Инструкция по установке

Введение

DAMASK это Средство Защиты Информации реализованное в формате доверенного высокопроизводительного программно-аппаратного комплекса (ДПАК), использующего метод динамической подмены данных (ДПД) для обеспечения безопасной обработки конфиденциальной данных в различных сценариях.
Система DAMASK является программно-аппаратным комплексом, данная инструкция ориентирована на установку программной части DAMASK на аппаратную часть.

Схема физического развертывания DAMASK

Ниже приведена схема физического развертывания DAMASK на примере решения с двумя узлами. Расширение количество узлов принципиально ничего не поменяет. На данной схеме к DAMASK относится только то что обведено пунктирной линией и называется Кластер DAMASK. Остальная часть схемы демонстрирует способ взаимодействия DAMASK с существующей инфраструктурой, в которую внедряется данное решение.

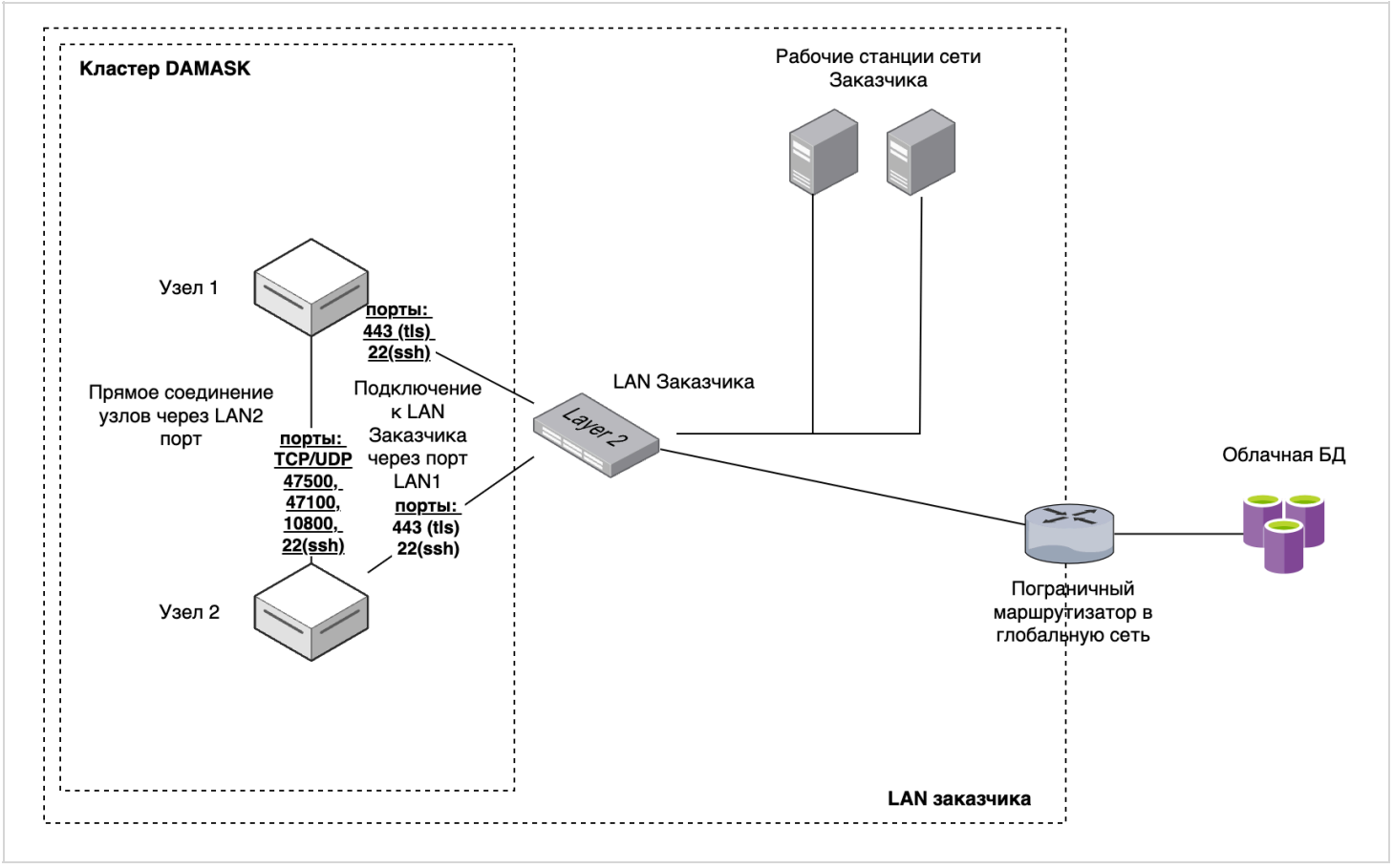

Диаграмма развертывания

На каждом узле DAMASK необходимо настроить единый виртуальный IP (ipv4), который должен быть прописан в вашем DNS сервере, для того чтобы если один узел перестанет быть доступен это не повлияло на доступность кластера.

Настройка сервера приложений

Директория установки - `/opt/damask` (может быть изменена при необходимость в процессе установки)
Для начала установки у вас должна быть установлена java 11 и утилита keytool.
В операционной системе необходимо создать группу и пользователя damask, от имени которого выполнять все операции, описанные ниже.

Генерация ключей и сертификатов

Для начала необходимо сгенерировать сертификаты для идентификации узлов кластера.

1. Генерация сертификата для первого узла кластера.

```
keytool -genkey -keystore primary.p12 -keyalg RSA -validity 365 -storepass password -ke
```

password - здесь и далее необходимо заменить на Ваш пароль.

2. Экспорт публичного сертификата из сгенерированного файла.

```
keytool -export -alias PrimaryNode -keystore primary.p12 -file PrimaryNode.cer -storepa
```

3. Генерация сертификата для второго узла кластера.

```
keytool -genkey -keystore secondary.p12 -keyalg RSA -validity 365 -storepass password -
```

4. Экспорт публичного сертификат из сгенерированного файла.

```
keytool -export -alias SecondaryNode -keystore secondary.p12 -file SecondaryNode.cer -s
```

5. Импорт сертификата первого узла в хранилище доверенных сертификатов второго узла.

```
keytool -import -keystore trust_for_node2.p12 -alias node2 -file PrimaryNode.cer
```

6. Импорт сертификата второго узла в хранилище доверенных сертификатов первого узла.

```
keytool -import -keystore trust_for_node1.p12 -alias node1 -file SecondaryNode.cer
```

7. Генерация ключа для шифрования данных на диске в хранилище (ключ должен быть одинаковым для всех узлов).

```
keytool -genseckey -alias damask.master.key -keystore master.p12 -storetype PKCS12 -key
```

8. Генерация ключа для шифрования данных на JWT токенов (ключ должен быть одинаковым для всех узлов).

```
keytool -genkey -keyalg RSA -alias damask.oauth.jwt -keystore damask.p12 -storepass pas
```

Настройка конфигурационного файла

Рядом с приложением необходимо разместить конфигурационный файл `damask.properties` .

```
spring.task.scheduling.pool.size=10
license.customerid=7700000000
app.security.jwt.keystore-location=/opt/damask/damask.p12
app.security.jwt.keystore-password=<password из предыдущего раздела>
app.security.jwt.key-alias=damask.oauth.jwt
app.security.jwt.private-key-passphrase=<password из предыдущего раздела>
app.jwtExpirationInMs=864000001
app.jwtSecret=JWTSuperSecretKey
damask.security.refresh_token_expiration=30
damask.workDirectory=/opt/damask/data
damask.instanceName=<название узла>
damask.security.nodeStore=/opt/damask/secondary.p12
damask.security.nodePassword=<password из предыдущего раздела>
damask.security.trustStore=/opt/damask/trust2.p12
damask.security.trustPassword=<password из предыдущего раздела>
damask.security.masterStore=/opt/damask/master.p12
damask.security.masterPassword=<password из предыдущего раздела>
damask.network.nodeAddresses=<ip адрес узла 1>, <ip адрес узла 2>
logging.file.name=damask_core.log
damask.security.masterKeyName=damask.master.key
```

Запуск приложения

1. Необходимом войти на каждый узел, перейти в папку, в которой размещен и настроен экземпляр программного обеспечения DAMASK.
2. Запустить экземпляр программного обеспечения DAMASK, выполнив команду `sh damask.sh` на каждом узле, последовательно.

После выполнения этих действий вы получите синхронизированный кластер DAMASK.

Настройка балансировки нагрузки

Для обеспечения отказоустойчивости и балансировки нагрузки используется сервер Nginx.
Его необходимо установить и настроить на каждом сервере.
Пример конфигурационного файла Nginx (<ваш домен DAMASK>.conf) приведен ниже.

```
shell
server {
    listen       443 ssl http2;
    server_name  <домен сервера DAMASK>;

    ssl_certificate     /etc/letsencrypt/live/<домен сервера DAMASK>/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/<домен сервера DAMASK>/privkey.pem;

    client_max_body_size 3000M;

    location / {
        proxy_pass http://localhost:59801;
        proxy_http_version 1.1;
        proxy_set_header Upgrade $http_upgrade;
        proxy_set_header Connection 'upgrade';
        proxy_set_header Host $host;
        proxy_cache_bypass $http_upgrade;
        proxy_read_timeout 3600;

        proxy_redirect     off;

        proxy_set_header X-Real-IP        $remote_addr;
        proxy_set_header X-Forwarded-For  $proxy_add_x_forwarded_for;

        client_max_body_size       3000m;
        client_body_buffer_size    128k;

    }
}
```

На каждом узле DAMASK необходимо настроить единый виртуальный IP, который должен быть прописан в вашем DNS сервере, для того чтобы если один узел перестанет быть доступен это не повлияло на доступность кластера.

Установка пользовательского интерфейса DAMASK

1. Разархивировать архив damask_ui.zip в папку /opt/damask_ui.
2. Поправить файл `.env` , прописав значение `https://<домен DAMASK>` в параметра `REACT_APP_DAMASK_API`
3. Внесите соответствующие изменения в настроечный файл Nginx на каждом сервере для маршрутизации запросов на к url `https://<домен DAMASK>/damask_ui` к файлу

```
/opt/damask_ui/index.html
```