Настройка двухфакторной аутентификации

Введение

Двухфакторная аутентификация (2FA) является важным компонентом обеспечения безопасности. Она добавляет дополнительный уровень защиты, требуя от пользователей предоставления двух различных факторов для подтверждения своей личности. В операционной системе НАЙС ОС можно настроить двухфакторную аутентификацию с использованием различных методов, включая TOTP (Time-based One-Time Password) и аппаратные токены. В этой документации мы рассмотрим процесс настройки двухфакторной аутентификации с использованием Google Authenticator и других инструментов.

Установка необходимых пакетов

Для настройки двухфакторной аутентификации в НАЙС ОС необходимо установить пакет `google-authenticator` и настроить PAM (Pluggable Authentication Modules).

Установка Google Authenticator

Установите пакет `google-authenticator` с помощью `dnf`:

```
sudo dnf install google-authenticator
```

Настройка PAM

Для интеграции Google Authenticator с системой необходимо настроить PAM. Откройте файл `/etc/pam.d/sshd` для редактирования:

```
sudo nano /etc/pam.d/sshd
```

Добавьте следующую строку в начало файла:

```
auth required pam_google_authenticator.so
```

Настройка SSH для двухфакторной аутентификации

Для настройки SSH на использование двухфакторной аутентификации необходимо изменить конфигурационный файл `sshd_config`.

Редактирование конфигурационного файла SSH

Откройте файл `/etc/ssh/sshd_config` для редактирования:

```
sudo nano /etc/ssh/sshd_config
```

Убедитесь, что следующие строки включены и настроены правильно:

```
ChallengeResponseAuthentication yes
AuthenticationMethods publickey,keyboard-interactive
```

Перезапуск службы SSH

Для применения изменений перезапустите службу SSH:

```
sudo systemctl restart sshd
```

Настройка пользователя для двухфакторной аутентификации

Каждому пользователю, для которого необходимо включить двухфакторную аутентификацию, нужно пройти процесс настройки Google Authenticator.

Запуск Google Authenticator для пользователя

Выполните команду `google-authenticator` от имени пользователя, для которого настраивается двухфакторная аутентификация:

```
google-authenticator
```

Следуйте инструкциям на экране для генерации секретного ключа, QR-кода и резервных кодов. Рекомендуется сохранить резервные коды в безопасном месте.

Настройка TOTP-клиента на мобильном устройстве

Для генерации одноразовых паролей (TOTP) на мобильном устройстве можно использовать приложения, такие как Google Authenticator, Authy или Microsoft Authenticator.

Сканирование QR-кода

Откройте приложение TOTP на мобильном устройстве и отсканируйте QR-код, отображаемый при настройке Google Authenticator на сервере. Это добавит учетную запись и начнет генерировать одноразовые пароли.

Проверка работы двухфакторной аутентификации

После настройки TOTP-клиента попробуйте выполнить вход на сервер с использованием SSH. После ввода пароля будет запрошен одноразовый пароль, сгенерированный TOTP-клиентом.

Настройка двухфакторной аутентификации для sudo

Для дополнительной безопасности можно настроить двухфакторную аутентификацию для команд, выполняемых с помощью sudo.

Редактирование конфигурационного файла sudo

Откройте файл `/etc/pam.d/sudo` для редактирования:

```
sudo nano /etc/pam.d/sudo
```

Добавьте следующую строку в начало файла:

```
auth required pam_google_authenticator.so
```

Проверка работы двухфакторной аутентификации для sudo

Попробуйте выполнить команду с использованием sudo. После ввода пароля будет запрошен одноразовый пароль.

Настройка двухфакторной аутентификации с использованием аппаратных токенов

Помимо TOTP, можно использовать аппаратные токены, такие как YubiKey, для двухфакторной аутентификации. Рассмотрим настройку YubiKey для использования с НАЙС ОС.

Установка пакетов для работы с YubiKey

Установите необходимые пакеты для работы с YubiKey:

```
sudo dnf install ykclient ykpers pam_yubico
```

Настройка PAM для использования YubiKey

Откройте файл `/etc/pam.d/sshd` для редактирования:

```
sudo nano /etc/pam.d/sshd
```

Добавьте следующую строку в начало файла:

```
auth required pam_yubico.so id=your_yubico_client_id key=your_yubico_secret_key
```

Получите `client_id` и `secret_key` для вашего YubiKey на сайте Yubico.

Перезапуск службы SSH

Для применения изменений перезапустите службу SSH:

```
sudo systemctl restart sshd
```

Настройка двухфакторной аутентификации с использованием Duo

Duo Security предоставляет удобный и надежный способ реализации двухфакторной аутентификации с использованием мобильных устройств. Рассмотрим настройку Duo для НАЙС ОС.

Установка Duo

Для установки Duo необходимо скачать и установить клиентские библиотеки Duo:

```
sudo dnf install duo_unix
```

Настройка Duo

Откройте файл `/etc/duo/login_duo.conf` для редактирования:

```
sudo nano /etc/duo/login_duo.conf
```

Добавьте следующие строки, заменив значения на ваши Duo integration key, secret key и API hostname:

```
[duo]
ikey = your_integration_key
skey = your_secret_key
```

```
host = your_api_hostname
```

Настройка PAM для использования Duo

Откройте файл `/etc/pam.d/sshd` для редактирования:

```
sudo nano /etc/pam.d/sshd
```

Добавьте следующую строку в начало файла:

```
auth required pam_duo.so
```

Перезапуск службы SSH

Для применения изменений перезапустите службу SSH:

```
sudo systemctl restart sshd
```

Мониторинг и управление двухфакторной аутентификацией

Для эффективного управления двухфакторной аутентификацией важно регулярно проверять журналы и следить за попытками аутентификации.

Просмотр журналов аутентификации

Для просмотра журналов аутентификации используйте команду `tail`:

```
sudo tail -f /var/log/auth.log
```

Управление пользователями и настройками 2FA

При необходимости вы можете обновить настройки двухфакторной аутентификации для пользователей, запустив `google-authenticator` от имени соответствующего пользователя и следуя инструкциям.

Заключение

Настройка двухфакторной аутентификации в НАЙС ОС значительно повышает уровень безопасности системы, добавляя дополнительный слой защиты. Используя различные методы, такие как TOTP, аппаратные токены и Duo Security, вы можете эффективно защитить свою систему от несанкционированного доступа. Следуя приведенным инструкциям, вы сможете

настроить двухфакторную аутентификацию и обеспечить надежную защиту вашей системы.