Сделано в России
Не зависит от
сторонних библиотек

PowerMF

Двухфакторная аутентификация пользователей
на VPN шлюзах
предварительное 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 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, **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.**.

При использовании одноразовых паролей, подбор пароля практический невозможен, так как злоумышленнику требуется:
Подобрать имя учетной записи, подобрать пароль и одноразовый пароль, а он в свою очередь при каждой итерации разный.

В случае если злоумышленнику известна учетная запись и пароль, он может попытаться подобрать одноразовый пароль, в случае включенной блокировки в Active Directory, через несколько попыток, учетная запись будет заблокирована в Active Directory, это будет означать что необходимо поменять пароль.

Работа с Active Directory

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

Для того чтобы пользователь мог подключаться по VPN 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** следующими 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 ключем для генерации TOTP.

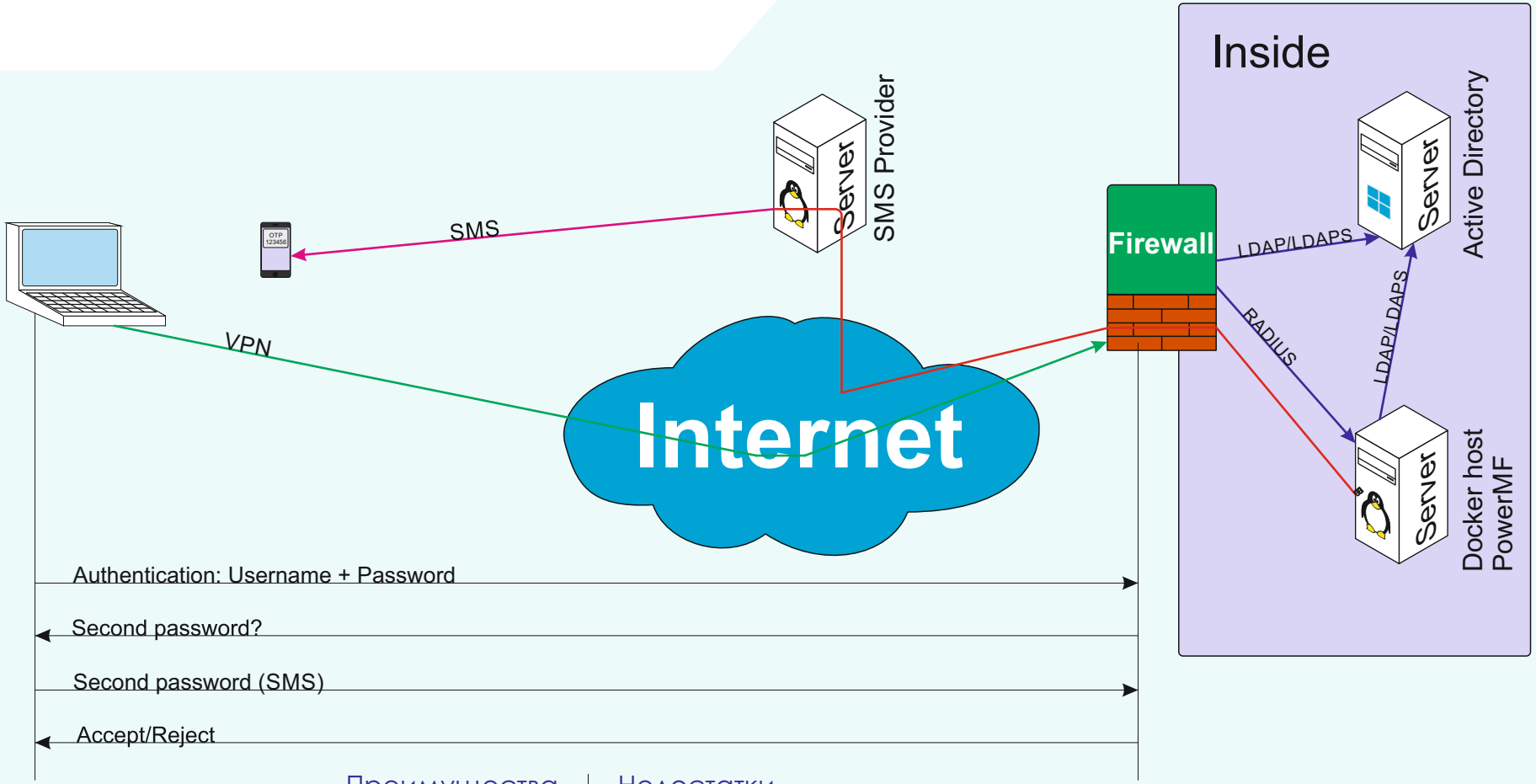
Альтернативные атрибуты являются приоритетными.

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**).

Использование LDAP over SSL
Необходимо наличие действительного сертификата на сервере а так же 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 убедится кому и кем он выдан

Схема работы SMS

Одноразовый пароль генерируется сервером
и посылается клиенту



Преимущества

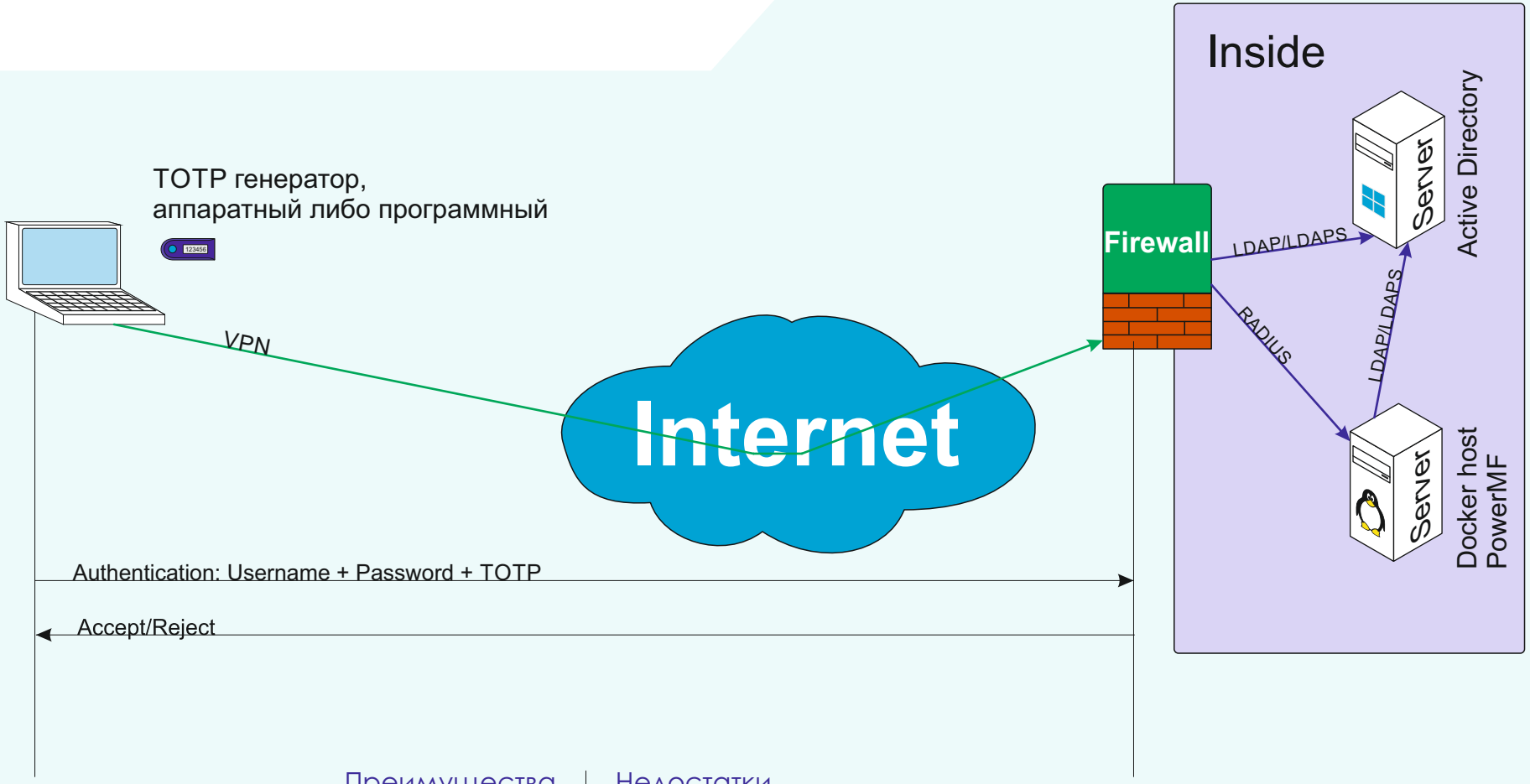
Не требуется токен
не требуется передача секретного ключа клиенту

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 безопасноть

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.

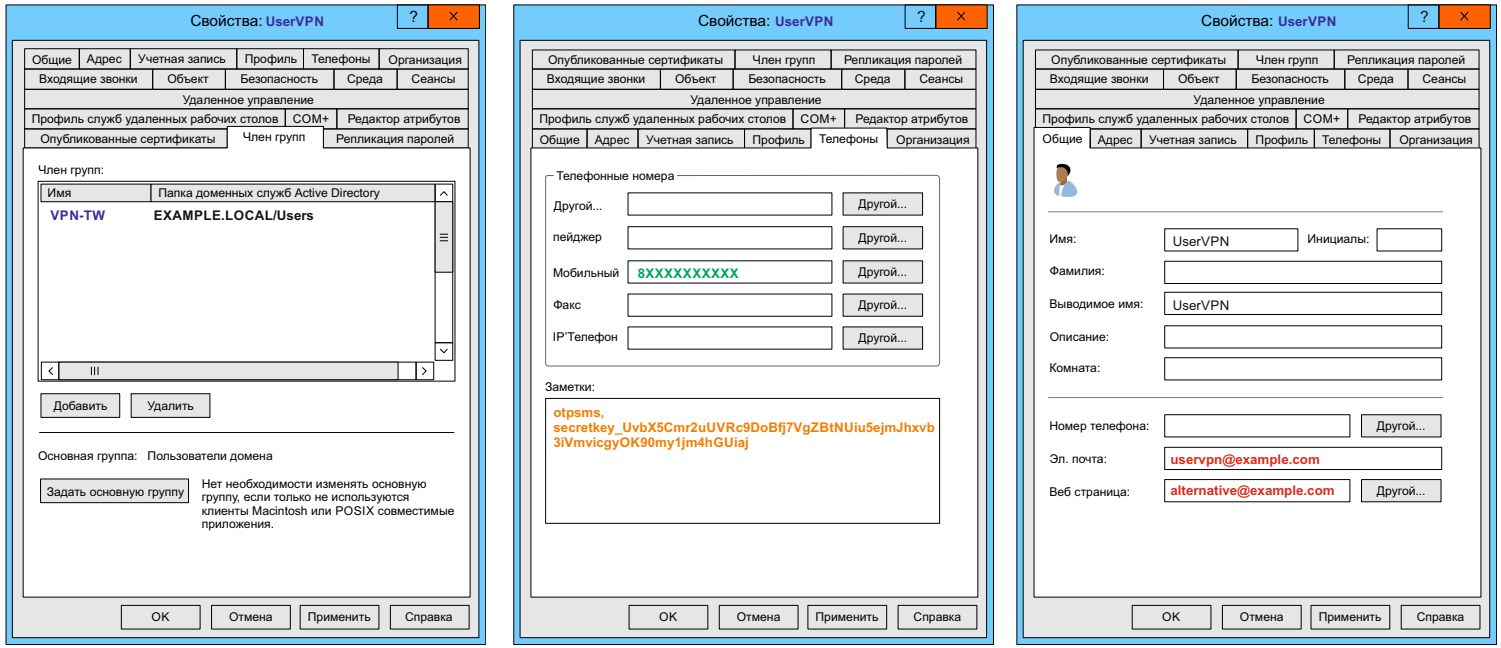
```
laaa-server ADLDAP protocol ldap
aaa-server ADLDAP (inside) host 192.168.0.2
 server-port 389
 ldap-base-dn dc=EXAMPLE, dc=LOCAL
 ldap-scope subtree
 ldap-naming-attribute sAMAccountName
 ldap-login-password TestPass123
 ldap-login-dn cn=ASA, cn=Users, dc=EXAMPLE, dc=LOCAL
 server-type microsoft

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



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
base_dn:	узел в дереве откуда начинать поиск пользователей
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

Секция radius_setting

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

Секция blockuser_params

attemps	количество попыток ввода OTP
intime_mins	в течение какого времени, в минутах (в случае блокировки в Active Directory, должно совпадать с политикой в домене)
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 пользователя в Active Directory

Настройка PowerMF

Параметры в файле settings.json

Секция otp_params

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

Секция smtp_params

mail_from:	пользователь, от которого будет производится отправка письма
mail_from_name:	"PowerMF"
smtpserver:	IP или FQDN адрес SMTP сервера
username:	имя пользователя для аутентификации на SMTP сервере
smtpport:	порт SMTP сервера
subject:	тема в письме
message:	текст помимо пароля
domain:	smtp домен, например yamdex.ru
smtp_password:	пароль на SMTP соединение
tls:	укажите 1 если используется SMTP over TLS или укажите 0 для использования метода STARTTLS

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:	1 - Использовать формат json (для указанного выше URL это так)
smsca:	корневой сертификат - не обязателен
authbycert:	Если аутентификация по логину/паролю то 0, если по сертификату то 1 (для СМС Дисконт - 0)
checkidentity:	1 - если проверять валидность сертификата сервера и 0 если не проверять

Настройка PowerMF

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

```
{
  "ldap_setting":{
    "fqdn":"dc01.example.local",
    "fqdn2":"dc02.example.local",
    "ldap_port":389,
    "ldaps_port":636,
    "Ldaps_enabled":1,
    "base_dn":"dc=example,dc=local",
    "username_attr": "sAMAccountName",
    "bind_username_upn":"admin@example.local",
    "bind_password":"Password123",
    "otp_group":"CN=OTP-VPN,CN=Users,DC=example,DC=LOCAL",
    "a_phone_attr":"extensionAttribute6",
    "a_mail_attr":"extensionAttribute8",
    "a_method_attr":"extensionAttribute5",
    "otp_bypass_group":"CN=NOOTP-VPN,CN=Users,DC=example,DC=LOCAL",
    "fakepassword": "12345fakepassword"
  },
  "radius_setting":{
    "shared_secret":"ShSecret123",
    "port": 1812,
    "address": "",
    "ttimeotp": 0
  },
  "syslog_params":{
    "address":"127.0.0.1",
    "port": 514
  },
  "otp_params":{
    "valid_interval":60,
    "otp_len": 6,
    "otp_key_encrypt": "EnkKey123"
  },
  "blockuser_params":{
    "attemps":3,
    "intime_mins":5,
    "blockfor_mins":15,
    "enabled": 1
  },

  "smtp_params":{
    "mail_from":"testmailexloc123@yandex.ru",
    "mail_from_name":"LArañiaOTP",
    "smtpserver":"smtp.yandex.ru",
    "smtpport":465,
    "subject":"Your OTP",
    "message":"OTP valid until  30 sec",
    "smtp_password":"smtppass123",
    "domain": "yandex.ru",
    "tls": 1
  },

  "sms_params":{
    "smsurl":"https://api.iqsms.ru/messages/v2/send.json",
    "smscert": "",
    "smskey": "",
    "message":"OTP valid until 50 sec",
    "smslogin":"user01",
    "smspassword":"12345",
    "authbycert": 0,
    "json": 1,
    "smsca":"",
    "checkidentity": 1
  }
}
```

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 encrypttkey.
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 фйл)

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:

```
encrypttkey.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\testuser.png
```

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 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 под 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