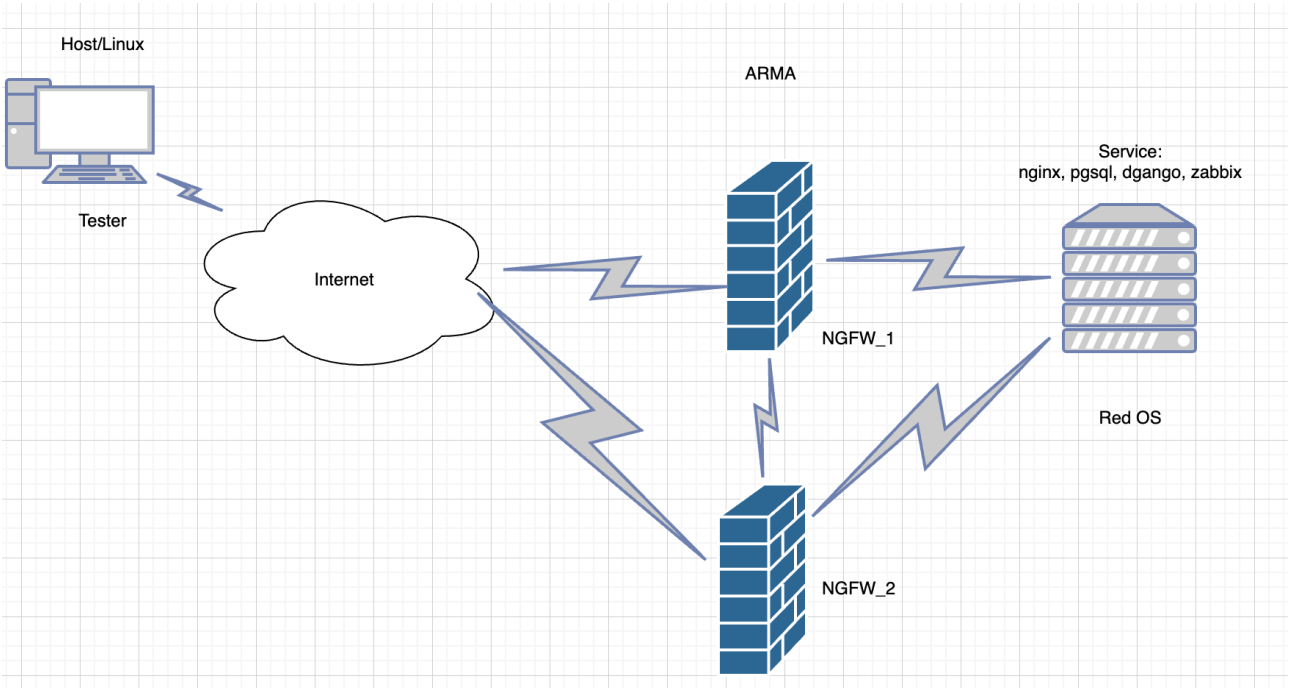
1. Вводная информация

Второе задание конкурса рассматривает вопросы, связанные с настройкой средств защиты информации, используя межсетевые экраны нового поколения, а также реализацию защищенной части сетевой инфраструктуры по принципу SIaC.

Перед вами стоит задача, связанная с подготовкой NGFW в виртуальном исполнении и составлением конфигурационного файла для автоматической настройки инфраструктуры за ngfw. Есть компания, которая находится удаленно и не имеет специалистов, реализация защищённого канала связи через ВЧС не представляется возможным. Ваша задача – сделать все с первого раза, поэтому вначале необходимо все спроектировать, проверить и затем предоставить компании в эксплуатацию.

Задание

Схема стенда



Часть 1 NGFW

Для выполнения первой части задания вам необходимо собрать стенд согласно схеме и выполнить следующие условия:

- Настроить сетевые интерфейсы InfoWatch ARMA NGFW для работы в сети. Убедиться, что устройство правильно подключено к внешним и внутренним сегментам сети. Определить количество физических интерфейсов и назначить каждому интерфейсу свою роль (например, WAN-интерфейсы для подключения к Интернету, LAN-интерфейсы для внутренней сети).

- Убедиться, что маршруты настроены таким образом, чтобы трафик между внутренними сегментами и внешними ресурсами проходил через InfoWatch ARMA NGFW.

- Использовать трансляцию адресов (NAT), добавить соответствующие правила для преобразования внутренних IP-адресов в публичный внешний адрес. Убедиться, что добавленные маршруты работают корректно.

- Создать набор правил для IDS/IPS, который будет блокировать нежелательные пакеты и защищать сеть от атак. Создать правила для блокировки определенных типов пакетов, известных уязвимых портов. Провести тестовые атаки и убедиться, что система корректно обнаруживает и предотвращает вторжения.

- Создать отказоустойчивый кластер из двух InfoWatch ARMA NGFW устройств с использованием протокола VRRP для обеспечения высокой доступности. В каждом устройстве создать виртуальные IP-адреса с помощью VRRP. Проверить работу отказоустойчивого кластера, отключив одно из устройств и убедиться, что второе продолжает обслуживать запросы.

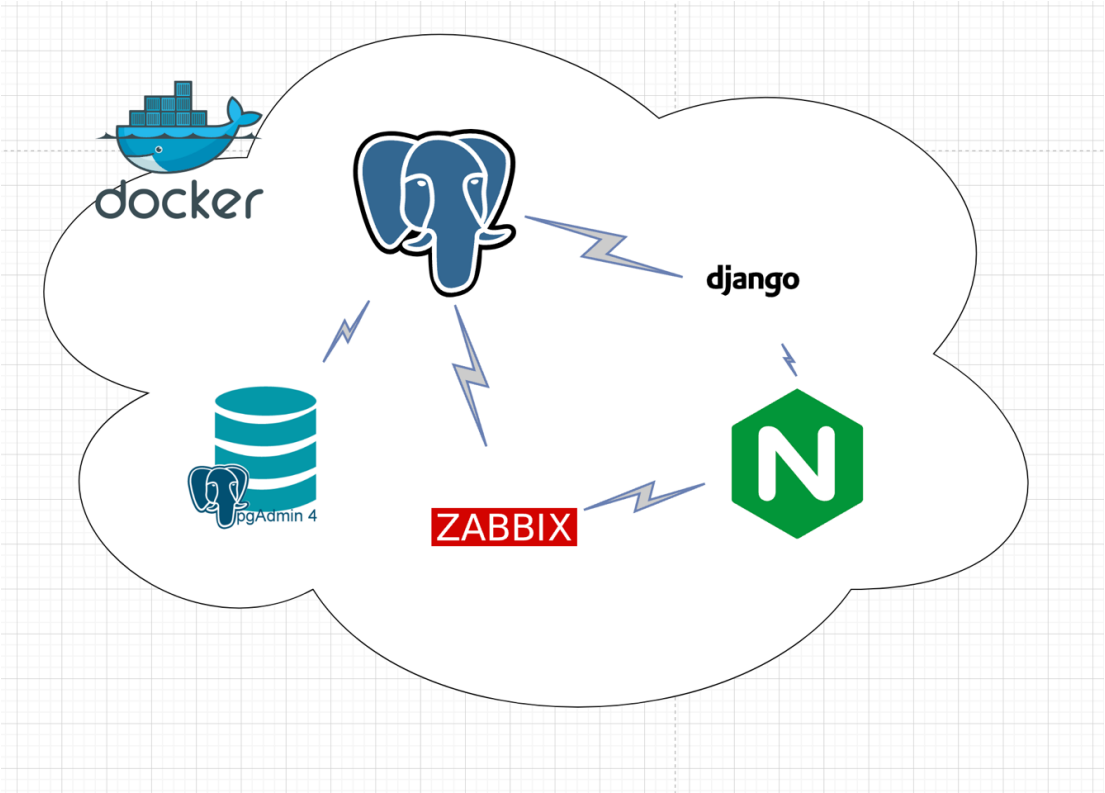
- Настроить сбор статистики по трафику с использованием технологии NetFlow для последующего анализа и отчетности. Самостоятельно определить, какие данные будут собираться. Убедиться, что данные экспортируются на сервер и собираются корректно.

Для скачивания дистрибутива и запроса лицензии перейдите по ссылке:

https://files.infowatch.com/s/T8eHG3fxPtnzZ27

Часть 2 Конфигурация

Для выполнения задачи нужно развернуть сервисы (nginx, pgadmin, postgres, zabbix-web, zabbix, django) на виртуальной машине с предустановленной операционной системой Red OS, используя контейнерную виртуализацию docker compose, для этого надо учесть вопросы защиты информации (логины, пароли, защищенное соединение, шифрование дисков, бэкапы). Все процессы должны быть протестированы.



Руководство компании очень переживает за результат, поэтому все шаги должны быть протестированы и описаны.

2. Отправка решения

Вашим решением будут следующие файлы:

- Конфигурационной файл.
- Отчет в формате docker-compose.yml.
- Отчет со скриншотами (не менее 10) с проверкой работоспособности соответствующих настроек.

3. Рекомендуемые материалы

- https://docs.docker.com
- https://docs.docker.com/engine/security/
- https://www.zabbix.com/container_images
- https://hub.docker.com/_/nginx
- https://nginx.org/ru/
- https://www.zabbix.com/documentation/current/en/manual

- https://docs.djangoproject.com/en/5.1/
- https://hub.docker.com/_/django/
- https://hub.docker.com/r/dpage/pgadmin4/
- https://www.postgresql.org/docs/
- https://hub.docker.com/_/postgres
- В. Олифер, Н. Олифер - Компьютерные сети. Принципы, технологии, протоколы
- Бирюков, А. А. Информационная безопасность: защита и нападение / А. А. Бирюков. — 2-е изд. — Москва : ДМК Пресс, 2017. — 434 с
- https://docs.iwarma.ru/
- https://docs.iwarma.ru/NGFW/rp_ngfw_v4.4/index_ngfw_v4.4_cli_rp.html

4. Критерии оценки работ и выбора победителей этапа

Критерий	**Комментарий**	**Баллы**
Файл конфигурации yml	Критерии оценки: 20%-0 баллов, 21-50% - 5 баллов, 50-70%- 7 баллов, 70-90%-9 баллов, 90-100 - 10 баллов	10
Соблюдены требования безопасности	Выставлены пароли, логины не по умолчанию, порты отличаются от по умолчанию, данные шифруя, соединении через https, образы были протестированы Критерии оценки: 20%-0 баллов, 21-50% - 5 баллов, 50-70%- 10 баллов, 70-90%-15 баллов, 90-100 - 20 баллов	20
Приведены тесты системы (инфраструктуры)	Все части тестов приустают (каждый сервис, работает, безопасность на уровне) Критерии оценки: 20%-0 баллов, 21-50% - 7 баллов, 50-70%- 10 баллов, 70-90%-13 баллов, 90-100 - 15 баллов	15
Написан отчет	Отчет содержит информацию Критерии оценки: 20%-0 баллов, 21-50% - 5 баллов, 50-70%- 7 баллов, 70-90%-9 баллов, 90-100 - 10 баллов	10
Настройка интерфейсов	Интерфейсы настроены согласно топологии	10

	Критерии оценки: 20%-0 баллов, 21-50% - 5 баллов, 50-70%- 7 баллов, 70-90%-9 баллов, 90-100 - 10 баллов	
Трансляция адресов	Выполнено преобразование внутренних IP-адресов в публичный внешний адрес. Критерии оценки: 20%-0 баллов, 21-50% - 10 баллов, 50-70%- 15 баллов, 70-90%-17 баллов, 90-100 - 20 баллов	20
Система обнаружения и предотвращения вторжений	Выполнен полный цикл настройки системы. Созданы правила, проведены тестирования. Критерии оценки: 20%-5 баллов, 21-50% - 10 баллов, 50-70%- 15 баллов, 70-90%-20 баллов, 90-100 - 30 баллов	30
Создание отказоустойчивого кластера	Создан отказоустойчивый кластер из двух InfoWatch ARMA NGFW устройств с использованием протокола VRRP, при выключении одного из NGFW включается резервный. Критерии оценки: 20%-0 баллов, 21-50% - 10 баллов, 50-70%- 15 баллов, 70-90%-17 баллов, 90-100 - 20 баллов	20
Сбор статистики NetFlow	Настроен сбор статистики по трафику с использованием технологии NetFlow Критерии оценки: 20%-0 баллов, 21-50% - 5 баллов, 50-70%- 10 баллов, 70-90%-12 баллов, 90-100 - 15 баллов	15

Максимальное количество баллов, которое можно набрать в данном этапе – 150 баллов.

Подведение итогов

Каждая работа участника оценивается по приведённым выше критериям, результатом оценки является сумма баллов за все критерии.

В следующий этап будут приглашены 20 участников, чьи работы получили наиболее высокие оценки экспертов. Оргкомитет имеет право приглашать в следующий этап дополнительных участников, находящихся следующими в рейтинговой таблице.

Результаты отборочного этапа публикуются в формате протоколов на странице конкурса не позднее 28 апреля 2025 года.