работа.				0/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 5. Внедрение системы предотвращения вторжений** 5.1 Технологии IPS 5.2 Сигнатуры IPS 5.3 Внедрение IPS	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №8. Packet Tracer - Настройка системы предотвращения вторжений IOS (IPS) с помощью CLI			4/2		Отчёт по практической работе
	Самостоятельная работа				0/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 6. Обеспечение безопасности локальной сети (LAN)** 6.1 Безопасность оконечных устройств 6.2 Факторы, которые необходимо учитывать при обеспечении безопасности на уровне 2	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №9. Packet Tracer - Обеспечение безопасности на 2-м уровне			4/2		Отчёт по практической работе
	Практическая работа №10. Packet Tracer - Обеспечение безопасности VLAN на 2-м уровне			4/2		Отчёт по практической работе
	Самостоятельная работа				1/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 7. Криптографические системы** 7.1 Криптографические сервисы 7.2 Обеспечение базового уровня целостности и аутентификации 7.3 Конфиденциальность 7.4 Криптография с открытыми ключами	4/2				Внеаудиторное тестирование (тест)
	Самостоятельная работа				1/4	Самостоятельное изучение учебных мате-

Планируемые результаты освоения: код формируемой компетенции и индикаторы достижения компетенций	Наименование разделов, тем	Виды учебной работы				Формы текущего контроля (наименование оценочного средства)
		Контактная работа			Самостоятельная работа, час	
		Лекции, час	Лабораторные занятия, час	Практические занятия, час		
						риалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 8. Внедрение виртуальных частных сетей (VPN)** 8.1 Сети VPN 8.2 Компоненты сети IPsec VPN и их функционирование 8.3 Реализация сетей Site-to-Site IPsec VPN с помощью CLI	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №11. Packet Tracer - Настройка и проверка VPN IPsec типа "сеть-сеть" с помощью CLI			4/4		Отчёт по практической работе
	Самостоятельная работа				1/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 9. Внедрение многофункционального устройства защиты Cisco Adaptive Security Appliance** 9.1 Знакомство с ASA 9.2 Конфигурация межсетевого экрана ASA	4/2				Внеаудиторное тестирование (тест)
	Практическая работа №12. Packet Tracer - Настройка основных параметров ASA и брандмауэра с помощью CLI			4/4		Отчёт по практической работе
	Самостоятельная работа				1/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 10. Многофункциональное устройство обеспечения безопасности Cisco ASA с расширенным функционалом** 10.1 ASA Security Device Manager 10.2 Настройка VPN в ASA	4/2				Внеаудиторное тестирование (тест)
	Самостоятельная работа				1/4	Самостоятельное изучение учебных материалов
ОПК-10: ИОПК-10.3; ПК-6: ИПК-6.2	**Тема 11. Управление безопасной сетью** 11.1 Тестирование безопасности сети 11.2 Разработка комплексной политики безопасности	4/2				
	Практическая работа №13. Packet Tracer - Задача по интеграции навыков			4/4		Отчёт по практической работе
	Самостоятельная работа				1/4	
	ИТОГО	**44/20**	**10/10**	**48/32**	**6/42**	

Примечание : -/ - *объем часов соответственно для очной/очно-заочной формы обучения*

4. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

4.1. Общие методические рекомендации по освоению дисциплины, образовательные технологии

Дисциплина реализуется посредством проведения контактной работы с обучающимися (включая проведение текущего контроля успеваемости), самостоятельной работы обучающихся и промежуточной аттестации.

При проведении учебных занятий по дисциплине обеспечивается развитие у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств (включая проведение групповых практических работ).

Преподавание дисциплины ведется с применением следующих видов **образовательных технологий:**

- балльно-рейтинговая технология оценивания;
- электронное обучение;

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

4.2. Методические указания для обучающихся по освоению дисциплины на занятиях лекционного типа

Лекционный курс предполагает систематизированное изложение основных вопросов тематического плана. В ходе лекционных занятий раскрываются базовые вопросы в рамках каждой темы дисциплины. Обозначаются ключевые аспекты тем, а также делаются акценты на наиболее сложные и важные положения изучаемого материала.

Лекционные занятия проводятся в поточной аудитории с применением мультимедийного проектора в виде учебной презентации или в ЭИОС университета.

В ходе лекционных занятий рекомендуется конспектирование учебного материала. Возможно ведение конспекта лекций в виде интеллект-карт.

Отдельные темы предлагаются для самостоятельного изучения (конспектируются).

Материалы лекций являются опорной основой для подготовки обучающихся к практическим занятиям / лабораторным работам и выполнения заданий самостоятельной работы, а также к мероприятиям текущего контроля успеваемости и промежуточной аттестации по дисциплине.

4.3. Методические указания для обучающихся по освоению дисциплины на лабораторных работах

Подготовку к каждой лабораторной работе студент должен начать с ознакомления с планом занятия, который отражает содержание предложенной темы. Каждая выполненная работа с оформленным отчетом по ней подлежит защите преподавателю.

При оценивании лабораторных работ учитывается следующее:

- качество выполнения экспериментально-практической части работы и степень соответствия результатов работы заданным требованиям;
- качество оформления отчета по работе;
- качество устных ответов на контрольные вопросы при защите работы.

Лабораторные работы организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение всех заданий на практических занятиях.

4.3. Методические указания для обучающихся по освоению дисциплины на занятиях семинарского типа/ на практических занятиях

Практические (семинарские) занятия представляют собой детализацию лекционного теоретического материала, проводятся в целях закрепления курса и охватывают все основные разделы. Основной формой проведения практических занятий является решение задач по сетевому проектированию и настройке сетевого оборудования с использованием возможностей сетей лаборатории Высшей школы передовых и производственных технологий, а также с использованием специализированного программного обеспечения: Wireshark, Cisco Packet Tracer, Tera Term, PuTTY.

Практические занятия обучающихся обеспечивают:

- проверку и уточнение знаний, полученных на лекциях;
- получение умений и навыков проектирования, моделирование, организацию сетей. Поиск и устранение неисправностей;
- подведение итогов занятий по рейтинговой системе, согласно технологической карте дисциплины.

Практические занятия организуются, в том числе в форме практической подготовки, которая предусматривает участие обучающихся в выполнении отдельных элементов работ, связанных с будущей профессиональной деятельностью.

Практическая подготовка предусматривает: выполнение всех заданий на практических занятиях.

4.4. Методические указания по самостоятельной работе обучающихся

Самостоятельная работа обеспечивает подготовку обучающегося к аудиторным занятиям и мероприятиям текущего контроля и промежуточной аттестации по изучаемой дисциплине. Результаты этой подготовки проявляются в активности обучающегося на занятиях и в качестве выполненных практических заданий и других форм текущего контроля.

Самостоятельная работа студентов включает:

1. Изучение учебной литературы по курсу.
2. Работу с ресурсами Интернет
3. Самостоятельное изучение учебных материалов

При выполнении заданий для самостоятельной работы рекомендуется проработка материалов лекций по каждой пройденной теме, а также изучение рекомендуемой литературы.

Для обучающихся по заочной форме обучения самостоятельная работа является основным видом учебной деятельности.

Для обеспечения самостоятельной работы обучающихся используется электронный учебный курс, созданный в ЭИОС университета http://sdo.tolgas.ru/.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Вся литература, включённая в данный перечень, представлена в виде электронных ресурсов в электронной библиотеке университета (ЭБС). Литература, используемая в печатном виде, представлена в научной библиотеке университета в объёме не менее 0,25 экземпляров на одного обучающегося.

Основная литература:

1. Защита информации : учеб. пособие для вузов по направлению подгот. Инфокоммуникац. технологии и системы связи квалификации (степ.) "бакалавр" и квалификации (степ.) "магистр" / А. П. Жук, Е. П. Жук, О. М. Лепешкин, А. И. Тимошкин. - 3-е изд. - Документ read. - Москва : РИОР [и др.], 2024. - 400 с. - (Высшее образование). – URL: https://znanium.ru/read?id=443251 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. – ISBN 978-5-369-01759-3. - 978-5-16-106478-8. – Текст : электронный.

2. Салкин, Д. А. Компьютерные сети. Технологии сетевых интерфейсов. Программное обеспечение и методы диагностики : учебное пособие / Д. А. Салкин, С. Н. Ивлиев, А. В. Пантелеев. - Документ read. – Москва [и др.] : Инфра-Инженерия, 2024. – 220 с. – URL: https://znanium.ru/read?id=451736 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. – ISBN 978-5-9729-1917-8. – Текст : электронный.

3. Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений : учеб. пособие / С. Н. Никифоров. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2023. - 93 с. – Прил. – URL: https://reader.lanbook.com/book/288974 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. – ISBN 978-5-507-45868-4. – Текст : электронный.

4. Никифоров, С. Н. Методы защиты информации. Защищенные сети : учеб. пособие / С. Н. Никифоров. - Документ Reader. - Санкт-Петербург [и др.] : Лань, 2021. - 94 с. - (Учебники для вузов. Специальная литература). - URL: https://e.lanbook.com/reader/book/169311/#1 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. - ISBN 978-5-8114-3099-4. - Текст : электронный.

5. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. - Изд. 5-е, стер. - Документ Reader. - Санкт-Петербург : Лань, 2023. - 122 с. – URL: https://reader.lanbook.com/book/293009 (дата обращения: 24.02.2025). - Режим доступа: для авториз. пользователей. – ISBN 978-5-507-46010-6. – Текст : электронный.

Дополнительная литература:

6. Семыкина, Н. А. Методы теории оптимального управления в задачах защиты компьютерных систем от вирусных атак : учеб. пособие по специальности 10.05.01 Компьютер. безопасность / Н. А. Семыкина ; Твер. гос. ун-т. - Документ read. - Тверь : ТГУ, 2020. - 100 с. - URL: https://reader.lanbook.com/book/217949 (дата обращения: 12.12.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-7609-1574-0. - Текст : электронный.

7. Баланов, А. Н. Защита информационных систем. Кибербезопасность : учеб. пособие / А. Н. Баланов. - Изд. 2-е, стер. - Документ read. - Санкт-Петербург [и др.] : Лань, 2025. - 277 с. - Прил. - URL: https://reader.lanbook.com/book/438971 (дата обращения: 14.11.2024). - Режим доступа: для авториз. пользователей. - ISBN 978-5-507-50467-1. - Текст : электронный.

8. Сычев, Ю. Н. Защита информации и информационная безопасность : учеб. пособие для студентов высш. учеб. заведений по направлению подгот. 10.03.01. "Информационная безопасность" (квалификация (степень) "бакалавр") / Ю. Н. Сычев. - Документ read. - Москва : ИНФРА-М, 2023. – 201 с. – (Высшее образование - Бакалавриат). – Прил. – URL: https://znanium.ru/read?id=420080 (дата обращения: 29.04.2025). - Режим доступа: для авториз. пользователей. – ISBN 978-5-16-107471-8. – Текст : электронные.

5.2. Профессиональные базы данных, информационно-справочные системы, интернет-ресурсы

1. eLIBRARY.RU: научная электронная библиотека: сайт. – Москва, 2000 - . - URL:https://elibrary.ru (дата обращения: 09.11.2019). – Режим доступа: для зарегистрир. пользователей. – Текст: электронный.
2. Polpred.com. Обзор СМИ. Полнотекстовая, многоотраслевая база данных (БД): сайт. – Москва. – URL: http://polpred.com/ (дата обращения: 11.05.2025). – Режим доступа: по подписке.
3. Znanium.com: электронно-библиотечная система: сайт. – Москва. – URL: http://znanium.com/ (дата обращения: 11.05.2024). – Режим доступа: для зарегистрированных пользователей.
4. Всероссийский институт научной и технической информации (ВИНИТИ РАН): базы данных по естественным, точным и техническим наукам: сайт. – Москва. – URL: http://www.viniti.ru/ (дата обращения: 11.05.2024). – Режим доступа: открытый.
5. Издательство Лань: электронно-библиотечная система: сайт. – Санкт-Петербург. – URL: https://e.lanbook.com/ (дата обращения: 11.05.2024). – Режим доступа: для зарегистрированных пользователей.
6. КонсультантПлюс: справочная правовая система: сайт / ЗАО "КонсультантПлюс". – Москва, 1992 - . - URL: http://www.consultant.ru (дата обращения 26.10.2020). - Текст: электронный.
7. Открытое образование: образовательная платформа: сайт. – Москва. – URL: https://openedu.ru/ (дата обращения: 11.05.2024). – Режим доступа: открытый.
8. Электронная библиотека: библиотека диссертаций: сайт / Российская государственная библиотека. – Москва : РГБ, 2003 - . - URL: http://diss.rsl.ru/?lang=ru (дата обращения: 20.10.2020). – Режим доступа: для зарегистрир. пользователей. – Текст:электронный.
9. Электронная библиотечная система Поволжского государственного университета сервиса: сайт. – Тольятти–. – URL: http://elib.tolgas.ru/ (дата обращения: 11.05.2024). – Режим доступа: для зарегистрированных пользователей.
10. Cisco VIRL (Virtual Internet Routing Lab): среда проектирования и моделирования сетей: сайт. – Сан-Хосе. – URL: https://learningnetwork.cisco.com/s/virl (дата обращения: 11.05.2025). – Режим доступа: открытый.
11. Cisco dCloud: демонстрационная облачная платформа: сайт. – Сан-Хосе. – URL: http://dcloud.cisco.com (дата обращения: 11.05.2025). – Режим доступа: открытый.

5.3. Программное обеспечение

Информационное обеспечение учебного процесса по дисциплине осуществляется с использованием следующего программного обеспечения (лицензионного и свободно распространяемого), в том числе отечественного производства:

№ п/п	Наименование	Условия доступа
1.	Microsoft Windows	из внутренней сети университета (лицензионный договор)
2.	Microsoft Office	из внутренней сети университета (лицензионный договор)
3.	СДО MOODLE	из любой точки, в которой имеется доступ к сети Интернет (лицензионный договор)
4.	Браузер	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
5.	Wireshark	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое
6.	Cisco Packet Tracer/GNS3	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое

№ п/п	Наименование	Условия доступа
7.	Tera Term	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое
8.	PuTTY	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)
9.	Oracle VirtualBox	из любой точки, в которой имеется доступ к сети Интернет (свободно распространяемое)

6. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Помещения представляют собой учебные аудитории для проведения учебных занятий, предусмотренных учебным планом и рабочей программой дисциплины, оснащенные оборудованием и техническими средствами обучения.

Занятия лекционного типа. Учебные аудитории для занятий лекционного типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук), учебно-наглядные пособия (презентации по темам лекций), обеспечивающие тематические иллюстрации, соответствующие данной программе дисциплины.

Занятия семинарского типа. Учебные аудитории для занятий семинарского типа укомплектованы мебелью и техническими средствами обучения, служащими для представления учебной информации (стационарные или переносные наборы демонстрационного оборудования (проектор, экран, компьютер/ноутбук).

– 10 ПК с двумя сетевыми картами (iP2.6Ghz/intel/775/2GbDDR/250G/ LCd 19", с установленным программным обеспечением: Браузер, Wireshark, Cisco Packet Tracer/GNS3, Tera Term/PuTTY, Oracle VirtualBox;

– локальная сеть 100 мб с доступом в Интернет 50 мб;

– проектор мультимедийный;

– проекционный экран.

Лабораторные работы. Для проведения лабораторных работ используется учебная аудитория «Т407» или любая аудитория ВУЗа, оснащённая следующим оборудованием и программным обеспечением:

– Коммутационные стойки с сетевым оборудованием 2 шт ;

1. CISCO 2801, Маршрутизатор 2801 Router/AC PWR,2FE, 4slots (2HWICs) - 6 шт.
2. CAB-SS-V35FC, Кабель V.35 Cable, DCE Female to Smart Serial, - 6 шт.
3. CAB-SS-V35MT, Кабель V.35 Cable, DTE Male to Smart Serial, 10 - 6 шт.
4. HWIC-2A/S, Модуль 2-Port Async/Sync Serial WAN Interface Card - 6 шт.
5. WS-C2960-24TT-L, Коммутатор Catalyst 2960 24 10/100 + 2 1000B - 6 шт.
6. Неуправляемый коммутатор D-Link DES-1016D, 16-портовый, 10/100Base-TX - 2 шт.
7. Управляемый коммутатор D-link-3200 - 2 шт.
8. D-link 3810 управляемый коммутатор 3 уровня с 24 портами 10/100Base-TX и 4 комбопортами 100/1000Base-T/SFP - 2 шт.
9. Беспроводные маршрутизаторы D-Link - 2 шт.

– локальная сеть 100 мб с доступом в Интернет 50 мб;

– проектор мультимедийный Acer X1273;

– проекционный экран Seha;

– 10 ПК с двумя сетевыми картами (iP2.6Ghz/intel/775/2GbDDR/250G/ LCd 19"). с установленным программным обеспечением: Браузер, Wireshark, Cisco Packet Tracer/GNS3, Tera Term/PuTTY, Oracle VirtualBox;

Промежуточная аттестация. Для проведения промежуточной аттестации по дисциплине используются компьютерные классы, оснащенные компьютерной техникой с возможностью подключения к сети Интернет и обеспечением доступа в электронную информационно-образовательную среду университета и/или учебные аудитории, укомплектованные мебелью и техническими средствами обучения.

Самостоятельная работа. Помещения для самостоятельной работы оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и доступом к электронной информационно-образовательной среде университета. Для организации самостоятельной работы обучающихся используются:

– компьютерные классы университета;

– библиотека (медиазал), имеющая места для обучающихся, оснащенные компьютерами с доступом к базам данных и сети Интернет.

Электронная информационно-образовательная среда университета (ЭИОС). Каждый обучающийся в течение всего периода обучения обеспечен индивидуальным неограниченным доступом к электронной информационно-образовательной среде университета (ЭИОС) http://sdo.tolgas.ru/ из любой точки, в которой имеется доступ к информационно-телекоммуникационной сети "Интернет", как на территории университета, так и вне ее.

ЭИОС университета обеспечивает:

– доступ к учебным планам, рабочим программам дисциплин (модулей), программам практик, электронным учебным изданиям и электронным образовательным ресурсам, указанным в рабочих программах дисциплин (модулей), программах практик;

– формирование электронного портфолио обучающегося, в том числе сохранение его работ и оценок за эти работы.

В случае реализации образовательной программы с применением электронного обучения, дистанционных образовательных технологий ЭИОС дополнительно обеспечивает:

– фиксацию хода образовательного процесса, результатов промежуточной аттестации и результатов освоения образовательной программы;

– проведение учебных занятий, процедур оценки результатов обучения, реализация которых предусмотрена с применением электронного обучения, дистанционных образовательных технологий;

– взаимодействие между участниками образовательного процесса, в том числе синхронное и (или) асинхронное взаимодействия посредством сети "Интернет".

7. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБУЧЕНИЯ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

При необходимости рабочая программа дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для дистанционного обучения. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).

В случае необходимости, обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося) а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида, могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей, в том числе с применением электронного обучения и дистанционных технологий:

- для лиц с нарушениями зрения: в печатной форме увеличенным шрифтом; в форме электронного документа; в форме аудиофайла (перевод учебных материалов в аудиоформат); в печатной форме на языке Брайля; индивидуальные консультации с привлечением тифлосурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями слуха: в печатной форме; в форме электронного документа; видеоматериалы с субтитрами; индивидуальные консультации с привлечением сурдопереводчика; индивидуальные задания и консультации.
- для лиц с нарушениями опорно-двигательного аппарата: в печатной форме; в форме электронного документа; в форме аудиофайла; индивидуальные задания и консультации.

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

8.1. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Для оценки знаний, умений, навыков и уровня сформированности компетенции по дисциплине применяется балльно-рейтинговая система контроля и оценки успеваемости студентов. В основу балльно-рейтинговой системы положены принципы, в соответствии с которыми формирование рейтинга студента осуществляется в ходе текущего контроля успеваемости. Максимальное количество баллов в семестре – 100.

Шкала оценки результатов освоения дисциплины, сформированности результатов обучения

Форма проведения промежуточной аттестации	**Шкалы оценки уровня сформированности результатов обучения**		**Шкала оценки уровня освоения дисциплины**		
	Уровневая шкала оценки компетенций	100 бальная шкала, %	100 бальная шкала, %	5-балльная шкала, дифференцированная оценка/балл	недифференцированная оценка
Зачёт	допороговый	ниже 61	ниже 61	«неудовлетворительно» / 2	не зачтено
	пороговый	61-85,9	61-69,9	«удовлетворительно» / 3	зачтено
			70-85,9	«хорошо» / 4	зачтено
	повышенный	86-100	86-100	«отлично» / 5	зачтено

По итогам текущей успеваемости студенту может быть выставлена оценка по промежуточной аттестации в соответствии за набранными за семестр баллами (по накопительному рейтингу). Студентам, набравшим в ходе текущего контроля успеваемости по дисциплине от 61 до 100 баллов и выполнившим все обязательные виды запланированных учебных занятий, по решению преподавателя без прохождения промежуточной аттестации выставляется оценка в соответствии со шкалой оценки результатов освоения дисциплины.

***Результат обучения считается сформированным (повышенный уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент исчерпывающе, последовательно, четко и логически стройно излагает учебный материал; свободно справляется с задачами, вопросами и другими видами заданий, требующих применения знаний, использует в ответе дополнительный материал; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 86 до 100, что соответствует повышенному уровню сформированности результатов обучения.*

***Результат обучения считается сформированным (пороговый уровень)**, если теоретическое содержание курса освоено полностью; при устных собеседованиях студент последовательно, четко и логически стройно излагает учебный материал; справляется с задачами, вопросами и другими видами заданий, требующих применения знаний; все предусмотренные рабочей учебной программой задания выполнены в соответствии с установленными требованиями, студент способен анализировать полученные результаты; проявляет самостоятельность при выполнении заданий, качество их выполнения оценено числом баллов от 61 до 85,9, что соответствует пороговому уровню сформированности результатов обучения.*

***Результат обучения считается несформированным**, если студент при выполнении заданий не демонстрирует знаний учебного материала, допускает ошибки, неуверенно, с большими затруднениями выполняет задания, не демонстрирует необходимых умений, качество выполненных заданий не соответствует установленным требованиям, качество их выполнения оценено числом баллов ниже 61, что соответствует допороговому уровню.*

Формы текущего контроля успеваемости

Формы текущего контроля	Количество контрольных точек	Количество баллов за 1 контр. точку	Макс. возм. кол-во баллов
Отчёт по практической работе	13	2	26
Отчёт по лабораторной работе	3	2	6
Тестирование по темам лекционных занятий	11	3	33
Творческий рейтинг (участие в конференциях, олимпиадах, проектной деятельности и т.п.)	1	35	35
Итого по дисциплине			**100 баллов**

Система оценивания представлена в электронном учебном курсе по дисциплине http://sdo.tolgas.ru/.

8.2. Типовые контрольные задания или иные материалы для ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

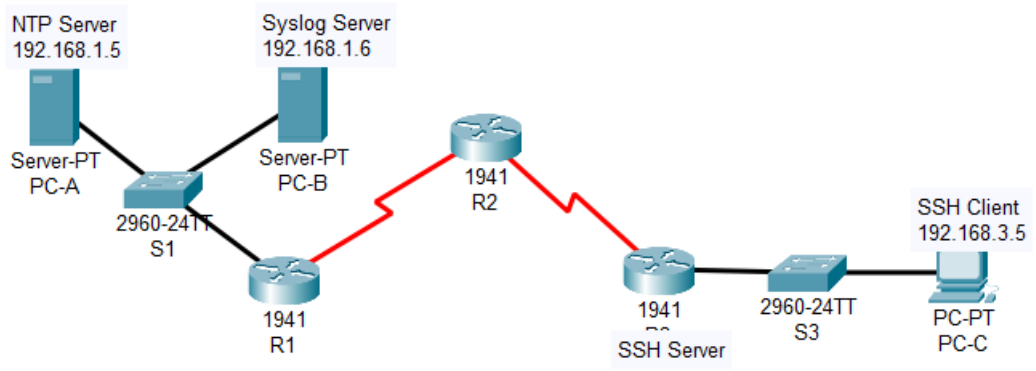
8.2.1. Типовые задания к практическим (семинарским) занятиям

Практическая работа №1 Packet Tracer - Настройка маршрутизаторов Cisco для операций Syslog, NTP и SSH.

Цель работы: получение навыков настройки маршрутизаторов Cisco для операций Syslog, NTP и SSH

Задачи:
1. Настройка аутентификации OSPF MD5.
2. Настройка NTP.
3. Настройка маршрутизаторов для записи сообщений в журнал на сервере Syslog.
4. Настройка маршрутизатора R3 для поддержки подключений SSH.

Топология:



Сценарий:
В этом задании вы настроите аутентификацию OSPF MD5 для защиты обновлений маршрутизации.
NTP Server является главным NTP-сервером в этом задании. Вы настроите аутентификацию на NTP-сервере и маршрутизаторах. Вы настроите маршрутизаторы так, чтобы NTP-сервер мог синхронизировать программные часы с сервером времени. Вы также настроите маршрутизаторы для периодического обновления аппаратных часов с учетом времени, полученного с NTP-сервера.
Сервер Syslog будет обеспечивать ведение журнала сообщений в данном задании. Вы настроите маршрутизаторы для определения удаленного хоста (сервера Syslog), который будет получать сообщения журнала.
Потребуется настроить сервис временных меток для ведения журналов на маршрутизаторах. Очень важно, чтобы в сообщениях Syslog отображались правильные дата и время, когда служба Syslog используется для мониторинга сети.
Вы настроите защищенное управление маршрутизатором R3 с помощью протокола SSH вместо Telnet. Серверы были предварительно настроены для использования служб NTP и Syslog соответственно. Для NTP не потребуется аутентификация. На маршрутизаторах были предварительно настроены следующие пароли.
- Пароль привилегированного доступа: **ciscoenpa55**
- Пароль для линий VTY: **ciscovtypa55**

Примечание. Примечание. MD5 – самый стойкий алгоритм шифрования, поддерживаемый в версии Packet Tracer, которая использовалась для разработки этого задания (6.2). Хотя MD5 имеет известные уязвимости, следует использовать алгоритм шифрования, отвечающий требованиям вашей организации к безопасности. В этом задании требования к безопасности предписывают использовать MD5.

Таблица адресации

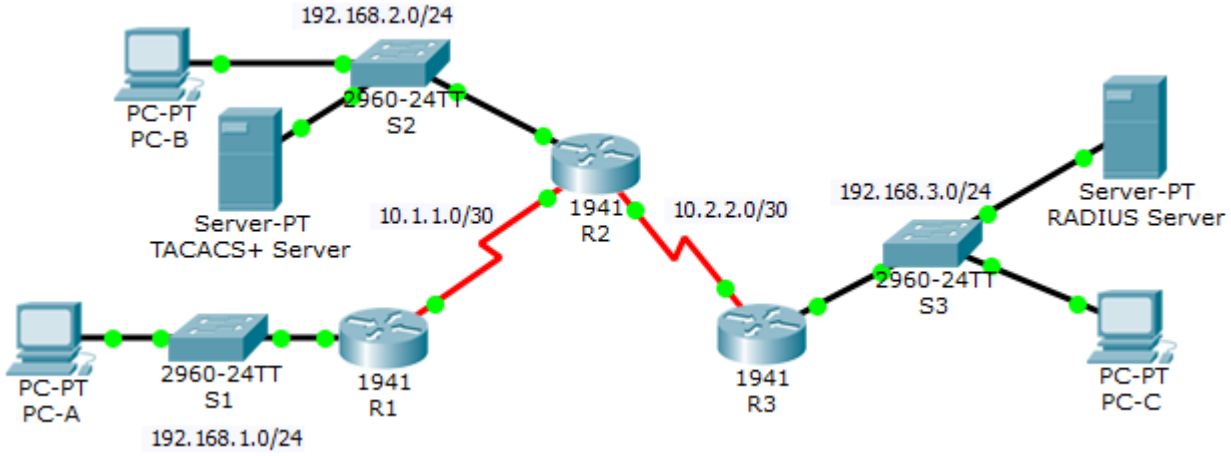
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммутатора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/5
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.5	255.255.255.0	192.168.1.1	S1 F0/6
PC-B	NIC	192.168.1.6	255.255.255.0	192.168.1.1	S2 F0/18
PC-C	NIC	192.168.3.5	255.255.255.0	192.168.3.1	S3 F0/18

Практическая работа №2 Packet Tracer - Настройка аутентификации AAA на маршрутизаторах Cisco Routers.

Цель работы: закрепление навыков настройки учётной записи локального пользователя на маршрутизаторе и настройка аутентификации на линиях консоли и VTY с использованием локального решения AAA

Задачи:
1. Настройка учётной записи локального пользователя на маршрутизаторе R1 и настройка аутентификации на линиях консоли и VTY с использованием локального решения AAA.
2. Проверка локальной аутентификации AAA с консоли R1 и клиента PC-A.
3. Настройка серверной аутентификации AAA по протоколу TACACS+.
4. Проверка серверной аутентификации AAA с клиента PC-B.
5. Настройка серверной аутентификации AAA по протоколу RADIUS.
6. Проверка серверной аутентификации AAA с клиента PC-C.

Топология:



Сценарий:

Топология сети включает маршрутизаторы R1, R2 и R3. В настоящее время все административные меры безопасности основаны на знании секретного пароля. Ваша задача – настроить и проверить решения AAA на базе сервера.

Вы создадите учётную запись локального пользователя и настроите локальную аутентификацию AAA на маршрутизаторе R1 для проверки входа в консоль и VTY.

- Учетная запись пользователя: Admin1 и пароль admin1pa55

Затем на маршрутизаторе R2 вы настроите поддержку серверной аутентификации по протоколу TACACS+. Сервер TACACS+ был предварительно настроен следующим образом.

- Клиент: R2 с ключевым словом tacacspa55
- Учетная запись пользователя: Admin2 и пароль admin2pa55

Наконец, на маршрутизаторе R3 вы настроите поддержку серверной аутентификации по протоколу RADIUS. Сервер RADIUS был предварительно настроен следующим образом.

- Клиент: R3 с ключевым словом radiuspa55
- Учетная запись пользователя: Admin3 и пароль admin3pa55

На маршрутизаторах также были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Протокол маршрутизации OSPF с аутентификацией MD5, пароль: MD5pa55

Примечание. Линии консоли и линии vty не были предварительно настроены.

Примечание. IOS версии 15.3 использует SCRYPT в качестве алгоритма хеширования для надёжного шифрования, но текущая версия IOS, поддерживаемая в Packet Tracer, использует алгоритм MD5. Используйте всегда наиболее надёжный вариант, доступный на вашем оборудовании.

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 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	Н/П	Н/П
R2	G0/0	192.168.2.1	255.255.255.0	Н/П	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.1	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	10.2.2.2	255.255.255.252	Н/П	Н/П
Сервер TACACS+	NIC	192.168.2.2	255.255.255.0	192.168.2.1	S2 F0/6
Сервер RADIUS	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

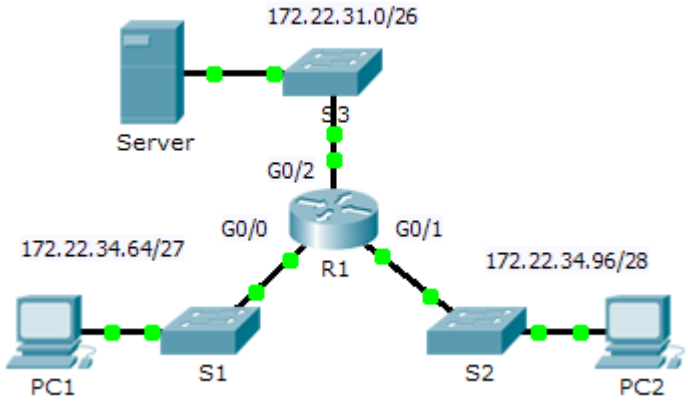
Практическая работа №3 Packet Tracer - Настройка расширенных списков ACL Сценарий 1.

Цель работы: закрепить навыки настройки расширенных списков контроля доступа (ACL)

Задачи:

1. Настройка, применение и проверка расширенного нумерованного списка ACL
2. Настройка, применение и проверка расширенного именованного списка ACL

Топология:



Сценарий:
Двум сотрудникам требуется доступ к сервисам, которые предоставляет сервер. Компьютеру PC1 нужен только FTP доступ, а компьютеру PC2 – только веб-доступ. Оба компьютера могут отправлять эхо-запросы серверу, но не друг другу.

Таблица адресации

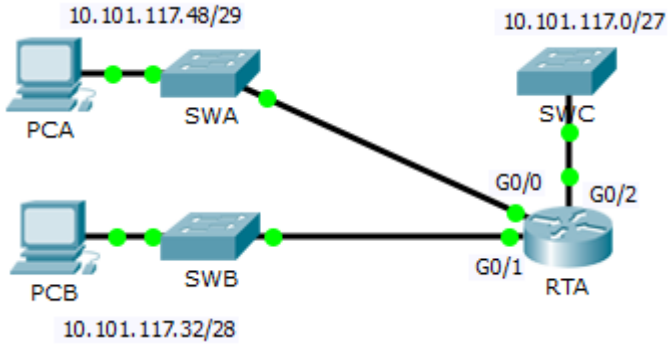
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	172.22.34.65	255.255.255.224	Н/П
	G0/1	172.22.34.97	255.255.255.240	Н/П
	G0/2	172.22.34.1	255.255.255.192	Н/П
Сервер	NIC	172.22.34.62	255.255.255.192	172.22.34.1
PC1	NIC	172.22.34.66	255.255.255.224	172.22.34.65
PC2	NIC	172.22.34.98	255.255.255.240	172.22.34.97

Практическая работа №4 Packet Tracer - Настройка сценария расширенных списков ACL 2.

Цель работы: применение и проверка расширенного нумерованного списка ACL

Задачи:
1. Настройка, применение и проверка расширенного нумерованного списка ACL
2. Вопросы для повторения

Топология:



Сценарий:
В этом сценарии устройствам в одной локальной сети разрешён удалённый доступ к устройствам в другой локальной сети по протоколу SSH. Весь трафик из других сетей, кроме ICMP, отклоняется.
На коммутаторах и маршрутизаторе также были предварительно настроены следующие параметры.
- Пароль привилегированного доступа: ciscoenpa55
- Пароль консоли: ciscoconpa55
- Имя локального пользователя и пароль: Admin/Adminpa55

Таблица адресации

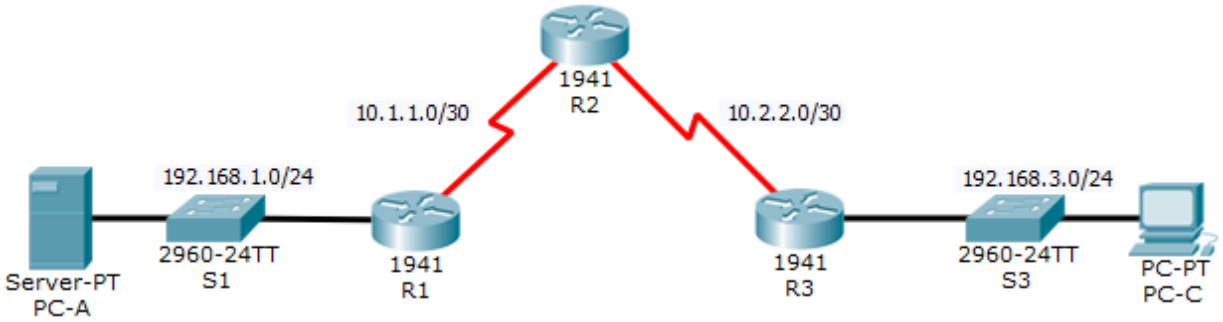
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
RTA	G0/0	10.101.117.49	255.255.255.248	Н/П
	G0/1	10.101.117.33	255.255.255.240	Н/П
	G0/2	10.101.117.1	255.255.255.224	Н/П
PCA	NIC	10.101.117.51	255.255.255.248	10.101.117.49
PCB	NIC	10.101.117.35	255.255.255.240	10.101.117.33
SWA	VLAN 1	10.101.117.50	255.255.255.248	10.101.117.49
SWB	VLAN 1	10.101.117.34	255.255.255.240	10.101.117.33
SWC	VLAN 1	10.101.117.2	255.255.255.224	10.101.117.1

Практическая работа №5 Packet Tracer - Настройка списков управления доступом IP для смягчения атак.

Цель работы: получить практические навыки настройки списков ACL на маршрутизаторах R1 и R3 для нейтрализации атак

Задачи:
1. Проверка связи между устройствами перед настройкой межсетевого экрана.
2. Использование списков ACL для настройки удалённого доступа к маршрутизаторам доступно только со станции управления PC-C.
3. Настройка списков ACL на маршрутизаторах R1 и R3 для нейтрализации атак.
4. Проверка работоспособности функции ACL

Топология:



Сценарий:
Доступ к маршрутизаторам R1, R2 и R3 должен быть разрешен только со станции управления PC-C. PC-C также используется для проверки связи с PC-A – сервером, предоставляющим сервисы DNS, SMTP, FTP и HTTPS.
Стандартный порядок действий – применить списки ACL на граничных маршрутизаторах для нейтрализации обычных угроз на основе IP-адресов источника и назначения. В этом задании

вы с данной целью создадите списки ACL на граничных маршрутизаторах R1 и R3. Затем вы проверите работоспособность списков ACL с внутренних и внешних хостов.

На маршрутизаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Пароль для консоли: ciscoconpa55
- Имя пользователя и пароль для входа SSH: SSHadmin/ciscosshpa55
- IP-адресация
- Статическая маршрутизация

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
	Lo0	192.168.2.1	255.255.255.0	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/П	Н/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

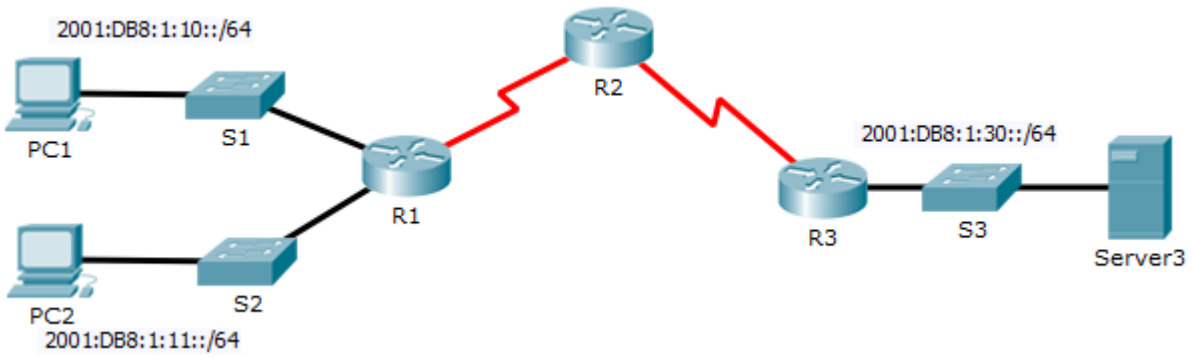
Практическая работа №6 Packet Tracer - Настройка IPv6 ACLS.

Цель работы: получить практические навыки настройки IPv6 ACLS

Задачи:

1. Настройка, применение и проверка списка ACL для IPv6
2. Настройка, применение и проверка второго списка ACL для IPv6

Топология:



Сценарий:

Данные журналов свидетельствуют о том, что компьютер в сети 2001:DB8:1:11::0/64 многократно обновляет веб страницу. Это вызывает атаку «Отказ в обслуживании» (DoS) на сервер Server3. Пока не удастся идентифицировать клиент и решить проблему, необходимо блокировать HTTP- и HTTPS-доступ к этой сети с помощью списка контроля доступа.

Таблица адресации

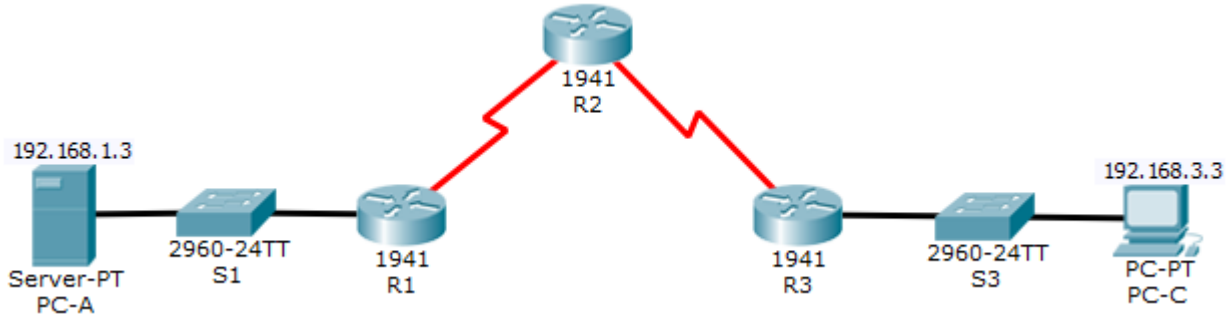
Устройство	Интерфейс	Адрес IPv6/префикс	Шлюз по умолчанию
Server3	NIC	2001:DB8:1:30::30/64	FE80::30

Практическая работа №7 Packet Tracer - Настройка межзонного межсетевого экрана (ZPF).

Цель работы: получить навыки настройки зонального межсетевого экрана

Задачи:
1. Проверка связи между устройствами перед настройкой межсетевого экрана.
2. Настройка зонального межсетевого экрана (ZPF) на маршрутизаторе R3.
3. Проверка работоспособности межсетевого экрана ZPF с помощью эхо-запросов, SSH-подключения и веб браузера.

Топология:



Сценарий:

ZPF – новейшее достижение в технологиях межсетевых экранов Cisco. В этом задании вы настроите простой межсетевой экран ZPF на граничном маршрутизаторе R3, разрешающий внутренним хостам доступ к внешним ресурсам и блокирующий доступ внешних хостов к внутренним ресурсам. Затем вы проверите работоспособность межсетевого экрана с внутренних и внешних хостов.

На маршрутизаторах были предварительно настроены следующие параметры.
- Пароль консоли: ciscoconpa55
- Пароль для линий VTY: ciscovtypa55
- Пароль привилегированного доступа: ciscoenpa55
- Имена и IP-адреса хостов
- Имя локального пользователя и пароль: Admin/Adminpa55
- Статическая маршрутизация

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

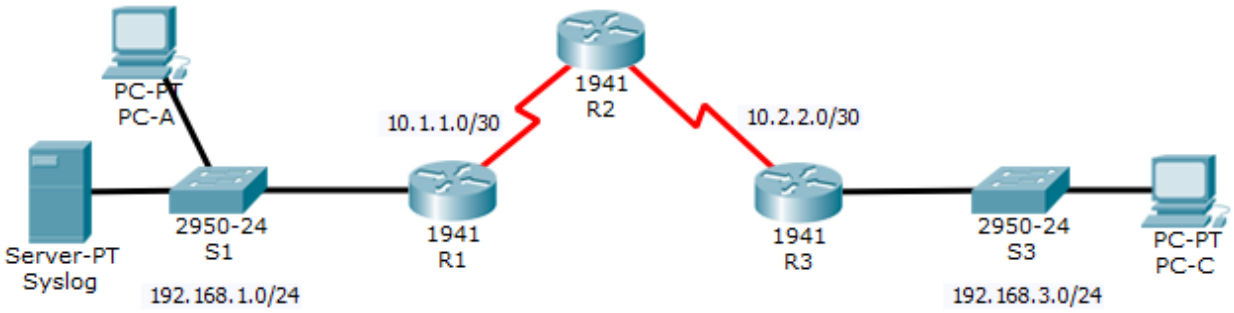
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.1	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/6
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

Практическая работа №8 Packet Tracer - Настройка системы предотвращения вторжений IOS (IPS) с помощью CLI.

Цель работы: получение навыков настройки предотвращения вторжений

Задачи:
1. Включение IOS IPS.
2. Настройка ведения журнала.
3. Изменение сигнатуры IPS.
4. Проверка IPS.

Топология:



Сценарий:

Ваша задача – включить систему IPS на маршрутизаторе R1 для проверки трафика, поступающего в сеть 192.168.1.0.

Сервер Syslog используется для ведения журнала сообщений IPS. Вы должны настроить маршрутизатор для идентификации сервера Syslog, который будет получать сообщения журнала. При использовании сервиса Syslog для мониторинга сети очень важно, чтобы в сообщениях syslog отображались правильные дата и время. Настройте часы и сервис временных меток для ведения журналов на маршрутизаторах. Наконец, включите систему IPS для выдачи оповещения и отбрасывания пакетов ICMP Echo Reply во внутриканальном режиме.

Сервер и компьютеры были предварительно настроены. На маршрутизаторах также были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Пароль консоли: ciscoconpa55
- Имя пользователя и пароль SSH: SSHadmin/ciscosshpa55
- OSPF 101

Таблица адресации

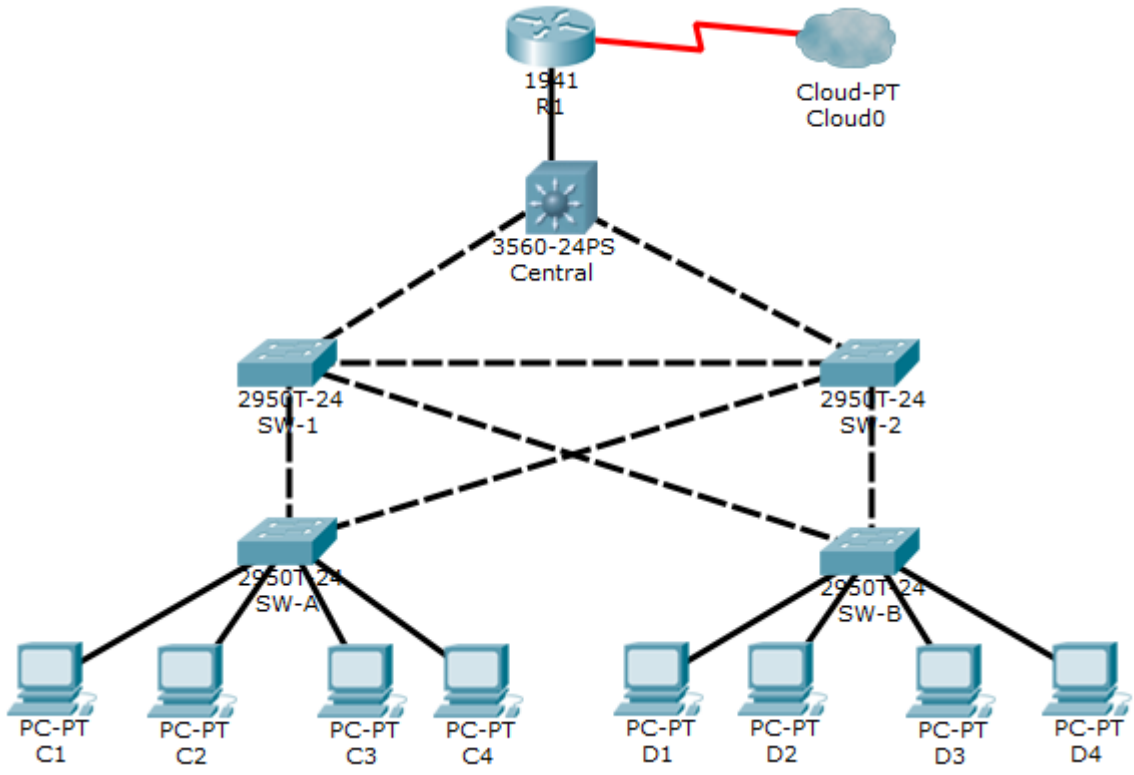
Устройство	Интер-фейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт комму-татора
R1	G0/1	192.168.1.1	255.255.255.0	Н/П	S1 F0/1
	S0/0/0	10.1.1.1	255.255.255.252	Н/П	Н/П
R2	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П	Н/П
R3	G0/1	192.168.3.1	255.255.255.0	Н/П	S3 F0/1
	S0/0/0	10.2.2.1	255.255.255.252	Н/П	Н/П
Syslog	NIC	192.168.1.50	255.255.255.0	192.168.1.1	S1 F0/2
PC-A	NIC	192.168.1.2	255.255.255.0	192.168.1.1	S1 F0/3
PC-C	NIC	192.168.3.2	255.255.255.0	192.168.3.1	S3 F0/2

Практическая работа №9 Packet Tracer - Обеспечение безопасности на 2-м уровне.

Цель работы: получение навыков настройки безопасности на уровне 2 модели OSI

Задачи:
1. Назначение коммутатора Central в качестве корневого моста.
2. Защита параметров связующего дерева для предотвращения атак путём манипуляций STP.
3. Включение защиты портов для предотвращения атак путём переполнения таблиц CAM.

Топология:



Сценарий:

Недавно сеть подверглась нескольким атакам. Поэтому сетевой администратор поручил вам настроить безопасность на 2-м уровне.

Для обеспечения оптимальной производительности и безопасности администратор хочет, чтобы в качестве корневого моста использовался коммутатор 3560 Central. Чтобы предотвратить атаки путем манипуляций с протоколом STP, администратору требуется гарантированная защита параметров STP. Чтобы предотвратить атаки путем переполнения таблиц CAM, сетевой администратор решил настроить защиту портов для ограничения количества MAC-адресов, которые может определить каждый порт коммутатора. Если число MAC-адресов превышает заданное ограничение, администратор должен выключить порт.

На всех коммутаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Пароль консоли: ciscoconpa55
- Имя пользователя и пароль SSH: SSHadmin/ciscosshpa55

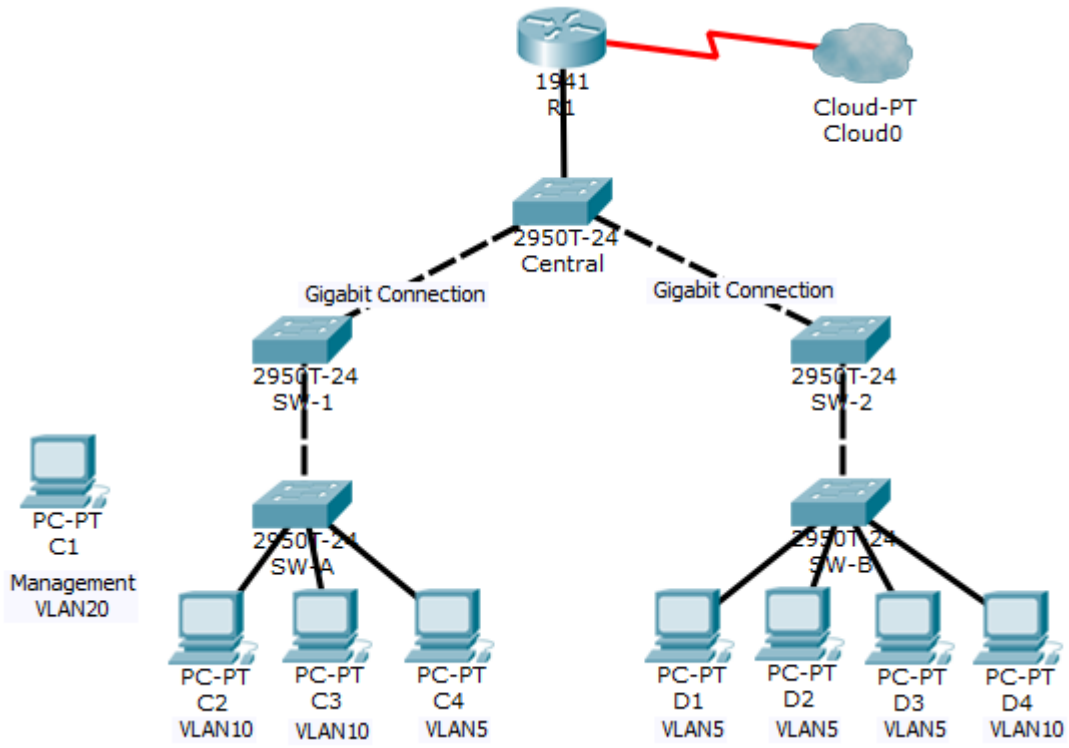
Практическая работа №10 Packet Tracer - Обеспечение безопасности VLAN на 2-м уровне.

Цель работы: закрепление навыков настройки безопасности на уровне 2 модели OSI

Задачи:

1. Создание нового резервного канала между коммутаторами SW-1 и SW-2.
2. Включение транкинга и конфигурирование защиты в новом магистральном канале между коммутаторами SW 1 и SW-2.
3. Создание новой управляющей сети VLAN (VLAN 20) и подключение к ней управляющего ПК.
4. Создание списка ACL для предотвращения доступа внешних пользователей к управляющей VLAN.

Топология:



Сценарий:

В настоящее время в сети компании настроено использование двух отдельных сетей VLAN: VLAN 5 и VLAN 10. Кроме того, для всех магистральных портов настроена нативная сеть VLAN 15. Сетевой администратор хочет добавить резервный канал между коммутаторами SW-1 и SW-2. Для канала должен быть включён транкинг и выполнены все требования безопасности.

Кроме того, сетевой администратор хочет подключить управляющий компьютер к коммутатору SW-A. Управляющий компьютер должен иметь возможность подключаться ко всем коммутаторам и маршрутизатору, но любые другие устройства не должны подключаться к управляющему компьютеру или коммутаторам. Администратор хочет создать новую сеть VLAN 20 для целей управления.

На всех устройствах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Пароль консоли: ciscoconpa55
- Имя пользователя и пароль SSH: SSHadmin/ciscosshpa55

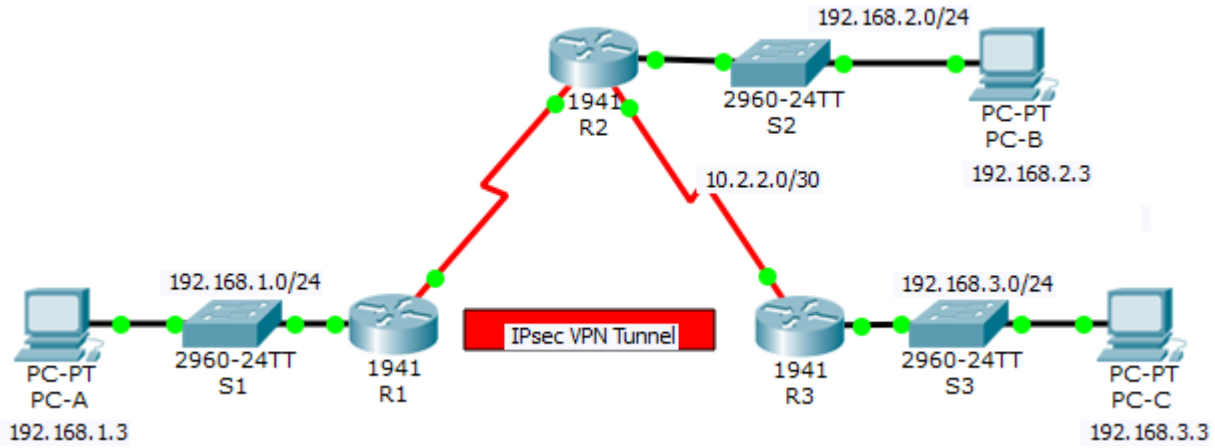
Практическая работа №11 Packet Tracer - Настройка и проверка VPN IPsec типа "сеть-сеть" с помощью CLI

Цель работы: настройка и проверка VPN IPsec типа "сеть-сеть"

Задачи:

1. Проверка связи в сети
2. Настройка маршрутизатора R1 для поддержки сети Site-to-Site IPsec VPN с маршрутизатором R3

Топология:



Сценарий:

Топология сети включает три маршрутизатора. Ваша задача заключается в том, чтобы настроить маршрутизаторы R1 и R3 для поддержки сети site-to-site IPsec VPN (между двумя пунктами) при передаче трафика между соответствующими локальными сетями. Туннель IPsec VPN проходит от маршрутизатора R1 к маршрутизатору R3 через R2. Маршрутизатор R2 играет роль транзитного узла и не имеет информации о VPN. IPSec обеспечивает безопасную передачу конфиденциальной информации по незащищенным сетям, например по Интернету. IPSec функционирует на сетевом уровне и выполняет функцию как защиты, так и аутентификации IP-пакетов между соответствующими устройствами IPsec (узлами), такими как маршрутизаторы Cisco.

Параметры политики ISAKMP, фаза 1

Параметры		R1	R3
Метод распределения ключей	Вручную или ISAKMP	ISAKMP	ISAKMP
Алгоритм шифрования	DES, 3DES или AES	AES 256	AES 256
Алгоритм хеширования	MD5 или SHA-1	SHA-1	SHA-1
Метод аутентификации	Общие ключи или RSA	pre-share	pre-share
Обмен ключами	Группа DH 1, 2 или 5	DH 5	DH 5
Время существования IKE SA	86 400 с или меньше	86400	86400
Ключ ISAKMP		vpnpa55	vpnpa55

Параметры политики IPsec, фаза 2

Параметры	R1	R3
Имя набора преобразований	VPN-SET	VPN-SET
Шифрование преобразования ESP	esp-aes	esp-aes
Аутентификация преобразования ESP	esp-sha-hmac	esp-sha-hmac
IP-адрес узла	10.2.2.2	10.1.1.2
Трафик, подлежащий шифрованию	access-list 110 (source 192.168.1.0 dest 192.168.3.0)	access-list 110 (source 192.168.3.0 dest 192.168.1.0)
Имя криптографической карты	VPN-MAP	VPN-MAP
Установление SA	ipsec-isakmp	ipsec-isakmp

На маршрутизаторах были предварительно настроены следующие параметры.
- Пароль для линии консоли: ciscoconpa55
- Пароль для линий VTY: ciscovtypa55
- Пароль привилегированного доступа: ciscoenpa55
- Имя пользователя и пароль SSH: SSHadmin/ciscosshpa55
- OSPF 101

Таблица адресации

Устрой-ство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт коммута-тора
R1	G0/0	192.168.1.1	255.255.255.0	Н/П	S1 F0/1
	S0/0/0 (DCE)	10.1.1.2	255.255.255.252	Н/П	Н/П
R2	G0/0	192.168.2.1	255.255.255.0	Н/П	S2 F0/2
	S0/0/0	10.1.1.1	255.255.255.252	Н/П	Н/П
	S0/0/1 (DCE)	10.2.2.1	255.255.255.252	Н/П	Н/П
R3	G0/0	192.168.3.1	255.255.255.0	Н/П	S3 F0/5
	S0/0/1	10.2.2.2	255.255.255.252	Н/П	Н/П
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1	S1 F0/2
PC-B	NIC	192.168.2.3	255.255.255.0	192.168.2.1	S2 F0/1
PC-C	NIC	192.168.3.3	255.255.255.0	192.168.3.1	S3 F0/18

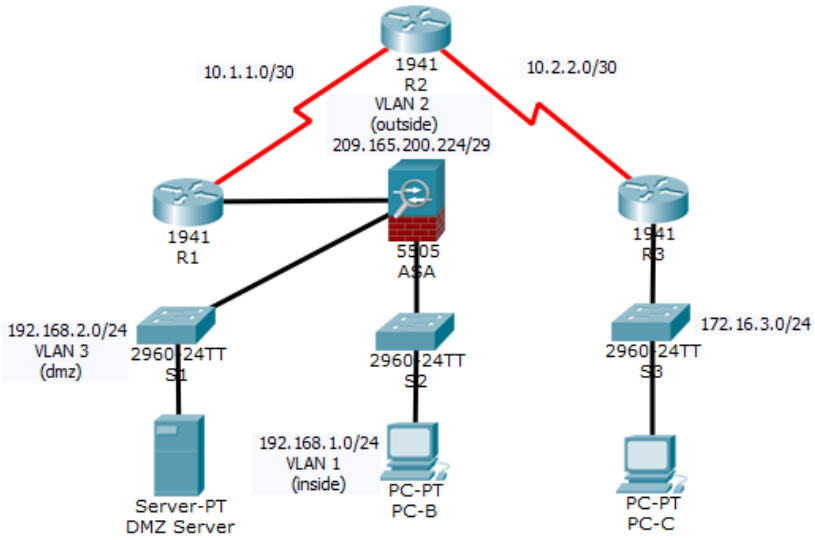
Практическая работа №12 Packet Tracer - Настройка основных параметров ASA и брандмауэра с помощью CLI

Цель работы: научиться настраивать базовые параметры ASA и межсетевого экрана с использованием интерфейса командной строки (CLI)

Задачи:

1. Проверка связи и знакомство с ASA
2. Настройка основных параметров ASA и уровней безопасности интерфейса с помощью интерфейса командной строки
3. Настройка маршрутизации, преобразования адресов и политики инспектирования с помощью интерфейса командной строки
4. Настройка DHCP, AAA и SSH
5. Настройка DMZ, статического преобразования сетевых адресов (NAT) и списков контроля доступа (ACL)

Топология:



Сценарий:

В вашей компании есть один пункт, подключённый к ISP. Маршрутизатор R1 представляет собой конечное устройство (CPE) под управлением ISP. R2 – это промежуточный интернет-маршрутизатор. R3 – это поставщик ISP, подключающий компьютер администратора из компании управления сетью, который был нанят на работу для дистанционного управления вашей сетью. ASA – это граничное устройство безопасности, подключающее внутрикорпоративную сеть и DMZ к ISP и одновременно предоставляющее сервисы NAT и DHCP внутренним хостам. Устройство ASA необходимо сконфигурировать для управления администратором во внутренней сети, а также удалённым администратором. Интерфейсы VLAN 3-го уровня обеспечивают доступ к трем зонам, созданным в этом задании: внутренней, внешней и DMZ. ISP назначил пространство общедоступных IP-адресов 209.165.200.224/29, которое будет использовано для преобразования адресов на ASA.

На всех маршрутизаторах и коммутаторах были предварительно настроены следующие параметры.

- Пароль привилегированного доступа: ciscoenpa55
- Пароль консоли: ciscoconpa55
- Имя пользователя и пароль администратора: admin/adminpa55

Таблица адресации

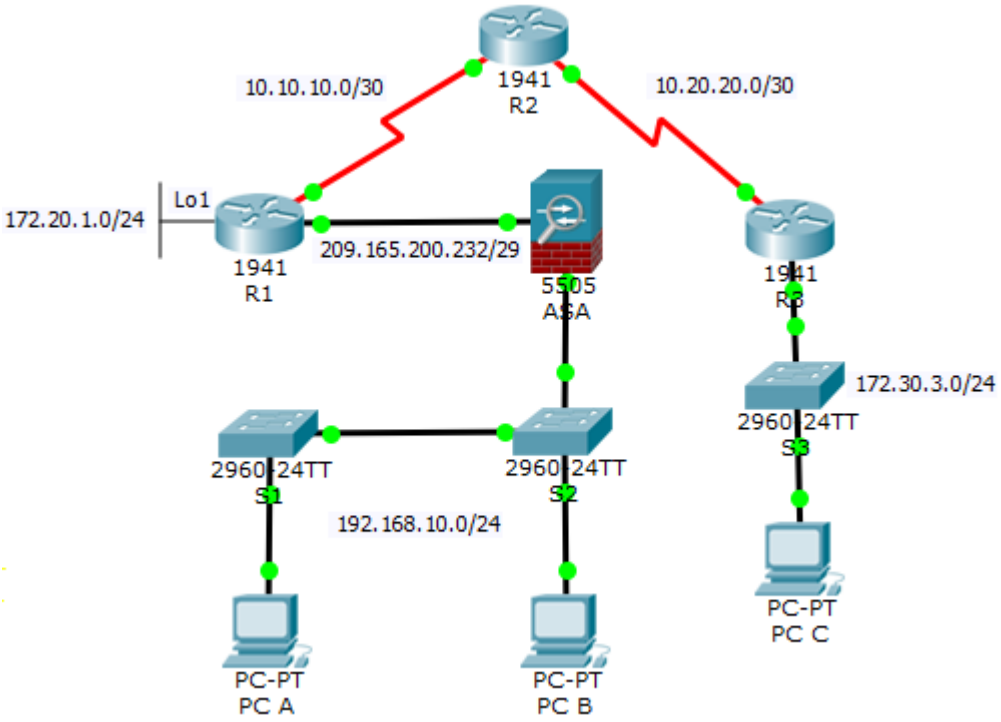
Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолча-нию
R1	G0/0	209.165.200.225	255.255.255.248	Н/П
	S0/0/0 (DCE)	10.1.1.1	255.255.255.252	Н/П
R2	S0/0/0	10.1.1.2	255.255.255.252	Н/П
	S0/0/1 (DCE)	10.2.2.2	255.255.255.252	Н/П
R3	G0/1	172.16.3.1	255.255.255.0	Н/П
	S0/0/1	10.2.2.1	255.255.255.252	Н/П
ASA	VLAN 1 (E0/1)	192.168.1.1	255.255.255.0	Н/П
ASA	VLAN 2 (E0/0)	209.165.200.226	255.255.255.248	Н/П
ASA	VLAN 3 (E0/2)	192.168.2.1	255.255.255.0	Н/П
Сервер DMZ	NIC	192.168.2.3	255.255.255.0	192.168.2.1
PC-B	NIC	192.168.1.3	255.255.255.0	192.168.1.1
PC-C	NIC	172.16.3.3	255.255.255.0	172.16.3.1

Практическая работа №13 Packet Tracer - Задача по интеграции навыков.

Цель работы: выполнить усложнённое задание на совокупное использование навыков

Задачи:
1. Настройка базового уровня безопасности маршрутизатора
2. Настройка базового уровня безопасности коммутатора
3. Настройка локальной аутентификации AAA
4. Настройка SSH
5. Защита от атак методом подбора учетных данных
6. Настройка сетей site-to-site IPsec VPN
7. Настройка параметров межсетевого экрана и системы предотвращения вторжений (IPS)
8. Настройка базовых параметров безопасности ASA и межсетевого экрана

Топология:



Сценарий:

Это итоговое задание охватывает многие навыки, которые вы приобрели в ходе данного курса. Для маршрутизаторов и коммутаторов предварительно настроены базовые параметры устройств, такие как IP-адресация и маршрутизация. С помощью интерфейса командной строки (CLI) вы настроите различные функции IOS, связанные с безопасностью, включая AAA, SSH и зональный межсетевой экран (ZPF), для защиты маршрутизаторов. Вы настроите сеть site-to-site VPN (VPN между двумя пунктами) между маршрутизаторами R1 и R3. Вы обеспечите безопасность коммутаторов в сети. Кроме того, вы также настроите функции межсетевого экрана на ASA.

Таблица адресации

Устройство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию
R1	G0/0	209.165.200.233	255.255.255.248	Н/П
	S0/0/0 (DCE)	10.10.10.1	255.255.255.252	Н/П
	Loopback 1	172.20.1.1	255.255.255.0	Н/П
R2	S0/0/0	10.10.10.2	255.255.255.252	Н/П
	S0/0/1 (DCE)	10.20.20.2	255.255.255.252	Н/П
R3	G0/1	172.30.3.1	255.255.255.0	Н/П
	S0/0/1	10.20.20.1	255.255.255.252	Н/П
S1	VLAN 1	192.168.10.11	255.255.255.0	192.168.10.1
S2	VLAN 1	192.168.10.12	255.255.255.0	192.168.10.1
S3	VLAN 1	172.30.3.11	255.255.255.0	172.30.3.1
ASA	VLAN 1 (E0/1)	192.168.10.1	255.255.255.0	Н/П
	VLAN 2 (E0/0)	209.165.200.234	255.255.255.248	Н/П
PC-A	NIC	192.168.10.2	255.255.255.0	192.168.10.1
PC-B	NIC	192.168.10.3	255.255.255.0	192.168.10.1
PC-C	NIC	172.30.3.3	255.255.255.0	172.30.3.1

8.2.2. Типовые задания к лабораторным работам

Лабораторная работа №1. Социальная инженерия

Цель: изучить примеры социальной инженерии.

Задача: изучите примеры социальной инженерии, определите пути ее определения и противодействия ей.

Ресурсы: Компьютер с доступом в Интернет

Задание:
1. С помощью любого браузера найдите информацию о случаях применения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.
2. Определение признаков социальной инженерии
Социальные инженеры – не что иное, как воры или шпионы. Вместо того чтобы получить доступ к вашей сети через Интернет, они пытаются получить его, используя желание человека быть любезным. Приведите пример, каким образом ничего не подозревающий человек может невольно разгласить конфиденциальную информацию. Найдите способы определения социальной инженерии. Опишите три обнаруженных в ходе исследования примера.
3. Анализ способов предотвращения применения социальной инженерии
Приняты ли в вашем университете процедуры, призванные предотвращать применение социальной инженерии? Если да, в чем заключаются эти процедуры? Найдите в Интернете процедуры, принятые в организациях для того, чтобы предотвратить получение доступа к конфиденциальной информации при помощи социальной инженерии. Перечислите найденное.

Лабораторная работа №2. Изучение сетевых атак, а также инструментов для аудита безопасности и проведения атак

Задачи
Часть 1. Изучение сетевых атак
- Изучите сетевые атаки, которые были реализованы.
- Выберите сетевую атаку и составьте по ней отчёт для представления его аудитории.
Часть 2. Изучение инструментов аудита безопасности и проведения атак
- Изучите инструменты аудита безопасности.
- Выберите инструмент и составьте по нему отчёт для представления его аудитории.

Исходные данные/сценарий

За многие годы злоумышленники разработали множество инструментов для проведения атак и компрометации сетей. Эти атаки имеют множество форм, но чаще всего они направлены на получение конфиденциальной информации, уничтожение ресурсов или блокирование доступа легальных пользователей к ресурсам. Когда сетевые ресурсы оказываются недоступны, может страдать продуктивность работника, приводя к упущенной выгоде для всего бизнеса.

Чтобы понять, как защитить сеть от атак, администратор должен определить уязвимости сети. Специальные программы аудита безопасности, разработанные производителями оборудования и программного обеспечения, помогают определить потенциальные уязвимости. Инструменты, которые применяются для атак на сеть, могут быть использованы и сетевыми специалистами для тестирования способности сети противостоять этим атакам. После определения уязвимостей можно предпринимать меры для защиты сети.

Эта лабораторная работа представляет собой структурированный исследовательский проект, разделённый на две части: изучение сетевых атак и инструментов аудита безопасности. Сообщите инструктору, какие сетевые атаки и инструменты для аудита безопасности вы выбрали для

изучения. Таким образом, участники группы расскажут о целом наборе сетевых атак и инструментов для определения уязвимостей.

В части 1 изучите реально произошедшие сетевые атаки. Выберите одну из этих атак и опишите, каким образом она была совершена, объем урона, нанесённого сети, и время простоя. Затем проанализируйте, каким образом данная атака могла бы быть нейтрализована и какие техники нейтрализации можно реализовать для предотвращения будущих атак. В конце подготовьте отчет по форме, описанной в этой лабораторной работе.

В части 2 изучите инструменты аудита безопасности и проведения атак. Изучите один из инструментов, который можно использовать для определения уязвимостей сетевых устройств или хостов. Составьте отчет на одну страницу по этому инструменту по форме, описанной в этой лабораторной работе. Подготовьте короткую (на 5-10 минут) презентацию для группы.

Вы можете работать в парах, где один человек рассказывает о сетевой атаке, а другой – об инструментах. Каждый участник группы составляет короткий рассказ о результатах своего анализа. Можно использовать презентации PowerPoint или просто продемонстрировать полученные результаты.

Необходимые ресурсы

- Компьютер с доступом в Интернет
- Компьютер для проведения презентаций с установленным PowerPoint или другим программным обеспечением для презентаций
- Видеопроектор и экран для демонстраций и презентаций

Лабораторная работа №3. Защита маршрутизатора для административного доступа

Цель: закрепить навыки обеспечения основных параметров безопасности маршрутизатора

Задачи:

1. Настройка основных параметров устройства
- Подключение сетевых кабелей, как показано на топологической схеме
- Настройка базовых параметров IP-адресации для маршрутизаторов и компьютеров
- Настройка OSPF-маршрутизации
- Настройка хост-компьютеров
- Проверка связи между хостами и маршрутизаторами
2. Контроль административного доступа для маршрутизаторов
- Настройка и шифрование всех паролей
- Настройка предупреждающего баннера при входе в систему
- Настройка расширенных функций безопасности
- Настройка SSH-сервера на маршрутизаторе
- Настройка SSH-клиента и проверка связи
- Настройка SCP-сервера на маршрутизаторе
3. Настройка административных ролей
- Создание нескольких представлений ролей и предоставление им различных привилегий
- Проверка и сравнение представлений
4. Настройка отчётов о защите и управлении Cisco IOS
- Защита файлов образа и конфигурации Cisco IOS
- Настройка функции SNMPv3 Security с помощью ACL
- Настройка маршрутизатора в качестве источника синхронизированного времени для других устройств по протоколу NTP
- Настройка поддержки Syslog на маршрутизаторе
- Установка и активация сервера Syslog на компьютере
- Внесение изменений на маршрутизаторе и отслеживание результатов в системном журнале на компьютере

Топология:

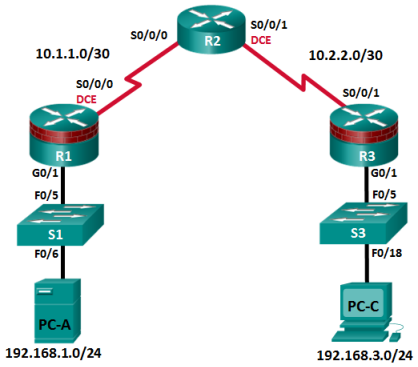


Таблица IP-адресов

Устрой-ство	Интерфейс	IP-адрес	Маска подсети	Шлюз по умолчанию	Порт ком-мутатора
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/П	Н/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

8.3. Типовые контрольные задания или иные материалы для проведения ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

Форма проведения промежуточной аттестации по дисциплине: *зачёт (по результатам накопительного рейтинга или в форме компьютерного тестирования).*

Устно-письменная форма по экзаменационным билетам предполагается, как правило, для сдачи академической задолженности

Примерный перечень вопросов и заданий для подготовки к зачёту

№	Содержание вопроса
ОПК-10. Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	
1.	Какие критерии используются для фильтрации трафика?
2.	Какой метод аутентификации используется для доступа к сетевым устройствам?
3.	Какую задачу выполняют административные роли?
4.	Какой протокол используется для мониторинга устройств?
5.	Какой протокол используют для централизованной аутентификации AAA?
6.	Какой тип межсетевого экрана отслеживает состояние соединений?
7.	Какой командой можно настроить SNMP на маршрутизаторе?
8.	Какой инструмент можно использовать для тестирования безопасности сети? a) Nmap) b) DHCP-сервер c) FTP-клиент d) SNMP
9.	Какой из перечисленных методов относится к пассивным атакам на сеть? a) Перехват трафика) b) SQL-инъекция c) DDoS-атака d) Внедрение вредоносного кода
10.	Что представляет собой двухфакторная аутентификация? a) Использование двух различных методов подтверждения личности) b) Использование двух паролей c) Аутентификация через VPN-соединение d) Применение сложных паролей
11.	Какой механизм безопасности относится к методам защиты оконечных устройств? a) Антивирусное ПО) b) NAT c) Межсетевой экран d) MAC-фильтрация
12.	Какую функцию выполняет протокол IPsec в VPN-сетях? a) Обеспечивает конфиденциальность и целостность данных) b) Назначает IP-адреса клиентам c) Управляет пропускной способностью сети d) Перенаправляет трафик через прокси-сервер
13.	Какое утверждение о межсетевых экранах верно? a) Они фильтруют трафик на основе заранее заданных правил) b) Они работают только на уровне приложения c) Они не могут анализировать состояние соединений d) Они заменяют антивирусные решения
14.	Какой инструмент можно использовать для тестирования безопасности сети?

№	Содержание вопроса
	a) Nmap) b) DHCP-сервер c) FTP-клиент d) SNMP
ПК-6 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности	
15.	Какой командой можно отключить службу восстановления паролей?
16.	Какую команду используют для обновления списка доступа?
17.	Какой командой можно просмотреть таблицу маршрутизации?
18.	Какой командой можно установить ACL на интерфейс?
19.	Какой командой можно проверить состояние доступа к VTY-портам?
20.	Какая команда позволяет настроить SSH на маршрутизаторе?
21.	Какую команду следует использовать для генерации RSA-ключей?
22.	Что будет отключено при выполнении команды no service password-recovery?
23.	Какой из следующих алгоритмов используется для симметричного шифрования? a) AES) b) RSA c) ECC d) SHA-256
24.	Что из перечисленного относится к серверному решению AAA? a) RADIUS) b) VPN c) DHCP d) NAT
25.	Какую роль выполняет Security Device Manager в ASA? a) Обеспечивает графический интерфейс для управления устройством) b) Увеличивает скорость передачи данных c) Фильтрует трафик на уровне 2 d) Управляет маршрутизацией трафика
26.	Какой из следующих протоколов обеспечивает шифрование данных в VPN-сетях? a) IPsec) b) HTTP c) FTP d) SMTP
27.	Что из перечисленного является основным компонентом технологии IPS? a) Сигнатуры) b) VPN-туннели c) NAT d) VLAN
28.	Какой алгоритм используется для генерации открытого и закрытого ключей? a) RSA) b) MD5 c) SHA-1 d) DES
29.	Какую функцию выполняет сервер TACACS+? a) Аутентификация, авторизация и учет пользователей) b) Управление межсетевым экраном c) Мониторинг сети d) Динамическое распределение IP-адресов
30.	Какой принцип лежит в основе зональных межсетевых экранов? a) Разделение сети на зоны с различными уровнями доверия)

№	Содержание вопроса
	b) Анализ поведения пользователей c) Шифрование данных d) Использование NAT
31.	Какой механизм защиты используется для предотвращения атак с подделкой MAC-адресов? a) Port Security) b) ACL c) NAT d) VPN