PowerMF

Двухфакторная аутентификация пользователей
на VPN шлюзах, краткое описание

POWER live

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 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 службе каталогов

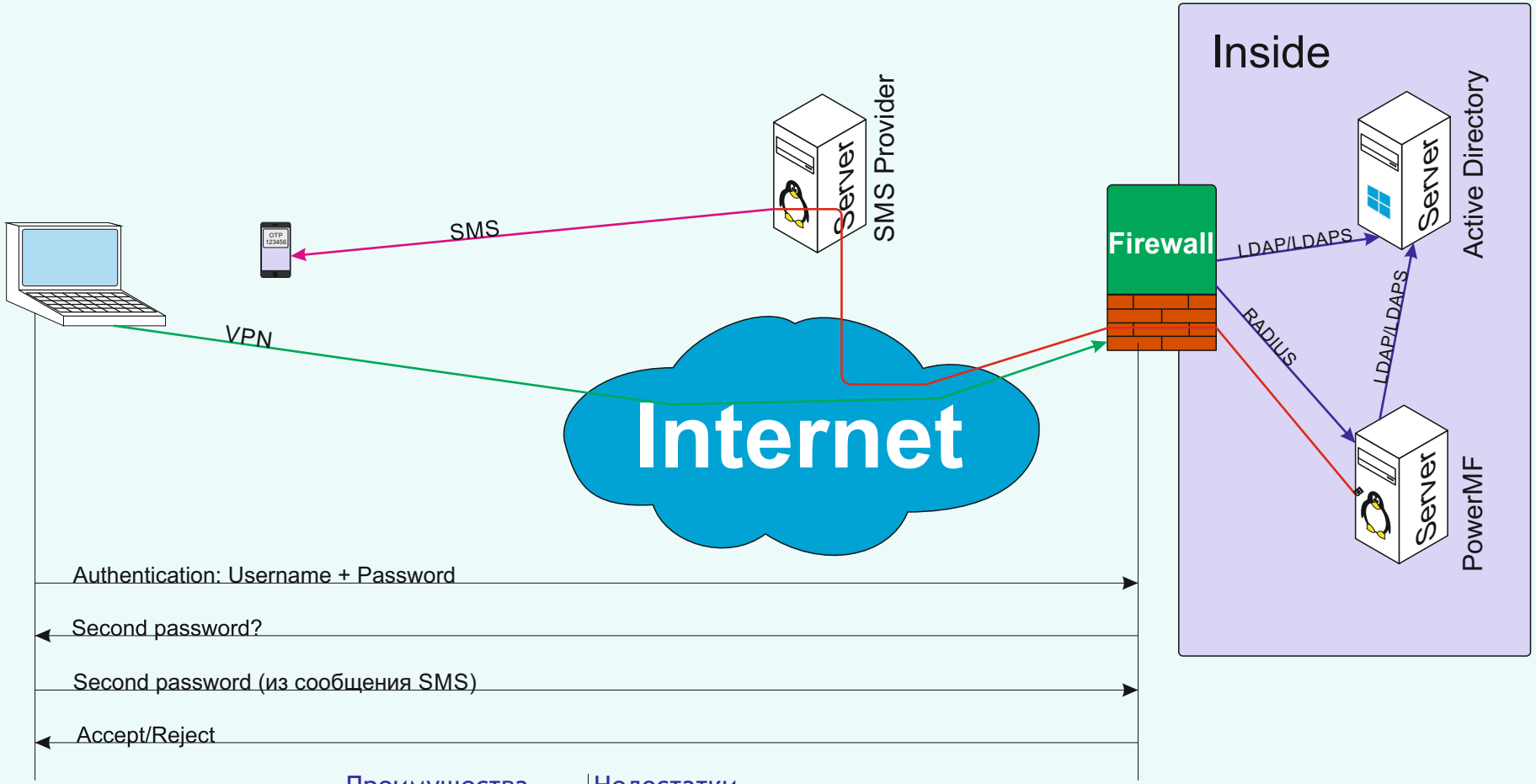
Информацию об аутентификации, статистику, информацию об ошибках можно отправить в Syslog или SIEM.

То есть сам по себе сервис не требует какого-либо внимания со стороны администраторов в течение 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, **otpmail** для отправки одноразового пароля по электронной почте, **otpsms** для отправки одноразового пароля по SMS или **otpwww** для отправки одноразового пароля по электронной почте на альтернативный почтовый ящик указанный в атрибуте **wWWHomePage** .
Так же тут хранится зашифрованный секретный ключ для генераторов TOTP, если в этом поле уже имеется текст, укажите метод доставки и если надо ключ, в конце текста, отделив его запятой или пробелом.
В случае если атрибут **mobile** пустой, то будет использоваться атрибут **telephoneNumber.**.

Схема работы при доставке кода через сервис SMS

Одноразовый пароль генерируется сервером
и посылается клиенту



Преимущества

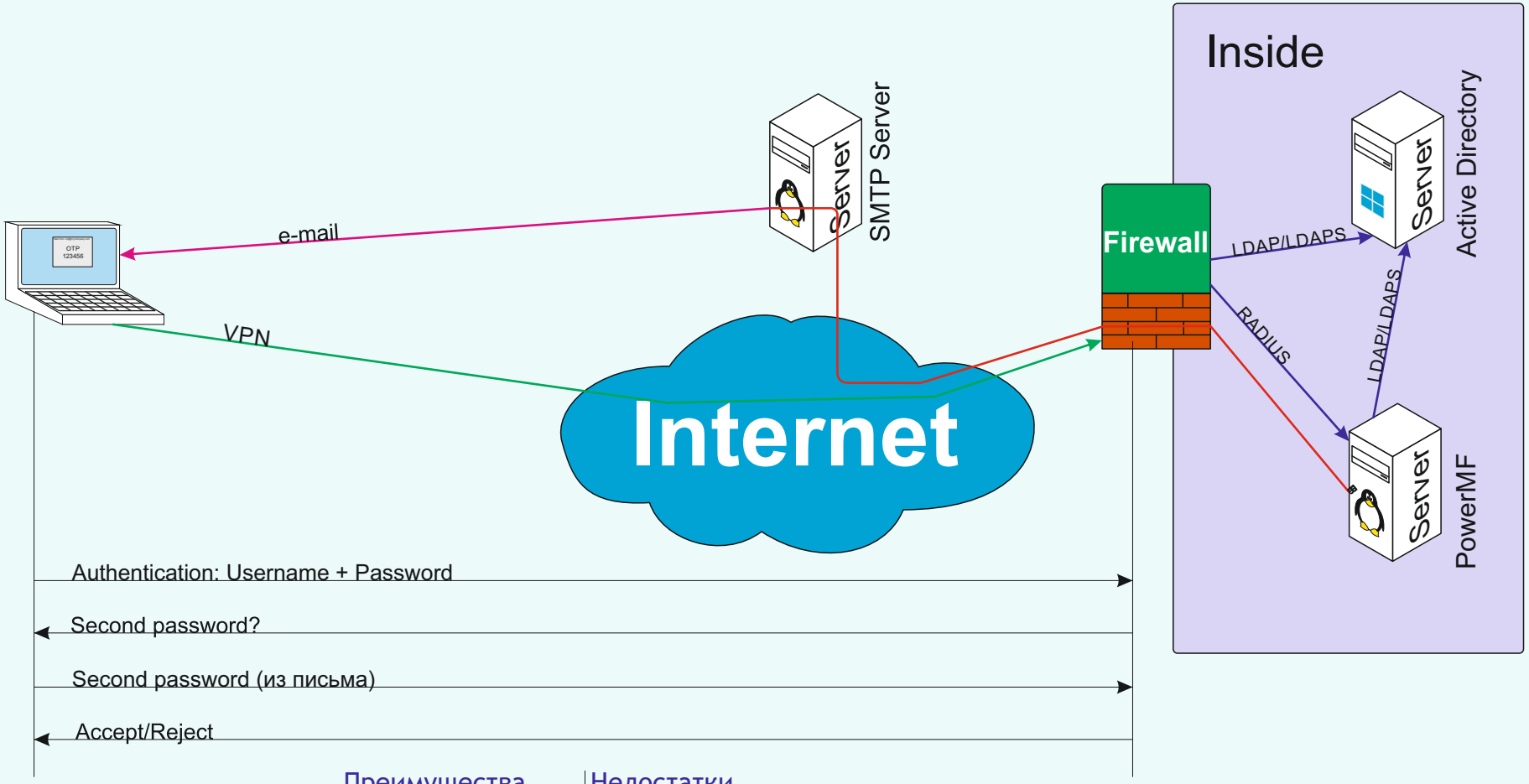
Не требуется токен
не требуется передача секретного ключа клиенту

Недостатки

Для получения SMS необходимо наличие сотовой связи
Услуги провайдера SMS не бесплатны

Схема работы при доставке кода по электронной почте

Одноразовый пароль генерируется сервером
и посылается клиенту



Преимущества

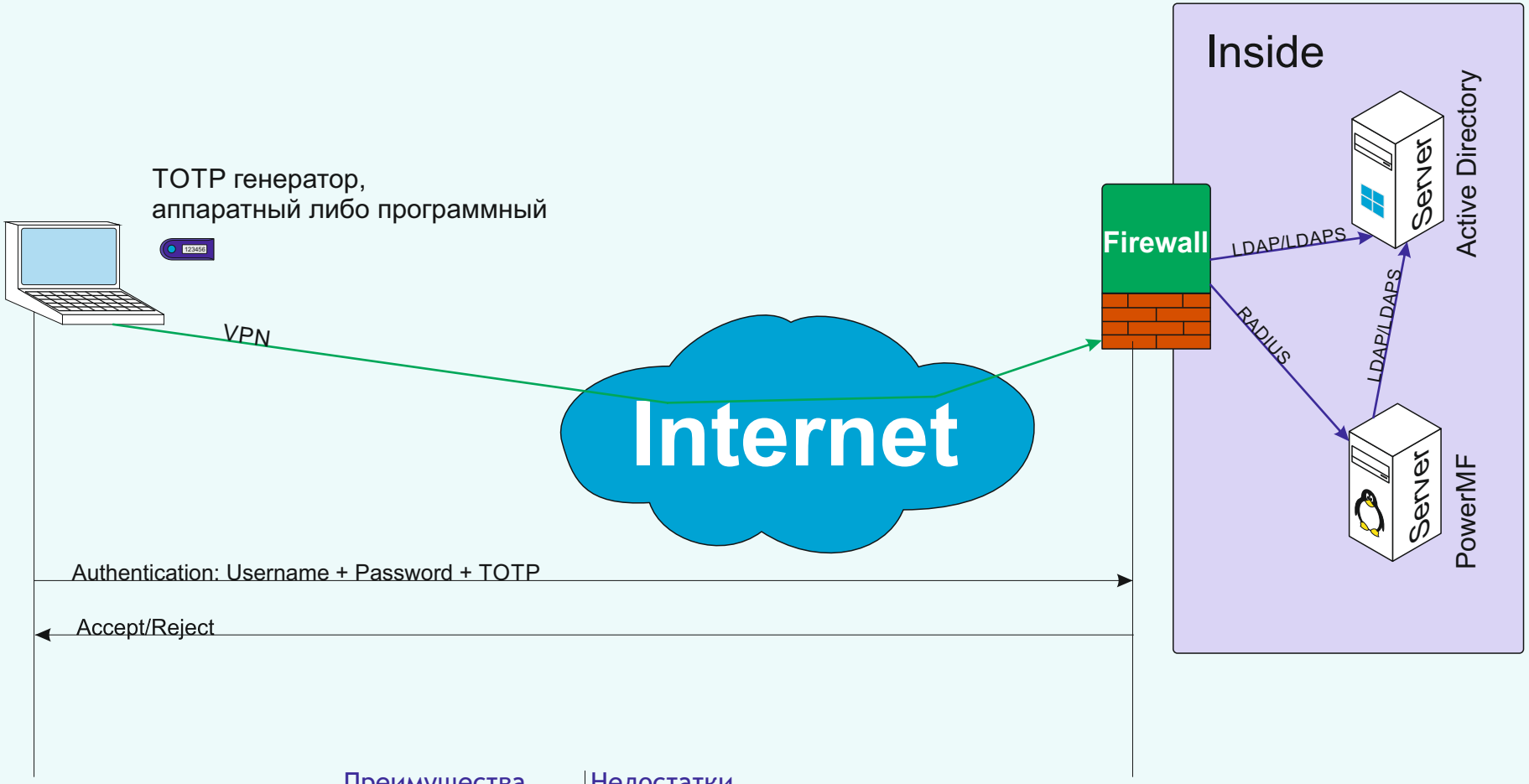
Не требуется токен
не требуется передача секретного ключа клиенту

Недостатки

Для получения письма по e-mail необходим доступ к почтовому ящику

Схема работы с использованием генератора кода 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 безопасноть

Недостатки

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

Работа с Active Directory

Все управление пользователями, производится через **Active Directory**

Для того чтобы пользователь мог подключаться, его необходимо сделать членом группы, указанной в конфигурационном файле (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, **otpmail** для отправки одноразового пароля по электронной почте, **otpsms** для отправки одноразового пароля по SMS или **otpwww** для отправки одноразового пароля по электронной почте на альтернативный почтовый ящик указанный в атрибуте **wWWHomePage**.

Так же тут может хранится зашифрованный секретный ключ для генераторов TOTP, если в этом поле уже имеется текст, укажите метод доставки и если надо ключ, в конце текста, отделив его запятой или пробелом.

В случае если атрибут **mobile** пустой, то будет использоваться атрибут **telephoneNumber.**
Так же, в случае если по каким то причинам, невозможно использовать выше указанные атрибуты, можно создать в схеме Active Directory дополнительные атрибуты и указать их в файле **settings.json** следующим образом:
a_phone_attr приоритетный атрибут с телефонным номером
a_mail_attr приоритетный атрибут с телефонным адресом электронной почты
a_method_attr приоритетный атрибут с методом отправки и зашифрованным секретным ключом для генерации TOTP.

Альтернативные атрибуты являются приоритетными.

В связи с тем что на VPN шлюзах **checkpoint** нет возможности разрешить какой то части пользователей подключаться без одноразового пароля, мы добавили возможность указать группу, члены которой могут вводить любой одноразовый пароль.
(параметр **otp_bypass_group** в секции **ldap_setting** файла **settings.json**).

Так же в некоторых случаях может быть удобно членами группы **otp_group** делать не непосредственно пользователей а другую группу, членами которой в свою очередь являются пользователи, в таком случае надо включить поиск по вложенным группам, установив параметр **nestedgroup** в **true**

Использование LDAP over SSL

Для работы со службой каталогов по протоколу LDAP over SSL, необходимо наличие действительного сертификата на сервере а также установленного корневого сертификата удостоверяющего центра, выдавшего сертификат для службы LDAP over SSL в доверенных корневых центрах сертификации, на сервере где выполняется PowerMF.
Так же в настройках PowerMF нужно указать FQDN LDAPS сервера в случае если сертификат не содержит альтернативного имени - IP адреса.

Далее рассмотрим работу с Active Directory а в качестве Linux OS на которой выполняется PowerMF считаем Red Hat и подобные OS
Добавим корневой сертификат нашего удостоверяющего центра в доверенные на Linux OS:

```
yum install ca-certificates
update-ca-trust force-enable
cp ourrootca.crt /etc/pki/ca-trust/source/anchors/
update-ca-trust extract
```

Посмотреть какой именно сертификат используется сервисом LDAP over SSL можно утилитой openssl:

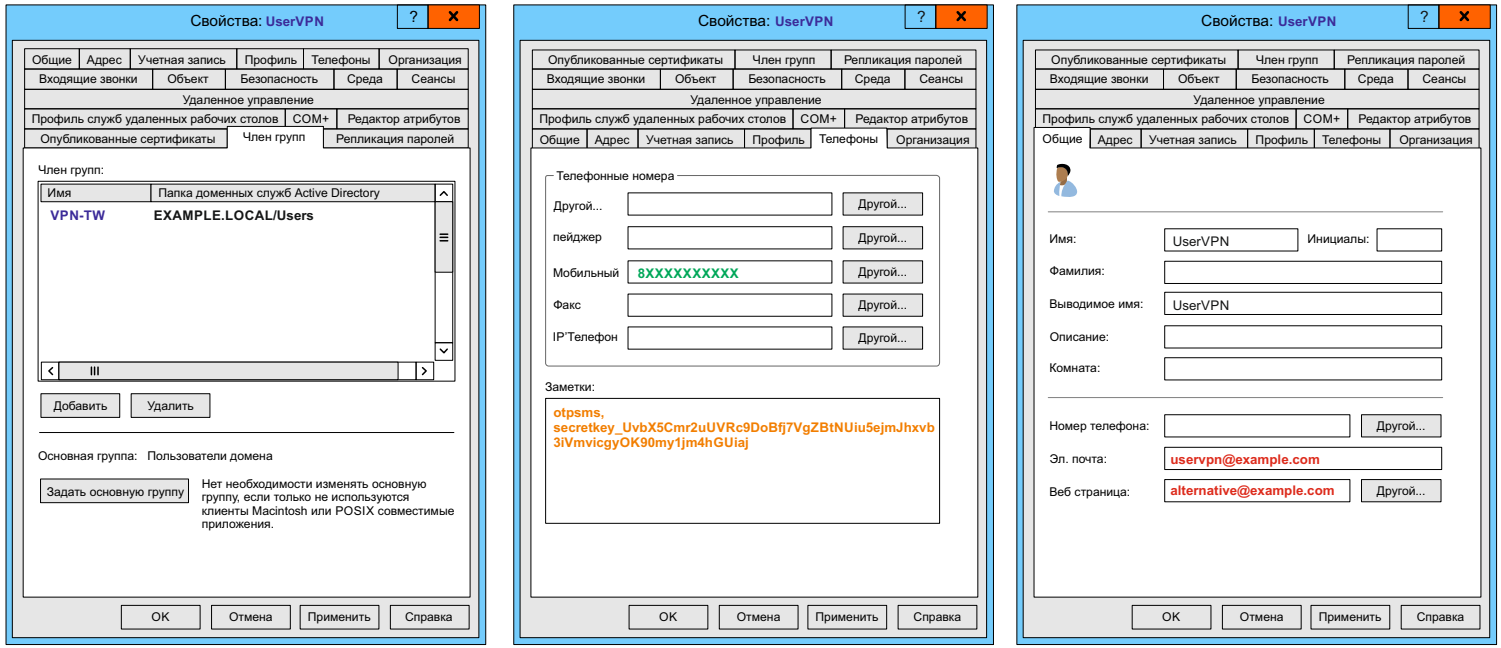
```
openssl s_client -showcerts -connect <LDAP over SSL сервер>:636
```

Получив сертификат можно убедиться кому и кем он выдан

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



Блокировка при попытках подбора OTP

Существует возможность временной блокировки пользователя например на 15 минут,
при нескольких подряд неуспешных попытках аутентификации в течение заданного времени.

За это отвечает секция **blockuser_params** в файле **settings.json**
Однако следует помнить, что если производятся попытки подбора OTP, значит пароль на учетную запись уже скомпрометирован.

Так же, есть возможность включить режим блокировки в Active Directory, тогда сохраняется концепция управления всем функционалом в Active Directory с одной стороны, и позволяет обратить внимание на факт утечки пароля учетной записи с другой стороны.

Блокировка пользователя в службе каталогов, производится путем многократных попыток аутентификации с неверным паролем, указанным в параметре **fakepassword** секции **ldap_setting,** данный пароль не должен использоваться в службе каталогов

Для правильной работы блокировки, необходимо так же указать в параметре **attemps** секции **blockuser_params** количество попыток ввода пароля, такое же как и в службе каталогов. А так же настроить политику блокировки в службе каталогов

Блокировка по странам и IP адресам

Параметры блокировки адресов и стран указываются в файле **countryacl.json**
Существует два режима работы блокировки по странам и адресам:
1.Списки разрешенных адресов/стран **(ip_allowlist** и **country_allowlist)** и запрещено все что в них не разрешено.
2.Списки запрещенных адресов/стран **(ip_denylist** и **country_denylist**) и разрешено все что в них не запрещено

Режим работы определяется параметрами **ip_default_block** и **country_default_block,** значение **true** означает использование списка разрешенных адресов/стран, значение **false** означает использование списка запрещенных адресов/стран.

Адреса IPv4 указываются в формате xx.xx.xx.xx или xx.xx.xx.xx/xx, например, 1.2.3.4, 8.8.0.0/16 и разделяются запятой.
Страны указываются в формате XX (так же как в базе данных RIPE), например RU, BY, US и разделяются запятой

Пример настройки.
В данном примере возможны соединения только из России и Объединенных арабских эмиратов

Файл **countryacl.json**

```
{
 "country_allowlist": "RU,AE",
 "country_denylist": "",
 "country_na_block":false,
 "country_default_block":true,
 "ip_allowlist": "",
 "ip_deny": "",
 "ip_default_block":false
}
```

Настройка PowerMF

Параметры в файле settings.json

Секция ldap_setting

fqdn	FQDN или IP адрес LDAP сервера.
fqdn2	FQDN или IP адрес резервного LDAP сервера.
ldap_port	LDAP порт (обычно 389)
ldaps_port	LDAP over SSL порт (обычно 636)
ldaps_enabled	включение LDAP over SSL (true/false)
base_dn	узел в дереве откуда начинать поиск пользователей
username_attr	атрибут имени пользователя, для Active Directory это sAMAccountName
bind_username_upn	имя пользователя от имени которого будет производится обращение по LDAP к контроллеру домена 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)
a_phone_attr	альтернитивный атрибут в службе каталогов для телефонного номера
a_mail_attr	альтернативный атрибут в службе каталогов для электронной почты
a_method_attr	альтернативный атрибут в службе каталогов для указания метода доставки одноразового пароля
otp_bypass_group	имя группы, членам которой разрешена аутентификация при вводе любого одноразового пароля
fakepassword	не действительный пароль, который будет использоваться для блокировки пользователя в Active Directory
nestedgroup	искать принадлежность пользователя к группе рекурсивно (вложенные группы) (true/false)

Секция radius_setting

shared_secret	секретный ключ
port	порт (обычно 1812)
address	адрес, на котором слушать RADIUS-дейтаграммы (можно оставить пустым)
ttimeotp	используется в тестовых целях и должен быть false

Секция blockuser_params

attemps	количество попыток ввода OTP (в случае блокировки в Active Directory, должно совпадать с политикой в домене)
ntime_mins	в течение какого времени, в минутах
blockfor_mins	блокировать на время, в минутах (в случае блокировки в Active Directory, не имеет значения так как настраивается политикой в домене)
enabled	0 - блокировка выключена, 1 - блокировка на уровне OTP, 2 - блокировка в Active Directory
listblockedusers	Выводить в файл лога информацию о заблокированных пользователях
country_list	использовать список блокировки по странам в файле countryacl.json, true/false
iplist	использовать список блокировки по IP адресам в файле countryacl.json, true/false

Секция otp_params:

valid_interval	интервал в течение которого временный пароль действителен
otp_len	количество цифр в одноразовом пароле - 6

Настройка PowerMF

Параметры в файле settings.json

Секция smtp_params:

mail_from	пользователь, от которого будет производиться отправка письма
mail_from_name	имя, от которого будет отправлено письмо
smtpserver	IP или FQDN адрес SMTP сервера
username	имя пользователя для аутентификации на SMTP сервере
smtpport	порт SMTP сервера
subject	тема письма
message	текст помимо пароля
domain	smtp домен, например yamdex.ru
smtp_password	пароль для SMTP соединения
tls	укажите true если используется SMTP over TLS или укажите false для использования метода STARTTLS
plain	если параметр установлен в true и параметр tls установлен в false, то отправка будет производиться открытым текстом

Секция sms_params:

smsurl	URL шлюза SMS - сейчас возможен только СМС Дисконт - «https://api.iqsms.ru/messages/v2/send.json"
smslogin	Имя пользователя для аутентификации на SMS шлюзе
smspassword	Пароль для аутентификации на SMS шлюзе
smscert	Сертификат для аутентификации на SMS шлюзе
smskey	Закрытый ключ
json	true - Использовать формат json (для указанного выше URL это так)
smsca	корневой сертификат - не обязателен
authbycert	Если аутентификация по логину/паролю то false, если по сертификату то true (для СМС Дисконт - false)
checkidentity	true - если проверять валидность сертификата сервера и false если не проверять

Настройка PowerMF

Параметры в файле countryacl.json

country_allowlist	список разрешенных стран
country_denylist	список запрещенных стран
country_na_block	блокировать пользователя, в случае невозможности получения информации о стране true/false
country_default_block	если установлен как true, то будет использоваться список разрешенных стран country_allowlist, а все остальные блокируются, если же установлен как false, то используется список запрещенных стран, country_denylist, а все остальные разрешены
ip_allowlist	список разрешенных IP адресов
ip_denylist	список запрещенных IP адресов
ip_default_block	если установлен как true, то будет использоваться список разрешенных IP адресов ip_allowlist, а все остальные блокируются, если же установлен как false, то используется список запрещенных адресов, ip_denylist, а все остальные разрешены

Настройка PowerMF

Пример настройки сервиса. В данном примере отправка почты производится через SMTP сервер Yandex

Файл settings.json

```
{
  "ldap_setting": {
    "fqdn": "dc01.testzone.local",
    "fqdn2": "192.168.1.20",
    "ldap_port": 389,
    "ldaps_port": 636,
    "Ldaps_enabled": true,
    "base_dn": "dc=testzone,dc=local",
    "bind_username_upn": "dcb@testzone.local",
    "bind_password": "P1728Ar$1t",
    "otp_group": "CN=OTP-VPN,CN=Users,DC=TESTZONE,DC=LOCAL",
    "a_phone_attr": "extensionAttribute6",
    "a_mail_attr": "extensionAttribute8",
    "a_method_attr": "extensionAttribute5",
    "otp_bypass_group": "",
    "nestedgroup": true
  },
  "radius_setting": {
    "shared_secret": "ShR1211Asb7",
    "port": 1814,
    "address": "",
    "ttimeotp": false,
    "debuglevel": 0
  },
  "syslog_params": {
    "address": "127.0.0.1",
    "port": 514
  },
  "otp_params": {
    "valid_interval": 60,
    "otp_len": 6,
    "otp_key_encrypt": "Tgkrwe12070"
  },
  "blockuser_params": {
    "attemps": 3,
    "intime_mins": 5,
    "blockfor_mins": 15,
    "enabled": 1,
    "listblockedusers": true,
    "country_list": true,
    "iplist": true
  },
  "smtp_params": {
    "mail_from": "otptest@yandex.ru",
    "mail_from_name": "LArañiaTools",
    "smtpserver": "smtp.yandex.ru",
    "smtpport": 465,
    "username": “otptest@yandex.ru",
    "smtp_password": "someyandexpassword",
    "domain": "yandex.ru",
    "tls": true,
    "plain": false,
    "debuglevel": 0
  },
  "sms_params": {
    "smsurl": "https://api.iqsms.ru/messages/v2/send.json",
    "smscert": "",
    "smskey": "",
    "message": "OTP valid until 50 sec",
    "smslogin": "z111111111111",
    "smspassword": "1111111",
    "authbycert": false,
    "json": true,
    "smsca": "",
    "checkidentity": true
  }
}
```

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
```

Работа с TOTP

Для использования генераторов TOTP необходимо чтоб секретный ключ был известен обеим 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 (“параметр **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 фйл)
-sqr показать QR код в терминале

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:

```
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
```

Инструменты тестирования

Утилиты для тестирования используют файл настройки **settings.json** и таким образом можно проверить корректность настроек.
Для проверки связи с каталогом пользователей, а так же какие атрибуты будут использоваться,
можно воспользоваться утилитой **testldap:**
./testldap -u <Имя пользователя>
Примеры работы с утилитой:

```
./testldap  -u User1
Пользователь User1 член группы CN=VTEST-VPN,CN=Users,DC=EXAMPLE,DC=LOCAL
номер мобильного телефона (LDAP атрибут extensionAttribute6): +7XXXXXXX
E-Mail (LDAP атрибут extensionAttribute8): user1@example.local
Метод доставки сообщения (параметр в атрибуте extensionAttribute5): SMS на номер мобильного телефона
```

Для проверки работоспособности доставки почты, можно воспользоваться утилитой **testmail**
Она принимает один параметр **-to** адрес получателя тестового письма.

Так же можно проверить доставку SMS сообщений утилитой **testsms**
Она принимает один параметр **-phone** номер телефона на который отправить тестовое сообщение

Данные о принадлежности адресов к стране, получаются из базы данных RIPE.
Для проверки ее доступности можно использовать утилиту **ripetest** указав в качестве параметра **-i** IPv4 адрес.
Пример:

```
./ripetest -i 113.1.2.7
Country: CN
Network: 113.0.0.0/13
Maintainer: MAINT-AS58453
Origin AS 4837
```

Работа с журналом

Журнал событий связанных с аутентификацией пользователей пишется в файл **radius.log** в директорию **./logs**
а также может отправляться в Syslog коллектор

Пример сообщений из журнала:

Пользователь Usertest подключается не заполняя сразу поле второго пароля, он получает одноразовый пароль или по рочте или по SMS

2025/02/19 19:28:49 NAS: 192.168.0.19:27203, client ip: 176.15.XXX.XXX, Sent OTP to user: Usertest, Challenge

Пользователь Usertest ввел полученный одноразовый пароль но ввел его неверно

2025/02/19 19:29:13 NAS: 192.168.0.19:27203, client ip: 176.15.XXX.XXX,Invalid OTP, user: Usertest, Rejected
2025/02/19 19:29:13 NAS: 192.168.0.19:27203, client ip: 176.15.XXX.XXX,Invalid OTP, user: Usertest, has been removed from the waiting list

Здесь показано, что в списке заблокированы пользователей есть Usertest, но он еще не заблокирован, а только ведется подсчет попыток ввода

2025/02/19 19:29:24 Number of temporary blocked users in local blocklist: 1
2025/02/19 19:29:24 User: Usertest, nuber of invalid OTP entered: 1 ,not blocked

Пользователь Usertest подключается не заполняя сразу поле второго пароля, он получает одноразовый пароль или по рочте или по SMS

2025/02/19 19:29:33 NAS: 192.168.0.19:27203, client ip: 176.15.XXX.XXX, Sent OTP to user: Usertest, Challenge

Пользователь Usertest ввел полученный одноразовый пароль верно

2025/02/19 19:30:08 NAS: 192.168.0.19:27203, client ip: 176.15.XXX.XXX, User: Usertest, entered valid OTP, Accepted

Пользователь Usertest подключается с внешним IP адресом, который принадлежит провайдеру из США, а в списке разрешенных стран указана только RU

2025/02/19 21:45:08 User: Usertest, client ip: 69.XX.XXX.XXX, blocked by ACL country US is not in allow list , Reject

Установка из репозитория Github

Перейти в папку /opt
cd /opt
выполнить:
git clone https://github.com/OlegPowerC/powermf.git
перейти в папку powermf
cd powermf
сделать исполняемым файл init.sh
chmod +x ./init.sh
и выполнить его
./init.sh
Дождаться появления информации о лицензии и сохранить ее
Связаться с нами по e-mail: **info@powerc**.ru или по телефону и приобрести лицензию
После получения файла **license.dat** скопировать его в папку **lic**
Для запуска как сервис включить сервис
systemctl enable /opt/powermf/powermf.service
Запустить
service powermf start
Разрешить принимать дейтаграммы на нужный порт в файрволе
firewall-cmd --zone=public --permanent --add-port=1812/udp
firewall-cmd --reload

Roadmap

Данное программное обеспечение создавалось с целью сделать более безопасным удаленную рабу 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
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 ля 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