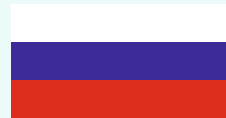
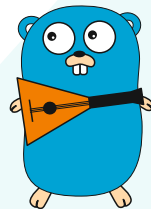


PowerC



Сделано в России
Не зависит от
сторонних библиотек

PowerMF

Двухфакторная аутентификация пользователей
на VPN шлюзах
предварительное краткое описание

Краткое описание

Если ваша компания использует какие-либо сервисы доступные через Internet, такие как VPN, то в случае утечки учетных записей пользователей, которые эти сервисы используют, велик риск проникновения злоумышленника в ваши внутренние ресурсы. Для минимизации рисков часто используется довольно простая идея - для идентификации пользователя недостаточно только учетной записи и пароля или даже сертификата, необходим еще какой-то фактор того, что вы это вы. Можно использовать биометрию, программные или аппаратные устройства генерации одноразовых паролей, а также доставку временных одноразовых паролей через SMS или электронную почту. Временные одноразовые пароли широко используются банками для подтверждения оплаты по карте и с ними все хорошо знакомы. Существует множество программных продуктов как облачных, так и локальных, позволяющих реализовать двухфакторную аутентификацию. Однако они либо достаточно сложны для небольших компаний, либо дороги.

Мы создали продукт, который очень легко настраивать, и он хоть и не является бесплатным, но доступен для любой компании.

Ключевые отличия нашего продукта:

Управление параметрами пользователя осуществляется полностью в Active Directory (либо любой другой службе каталогов) посредством задания атрибутов и членства в группах.

Отсутствие интерфейса управления как такового ввиду настройки параметров пользователей непосредственно в каталоге (AD или похожие)

Информацию об аутентификации, статистику, информацию об ошибках можно отправить в Syslog или SIEM.

То есть сам по себе сервис не требует какого-либо внимания со стороны администраторов в течении его нормальной работы.

Работа сервиса:

Сервис получает по протоколу **RADIUS** запрос на аутентификацию пользователя.

Производится поиск пользователя в **Active Directory**

в случае успеха, проверяется его членство в группе, разрешающей подключение по **VPN** (параметр **otp_group** в секции **ldap_setting** файла **settings.json**) если пользователь является членом этой группы, проверяются атрибуты:

Мобильный телефон (**mobile**)

Электронная почта (**mail**)

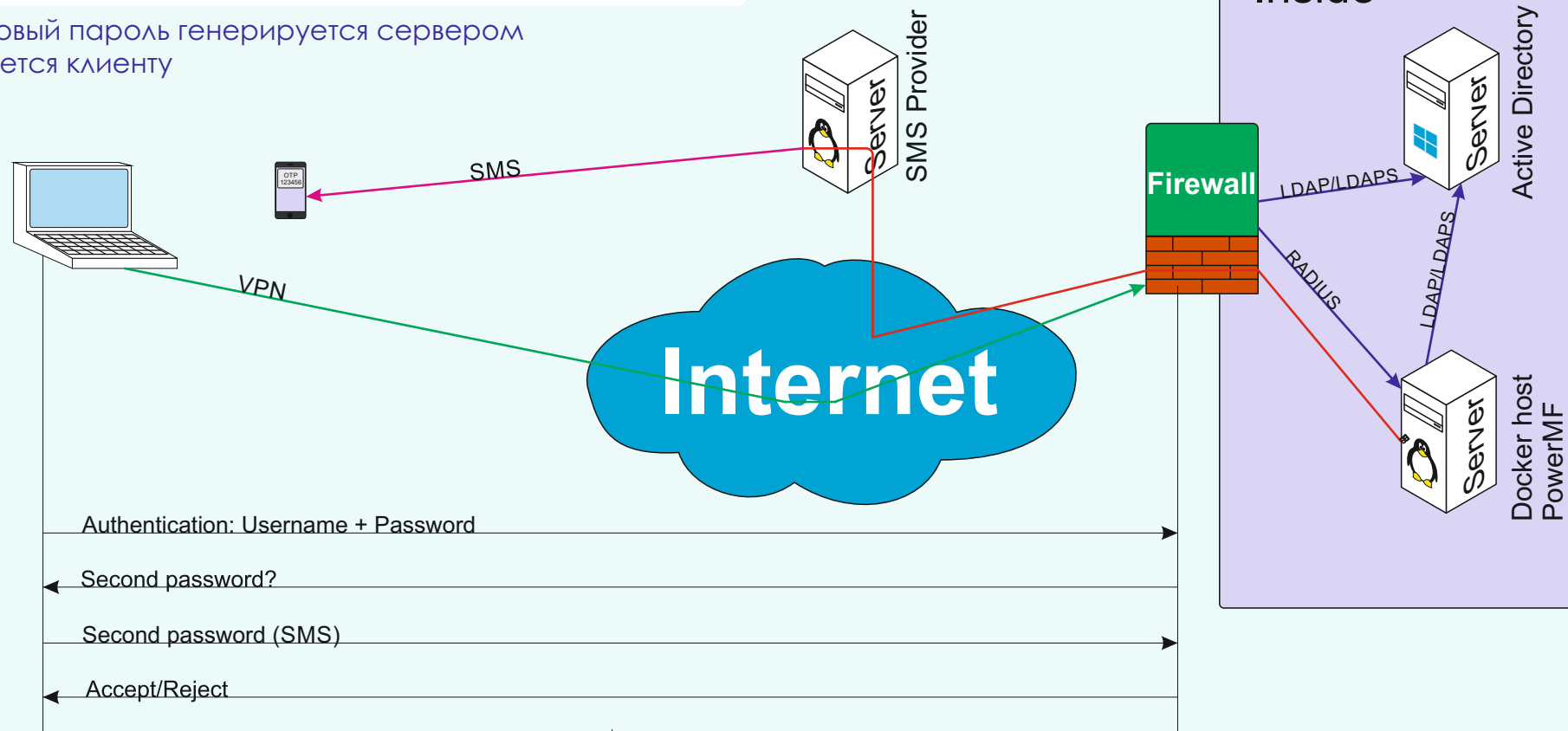
А также Заметки на вкладке телефоны (**info**)

В поле Заметки можно указать предпочитаемый метод доставки одноразового пароля, либо otpmail либо otpsms. Так же тут хранится зашифрованный секретный ключ для генераторов TOTP

если в этом поле уже имеется текст, укажите метод доставки в конце текста, отделив его запятой или пробелом.

Схема работы SMS

Одноразовый пароль генерируется сервером и посылается клиенту



Преимущества

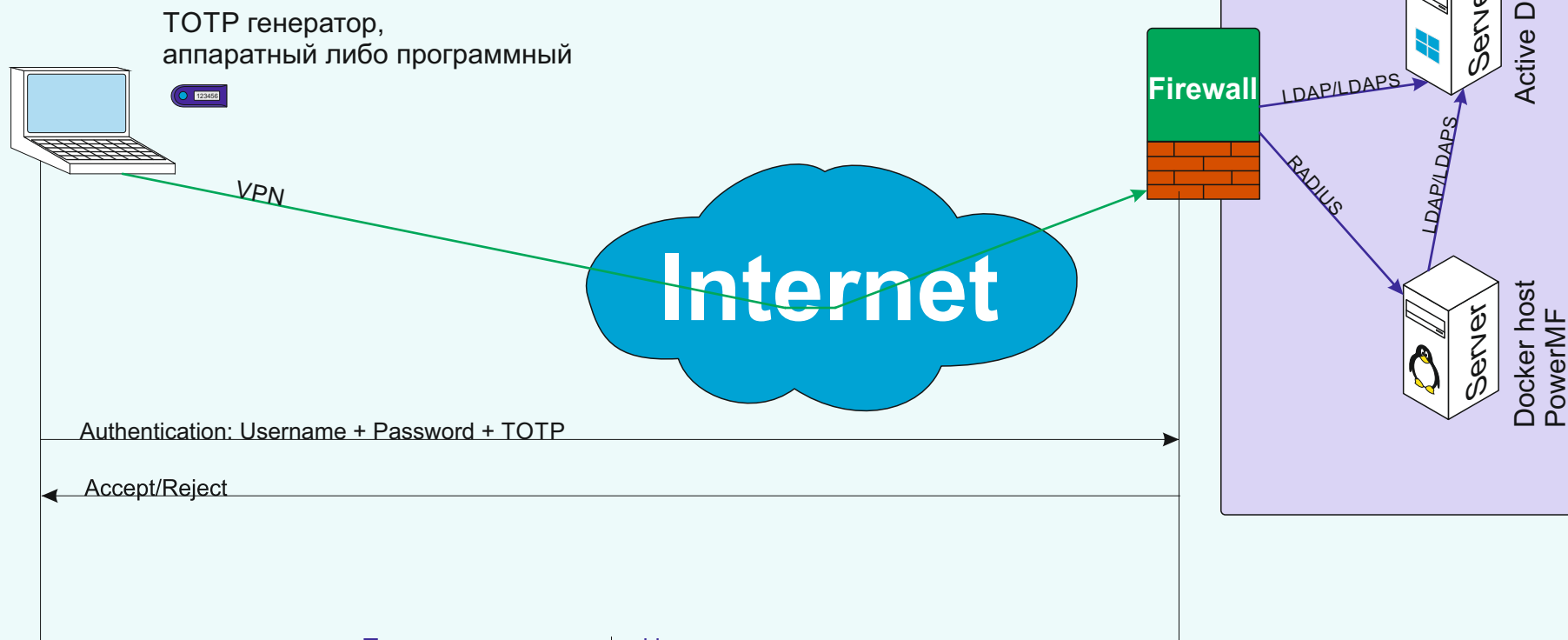
Не требуется токен
не требуется передача секретного ключа клиенту

Недостатки

Для получения SMS необходимо наличие сотовой связи
Для получения письма по e-mail необходим доступ к почтовому ящику

Схема работы TOTP

Одноразовый пароль генерируется клиентом и сервером на основе секретного ключа и времени



Преимущества

- Не требуется наличие сотовой связи или доступ к почтовому ящику
- Нет необходимости ждать прихода одноразового пароля
- В случае аппаратного токена выше безопасность

Недостатки

- В случае использования программных токенов или аппаратных программируемых токенов необходимо безопасно передать секретный ключ клиенту

Cisco ASA

Настройки на Cisco ASA, пример (192.168.0.5 IP адрес сервера, где запущен сервис а 192.168.0.2 IP адрес контроллера домена)
В примере производится первичная аутентификация в Active Directory а вторичная отправит пользователю одноразовый пароль и после его ввода проверит его валидность и либо разрешит подключение либо отклонит.

```
laaa-server ADLDAP protocol ldap
aaa-server ADLDAP (inside) host 192.168.0.2
server-port 389
ldap-base-dn dc=EXAMPLE, dc=LOCAL
ldap-scope subtree
ldap-naming-attribute sAMAccountName
ldap-login-password TestPass123
ldap-login-dn cn=ASA, cn=Users, dc=EXAMPLE, dc=LOCAL
server-type microsoft

aaa-server RDTEST protocol radius
aaa-server RDTEST (inside) host 192.168.0.5
key radiuskeytest123
authentication-port 1812

tunnel-group TWTEST type remote-access
tunnel-group TWTEST general-attributes
authentication-server-group ADLDAP
secondary-authentication-server-group RDTEST use-primary-username
```

Active Directory

Пример разрешения пользователю UserVPN получать одноразовые пароли.

В примере группа VPN-TW группа членом которой разрешается подключаться по VPN с одноразовыми паролями

В поле «заметки» указан способ доставки одноразового пароля, а также зашифрованный секретный ключ для TOTP генераторов аппаратных или программных (FreeOTP, Google Authenticator) которые используют SHA1-HMAC

Свойства: UserVPN

Общие	Адрес	Учетная запись	Профиль	Телефоны	Организация
Входящие звонки	Объект	Безопасность	Среда	Сеансы	

Удаленное управление

Профиль служб удаленных рабочих столов | COM+ | Редактор атрибутов

Опубликованные сертификаты | Член групп | Репликация паролей

Член групп:

Имя: Папка доменных служб Active Directory

VPN-TW EXAMPLE.LOCAL/Users

Добавить Удалить

Основная группа: Пользователи домена

Задать основную группу

Нет необходимости изменять основную группу, если только не используются клиенты Macintosh или POSIX совместимые приложения.

OK Отмена Применить Справка

Свойства: UserVPN

Опубликованные сертификаты	Член групп	Репликация паролей
Входящие звонки	Объект	Безопасность
Среда	Сеансы	

Удаленное управление

Профиль служб удаленных рабочих столов | COM+ | Редактор атрибутов

Общие | Адрес | Учетная запись | Профиль | Телефоны | Организация

Телефонные номера

Другой... Другой...

пейджер Другой...

Мобильный 8XXXXXXXXXX Другой...

Факс Другой...

IP-Телефон Другой...

Заметки:

otpsms,
secretkey_UvbX5Cmr2uUVRc9DoBfj7VgZBtNUiu5ejmJhxbv
3iVmvicgyOK90my1jm4hGUiaj

OK Отмена Применить Справка

Свойства: UserVPN

Опубликованные сертификаты	Член групп	Репликация паролей
Входящие звонки	Объект	Безопасность
Среда	Сеансы	

Удаленное управление

Профиль служб удаленных рабочих столов | COM+ | Редактор атрибутов

Общие | Адрес | Учетная запись | Профиль | Телефоны | Организация

Имя: UserVPN Инициалы:

Фамилия:

Выводимое имя: UserVPN

Описание:

Комната:

Номер телефона: Другой...

Эл. почта: uservpn@example.com

Веб страница: Другой...

OK Отмена Применить Справка

Настройка PowerMF

Параметры в файле settings.json

Секция **ldap_setting**:

fqdn: FQDN или IP адрес контроллера домена.
ldap_port: LDAP порт
base_dn: узел в дереве откуда начинать поиск пользователей
bind_username_upn: имя пользователя от имени которого будет производиться обращение по LDAP к контроллеру в формате UPN (username@domain)
bind_password: пароль пользователя
otp_group: имя группы, членам которой разрешен доступ в VPN (в формате CN=<Группа>,CN=<контейнер>.....,DC=<домен>,DC=local)

Секция **radius_setting**

shared_secret: секретный ключ
port: порт (обычно 1812)
address: адрес на котором слушать Radius дейтаграммы (можно оставить пустым)

Секция **otp_params**:

valid_interval: интервал в течении которого временный пароль действителен
otp_len: количество цифр в одноразовом пароле
otp_key_encrypt: общий ключ который будет использоваться для дешифровки секретного ключа **TOTP** из параметров **LDAP**

Секция **smtp_params**:

mail_from: пользователь, от которого будет производиться отправка письма
mail_from_name: от кого отправляем почту
smtpserver: IP или FQDN адрес SMTP сервера
SMTPPort: порт SMTP сервера
subject: тема в письме
message: текст помимо пароля
smtp_password: пароль на SMTP соединение

Секция **sms_params**:

smsurl: URL шлюза SMS - сейчас возможен только Инплат - "https://pay.inplat.ru/smsc/send_sms?msisdn"
smscert: сертификат по которому авторизуется клиент
smskey: закрытый ключ
smsca: корневой сертификат - не обязателен
checkidentity: 1 - если проверять валидность сертификата сервера и 0 если не проверять
message: текст помимо пароля

Секция **syslog_params**:

address: адрес Syslog сервера
port: порт Syslog сервера (обычно 514)

Настройка PowerMF

Пример настройки сервиса.

В данном примере отправка почты производится через внутренний SMTP сервер без авторизации

```
{
  "ldap_setting":{
    "fqdn": "dc01.example.local",
    "ldap_port": 389,
    "base_dn": "dc=example,dc=local",
    "bind_username_upn": "potp@example.local",
    "bind_password": "TestPass123%",
    "otp_group": "CN=ADM-VPN,CN=Users,DC=EXAMPLE,DC=LOCAL"
  },
  "radius_setting":{
    "shared_secret":"Test327A",
    "port": 1814,
    "address": ""
  },
  "syslog_params":{
    "address": "192.168.0.187",
    "port": 51
  },
  "otp_params":{
    "valid_interval": 29,
    "otp_len": 4,
    "otp_key_encrypt": "Secret123"
  },
  "smtp_params":{
    "mail_from": "testmail@aotptest.net",
    "mail_from_name": "LArañaOTP",
    "smtpserver": "192.168.0.187",
    "SMTPPort": 25,
    "subject": "Your OTP",
    "message": "OTP valid until 29 sec",
    "smtp_password": ""
  },
  "sms_inplat_params":{
    "smsurl": "https://pay.inplat.ru/smsc/send_sms?msisdn",
    "smscert": "demo.crt",
    "smskey": "demo.key",
    "smsca": "",
    "checkidentity": 1,
    "message": "OTP valid until 29 sec"
  }
}
```


Работа с TOTP

Для использования генераторов TOTP необходимо чтоб секретный ключ был известен обоим сторонам. Существуют аппаратные TOTP токены с запрограммированным на производстве ключом, и программируемые. Программные же в любом случае требуют ввода ключа. Как правило это можно сделать либо сканированием QR кода, либо вводом строки в формате Base32

Для безопасности мы храним в LDAP зашифрованный ключ в виде Base64 строки.

Если у вас уже есть ключ в формате Base32, вы можете его зашифровать при помощи утилиты encryptkey. Она принимает следующие параметры:

- p пароль шифрования который указан в settings.json ("otp_key_encrypt":)
- k секретный ключ в формате Base32
- n если секретный ключ нужно сгенерировать (тогда параметр -k указывать не надо)
- qr имя файла с QR кодом (указать без расширения, будет создан PNG файл)

Если же его необходимо создать, то вы можете воспользоваться этой же утилитой, но с параметром -n а так же можно создать QR код в виде png файла и, например отправить его почтой.

Примеры работы с утилитой показаны ниже:

```
encryptkey.exe -p secret1 -n -qr testuser
Encrypted secret key for LDAP info:
secretkey_UvbX5Cmr2uUVRc9DoBfj7VgZBtNUiu5ejmJhxvb3iVmvicgyOK90my1jm4hGUiaj
Secret key in Base32 format: I6BRAZTMGU4BJSVDAWV2KMASEUJWWHJJ
QR code saved in: C:\Users\Tuser\Tools\anyuser.png
```

Roadmap

Данное программное обеспечение создавалось с целью сделать более безопасным удаленную работу сотрудникам небольших компаний. Специфика рынка ИБ для небольших компаний налагает на продукт следующие требования:

1. невысокая цена
2. простота развертывания
3. простота использования

Поэтому мы отказались от сложного пользовательского интерфейса и от отказоустойчивых кластеров тем не менее косвенно обеспечив отказоустойчивость и простоту использования следующим образом:

1. Управление пользователями производится полностью в службе каталогов (Active Directory или подобной) привычными администратору инструментами
2. Отказоустойчивость обеспечивается использованием двух экземпляров ПО

Что касается развертывания то будут доступны следующие варианты:

1. Docker контейнер
2. Linux сервис (доступен уже сейчас)
3. Сервис для Microsoft Windows Server

Совсем небольшие компании могут использовать, например один домен контроллер и на нем запустить сервис PowerMF.

На данный момент реализован сервис по Linux и Docker контейнер.

В перспективе создание графической оболочки для генерации QR кода с секретным ключом

Больше информации

Россия, Санкт-Петербург
Таллинская 6-В
Телефон: +7 (812) 7034338
<http://www.powerc.ru>

info@powerc.ru

