Интеграция NGFW UserGate 7.1 со службой каталога ALD Pro

06/10/2025

Содержание

UserGate NGFW – это межсетевой экран, обеспечивающий высокий уровень защиты от угроз для сетей любого формата и размера благодаря максимальной видимости событий безопасности, совмещает в себе систему обнаружения вторжения и межсетевой экран.

В настоящей инструкции описана процедура интеграции NGFW UserGate 7.1 со службой каталога ALD Pro. Данная интеграция обеспечит возможность получать информацию о пользователях и группах домена и использовать эти данные при настройке правил фильтрации и разграничении доступа. Также интеграция позволяет прозрачно аутентифицировать пользователей посредством протокола Kerberos и предоставлять пользователям и группам домена административный доступ к UserGate NGFW.

Данная инструкция описывает частный случай интеграции виртуального образа UserGate NGFW и не является исчерпывающей. В документе представлен алгоритм интеграции NGFW в домен и минимальные настройки для проверки возможности аутентификации пользователя и применения правил фильтрации.

1 Описание стенда

- Развернутый контроллер домена ALD Pro 2.2.0 con1.test.la (192.168.122.28).
- Развернутый по инструкции образ UGOS NGFW 7.1 (192.168.122.142) с одним сетевым интерфейсом, добавленным в зону «Management».

2 Работы на контроллере домена (или любом другом зарегистрированном в домене хосте)

2.1 В терминале хоста

Необходимо зарегистрировать сервер UserGate в домене и получить keytab-файл для дальнейших настроек:

```
kinit admin
ipa host-add --force --ip-address=192.168.122.142 auth.test.la
ipa service-add HTTP/auth.test.la
ipa-getkeytab -s con1.test.la -p HTTP/auth.test.la -k usergate.keytab
```

2.2 В вэб-интерфейсе управления контроллером домена «ALD Pro» в настройках «Службы разрешения имён»

1. Добавить DNS-записи типа A для домена страницы блокировки и для домена Logout captive-портала (logout.test.la, block.test.la) (Роли и службы сайта > Служба разрешения имён > test.la. > Новая DNS-запись);
2. Настроить форвард DNS-запросов на внешние серверы (Роли и службы сайта > Служба разрешения имён > Глобальная конфигурация DNS > Глобальные перенаправители).

3 Работы в вэб-интерфейсе UserGate

1. В меню «Сеть» в пункте «DNS» добавить адрес контроллера домена (192.168.122.28) в поле «Системные DNS-серверы».

2. В меню «UserGate» в пункте «Настройки» в поле «Модули»:

- установить в параметр «Домен Auth captive-портала» значение «auth.test.la»;
- установить в параметр «Домен Logout captive-портала» значение «logout.test.la»;
- установить в параметр «Домен страницы блокировки» значение «block.test.la».

3. В меню «Сеть» в пункте «Зоны» выбираем «Management».

- На вкладке «Контроль доступа» ставим флажок «HTTP(S)-прокси».

4. В меню «Пользователи и устройства» в пункте «Серверы аутентификации» добавить LDAP-коннектор:

- установить флажок«Использовать для соединений SSL»;
- доменное имя LDAP или IP-адрес: «con1.test.la»;
- Bind DN («логин»): uid=admin,cn=users,cn=accounts,dc=test,dc=la;
- ввести пароль учетной записи администратора домена;
- на вкладке «Домены LDAP» добавить домен test.la;
- на вкладке «Kerberos Keytab» загрузить сгенерированный ранее keytab-файл.

5. В меню «Пользователи и устройства» в пункте «Профили аутентификации» добавить новый профиль «1»:

- на вкладке «Методы аутентификации» добавить «Аутентификация Kerberos».

6. В меню «Пользователи и устройства» в пункте «Captive-профили» добавить новый профиль «1»:

- в поле «Метод аутентификации» выбрать «Запоминать cookie»;
- в поле «Профиль аутентификации» выбрать ранее созданный профиль «1».

7. В меню «Пользователи и устройства» в пункте «Captive-портал» добавить новое правило «1»:

- в поле «Captive-профиль» выбрать созданный ранее профиль «1».

8. В меню «Политики сети» в пункте «Межсетевой экран» добавить разрешающее правило «1» для всего трафика:

- в поле «Действие» выбрать «Разрешить»;
- в поле «Журналирование» выбрать «Журналировать начало сессии».
- на вкладке «Пользователи» добавить пользователя из LDAP-каталога по кнопке «Добавить пользователя LDAP». В открывшемся окне в строке поиска ввести имя пользователя и нажать «Поиск», выбрать нужного пользователя из представленного списка.

4 Работы на пользовательском ПК

В браузере настроить прокси-сервер для протоколов HTTP, HTTPS:

- сервер «auth.test.la»;
- порт: 8090.

5 Диагностика

1. Проверить корректность настроек можно в вэб-интерфейсе UserGate в разделе «Журналы и отчеты» меню «Журналы» раздел «Журнал трафика» в поле «Журналирование» выбрать «Журналировать начало сессии».
2. При необходимости включить журналирование запрещающего правила межсетевого экрана: меню «Политики сети» в пункте «Межсетевой экран» выбираем «Default block».