КОНКУРСНОЕ ЗАДАНИЕ КОМПЕТЕНЦИИ «СЕТЕВОЕ И СИСТЕМНОЕ АДМИНИСТРИРОВАНИЕ»

2023 г.

Конкурсное задание разработано экспертным сообществом и утверждено Менеджером компетенции, в котором установлены нижеследующие правила и необходимые требования владения профессиональными навыками для участия в соревнованиях по профессиональному мастерству.

Конкурсное задание включает в себя следующие разделы:

ИСПОЛЬЗУЕМЫЕ СОКРАЩЕНИЯ

1. ИКС – Информационно коммуникационная система
2. КС – Компьютерная сеть
3. ОС – Операционная система

1. ОСНОВНЫЕ ТРЕБОВАНИЯ КОМПЕТЕНЦИИ

1.1. ОБЩИЕ СВЕДЕНИЯ О ТРЕБОВАНИЯХ КОМПЕТЕНЦИИ

Требования компетенции (ТК) «Сетевое и системное администрирование» определяют знания, умения, навыки и трудовые функции, которые лежат в основе наиболее актуальных требований работодателей отрасли.

Целью соревнований по компетенции является демонстрация лучших практик и высокого уровня выполнения работы по соответствующей рабочей специальности или профессии.

Требования компетенции являются руководством для подготовки конкурентоспособных, высококвалифицированных специалистов / рабочих и участия их в конкурсах профессионального мастерства.

В соревнованиях по компетенции проверка знаний, умений, навыков и трудовых функций осуществляется посредством оценки выполнения практической работы.

Требования компетенции разделены на четкие разделы с номерами и заголовками, каждому разделу назначен процент относительной важности, сумма которых составляет 100.

1.2. ПЕРЕЧЕНЬ ПРОФЕССИОНАЛЬНЫХ ЗАДАЧ СПЕЦИАЛИСТА ПО КОМПЕТЕНЦИИ «Сетевое и системное администрирование»

Таблица №1

Перечень профессиональных задач специалиста

№ п/п	Раздел	Важность в %
1	Выполнение работ по выявлению и устранению инцидентов в информационно-коммуникационных системах	25
	- Специалист должен знать и понимать: Лицензионные требования по настройке и эксплуатации устанавливаемого программного обеспечения Основы архитектуры, устройства и функционирования вычислительных систем Принципы организации, состав и схемы работы операционных систем Стандарты информационного взаимодействия систем	

	Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе Инструкции по установке администрируемых сетевых устройств Инструкции по эксплуатации администрируемых сетевых устройств Инструкции по установке администрируемого программного обеспечения Инструкции по эксплуатации администрируемого программного обеспечения Требования охраны труда при работе с аппаратными, программно-аппаратными и программными средствами администрируемой информационно-коммуникационной системы.	
	- Специалист должен уметь: 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 Локализовать отказ и инициировать корректирующие действия Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий Производить мониторинг администрируемой информационно-коммуникационной системы Конфигурировать операционные системы сетевых устройств Пользоваться контрольно-измерительными приборами и аппаратурой Документировать учетную информацию об использовании сетевых ресурсов согласно утвержденному графику	
2	Обеспечение работы технических и программных средств информационно-коммуникационных систем	25
	- Специалист должен знать и понимать Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых	

	устройствах и операционных системах; Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы;	
	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе;	

	Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	
3	Реализация схемы резервного копирования, архивирования и восстановления конфигураций технических и программных средств информационно-коммуникационных систем по утвержденным планам	25
	- Специалист должен знать и понимать: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой информационно-коммуникационной системы; Инструкции по установке администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по эксплуатации администрируемых сетевых устройств информационно-коммуникационной системы; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая эталонная модель взаимодействия открытых систем для управления сетевым трафиком; Международные стандарты локальных вычислительных сетей Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	
	- Специалист должен уметь: Использовать процедуры восстановления данных; определять точки восстановления данных; работать с серверами архивирования и средствами управления	

	операционных систем; Пользоваться нормативно-технической документацией в области инфокоммуникационных технологий; Выполнять плановое архивирование программного обеспечения пользовательских устройств согласно графику;	
4.	Внесение изменений в технические и программные средства информационно-коммуникационных систем по утвержденному плану работ	25
	- Специалист должен знать и понимать: Использовать современные методы контроля производительности информационно-коммуникационной системы; Анализировать сообщения об ошибках в сетевых устройствах и операционных системах; Локализовывать отказ и инициировать корректирующие действия; Применять программно-аппаратные средства для диагностики отказов и ошибок сетевых устройств; Применять штатные программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы; Применять внешние программно-аппаратные средства для контроля производительности сетевой инфраструктуры информационно-коммуникационной системы;	
	- Специалист должен уметь: Общие принципы функционирования аппаратных, программных и программно-аппаратных средств администрируемой сети; Архитектура аппаратных, программных и программно-аппаратных средств администрируемой сети; Инструкции по установке администрируемых сетевых устройств; Инструкции по эксплуатации администрируемых сетевых устройств; Инструкции по установке администрируемого программного обеспечения; Инструкции по эксплуатации администрируемого программного обеспечения; Протоколы канального, сетевого, транспортного и прикладного уровней модели взаимодействия открытых систем; Базовая	

	эталонная модель взаимодействия открытых систем; Международные стандарты локальных вычислительных сетей; Модели информационно-телекоммуникационной сети «Интернет»; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Устройство и принцип работы кабельных и сетевых анализаторов; Средства глубокого анализа информационно-коммуникационной системы; Метрики производительности администрируемой информационно-коммуникационной системы; Регламенты проведения профилактических работ на администрируемой информационно-коммуникационной системе; Требования охраны труда при работе с сетевой аппаратурой администрируемой информационно-коммуникационной системы;	

Проверить/соотнести с ФГОС, ПС, Отраслевыми стандартами

1.3. ТРЕБОВАНИЯ К СХЕМЕ ОЦЕНКИ

Сумма баллов, присуждаемых по каждому аспекту, должна попадать в диапазон баллов, определенных для каждого раздела компетенции, обозначенных в требованиях и указанных в таблице №2.

Таблица №2

Матрица пересчета требований компетенции в критерии оценки

Критерий/Модуль					Итого баллов за раздел ТРЕБОВАНИЙ КОМПЕТЕНЦИИ
Разделы ТРЕБОВАНИЙ КОМПЕТЕНЦИИ		А	Б	В	
	1	5	5	10	20
	2	5	5	10	20
	3	10	10	10	30
	4	10	10	10	30
Итого баллов за критерий/модуль		30	30	40	**100**

1.4. СПЕЦИФИКАЦИЯ ОЦЕНКИ КОМПЕТЕНЦИИ

Оценка Конкурсного задания будет основываться на критериях, указанных в таблице №3:

Таблица №3

Оценка конкурсного задания

Критерий		Методика проверки навыков в критерии
А	**Настройка технических и программных средств информационно-коммуникационных систем**	Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием
Б	**Развертывание и сопровождение сетевой инфраструктуры**	Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием
В	**Обеспечение отказоустойчивости**	Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием
Г	**Поиск и устранение неисправностей**	Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием
Д	**Автоматизация**	Определяется регионом в соответствии с используемыми ОС и Сетевым оборудованием

1.5. КОНКУРСНОЕ ЗАДАНИЕ

Возрастной ценз: 14 лет и более

Общая продолжительность Конкурсного задания[1]: 12 ч.

Количество конкурсных дней: 3 дней

Вне зависимости от количества модулей, КЗ должно включать оценку по каждому из разделов требований компетенции.

Оценка знаний участника должна проводиться через практическое выполнение Конкурсного задания. В дополнение могут учитываться требования работодателей для проверки теоретических знаний / оценки квалификации.

1.5.1. Разработка/выбор конкурсного задания

Конкурсное задание состоит из 3 модулей, включает обязательную к выполнению часть (инвариант) – 2 модулей, и вариативную часть – 1 модуль. Общее количество баллов конкурсного задания составляет 100.

Обязательная к выполнению часть (инвариант) выполняется всеми регионами без исключения на всех уровнях чемпионатов.

Количество модулей из вариативной части, выбирается регионом самостоятельно в зависимости от материальных возможностей площадки соревнований и потребностей работодателей региона в соответствующих специалистах. В случае если ни один из модулей вариативной части не подходит под запрос работодателя конкретного региона, то вариативный (е) модуль (и) формируется регионом самостоятельно под запрос работодателя. При этом, время на выполнение модуля (ей) и количество баллов в критериях оценки по аспектам не меняются.

Таблица №4

Матрица конкурсного задания

Инструкция по заполнению матрицы конкурсного задания **(Приложение № 1)**

1.5.2. Структура модулей конкурсного задания (инвариант)

информацию из этого раздела.

В случае, если в тексте задания не указано иное, все пользовательские учетные записи должны иметь пароль P@ssw0rd.

На маршрутизаторе R0 логин/пароль по умолчанию - vyos/toor

На межсетевых экранах FW* логин/пароль по умолчанию - root/toor

На компьютерах с Debian 10/11 логин/пароль по умолчанию - user/P@ssw0rd и root/toor

[1] *Указывается суммарное время на выполнение всех модулей КЗ одним конкурсантом.*

Все проверки работы клиентских технологий (сайтов, клиентских VPN подключений и т.п.) будут выполняться из под пользователя user соответствующих клиентских машин. Сайты будут проверяться через стандартный браузер клиентской ОС (для Windows - Edge, для Linux - Firefox).
При выполнении настоящего задания всегда нужно руководствоваться правилом наименьших привилегий.
Консольный доступ к виртуальной машине провайдера ISP для участника не предполагается. Следите за тем, чтобы виртуальная машина ISP была включена в течение всего времени выполнения задания.

Модуль А. (*Настройка технических и программных средств информационно-коммуникационных систем*)

Время на выполнение модуля 4 часа…….

Задания:

Сеть	Устройство	Адрес/Маска	Шлюз
INTERNET	ClientEU	100.70.2.45/27	ISP – первый адрес в сети
	FW-AMS	100.70.3.45/26	ISP – первый адрес в сети
	FW-MSK	100.70.4.18/28	ISP – первый адрес в сети
	ClientSPB	100.70.5.55/28	ISP – первый адрес в сети
	VDS (EKB)	100.70.6.12/29	ISP – первый адрес в сети
	VPNClient (EKB)	100.70.6.13/29	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
FW–R0–MSK	FW-MSK	STATIC	
	R0-MSK	STATIC	FW-MSK (OSPF)
LAN–MSK	R0–MSK	STATIC	
	PC–MSK	DHCP	R0–MSK
SRV–MSK	R0–MSK	STATIC	
	SRV1–MSK	STATIC	R0–MSK
	SRV2–MSK	STATIC	R0–MSK
DMZ–MSK	FW–MSK	STATIC	
	APP–MSK	STATIC	FW–MSK
LAN–AMS	FW–AMS	STATIC	
	PC–AMS	DHCP	FW–AMS
DMZ–AMS	FW–AMS	STATIC	
	DMZ–AMS	STATIC	FW–AMS
	APP–AMS	STATIC	FW–AMS

ЗАДАНИЕ

1. Настройте статичные IPv4-адреса, шлюз по умолчанию и описания на интерфейсах FW* и R0 согласно схеме адресации.
2. Настройте статичные IPv4-адреса и шлюз по умолчанию на всех устройствах, где это требуется, согласно схеме адресации.

3. Настройте OSPFv2 между R0-MSK и FW-MSK

3.1. FW-MSK должен узнавать о сетях LAN-MSK и SRV-MSK через OSPF.

3.2. R0 должен получать маршрут по умолчанию и другие необходимые маршруты от FW-MSK через OSPF.

3.3. Не используйте статические маршруты до этих сетей. Статические маршруты применимы только в качестве временной меры.

3.4. R0-MSK должен быть защищен от вброса маршрутов с интерфейсов смотрящих в сторону сетей LAN-MSK и SRV-MSK

3.5. FW-MSK должен быть защищен от вброса маршрутов с интерфейса смотрящего в сторону сети DMZ-MSK.

4. Обеспечьте выход в интернет для всех устройств московского и амстердамского офисов.

5. Настройте сервер разрешения имен

5.1. Устройства в локальных сетях должны обращаться с DNS запросами к своим FW*

5.2. Пограничные маршрутизаторы FW* должны выполнять пересылку DNS запросов от локальных клиентов на DNS сервер по адресу 100.100.100.100.

5.3. ClientSPB и VDS должны обращаться с DNS запросами к 100.100.100.100.

6. Настройте имена устройств согласно топологии.

7. Настройте для всех устройств московского и амстердамского офисов доменные имена в зонах msk.jun39.wsr и ams.jun39.wsr соответственно.

7.1. Все устройства должны быть доступны в локальных сетях всех филиалов по именам в соответствии с топологией в доменах соответствующих филиалов. К примеру dmz-ams.ams.jun39.wsr или pc-msk.msk.jun39.wsr

7.2. В рамках каждого филиала короткие имена должны автоматически дополняться доменным именем соответствующего филиала

8. Настройте DHCP-сервер на SRV1–MSK для клиентов в сети LAN–MSK и DHCP-сервер на FW-AMS для сети LAN–AMS. DHCP-сервер должен передавать клиентам следующие опции:

8.1. Адрес хоста

8.2. Маску сети

8.3. Адрес шлюза

8.4. Имя домена (msk.jun39.wsr и ams.jun39.wsr соответственно.)

8.5. Адрес DNS (FW*)

8.6. Адрес NTP (FW*)

8.7. Выдаваемый диапазон адресов должен иметь запас в как минимум по 10 адресов в начале и конце сети, но не более 50 суммарного запаса.

9. Настройте DHCP Relay на маршрутизаторе R0-MSK таким образом, чтобы клиентам в сети LAN–MSK адреса выдавал сервер SRV1–MSK.

10. Настройте синхронизацию времени

10.1. Устройства в локальных сетях должны синхронизировать свое время с FW*.

10.2. Устройства с динамическими адресами должны получать получать информацию о сервере времени от своего DHCP сервера и использовать ее для работы.

10.3. Пограничные маршрутизаторы FW*, ClientSPB и VDS должны синхронизировать свое время с NTP сервером по адресу 100.101.102.103.

10.4. Настройте часовой пояс на всех устройствах в соответствии с их географическим расположением.

11. Настройте правила firewall так, чтобы устройства в сетях DMZ-* не могли инициировать соединения к клиентам в приватных сетях организации, при этом входящие соединения из всех локальных сетей в сети DMZ-* должны быть разрешены и машины в сети DMZ-* должны иметь доступ в интернет. При необходимости, допускается возможность штучно открывать дополнительные порты, необходимые для выполнения задания.

12. Настройте сетевое обнаружение по протоколу LLDP на всех сетевых устройствах и серверах.

13. Настроить удаленный доступ к VDS и R0-MSK по SSH

13.1. Устройство PC-MSK при входе под пользователем user должно иметь доступ к VDS под пользователем user с использованием SSH ключей, без необходимости ввода пароля.

13.2. Подключение к VDS с PC-MSK должно осуществляться по имени “VDS”

14. Настройте защищенный VPN-туннель FW-AMS<=>FW-MSK со следующими параметрами:

14.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.

14.2. Используйте современные надежные протоколы шифрования AES и SHA-2

14.3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.

14.4. Настройте маршрутизацию, NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не натировался и не блокировался

15. Настройте работу OSPF между FW*, чтобы устройства из московского офиса имели связанность с устройствами из амстердамского.

16. Обеспечьте подключение клиента VPNClient к серверу VPN на FW-MSK.

16.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.

16.2. Клиент должен иметь доступ к серверам в сети SRV-MSK

16.3. Соединение должно автоматически устанавливаться при включении компьютера или входе под пользователем user.

17. Настройте централизованный сбор журналов syslog на SRV1-MSK.

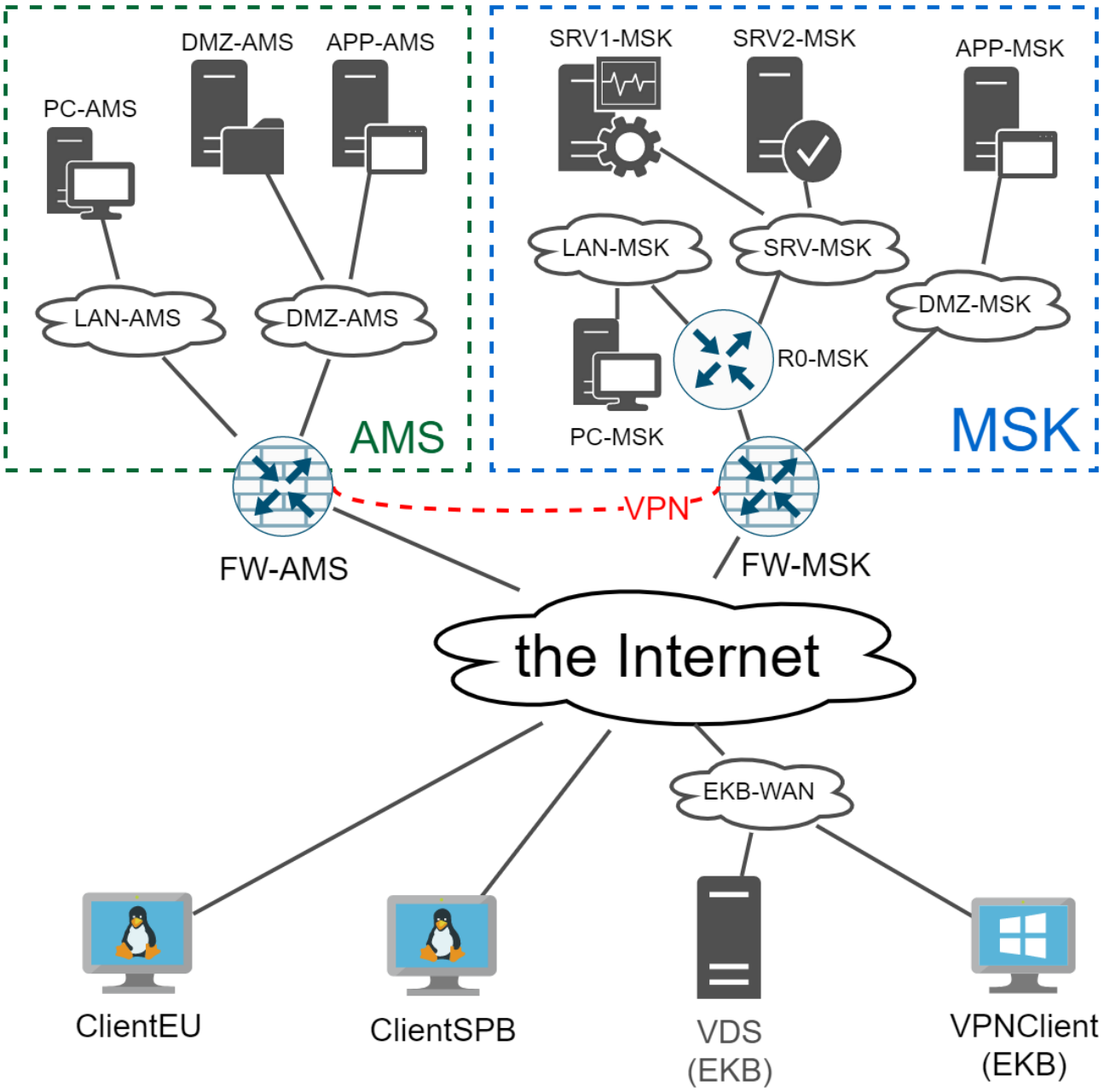
17.1. Журналы должны храниться в файлах /opt/logs/[hostname], где hostname - это короткое или полное доменное имя машины, предоставившей соответствующие сообщения.

17.2. PC-MSK должен записывать сообщения error и более важные.

17.3. SRV*-MSK должны записывать сообщения warning и более важные.

17.4. FW должен записывать сообщения от служб ospf и имеющихся на устройстве служб туннелирования (ipsec, openvpn, wireguard и т.д) уровня не менее notice.

Топология


DMZ-AMS
APP-AMS
PC-AMS
LAN-AMS
DMZ-AMS
AMS
SRV1-MSK
SRV2-MSK
APP-MSK
LAN-MSK
SRV-MSK
DMZ-MSK
R0-MSK
PC-MSK
MSK
VPN
FW-AMS
FW-MSK
the Internet
EKB-WAN
ClientEU
ClientSPB
VDS
(EKB)
VPNClient
(EKB)

Модуль Б. (*Развертывание и сопровождение сетевой инфраструктуры*)

Время на выполнение модуля 4 часа

Задания:

Схема IP-адресации.

Сеть	Устройство	Адрес/Маска	Шлюз
INTERNET	ClientEU	100.70.2.45/27	ISP – первый адрес в сети
	FW-AMS	100.70.3.45/26	ISP – первый адрес в сети
	FW-MSK	100.70.4.18/28	ISP – первый адрес в сети
	ClientSPB	100.70.5.55/28	ISP – первый адрес в сети
	VDS (EKB)	100.70.6.12/29	ISP – первый адрес в сети
	VPNClient (EKB)	100.70.6.13/29	ISP – первый адрес в сети
	FW-IKT	100.70.7.99/25	ISP – первый адрес в сети
	ClientVV	100.70.8.78/28	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
FW–R0–MSK	FW-MSK	STATIC	
	R0-MSK	STATIC	FW-MSK (OSPF)
LAN–MSK	R0–MSK	STATIC	
	PC–MSK	DHCP	R0–MSK
SRV–MSK	R0–MSK	STATIC	
	SRV1–MSK	STATIC	R0–MSK
	SRV2–MSK	STATIC	R0–MSK
DMZ–MSK	FW–MSK	STATIC	
	APP–MSK	STATIC	FW–MSK
LAN–AMS	FW–AMS	STATIC	
	PC–AMS	DHCP	FW–AMS
DMZ–AMS	FW–AMS	STATIC	
	DMZ–AMS	STATIC	FW–AMS
	APP–AMS	STATIC	FW–AMS
LAN–IKT	FW–IKT	STATIC	
	PC–IKT	DHCP	FW–IKT
	SRV1–IKT	STATIC	FW–IKT
DMZ–IKT	FW–IKT	STATIC	
	APP–IKT	STATIC	FW–IKT

ЗАДАНИЕ

1. В связи с большим спросом на наши услуги на Дальнем востоке, для обеспечения качественного соединения и разумного уровня задержек по передачи данных, руководство приняло решение открыть новый филиал в Сибири. Создайте необходимую инфраструктуру для нового филиала в Иркутске.
    1.1. Разверните необходимые машины из шаблонов и назначьте им параметры, указанные в таблице “Характеристики виртуальных машин в Иркутском филиале”
    1.2. Создайте виртуальные сети и соедините устройства согласно топологии
    1.3. Настройте IPv4-адресацию на устройствах в иркутском филиале и ClientVV и обеспечьте выход в интернет.
    1.4. Настройте сервер разрешения имен
    1.5. Устройства в локальных сетях должны обращаться с DNS запросами к своим FW–IKT.
    1.6. FW–IKT должны выполнять пересылку DNS запросов
    1.7. Настройте для всех новых устройств соответствующие им имена и доменное имя ikt.jun39.wsr.
    1.8. Настройте синхронизацию времени аналогично другим филиалам
2. Настройте защищенные VPN-туннели FW-IKT<=>FW-MSK со следующими параметрами:
    2.1. Технология VPN на ваш выбор: IPsec, OpenVPN, WireGuard.
    2.2. Используйте современные надежные протоколы шифрования AES и SHA-2
    2.3. Не допускается использование протоколов шифрования и аутентификации с длиной ключа/хеша менее 256 бит.
    2.4. Настройте NAT и межсетевой экран таким образом, чтобы трафик для другого офиса не натировался и не блокировался.
    2.5. Настройка тоннеля не должна помешать функционированию тоннеля между AMS и MSK.
3. Настройте работу OSPF, чтобы устройства из иркутского филиала имели связанность с устройствами из московского и амстердамского.
4. Настройте инфраструктуру DNS, чтобы устройства из иркутского филиала имели могли обратиться к устройствам других филиалов по доменным именам.

5. Создайте пользователя admin с паролем P@ssw0rd на SRV1–IKT, и добавьте в группу sudo.
6. Настройте общий доступ к файлам на SRV1–IKT по протоколу NFS.
    6.1. Каталог для хранения файлов /opt/nfs/rw должен быть доступен для чтения и записи.
    6.2. Каталог для хранения файлов /opt/nfs/ro должен быть доступен только для чтения.
    6.3. NFS должен быть доступен для клиентов в сети LAN-IKT.
7. Настройте клиент NFS на PC–IKT.
    7.1. Путь /opt/nfs/rw на SRV1–IKT должен быть смонтирован в каталог /home/user/Desktop/nfs_rw на PC–IKT.
    7.2. Путь /opt/nfs/ro на SRV1–IKTAMS должен быть смонтирован в каталог /home/user/Desktop/nfs_ro на PC–IKT.
    7.3. Монтирование должно восстанавливаться при перезагрузке виртуальной машины.
8. Настройте права доступа для каталога /opt/nfs/ на SRV1–IKT.
    8.1. Пользователь admin должен иметь права на чтение и запись в каталог /opt/nfs и все его подкаталоги.
9. На каждом из серверов APP-* должен быть развернут WEB-сервер.
    9.1. Сайт должен открываться по адресу web.jun39.wsr по протоколу HTTP на стандартном порте и должен быть доступен из сети интернет.
    9.2. Сайт должен содержать следующий текст: “Welcome to Minecraft server mc.jun39.wsr site in XX region”, где XX заменено на “European”, “Central”, “Siberian” соответственно региональному расположению.
10. На сервере VDS разверните сервер DNS
    10.1. Сервер должен расшифровывать зону jun39.wsr
    10.2. Имя jun39.wsr для клиентов в сети интернет должно расшифровываться в адрес сервера VDS.
    10.3. Имя web.jun39.wsr для для клиентов в сети интернет должно расшифровываться во внешний адрес FW-* в ближайшем к клиенту регионе.
    10.4. Не забудьте проконтролировать, что клиенты Client* обращаются с DNS-запросами к VDS.
11. Внутри филиалов имя web.jun39.wsr должно расшифровываться и в локальный адрес APP-* в соответствующем регионе и по нему должен открываться соответствующий сайт
12. Настройте CA на SRV2-MSK со следующими параметрами

12.1. Используйте /opt/ca в качестве корневой директории CA.
12.2. Страна RU;
12.3. Организация WSR
12.4. CN должен быть установлен как WSR CA.
12.5. Создайте корневой сертификат CA.
12.6. SRV2-MSK и PC-MSK должны доверять CA.

13. На сервере SRV1-MSK должен быть развернут WEB-сервер:
    13.1. Сайт должен открываться по адресу corp.msk.jun39.wsr
    13.2. Сайт должен содержать следующий текст “Welcome to secure corporate portal jun39.wsr”
    13.3. Сайт должен функционировать по протоколу HTTPS. При обращении по протоколу HTTP должен происходить автоматический редирект на HTTPS.
    13.4. WEB-сервер должен иметь сертификат, подписанный корпоративным центром сертификации
    13.5. Сайт должен открываться с PC1-MSK без ошибок и предупреждений
14. Обеспечьте подключение удаленного сотрудника с компьютера VPNclient к корпоративному порталу https://corp.msk.jun39.wsr посредством VPN-подключения. При этом открытие портала не должно вызывать ошибок и предупреждений безопасности.
15. На VDS разверните сервер Minecraft. Для этого непосредственно перед началом развертывания сервера выделите виртуальной машине побольше ресурсов, а именно 4 VCPU и 3 Gb оперативной памяти. После этого, разверните сервер Minecraft со следующими параметрами:
    15.1. Имя сервера: Jun39
    15.2. Ограничение кол-ва игроков: 12
    15.3. Порт: по умолчанию
    15.4. Проверка аккаунтов пользователей: отключена
    15.5. Сервер должен быть запущен в виде контейнера Docker
    15.6. Контейнер должен автоматически запускаться после перезагрузки компьютера
    15.7. Для проверки можете использовать tlauncher расположенный на вашем операторском рабочем месте. Подключение осуществляется по внешнему адресу ISP (в сети 172.16.0.0), можно получить в интерфейсе среды виртуализации.
16. На сервере DMZ-AMS разверните сервер облачного хранения данных. Для этого непосредственно перед началом развертывания сервера

выделите виртуальной машине побольше ресурсов, а именно 2 VCPU и 2 Gb оперативной памяти. После этого, разверните сервер со следующими параметрами:

16.1. Файловый сервер: NextCloud
16.2. База данных: MariaDB
16.3. Веб интерфейс БД: phpMyAdmin
16.4. Порт NextCloud: 8080
16.5. Порт phpMyAdmin: 8888
16.6. Все сервисы должны быть запущены в виде контейнеров Docker
16.7. Все контейнеры должны автоматически запускаться после перезагрузки компьютера

17. Обеспечьте подключение удаленного сотрудника с компьютера VPNclient к корпоративному облачному хранилищу на DMZ-AMS посредством имеющегося VPN-подключения.

Примерные задержки передачи данных между клиентами и филиалами.

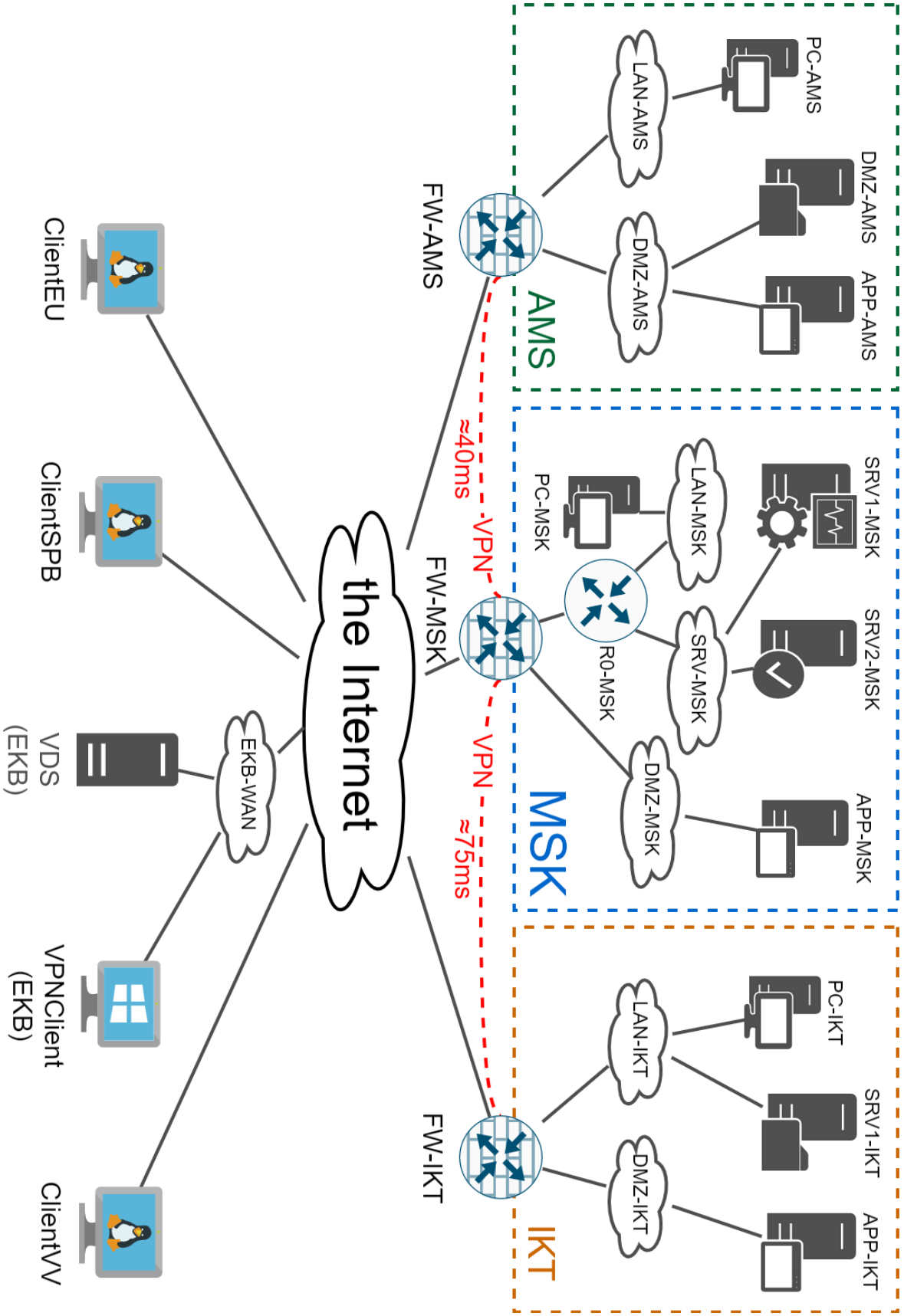
RTT	EU	AMS	MSK	SPB	EKB	IKT	VV
EU	-	10	50	60	74	130	174
AMS	10	-	44	44	70	124	170
MSK	50	44	-	10	24	74	110
SPB	60	44	10	-	30	74	120
EKB	74	70	24	30	-	40	90
IKT	130	124	74	74	40	-	50
VV	174	170	110	120	90	50	-

Характеристики виртуальных машин в Иркутском филиале.

VM	CPU	RAM (MB)
FW-IKT	2	1280
PC-IKT	1	768

SRV1-IKT	1	512
APP-IKT	1	384

Топология


AMS
PC-AMS
LAN-AMS
DMZ-AMS
APP-AMS
DMZ-AMS
FW-AMS
≈40ms
VPN
MSK
SRV1-MSK
SRV2-MSK
LAN-MSK
PC-MSK
R0-MSK
SRV-MSK
DMZ-MSK
APP-MSK
FW-MSK
VPN
≈75ms
IKT
PC-IKT
LAN-IKT
SRV1-IKT
DMZ-IKT
APP-IKT
FW-IKT
the Internet
EKB-WAN
ClientEU
ClientSPB
VDS
(EKB)
VPNClient
(EKB)
ClientVV

Модуль В. (*Название модуля*)

Время на выполнение модуля…….

Задания: *Описание задания…..*

Модуль Г. (*Поиск и устранение неисправностей*)

Время на выполнение модуля 4 часа

Задания:

Сеть	Устройство	Адрес/Маска	Шлюз
INTERNET	ClientEU	100.70.2.45/27	ISP – первый адрес в сети
	FW-AMS	100.70.3.45/26	ISP – первый адрес в сети
	FW-MSK	100.70.4.18/28	ISP – первый адрес в сети
	ClientSPB	100.70.5.55/28	ISP – первый адрес в сети
	VDS (EKB)	100.70.6.12/29	ISP – первый адрес в сети
	VPNClient (EKB)	100.70.6.13/29	ISP – первый адрес в сети
	FW-IKT	100.70.7.99/25	ISP – первый адрес в сети
	ClientVV	100.70.8.78/28	ISP – первый адрес в сети
	DNS-сервер	100.100.100.100	
	NTP-сервер	100.101.102.103	
FW–R0–MSK	FW-MSK	STATIC	
	R0-MSK	STATIC	FW-MSK (OSPF)
LAN–MSK	R0–MSK	STATIC	
	PC–MSK	DHCP	R0–MSK
SRV–MSK	R0–MSK	STATIC	
	SRV1–MSK	STATIC	R0–MSK
	SRV2–MSK	STATIC	R0–MSK
DMZ–MSK	FW–MSK	STATIC	
	APP–MSK	STATIC	FW–MSK
LAN–AMS	FW–AMS	STATIC	
	PC–AMS	DHCP	FW–AMS
DMZ–AMS	FW–AMS	STATIC	
	DMZ–AMS	STATIC	FW–AMS
	APP–AMS	STATIC	FW–AMS
LAN–IKT	FW–IKT	STATIC	
	PC–IKT	DHCP	FW–IKT
	SRV1–IKT	STATIC	FW–IKT
DMZ–IKT	FW–IKT	STATIC	
	APP–IKT	STATIC	FW–IKT

По результатам вашей успешной работы, руководство отправило вас на курсы повышения квалификации по теме “Поиск и устранение неисправностей в сетевых инфраструктурах малого и среднего бизнеса”. На время вашего отсутствия ваши обязанности временно исполнял студент-практикант. Качество его работы вызвало у руководства большие вопросы и теперь вам представляется уникальная возможность применить полученные на курсах

знания на реальной практике. На текущий момент были обнаружены следующие недостатки функционирования инфраструктуры:
Тикет 1. Клиенты из сети LAN-MSK потеряли доступ в сеть
Тикет 2. Компьютеры в филиале AMS не могут обращаться по именам к компьютерам в домене
Тикет 3. OSPF на R0 перестал обмениваться маршрутами. Временно сделана статическая маршрутизация, но ее нужно отключить как только заработает ospf.
Тикет 4. Сотрудник за PC–IKT не может обратиться на SRV1–MSK по внутреннему адресу
Тикет 5. Не работает тоннель между MSK и AMS
Тикет 6. Через пользователя user с паролем P@ssw0rd не удается подключиться к базе данных в phpMyAdmin
Тикет 7. Minecraft на VDS не работает, хотя контейнер запущен.
Тикет 8. На VDS было два пользователя: user1 и user2. Но при попытке зайти на машину, используя эти два логина ничего не получалось. Файлы и группы пользователей должны быть сохранены.
Тикет 9. Сотрудник работающий из дома не может подключиться к серверам во внутренней инфраструктуре организации.
Тикет 10. У сотрудников доступа к облачному хранилищу NextCloud по доменным именам. Интерфейс открывается, но с ошибкой. По IP адресу сервера доступ есть.
Тикет 11. Корпоративный портал открывается с ошибкой сертификата.
Тикет 12. Клиенты Client* попадают на неверные региональные сайты web.jun39.wsr. На ClientEU сайт не открывается вообще.
Тикет 13. Пользователь user на компьютере PC-IKT не может записывать файлы в примонтированную директорию nfs_rw
Тикет 14. У очень важного клиента из СПб на компьютере с ОС Debian 10 не загружается графическое окружение Mate. Директор сказал, что “Этому человеку ОЧЕНЬ НАДО ПОМОЧЬ!!!111”. Хорошо хоть ехать недалеко. При общении с пользователем было выяснено, что вчера машина работала нормально и была выключена штатно. Сегодня с утра она не загрузилась. Пользователь говорил, что вчера пытался сделать что-то с сетевой папкой. По информации от пользователя, ценных данных локально на компьютере не хранилось.
Тикет 15. На сервере централизованного хранения логов SRV1-MSK перестали появляться сообщения с FW-MSK.

2.1. Личный инструмент конкурсанта

Нулевой - нельзя ничего привозить.

2.2. Материалы, оборудование и инструменты, запрещенные на площадке

Мобильные устройства, устройства фото-видео фиксации, носители информации.

3. Приложения

Приложение №1 Инструкция по заполнению матрицы конкурсного задания

Приложение №2 Матрица конкурсного задания

Приложение №3 Критерии оценки

Приложение №4 Инструкция по охране труда и технике безопасности по компетенции «Сетевое и системное администрирование».

Приложение №5 Чертежи, технологические карты, алгоритмы, схемы и т.д.