|  |  |
| --- | --- |
| СогласованоООО НПП «Гарант-Уфа» Хайруллин Ильдар Вадимович\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |  |

Региональный этап чемпионата по

профессиональному мастерству «Профессионалы» и

чемпионата высоких технологий Республики

Башкортостан

*по компетенции:*

F8 «Информационная безопасность»

Конкурсное задание

День 1

СОДЕРЖАНИЕ

[МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 3](#_Toc136690326)

[МЕЖСЕТЕВОЙ ЭКРАН FW1 3](#_Toc136690327)

[МЕЖСЕТЕВОЙ ЭКРАН FW2 4](#_Toc136690328)

[ФИЛИАЛ «ПИТЕР» 5](#_Toc136690329)

[МАРШРУТИЗАТОР CHR-1 5](#_Toc136690330)

[ШЛЮЗ БЕЗОПАСНОСТИ С1 6](#_Toc136690331)

[РАБОЧИЕ СТАНЦИИ СОТРУДНИКОВ R1, AT1, A1, A2 7](#_Toc136690332)

[СЕРВЕР ALD1 8](#_Toc136690333)

[СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IDS GROUP 9](#_Toc136690334)

[ФИЛИАЛ «СТОЛИЦА» 10](#_Toc136690335)

[МАРШРУТИЗАТОР vESR-1 10](#_Toc136690336)

[ШЛЮЗ БЕЗОПАСНОСТИ С2 11](#_Toc136690337)

[РАБОЧИЕ СТАНЦИИ AT2, R2 12](#_Toc136690338)

[РАБОЧИЕ СТАНЦИИ A3, A4 13](#_Toc136690339)

[РАБОЧАЯ СТАНЦИЯ W-A 15](#_Toc136690340)

[РАБОЧАЯ СТАНЦИЯ ADM 16](#_Toc136690341)

[ПРИЛОЖЕНИЕ 1 17](#_Toc136690342)

[ПРИЛОЖЕНИЕ 2 18](#_Toc136690343)

[ПРИЛОЖЕНИЕ 3 19](#_Toc136690344)

[ПРИЛОЖЕНИЕ 4 20](#_Toc136690345)

[ПРИЛОЖЕНИЕ 5 21](#_Toc136690346)

# МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

МЕЖСЕТЕВОЙ ЭКРАН FW1

Межсетевой экран FW1 (pfSense) - дистрибутив для создания межсетевого экрана/маршрутизатора, основанный на FreeBSD. pfSense известен своей надежностью и предлагает функции, которые часто можно найти только в дорогих коммерческих межсетевых экранах.

Требования по настройке:

1. Настроить протокол автоматической раздачи IP-адресов, с ограниченным набором адресов, в количестве 100 шт.
2. Используйте функции фильтрации контента pfSense для блокировки следующих сайтов: vk.com, ok.ru, facebook.com, instagram.com, youtube.com, rutube.ru, tik-tok.com, skype.com, teams.microsoft.com, torrent-clients.com.
3. Создать список блокировки «SocialMediaBlockList» для блокировки контента п.2
4. Добавить правило для блокировки списка из п.3

МЕЖСЕТЕВОЙ ЭКРАН FW2

Межсетевой экран FW2 (xFirewall, АО «ИнфоТеКС») - это шлюз безопасности – межсетевой экран нового поколения (NGFW), сочетающий функции классического межсетевого экрана: анализ состояния сессии, проксирование, трансляция адресов; с расширенными функциями анализа и фильтрации трафика такими как: глубокая инспекция протоколов, выявление и предотвращение компьютерных атак, инспекция SSL/TLS-трафика, взаимодействие с антивирусными решениями, DLP и песочницами.

Требования по настройке:

1. Произвести активацию и первоначальную настройку, в том числе разрешить доступ к веб-интерфейсу по порту 8080.
2. Настроить протокол автоматической раздачи IP-адресов, с ограниченным набором адресов, в количестве 100 шт.
3. Разрешить прохождение ICMP-пакетов для подсети 192.168.100.0/24.
4. Запретить доступ к приложениям Telegram, WhatsApp.

# ФИЛИАЛ «УФА»

МАРШРУТИЗАТОР CHR-1

Маршрутизатор CHR-1 (Cloud Hosted Router, RouterOS, MikroTik) - сетевая операционная система на базе Linux. RouterOS предназначена для установки на маршрутизаторы MikroTik RouterBoard. Также данная система может быть установлена на ПК, превращая его в маршрутизатор с функциями брандмауэра, VPN-сервера/клиента, QoS, точки доступа и другими. Система также может служить в качестве Captive-портала на основе системы беспроводного доступа. RouterOS обеспечивает поддержку практически всех сетевых интерфейсов на ядре Linux.

Требования по настройке:

1. Произвести настройку DCHP-клиента;
2. Произвести настройку DHCP-сервера для сетевых интерфейсов, ограничить величину пулов до 50 адресов;
3. Добавить NAT правило для внешнего интерфейса маршрутизатора для подмены локальных IP адресов на адрес, предоставленный провайдером услуг;
4. Запретить доступ ко всем портам, кроме локального и SSH по порту 3224;
5. Создать второго пользователя c именем user01, добавив его в новую группу пользователей chruser, которой разрешен доступ исключительно к ssh, password, web, local);
6. Создать резервную копию, с названием backup01 и установить на нее пароль.

ШЛЮЗ БЕЗОПАСНОСТИ С1

Шлюз безопасности С1 (Coordinator HW, АО «ИнфоТеКС») - предназначен для построения виртуальной сети ViPNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика. Благодаря функциям криптографической защиты данных, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNet Coordinator HW является оптимальным средством защиты компьютерных сетей организаций от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи.

Требования по настройке:

1. Произвести активацию и первоначальную настройку, в том числе разрешить доступ к веб-интерфейсу по порту 8080;
2. Разрешить прохождение ICMP-пакетов для подсети 10.106.3.0/24;
3. Активировать защищенное соединение между двумя филиалами.

РАБОЧИЕ СТАНЦИИ СОТРУДНИКОВ R1, AT1, A1, A2

Рабочая станция R1 (RedOS, РЕДСОФТ) - операционная система на базе ядра Linux, являющаяся составным продуктом, построенным на базе решений с открытым исходным кодом и собственных разработок. Занесена в Единый реестр российских программ.

Рабочая станция AT1 (Альт Linux, Базальт СПО) - дистрибутив на базе ядра Linux, включающий в себя операционную систему и набор приложений для полноценной работы, поддерживающий различное дополнительное оборудование.

Рабочие станции A1, A2 (Astra Linux Orel, ГК «Астра») - единственная российская ОС, репозиторий которой размещен в открытом доступе международной некоммерческой организации The Linux Foundation.

Требования по настройке:

1. На рабочие станции R1, AT1 необходимо установить программное обеспечение для возможности подключения в роли клиента к защищенной сети шлюза безопасности С1.
2. Рабочие станции А1, А2 необходимо подключить к домену ald01.cybersec.info, согласно таблице 1.

**Таблица 1 - Доменная информация**

|  |  |  |
| --- | --- | --- |
| **РС** | **Имя пользователя** | **Домен** |
| A1 | user01 | ald01.cybersec.info |
| A2 | user02 | ald01.cybersec.info |

СЕРВЕР ALD1

Сервер ALD1 основан на дистрибутиве рабочей станции Astra Linux Orel (ГК «Астра») - Astra Linux Directory – реализация службы каталогов от компании АО «НПО РусБИТех».

Требования по настройке:

1. Установить и настроить службу Astra Linux Directory;
2. Настроить базу данных Kerberos;
3. Создать пользователей user01 и user02 для домена ald01.cybersec.info.

СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IDS GROUP

Система обнаружения вторжений IDS Group (HS, MC, NS, TIAS, АО «ИнфоТеКС») - программно-аппаратный комплекс, предназначенный для обнаружения вторжений в информационные системы на основе динамического анализа сетевого трафика стека протоколов TCP/IP для протоколов всех уровней модели взаимодействия открытых систем, начиная с сетевого и заканчивая прикладным. ViPNet IDS позволяет оперативно получать информацию для определения источников компьютерных инцидентов, связанных с функционированием информационных систем организации.

Требования по настройке:

Для IDS HS:

1. Установить соединение с IDS МС;
2. Устройства с «agent» перенести в основной раздел.

Для IDS MC:

1. Установить соединение с IDS HS;
2. Установить соединение с IDS NS.

Для IDS NS:

1. Установить соединение с IDS MC;
2. Установить базы правил обнаружений атак;
3. Установить базы сигнатур вредоносного ПО.

Для TIAS

1. Создать организацию, филиал, и задать сеть;
2. В защищаемую сеть добавить все сенсоры;
3. Установить соединение с каждым из сенсоров.

# ФИЛИАЛ «СТОЛИЦА»

МАРШРУТИЗАТОР vESR-1

Маршрутизатор vESR-1 (ООО «Предприятие Элтекс») - предназначен для использования в корпоративных сетях связи для подключения небольших и средних офисов компаний. Функциональность межсетевого экрана и маршрутизатора позволяет обеспечить безопасность при различных вариантах подключения через сеть Интернет. vESR поддерживает расширенные функции маршрутизации, функции организации территориально-распределенных сетей и функции обеспечения сетевой безопасности.

Требования по настройке:

1. Произвести настройку DHCP-клиента
2. Произвести настройку DHCP-сервера для сетевых интерфейсов.
3. Произвести настройку Firewall для работы DHCP

ШЛЮЗ БЕЗОПАСНОСТИ С2

Шлюз безопасности С2 (Coordinator HW, АО «ИнфоТеКС») - предназначен для построения виртуальной сети ViPNet и обеспечения безопасной передачи данных между её защищенными сегментами, а также фильтрации IP-трафика. Благодаря функциям криптографической защиты данных, межсетевого экранирования, а также наличию встроенных сетевых сервисов ПАК ViPNet Coordinator HW является оптимальным средством защиты компьютерных сетей организаций от несанкционированного доступа к ее ресурсам при передаче информации по открытым каналам связи.

Требования по настройке:

1. Произвести активацию и первоначальную настройку, в том числе разрешить доступ к веб-интерфейсу по порту 8080.
2. Настроить протокол автоматической раздачи IP-адресов, с ограниченным набором адресов, в количестве 100 шт.
3. Разрешить прохождение ICMP-пакетов для подсети 10.0.12.0/24
4. Активировать защищенное соединение между двумя филиалами.

РАБОЧИЕ СТАНЦИИ AT2, R2

Рабочая станция R2 (RedOS, РЕДСОФТ) - операционная система на базе ядра Linux, являющаяся составным продуктом, построенным на базе решений с открытым исходным кодом и собственных разработок. Занесена в Единый реестр российских программ.

Рабочая станция AT2 (Альт Linux, Базальт СПО) - дистрибутив на базе ядра Linux, включающий в себя операционную систему и набор приложений для полноценной работы, поддерживающий различное дополнительное оборудование.

Требования по настройке:

1. На рабочие станции R2, AT2 необходимо установить программное обеспечение для возможности подключения в роли клиента к защищенной сети шлюза безопасности С2.

РАБОЧИЕ СТАНЦИИ A3, A4

Рабочие станции A3, A4 (Astra Linux Orel, ГК «Астра») - единственная российская ОС, репозиторий которой размещен в открытом доступе международной некоммерческой организации The Linux Foundation.

Требования по настройке:

Для А3:

1. Авторизироваться в системе с высоким уровнем целостности;

2. Проверить отсутствие в ОС правил фильтрации для входящего трафика;

3. Отключить SNLSP механизм;

4. Сформировать правила фильтрации так, чтобы были разрешены входящие соединения по протоколу SMB (TCP/139, 445, UDP/137, 138) с отслеживанием состояния соединения и блокирован весь остальной TCP/UDP-трафик с логированием событий:

* 1. создать цепочки для входящего TCP- и UDP-трафика;
	2. перенаправить обработку входящего TCP- и UDP-трафика в новые цепочки;
	3. в цепочке для TCP-трафика создать правила фильтрации, чтобы разрешить входящий TCP-трафик только по портам 139, 445 с отслеживанием состояния соединения;
	4. в цепочке для TCP-трафика блокировать все остальные TCP-соединения с логированием событий;
	5. сформировать аналогичные правила для UDP/137, 138 в новой цепочке для UDP-трафика;

5. Настроить автоматическую загрузку правил фильтрации при загрузке ОС;

* 1. создайте файл для сохранения правил;
	2. ограничить чтение файла для предотвращения атак с использованием открытых портов;
	3. выгрузить текущие правила iptables в файл;
	4. создать сценарий для выполнения в автоматическом режиме перед включением сетевого интерфейса;
	5. сделать файл сценария исполняемым;

Для А4:

1. Авторизоваться в системе с высоким уровнем целостности;
2. Проверить работоспособность правил фильтрации на рабочей станции А3.

РАБОЧАЯ СТАНЦИЯ W-A

Рабочая станция W-A (Microsoft Windows 10 Pro) - операционная система для персональных компьютеров и рабочих станций, разработанная корпорацией Microsoft в рамках семейства Windows NT.

Требования по настройке:

1. Произвести установку и настройку Центра управления сетью для функционирования защищенной сети.
2. Произвести установку и настройку Удостоверяющего ключевого центра для выпуска лицензионных соглашений для устройств, функционирующих в защищенной сети.
3. Произвести установку программного обеспечения для возможности подключения к защищенной сети в роли клиента администратора сети.

# РАБОЧАЯ СТАНЦИЯ ADM

Рабочая станция ADM предназначена для администрирования защищенной сети в рамках данного конкурсного задания.

Требования по настройке:

1. Особых требований не предусмотрено

# ПРИЛОЖЕНИЕ 1

**ОБЩАЯ ТОПОЛОГИЯ СЕТИ**



# ПРИЛОЖЕНИЕ 2

**ФИЛИАЛ «УФА»**



# ПРИЛОЖЕНИЕ 3

**ФИЛИАЛ «СТОЛИЦА»**


# ПРИЛОЖЕНИЕ 4

**ТОПОЛОГИЯ IDS GROUP**


# ПРИЛОЖЕНИЕ 5

**ДОСТУП К ПО**

**Доступ к виртуальному стенду по ссылке:**

[**https://cyber-info.ru/**](https://cyber-info.ru/)

**Логин: root | Пароль: xxXX.1234**

**Таблица 2 - Доступ к программному обеспечению**

|  |  |  |
| --- | --- | --- |
| **ВМ** | **ЛОГИН** | **ПАРОЛЬ** |
| A1, A2, ALD | astra | 12345678 |
| A3,A4 | astra-admin | P@ssw0rd |
| AT1, AT2 | altroot | 1234567812345678 |
| R1, R2 | redroot | 1234567812345678 |
| W-A | admin | 12345678 |
| ADM | admin | 12345678 |
| MC | root | vipnetvipnet45 |
| NSNS Web | idsuseradmin | vipnetvipnet45vipnetvipnet45 |
| HS Host | admin | 12345678 |
| HS | admin | Vipnetvipnet45! |
| TIASTIAS Web | adminAdministrator | Vipnetvipnet45!Administrator |
| CHR-1 | admin |  |
| vESR-1 | admin | password |
| C1, C2 | user | user |
| FW1 | admin | pfsense |
| FW2 | user | user |

Подробный отчет о проделанной работе сохранить на рабочем столе хостовой машины с названием Report\_day\_1\_team.pdf и Report\_day\_1\_team.doc

В качестве team в названии отчета указать номер рабочего места