WALLIX

TRACE, AUDIT & TRUST

WALLIX PAM РЕШЕНИЯ ПО КИБЕРБЕЗОПАСНОСТИ И УПРАВЛЕНИЮ ДОСТУПА К ИНФОРМАЦИОННОЙ СИСТЕМЕ

Доклачик: Бозоров С.

Два опытных учредителя у руля

Jean-Noël de Galzain

Основатель и председатель правления

Основатель Aurora, сервисной компании, проданной Business & Decision в 2003 году.
Председатель-учредитель клуба HEXATRUST
Заместитель председателя бизнес-кластера «Систематический Парижский регион»

Amaury Rosset

Соучредитель и финансовый директор

Четыре года в Hachette Filipacchi Media в качестве финансового контролера, менеджера проектов в Азиатско-Тихоокеанском регионе (Гонконг), а затем помощника издателя гонконгских и китайских изданий Группы.
Основатель агентства мультимедийных коммуникаций XLAB.

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

Systematic
Paris Region Digital Ecosystem

01

***P**RIVILEGED **A**CCESS **M**ANAGEMENT*:

ПОСЛЕДНЕЕ ПОКОЛЕНИЕ

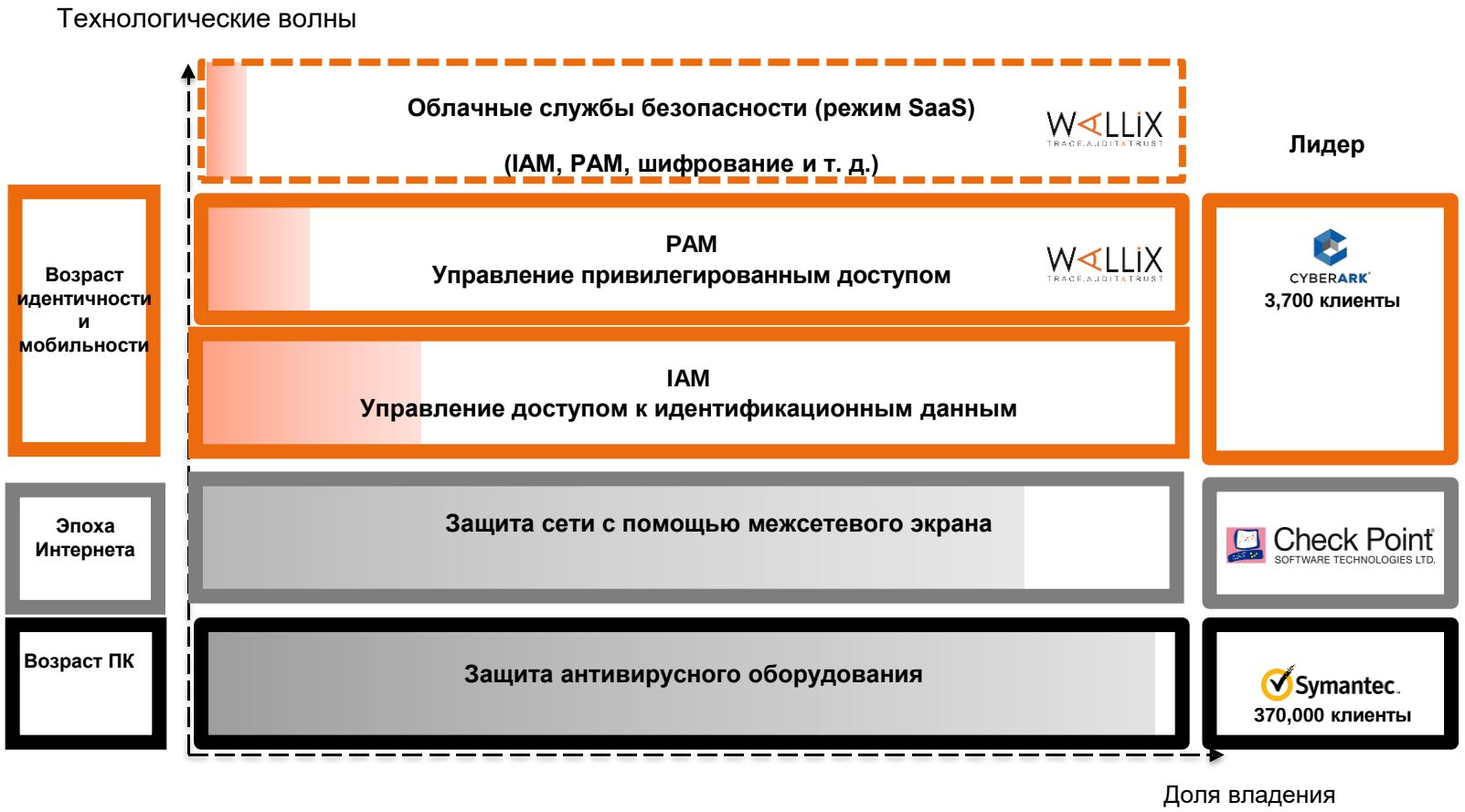
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

КИБЕРБЕЗОПАСНОСТИ

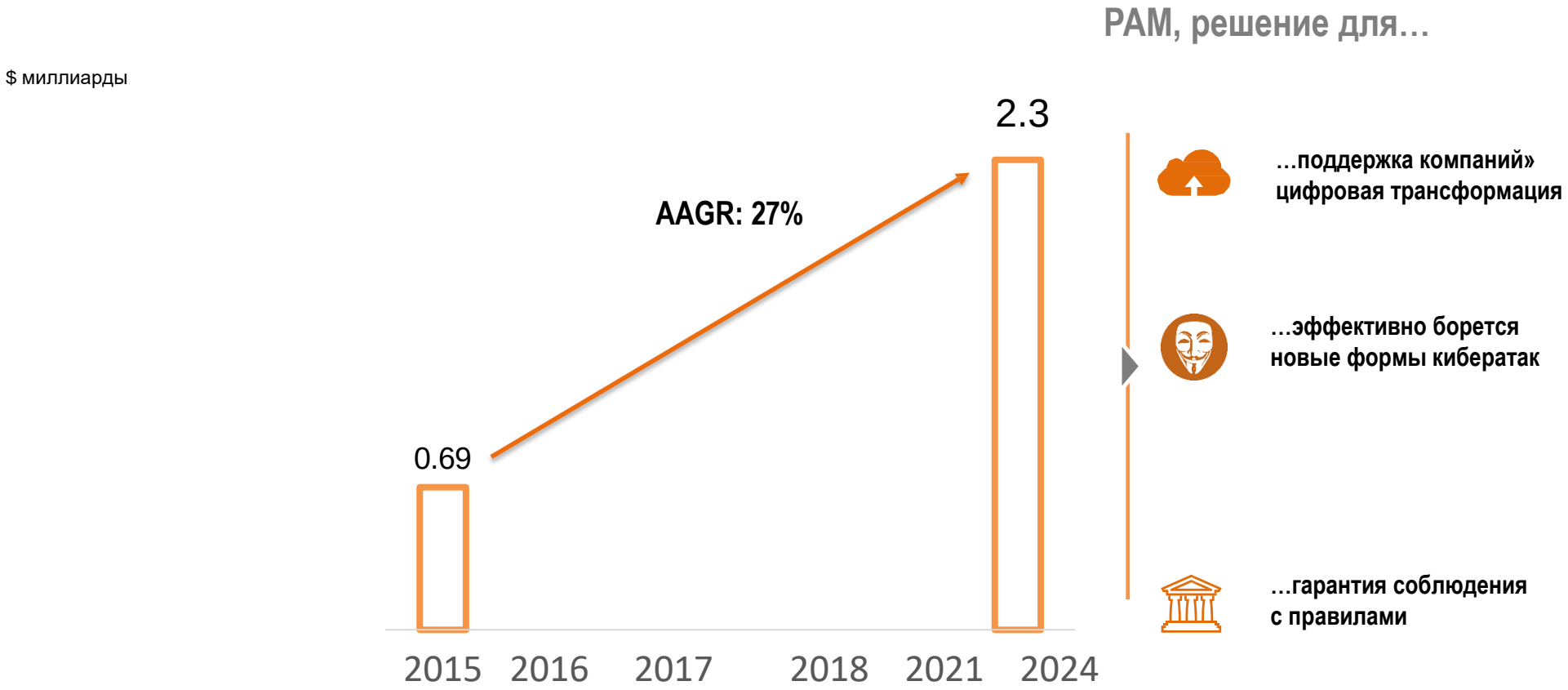
WALLIX

TRACE, AUDIT & TRUST

НОВАЯ ЭРА КИБЕРБЕЗОПАСНОСТИ

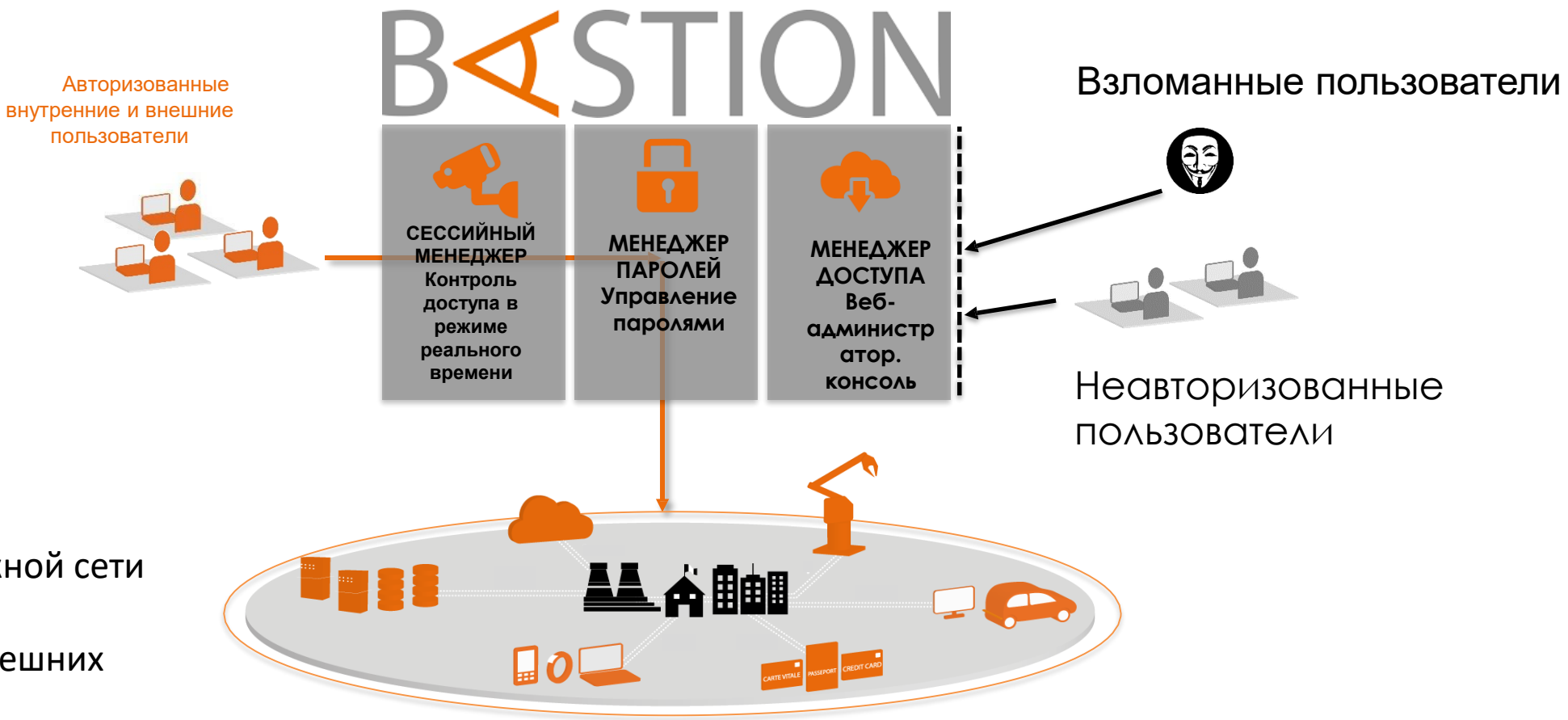


УПРАВЛЕНИЕ ПРИВИЛЕГИРОВАННЫМ ДОСТУПОМ: ЦЕЛЕВАЯ РЫНОЧНАЯ СТОИМОСТЬ 2 МЛРД ДОЛЛАРОВ В 2021 ГОДУ



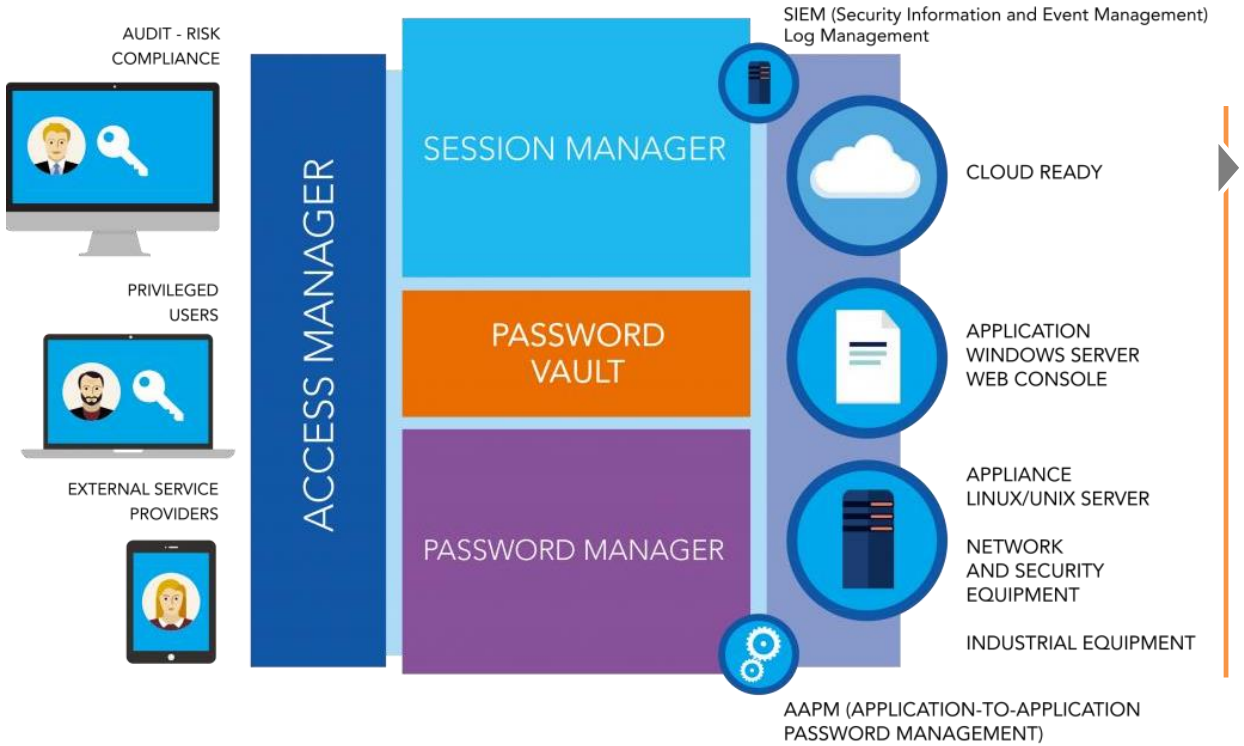
Источник: Гартнер

НОВЫЙ ВЫЗОВ: ЗАЩИТА КОРПОРАТИВНОЙ ДЕЯТЕЛЬНОСТИ
ЛИЧНОСТЬ, ДОСТУП И ДАННЫЕ



Создание надежной сети для отражения внутренних и внешних угроз.

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ



amazon web services

Microsoft Azure

Microsoft Hyper-V

vmware READY

InfoWorld BOSSIE 2017 AWARDS

БАСТИОН ВАЛЛИКС: ОСНОВНЫЕ СИЛЬНЫЕ СТОРОНЫ

CSPN-certified by ANSSI*

VISA DE SÉCURITÉ

- НЕНАВЯЗЧИВОЕ УДАЛЕННОЕ РАЗВЕРТЫВАНИЕ (ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ) НА ЗАЩИЩАЕМОМ ОБОРУДОВАНИИ
- КРАТЧАЙШИЙ ПУТЬ К СООТВЕТСТВИЮ
- УЛУЧШЕНИЕ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ТОЧЕК В ИНФОРМАЦИОННЫХ СИСТЕМАХ
- ЛЕГКОЕ ВНЕДРЕНИЕ, НЕ ВЛИЯЕТ НА ПРОИЗВОДИТЕЛЬНОСТЬ КОМАНДЫ
- ОПТИМИЗИРОВАННЫЕ РАСХОДЫ НА ПОКУПКУ И ЛИЦЕНЗИЮ

* Премиальный сертификат безопасности, выданный Французским национальным агентством кибербезопасности (ANSSI)

ОБЛАЧНОЕ РЕШЕНИЕ ДЛЯ СЛУЖБ БЕЗОПАСНОСТИ

DataPeps

Сквозное шифрование/решение E2EE, обеспечивающее защиту данных во всех приложениях

РЫНОК ШИФРОВАНИЯ ОЦЕНИВАЕТСЯ В 2 МЛРД ДОЛЛАРОВ*

Готов к GDPR

- Соответствие GDPR
- Защищает данные даже в случае кибератаки — данные непригодны для использования

Программное обеспечение как

- Технология, приобретенная путем покупки активов MLState
- **Простое развертывание (SDK, плагин Outlook)**
- Две совместные платформы :

FENTEC

HORIZON 2020

ANBLIC

FUI
FONDS UNIQUE INTERMINISTÉRIEL
PROJET SÉLECTIONNÉ

02

2013-2017: Эксплуатационные характеристики WALLIX PAM

WALLIX
TRACE, AUDIT & TRUST

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Централизованный контроль и мониторинг привилегированного доступа к конфиденциальным активам

Хакеры используют привилегированные учетные записи для проникновения и распространения внутри организаций. Управление привилегированным доступом (PAM) является основополагающим активом для смягчения кибератак. WALLIX PAM — ведущее решение PAM, которое обеспечивает надежную безопасность и контроль привилегированного доступа к критически важной ИТ-инфраструктуре. Как решение без агентов, WALLIX PAM может быть легко развернуто от локальной инфраструктуры до частных и публичных облачных инфраструктур. WALLIX PAM также доступен в качестве услуги, предлагающей более экономичный и менее ресурсоемкий вариант.

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Особенности и возможности

Уменьшить поверхность атаки

- Автоматически обнаруживайте активы и удаляйте все локальные привилегированные учетные записи
- Настройте правила авторизации для контроля доступа к критически важным системам
- Используйте наименее необходимые привилегии для выполнения задач
- Атрибут привилегий «Just in Time» для авторизованных пользователей

Управляйте секретами

- Безопасное хранение секретов пользователей-людей и не-людей
- Обновляйте пароли с автоматической ротацией на основе времени и/или использования
- Удаляйте пароли с дисков

Контрольные сеансы

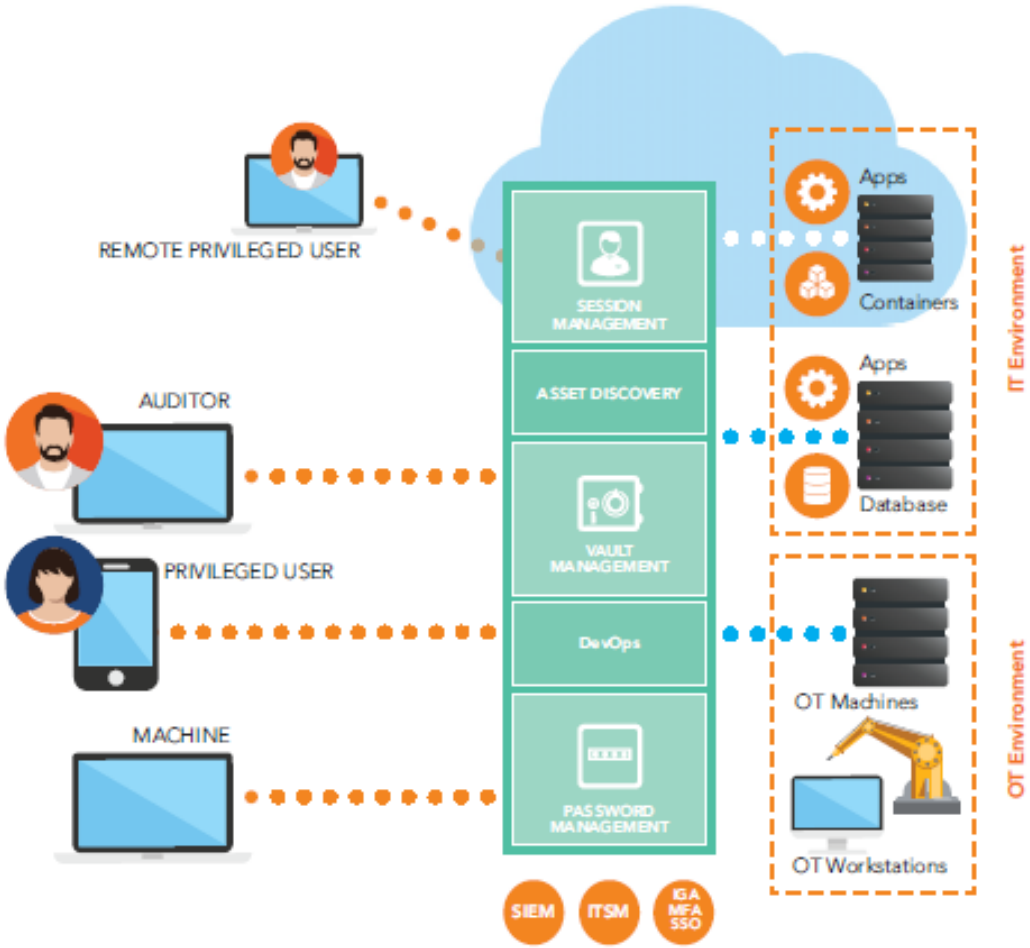
- Мониторинг сеансов в режиме реального времени с помощью Session Sharing
- Запись всех сеансов и извлечение связанных метаданных для анализа
- Подача сигналов тревоги после обнаружения вредоносной активности и завершение сеансов

Аудиторская деятельность

- Управляйте KPI с помощью отчетов и панелей мониторинга
- Сопоставляйте подозрительное поведение с интеграцией SIEM
- Быстро развертывайте без прерывания ежедневных рабочих процессов

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Как это работае



WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Преимущества

Обезвредить внутренние и внешние угрозы

Централизуйте безопасность Управление привилегированные пользователи и критические системы.

Безопасный по мере того, как ты растешь

Масштабируйте свой инфраструктура без всякого риска.

Развернуть во всех окружающая среда

Беспрепятственно интегрируйтесь в локальные, гибридные и облачный инфраструктуры. WALLIX также предлагает доставку SaaS ПАМ.

Обеспечить нормативное Согласие

Избегайте штрафов, защита и отслеживание критических доступ к данным.

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Безопасный доступ без VPN, без общих паролей и без ущерба для безопасности!

Большинство предприятий полагаются на внешних поставщиков услуг для выполнения удаленных задач, требующих привилегированного доступа к их ИТ- или ОТ-сети. Половина из них не имеет реестра доступа третьих лиц к своей сети, практически не имеет возможности наблюдать и контролировать свой удаленный цифровой доступ. Удаленный доступ WALLIX One помогает удовлетворить новые требования к обеспечению и обеспечению безопасного доступа для внешних поставщиков услуг, которым необходим доступ к критически важной инфраструктуре, управляемой WALLIX One.

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Функции

- Полное разделение каталога для внешних поставщиков (точно в срок без добавления удостоверений в корпоративный AD)
- Дальнейшее применение корпоративной политики безопасности
- Делегирование управления владельцам бизнеса
- Самостоятельный сброс пароля (SSPR)
- Никакого VPN для установки и управления, никаких дополнительных билетов для ИТ-персонала.

WALLIX BASTION: КОМПЛЕКТ ОБЛАЧНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

Полная видимость внешнего удаленного доступа

- Полная видимость внешнего удаленного доступа
- Создание авторизованного доступа в режиме реального времени
- Единый веб-портал со встроенными веб-клиентами RDP и SSH.
- Контроль и прозрачность деятельности третьих лиц
- Соответствие стандартам и рекомендациям Французского национального агентства по безопасности и информационным технологиям (ANSSI), а также бизнес-стандартам, гигиене безопасности.
- Нет общих паролей

03

2013-2017: РАЗВЕРТЫВАНИЕ И АДМИНИСТРИРОВАНИЕ

WALLIX
TRACE, AUDIT & TRUST

1. Настройка собственного сервера WALLIX Bastion

Будет использоваться образ сервера VMWare, который WALLIX размещает на своем веб-сайте.
а. Скачать Bastion можно по следующему адресу:
https://cloud.wallix.com/index.php/s/sT2xwYrgyWNX7ke?path=%2FBastion%209.0.2.9

1 - Выберите «VM VMware», затем загрузите файл «bastion-9.0.2.9-vmware.tbz».
2 - Распакуйте файл «bastion-9.0.2.9-vmware.tbz», чтобы получить локальные образы «bastion-9.0.2.9-vmware.ova» для развертывания.

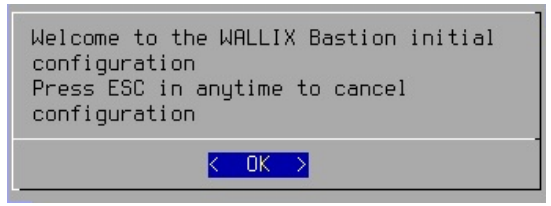
б) Установите Wallix Bastion из локального образа.
Устройство WALLIX Bastion поставляется в следующей заводской конфигурации:
•IP-адрес eth0: 192.168.10.5
•Шлюз по умолчанию: 192.168.10.1
•Логин и пароль системной учетной записи: "wabadmin"/"SecureWabAdmin"
•Логин и пароль учетной записи администратора WALLIX Bastion: «admin»/«admin»

WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

Шаги:
1 — Импортируйте файл «bastion-16-vmware.ova» в VMware Workstation
2 - Включите это виртуальное устройство WALLIX Bastion, выберите устройство по умолчанию «WALLIX Bastion 16».

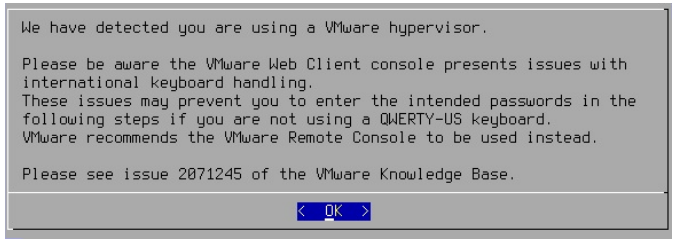
WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

3 - Отобразится окно начальной конфигурации WALLIX Bastion, как на следующем изображении. Нажмите «ОК», чтобы продолжить.



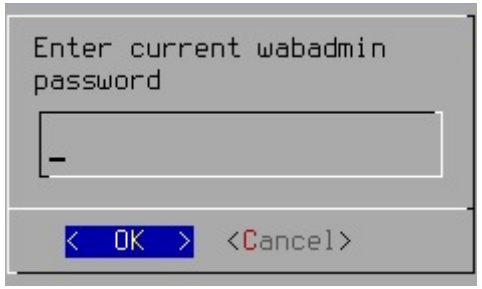
4 - В настройках клавиатуры выберите «Английский (американский)», нажмите «ОК».

5 — Нажмите «ОК», когда конфигурация Bastion будет обнаружена в VMware.

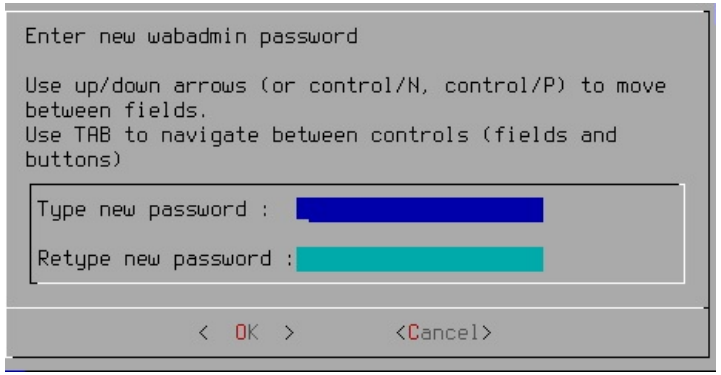


WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

6 - Введите пароль по умолчанию для пользователя «wabadmin», а именно: SecureWabAdmin

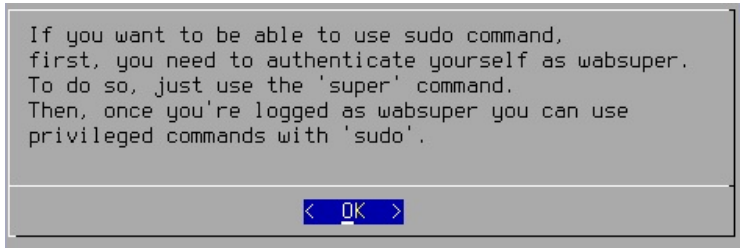


7 - Bastion попросит вас создать новый пароль для «wabadmin»

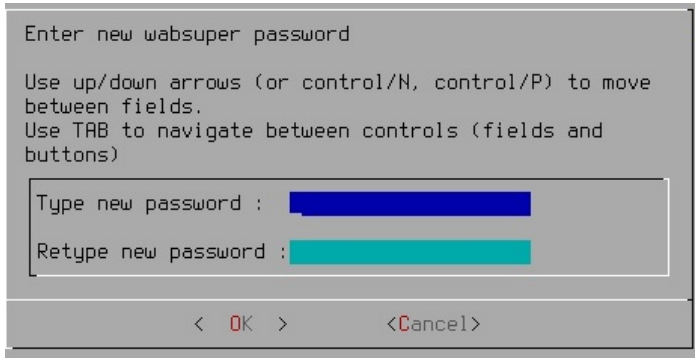


7.1 - Затем отображается сообщение после успешной смены пароля пользователя wabadmin.

7.2 - Появится панель уведомлений об использовании команды 'sudo', требующей учетной записи супер-администратора "wabsuper". Нажмите «ОК» на этой панели (ниже):



8 - Введите и подтвердите новый пароль wabsuper.

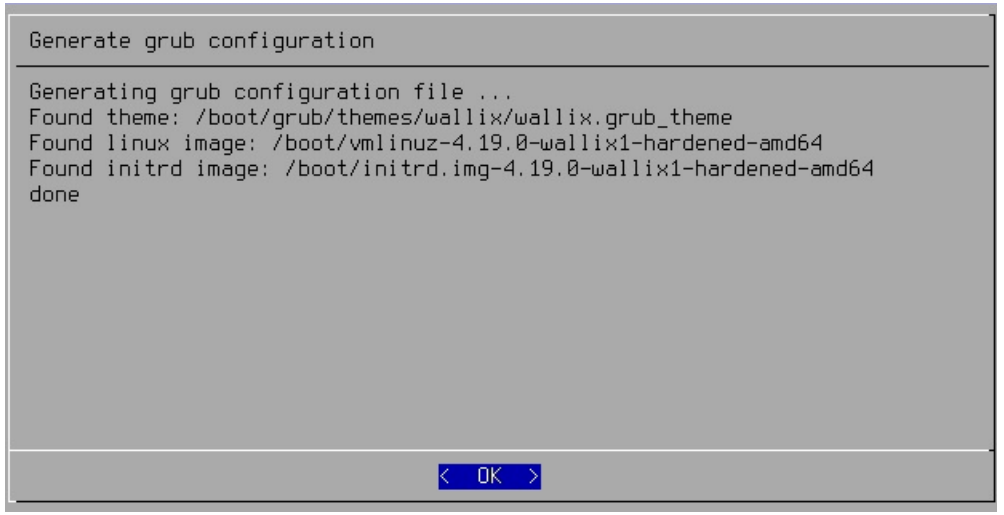


8.1 После успешной смены пароля пользователя wabsuper появится сообщение.

WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

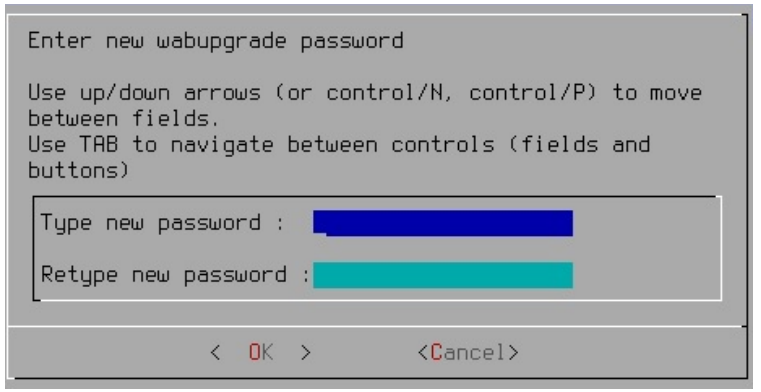
9 - Нажмите «Да», чтобы использовать тот же пароль пользователя «wabsuper» для системной учетной записи «wabrootadmin».

10 - Bastion инициирует создание файлов конфигурации



11 - Нажмите «ОК», когда Bastion уведомит вас о необходимости нового пользователя: «wabupgrade», функция которого заключается в том, чтобы разрешить безопасное обновление вашей установки Bastion.

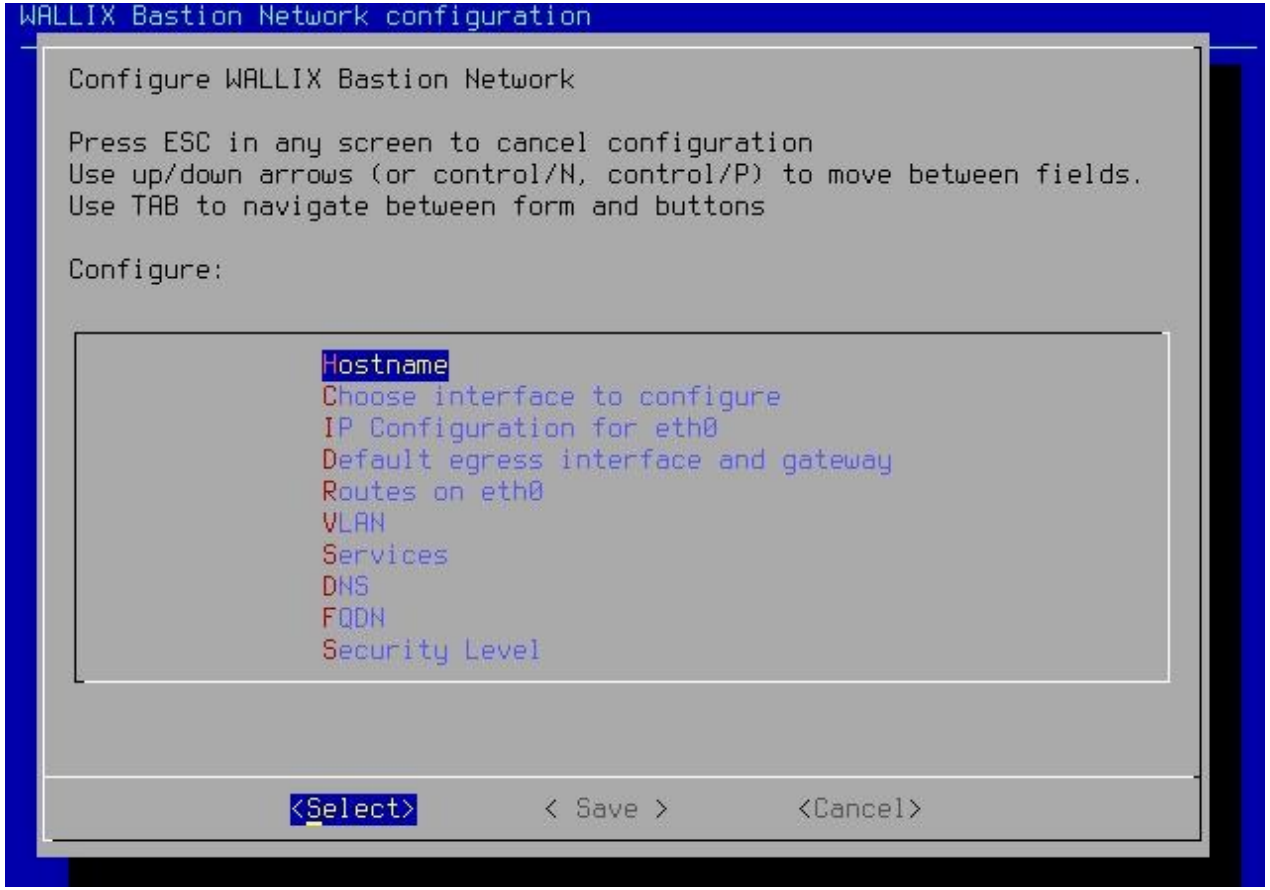
12 - Нажмите «ОК» в сообщении выше, затем на появившейся панели (см. ниже) введите и подтвердите пароль учетной записи wabupgrade.



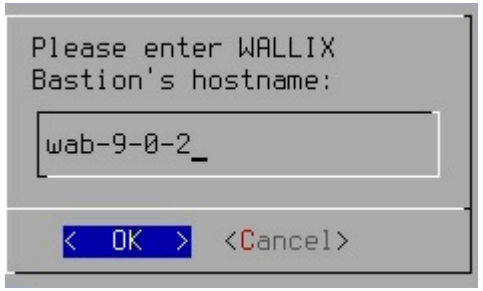
12.1 - Установщик отобразит сообщение после успешного создания нового пароля.

13 - Далее вам будет предложено настроить сеть WALLIX Bastion (как на изображении ниже). Нажмите «Да».

14 — Настройте важную сетевую информацию/элементы, такие как имя хоста, IP-адрес для eth0.

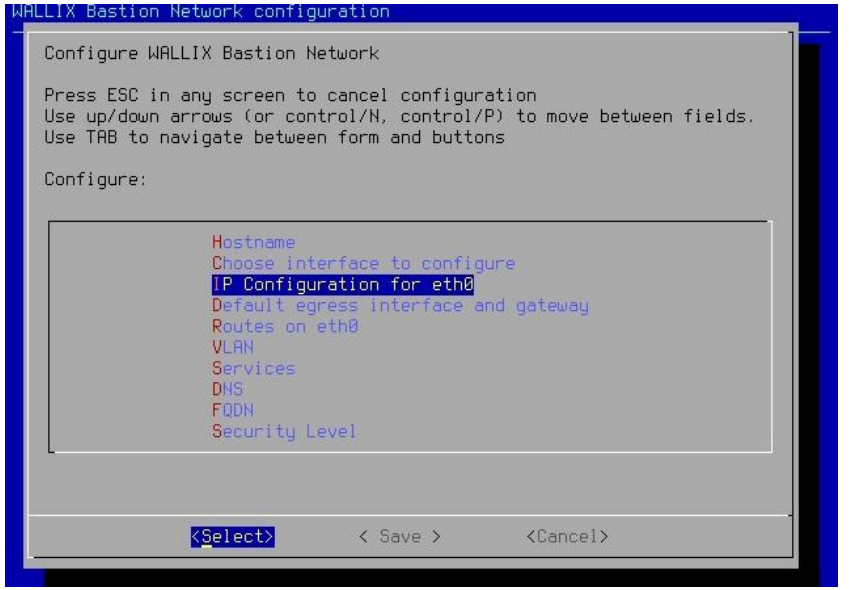


В поле «Имя хоста» введите имя хоста Bastion.

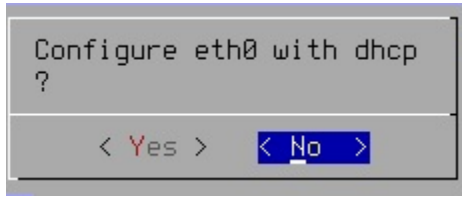


WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

14.1 — Определите IP-адрес для eth0:

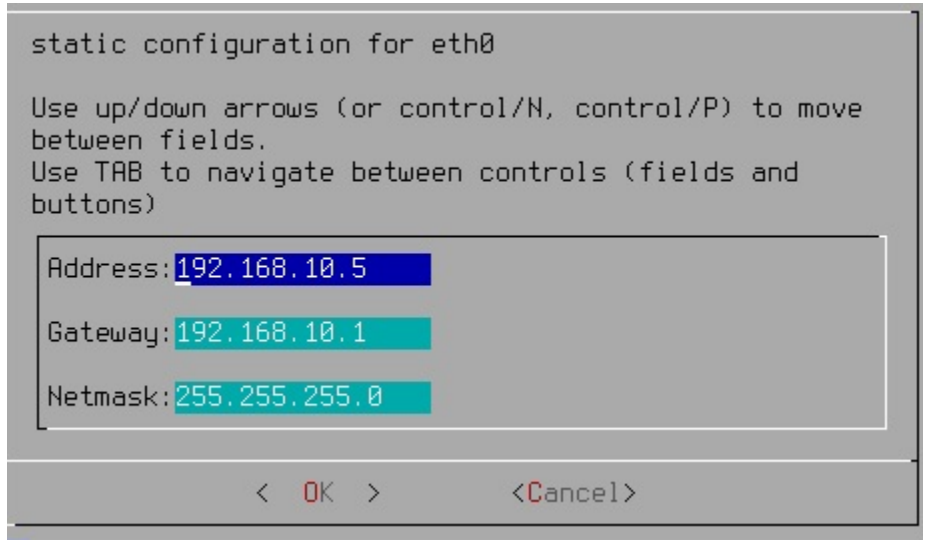


14.1.1 Нажмите «Выбрать», затем нажмите «Нет», чтобы отключить DHCP.



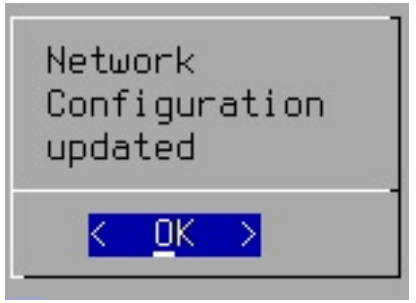
14.1.2 - Измените IP-адрес Bastion по умолчанию на ваш локальный IP-адрес (например, «192.168.1.5 – Шлюз: 192.168.1.1) и нажмите «ОК».

ПРИМЕЧАНИЕ: Это будет IP-адрес Bastion, используемый для входа в веб-интерфейс (GUI) WALLIX Bastion.



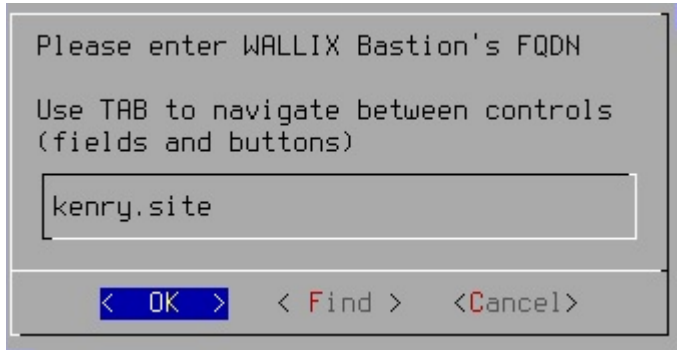
15 - После сохранения настроенного сетевого IP-адреса Bastion появится сообщение, как показано на рисунке ниже:

Нажмите «ОК», чтобы закрыть это сообщение и вернуться в меню.



WALLIX BASTION: УСТАНОВКА/НАСТРОЙКА WALLIX BASTION

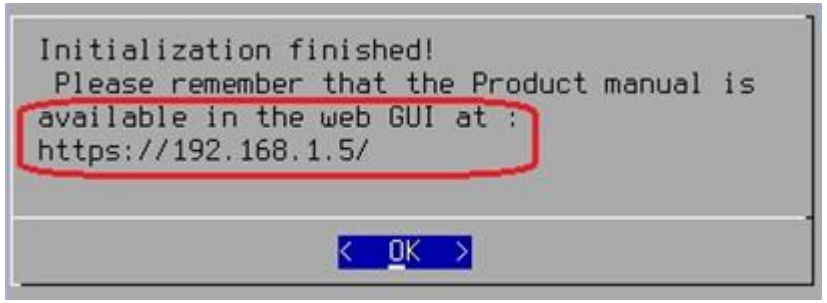
16 - Введите полное доменное имя (FQDN) Bastion, используя его локальный IP-адрес или доменное имя устройства.



16.1 - Появится сообщение, подтверждающее установку FQDN. Нажмите OK, чтобы закрыть его.

17 - Bastion сгенерирует модули и веб-GUI на основе только что настроенных вами элементов. Появится сообщение с индикатором выполнения, как на изображении ниже:

После завершения генерации модулей указанное выше сообщение с индикатором выполнения закроется, и появится следующий экран, напоминающий вам, где найти руководство по продукту и получить доступ к веб-интерфейсу.

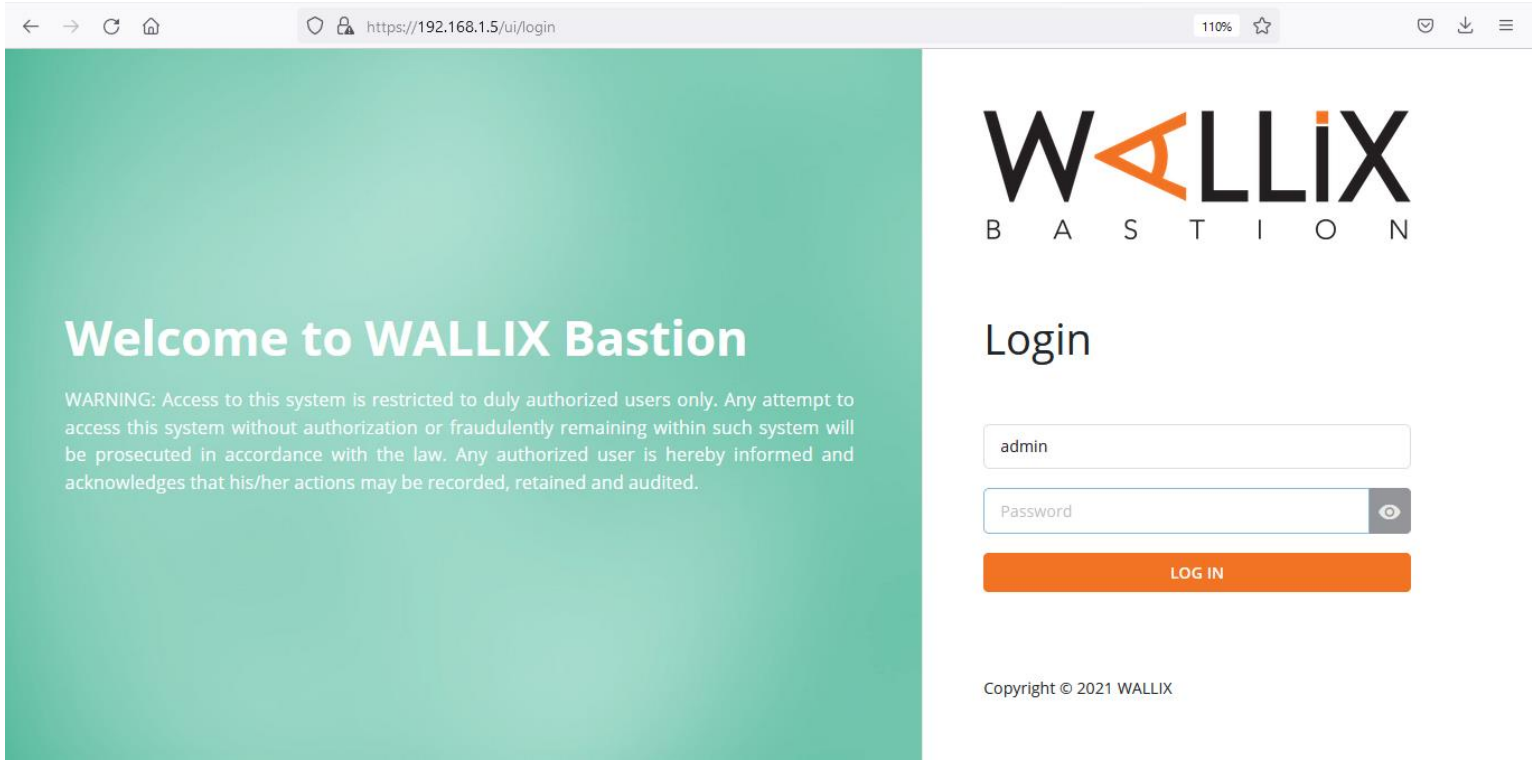


WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

Начальная конфигурация для пользователя-администратора Bastion:

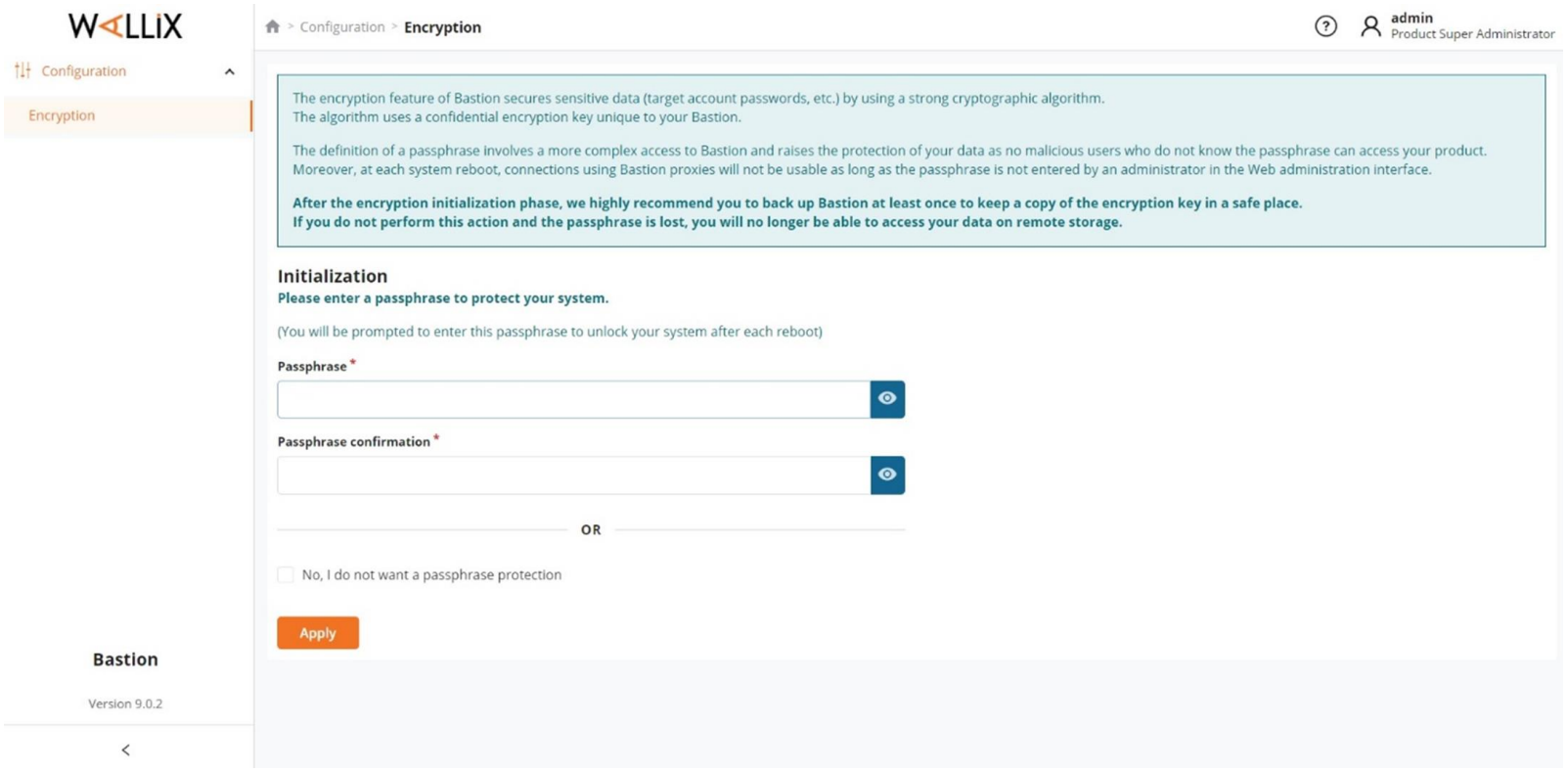
Откройте панель браузера по адресу https://192.168.1.5/ui/login, затем войдите в систему как администратор, используя следующие учетные данные по умолчанию:

- Имя пользователя: admin
- Пароль: admin



WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

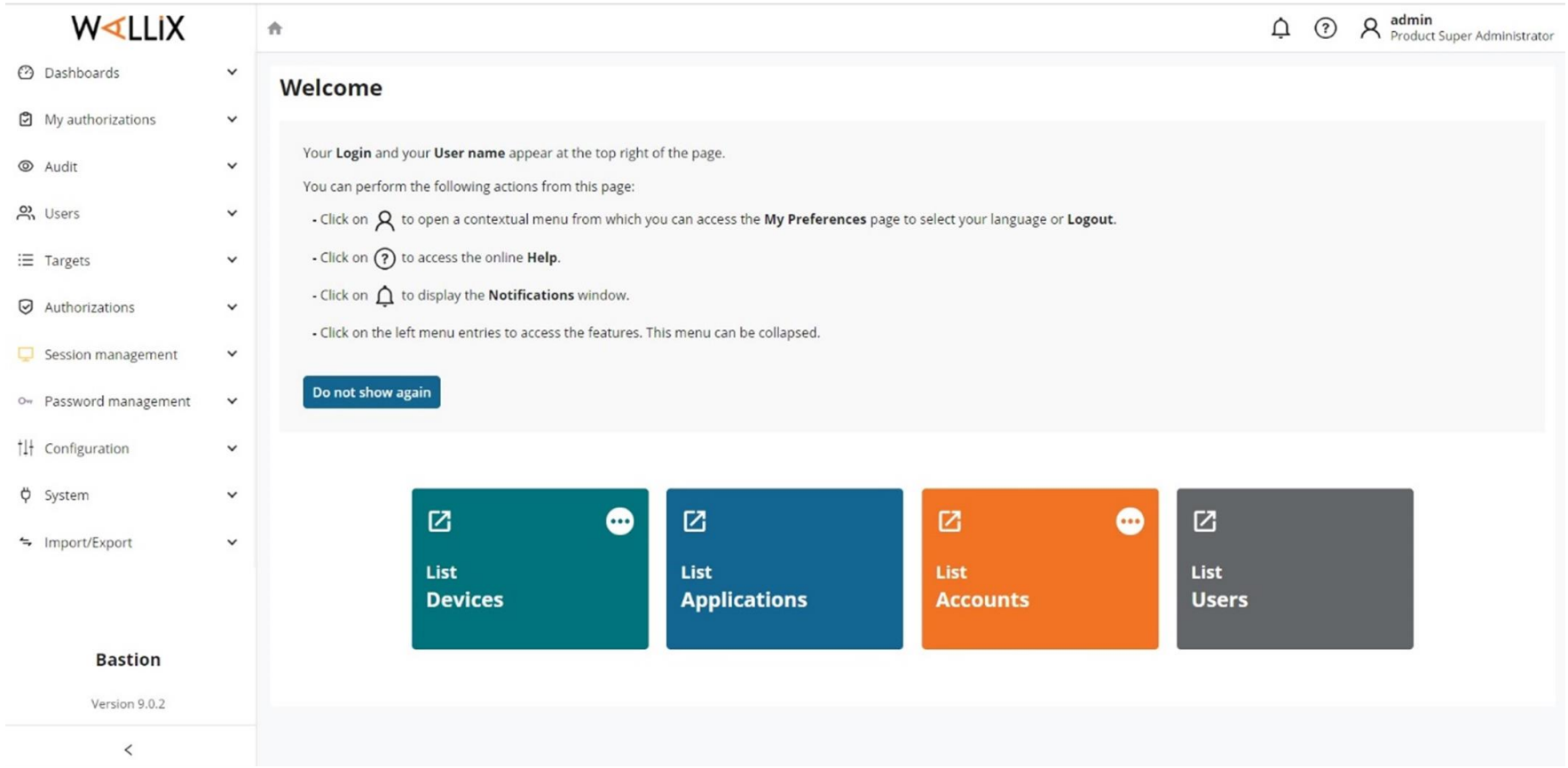
•Введите **парольную фразу** для защиты системы и нажмите «Применить», затем нажмите «Да», чтобы подтвердить использование этой парольной фразы.



Появится предупреждающее сообщение (см. изображение ниже) о том, что если пароль утерян/забыт, то система будет недоступна, если только ключ шифрования не сохранен в надежном месте.

WALLIX BASTION: НАСТРОЙКА АУТЕНТИФИКАЦИИ LDAP С ПОМОЩЬЮ ВЕБ-ИНТЕРФЕЙСА WALLIX BASTION

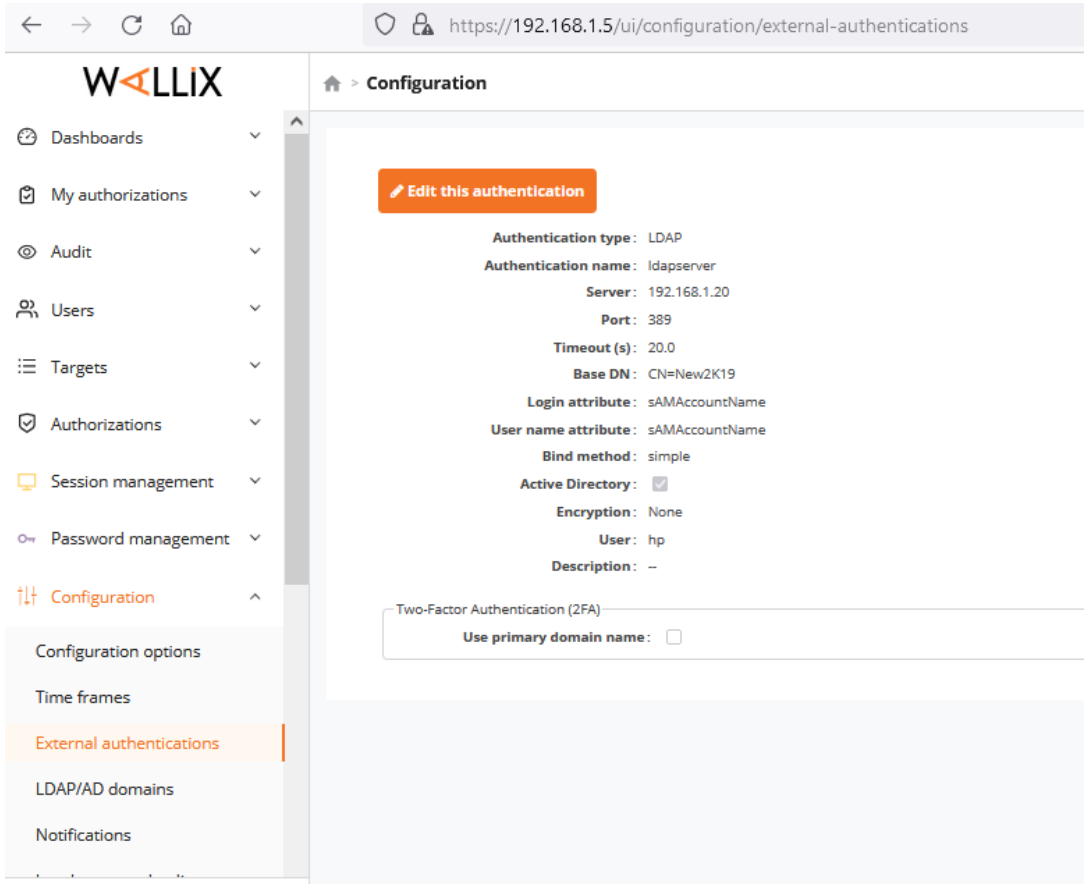
После успешного сохранения парольной фразы, созданной администратором Bastion, отобразится следующий экран:



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

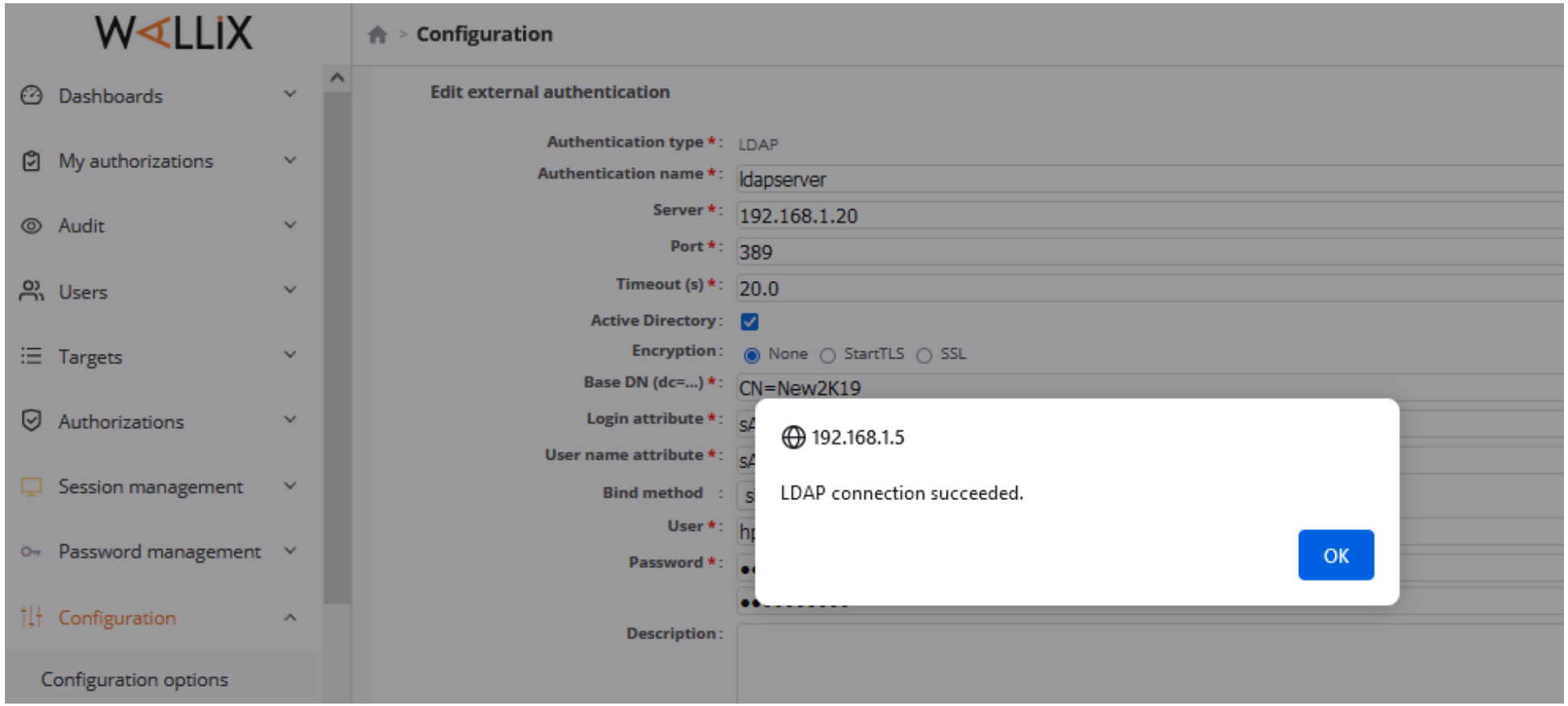
1 - Перейдите в раздел Конфигурация -> Внешние аутентификации и добавьте новую аутентификацию LDAP для нашего сервера LDAP (например, «ldapserver»), используя информацию о сервере SDIdP ниже:

•Сервер IdP: 192.168.1.20
•LDAP-порт 389
•Метод привязки: используйте «простой» или «анонимный»
•Включите опцию «Active Directory» (ПРИМЕЧАНИЕ: в настоящее время пользователь MagicEndpoint не будет работать при отключении этой опции)



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

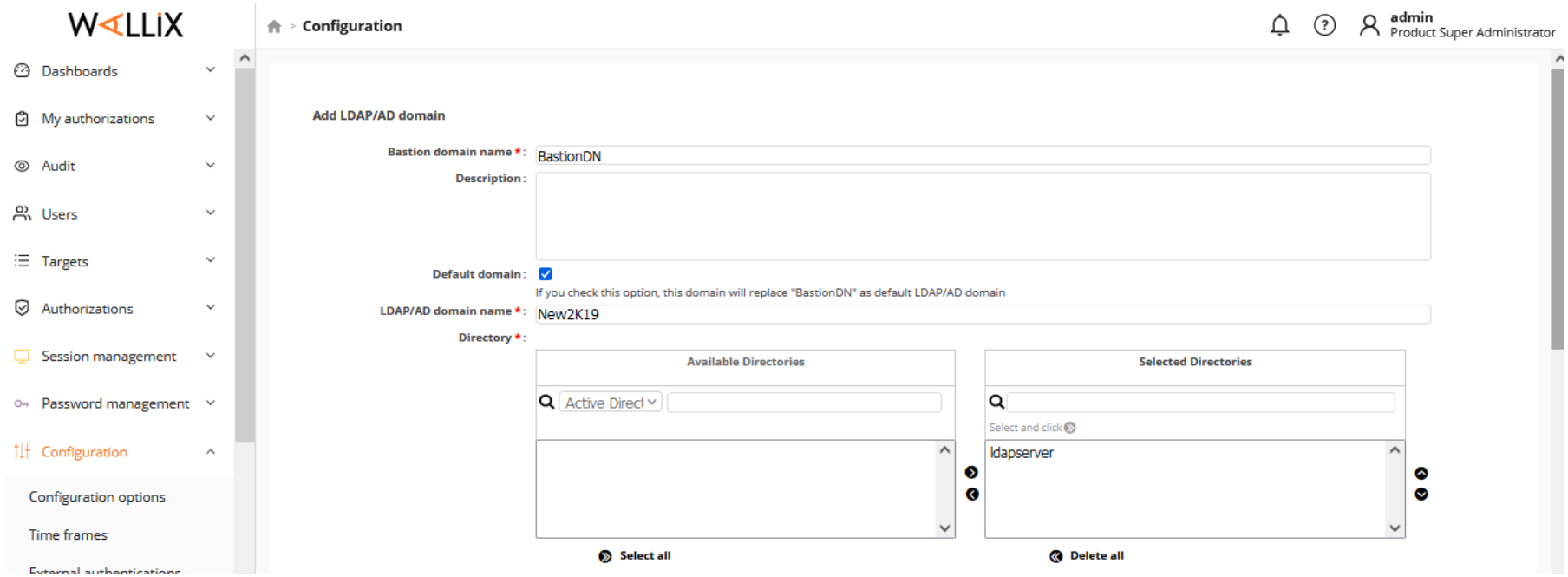
Проверьте соединение LDAP, чтобы убедиться, что Bastion может успешно получить доступ к серверу SDIdP, как показано на рисунке ниже:



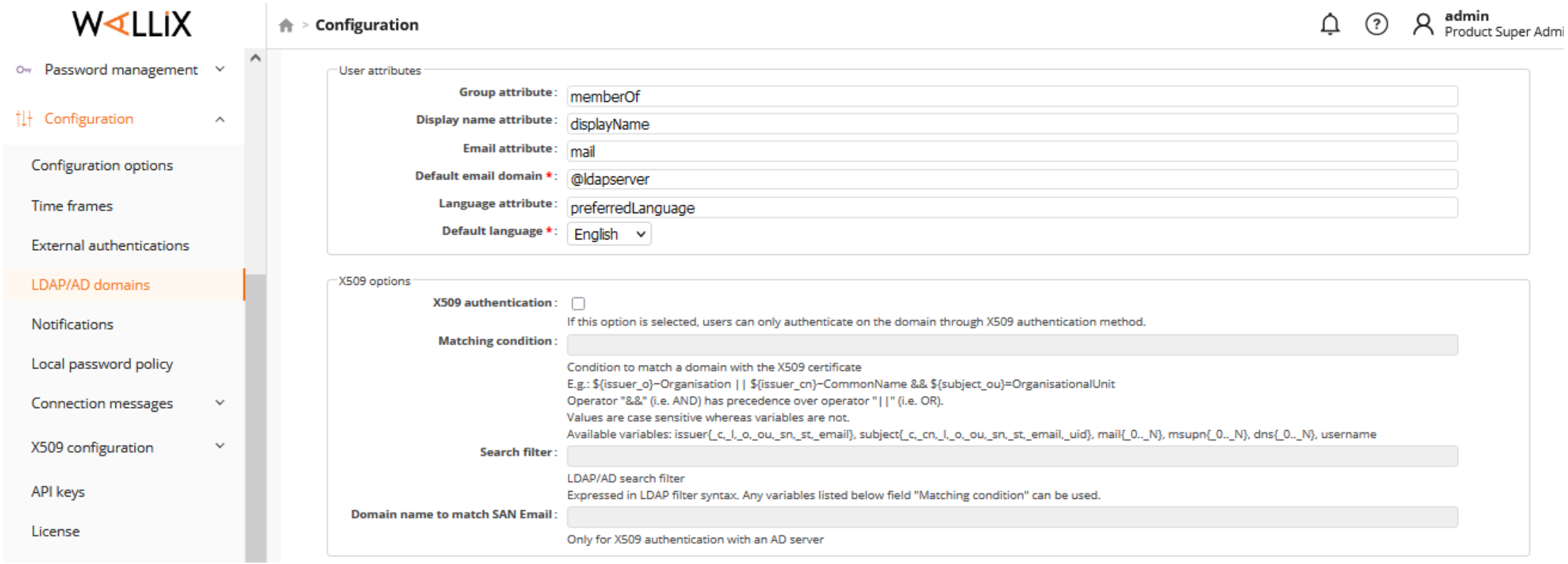
WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

Создайте домен LDAP/AD:

1 - В меню «Конфигурация > Домены LDAP/AD» нажмите «Добавить домен».
2 - В разделе «Доступный каталог» выберите указанное выше имя внешней аутентификации LDAP (например, «ldapserver») и используйте настройки по умолчанию для атрибутов пользователя / параметров X509.



WALLIX BASTION: НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

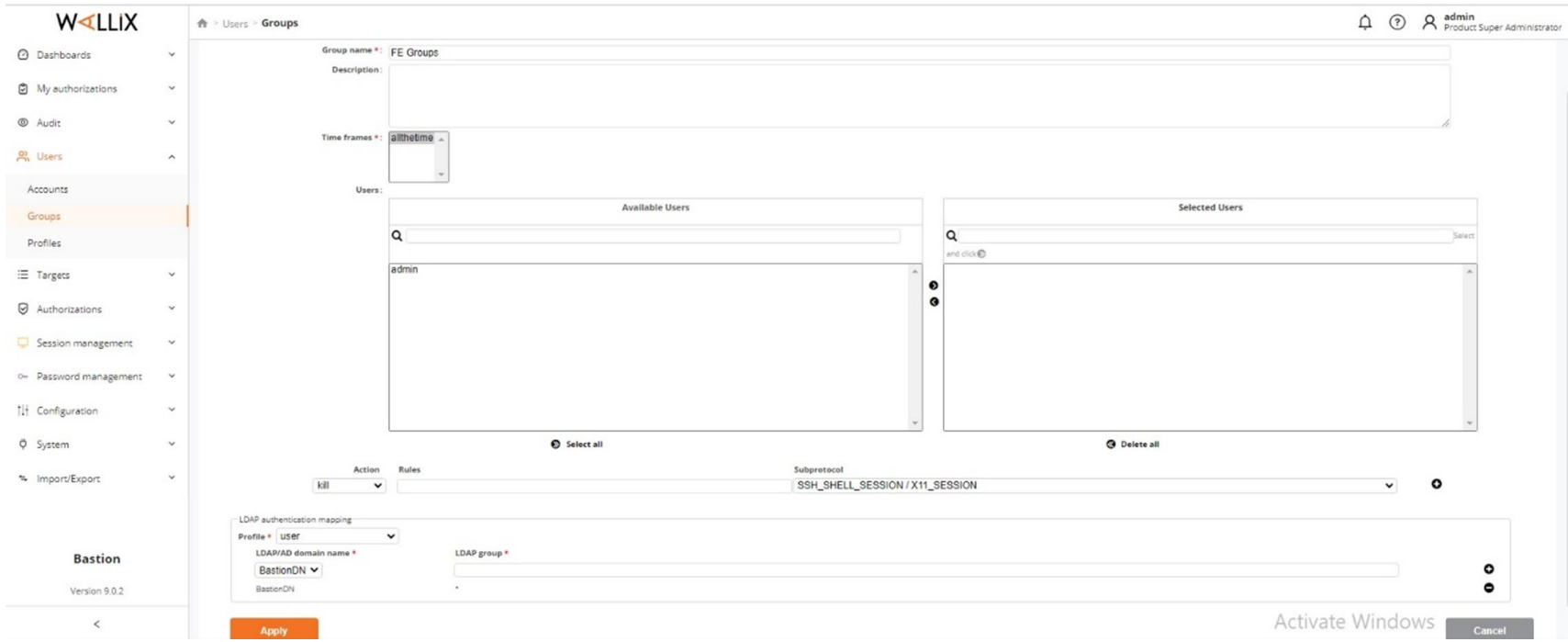


WALLIX BASTION:НАСТРОЙТЕ СЕРВЕР SDIDP LDAP В WALLIX BASTION

Создайте группу пользователей:

•В меню Пользователи -> Группы нажмите «Добавить группу» (например, «Группы FE»).

•Добавьте доменное имя Bastion «BastionDN» в LDAP/Domain выше (не добавляйте пользователей Bastion в эту группу)



Спасибо за внимание!