|  |  |
| --- | --- |
| УТВЕРЖДАЮ  Менеджер компетенции  Информационная безопасность  \_\_\_\_\_\_\_\_\_\_\_\_/Е. Е. Сверчков |  |

**ТЕХНИЧЕСКОЕ ЗАДАНИЕ**

**Module VIP**

СОДЕРЖАНИЕ

[МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ 2](#_Toc194331984)

[МЕЖСЕТЕВОЙ ЭКРАН FW1 2](#_Toc194331985)

[ШЛЮЗ БЕЗОПАСНОСТИ С1 3](#_Toc194331986)

[РАБОЧИЕ СТАНЦИИ СОТРУДНИКОВ PC1 4](#_Toc194331987)

[СИСТЕМА ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ IDS GROUP 5](#_Toc194331988)

[ШЛЮЗ БЕЗОПАСНОСТИ С2 6](#_Toc194331989)

[РАБОЧАЯ СТАНЦИЯ PC2 7](#_Toc194331990)

[ПРИЛОЖЕНИЕ 1 8](#_Toc194331991)

[ПРИЛОЖЕНИЕ 2 9](#_Toc194331992)

# МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

МЕЖСЕТЕВОЙ ЭКРАН FW1

Требования по настройке:

1. Настроить протокол автоматической раздачи IP-адресов, с ограниченным набором адресов, в количестве 100 шт.
2. Используйте функции фильтрации контента 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.

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
3. Активировать защищенное соединение между двумя компьютерами.

РАБОЧИЕ СТАНЦИИ СОТРУДНИКОВ PC1

Требования по настройке:

1. На рабочую станцию PC1 необходимо установить программное обеспечение для возможности подключения в роли клиента к защищенной сети шлюза безопасности С1.

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.

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
4. Активировать защищенное соединение между двумя филиалами.

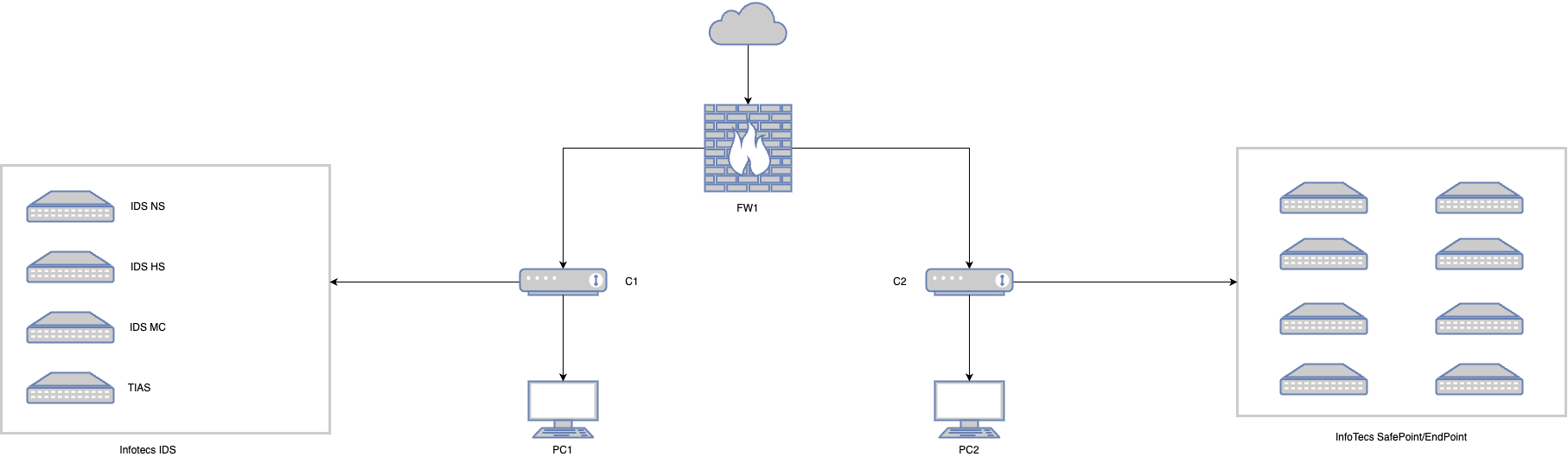
РАБОЧАЯ СТАНЦИЯ PC2

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.

# ПРИЛОЖЕНИЕ 1

**ОБЩАЯ ТОПОЛОГИЯ СЕТИ**



# ПРИЛОЖЕНИЕ 2

**ДОСТУП К ПО**

**Доступ к виртуальному стенду по ссылке:**

**Таблица 1 - Доступ к программному обеспечению**

|  |  |  |
| --- | --- | --- |
| **ВМ** | **ЛОГИН** | **ПАРОЛЬ** |
|  |  |  |