Безопасный доступ к 1С:Предприятие через Интернет

Организация доступа к информационным базам 1С:Предприятия через Интернет по сути своей аналогична установке шкафов с документами организации в стену здания, дверцами наружу. Вы в принципе рискуете и делаете возможным для любого прохожего с улицы:

1. Почитать документы, хранящиеся в этом шкафу
2. Что-то в них исправить или уничтожить
3. Положить туда свои документы, в т.ч. выдав их за Ваши
4. Заблокировать дверь, делая невозможным доступ к шкафу для всех

Насколько серьезны эти угрозы зависит конечно же от того, какую именно информационную базу Вы публикуете. А вот насколько легко эти угрозы осуществить и какие будут последствия зависит от «замков», которые Вы установите на дверях.

В этой статье мы собрали базовые рекомендации по организации безопасного онлайн доступа к информационным базам 1С:Предприятие с использованием свободного программного обеспечения.

На практике против Вас могут быть применены три типа атаки, вкратце объясним их суть и расскажем о методах противодействия

Возможные угрозы

Атака грубой силы

Цель такой атаки - подобрать пароль легального пользователя информационной системы, последовательно пробуя все возможные пароли и проникнуть внутрь под видом этого пользователя.

На практике используется метод метод перебора по словарю, он отличается от метода полного перебора тем, что в нем перебираются не все возможные пароли, а наиболее часто используемые в порядке убывания популярности. И начинается этот словарь с самых популярных паролей `12345678` и `qwerty`.

Разработано множество способов противостояния атаке грубой силы, но, к сожалению, большинство их недоступно для 1С:Предприятия, по крайней мере на уровне платформы.

Самый популярный инструмент защиты - капча, увы, отсутствует в платформе 1С. Автоматический таймаут после нескольких неудачных попыток ввода пароля - так же нам не доступен. Самый надежный способ - двухфакторная авторизация, увы, в платформе 1С:Предприятие тоже отсутствует.

Двухфакторную аутентификацию можно реализовать на уровне прикладного решения. Пользователь сначала проходит авторизацию в платформе, затем, уже в конфигурации его встречает Google Authenticator или просят ввести код, отправленный SMS.

Если Вы точно знаете откуда внешние пользователи будут подключаться к Вашей информационной базе и знаете их IP адреса, например, это может быть Ваш удаленный офис, просто ограничьте доступ к опубликованной информационной базе. Запретите его всем, кроме известных Вам адресов удаленного офиса.

Если внешние пользователи подключаются с динамических IP адресов, или они они не сидят на одном месте, но при этом они все-таки являются Вашими сотрудниками - объедините их в виртуальную частную сеть.

Если же Вы не можете спрятать доступ к информационной базе в виртуальной частной сети, например, когда речь идет о доступе для Вашего торгового партнера, было бы странно предлагать всем таким партнерам доступ к VPN, используйте двухступенчатую авторизацию через клиентские сертификаты.

Атака посредника

С такой атакой есть риск столкнуться в ненадежных сетях на стороне клиента. Злоумышленник в такой сети подменяет для клиента Ваш настоящий сервер своей прослойкой-ретранслятором, принимает запросы от клиента, перенаправляет их к Вам на сервер, получает ответы от Вашего сервера и возвращает их клиенту. При такой ретрансляции злоумышленник расшифрует весь трафик, который Вы пытались шифровать, настроив SSL соединение, он получит логины, пароли и любые данные, которые передаются между клиентом и сервером.

С такой угрозой можно столкнуться не только в бесплатной WiFi сети, но и практически в любой коммерческой сети, где вопросам безопасности уделяется мало внимания, например, в сетях микро-провайдеров, монопольно работающих в офисных и торговых центрах, в локальной сети арендованного склада, в любой сети, которую Вы не контролируете.

Для защиты от такой атаки существуют удостоверяющие центры (англ. Certification Authority - CA), которые подтверждают клиентам, что Ваш сервер именно тот, за кого он себя выдает. Разумеется, это работает только тогда, когда клиент принимает во внимание результаты такой проверки.

DDoS атака

Такая атака не позволит злоумышленнику проникнуть в Вашу информационную систему, что-то там украсть, удалить или испортить данные. Ее цель - сделать полностью невозможной работу с Вашей системой для всех.

Одновременно со множества IP адресов на Ваш сервер направляется большое количество запросов. Сами запросы могут быть вполне безобидными, например, на просмотр какой-то страницы сайта. Даже если запрашиваемой URL не существует, серверу придется ответить вопрошающему кодом ошибки 404, и он будет какое-то время этим занят. Цель атаки - завалить сервер таким количеством запросов, что бы у него ни на что больше не оставалось времени. Сервера для публикации информационных баз 1С как правило не отличаются большой производительностью и хорошей оптимизацией для работы в web. Пара тысяч таких запросов в секунду (весьма слабая по сегодняшним меркам атака) полностью обвалят такой сервер.

От серьезной DDoS атаки отбиться подручными средствами не получится. Если кто-то организовал серьезную атаку на Вашу инфраструктуру, потребуется помощь специалистов по информационной безопасности.

Что бы от такой атаки не пострадала работа Вашего предприятия придерживайтесь следующих рекомендаций:

1. Никогда, ни при каких обстоятельствах не публикуйте информационные базы в Интернет на том же сервере, на котором работает сервер приложений.
2. Если можно обойтись без публикации информационной базы непосредственно в Интернет, лучше обойтись VPN.
3. Никогда не подключайте сервер напрямую к Интернет, только через Firewall, используйте профессиональные роутеры, например, Cisco и квалифицированных специалистов для их настройки.
4. Организуйте DMZ, разместите Apache публикующий информационные базы в DMZ, а перед Apache установите проксирующий Nginx.

Методы противодействия угрозам

Ограничение доступа по IP адресам

Существует два подхода к вопросам информационной безопасности:

1. Разрешено все, что не запрещено,
2. Запрещено все, кроме того, что разрешено.

Если кто-то пытается подобрать пароль к Вашей системе, можно заблокировать его по IP адресу. Поняв, что его блокируют, злоумышленник очень быстро вернется к своему занятию с другого IP адреса. Такое противоборство может продолжаться бесконечно долго.

Есть способ проще. Можно по-умолчанию запретить доступ для всех IP адресов, и разрешать его только доверенным узлам или сетям, например, IP адресам филиалов или подсетей провайдеров, которыми они пользуются.

Хорошая практика - управлять доступностью через межсетевой экран, ограждающий сервер с Apache от Интернета. Настраиваете его сначала на полное блокирование входящих пакетов, а затем добавляете в исключения разрешенные IP адреса и подсети.

Если на Apahe публикуется несколько виртуальных хостов и не для всех приемлемы столь строгие ограничения доступа, ограничьте доступ на уровне настройки виртуального хоста Apahe или .htaccess, добавьте директивы

```
Order Deny,Allow
Deny from all
allow from xxx.xxx.xxx.xxx # Указываем разрешенные IP адреса и подсети
allow from xxx.xxx.xxx.xxx
allow from xxx.xxx.xxx.xxx
```

Построение виртуальной частной сети

Когда нужно решить задачу онлайн-доступа в информационную базу ваших собственных подразделений, филиалов, удаленных офисов или сотрудников, работающих вне офиса, лучше вообще не выставлять в Интернет прямой веб-доступ.

Гораздо безопаснее развернуть виртуальную частную сеть - VPN. Единственная «проходная» из Интернет к Вам в офис - это шлюз VPN, а при грамотной настройке это очень хорошо защищенная проходная.

Шлюз VPN можно поднять на роутере, практически все модели профессионального оборудования имеют такую встроенную функцию. Или это можно сделать на отдельном сервере.

В целях безопасности не устанавливайте шлюз VPN на том же сервере, где установлен сервер 1С:Предприятие

Оптимальный вариант - разместить шлюз в DMZ, он будет принимать входящие запросы из Интернет, следовательно он подвержен внешним угрозам. Для этого идеально подойдет небольшой сервер на Ubuntu с установленным на нем сервером OpenVPN.

Клиентские части OpenVPN есть для всех популярных платформ.

Если Ваши удаленные клиенты подключаются к Вам через канал со скоростью более 30 Мбит/сек, то нет никакой необходимости в использовании веб-сервера Apache, можно из VPN подключаться непосредственно к серверу 1С:Предприятие в режиме тонкого клиента, скорости соединения будет достаточно для комфортной работы.

Использование цифровых сертификатов пользователя

Когда без публикации информационной базы непосредственно в Интернет никак не обойтись, а риски взлома высоки, используйте возможности SSL. Помимо шифрования и безопасной передачи данных в этом протоколе есть возможность аутентификации веб-пользователей через SSL сертификаты.

Веб-сервер Apache и веб-клиетнт 1С:Предприятие поддерживают аутентификацию по SSL-сертификатам. Внешний пользователь сначала будет проверен средствами Apache, и только пользователь, предъявивший действующий сертификат будет допущен к форме ввода логина-пароля 1С:Предприятие.

Для начала нужно развернуть у себя Certification Authority (CA). Тут паранойя лишней не бывает, вот неплохой HOW-TO по безопасной установке CA.

Сгенерируйте и удостоверьте в CA нужное количество пользовательских сертификатов.

Обычно клиентские сертификаты выдаются пользователям в виде зашифрованных `.pfx` или `.p12` файлов. Такой файл можно передавать, копировать, пересылать по электронной почте, но для того, что бы им воспользоваться, нужно знать пароль, которым он зашифрован. Если такой уровень безопасности Вы считаете недостаточным и готовы увеличить свои расходы на информационную безопасность - используйте USB токены с поддержкой SSL.



Запишите пользовательский сертификат в токен и запретите его экспортировать. Теперь без этого токена никак к Вам не зайти.

Остается настроить Apache. В описании виртуального хоста, там где Вы настраивали HTTPS добавьте

```
<VirtualHost *:443>

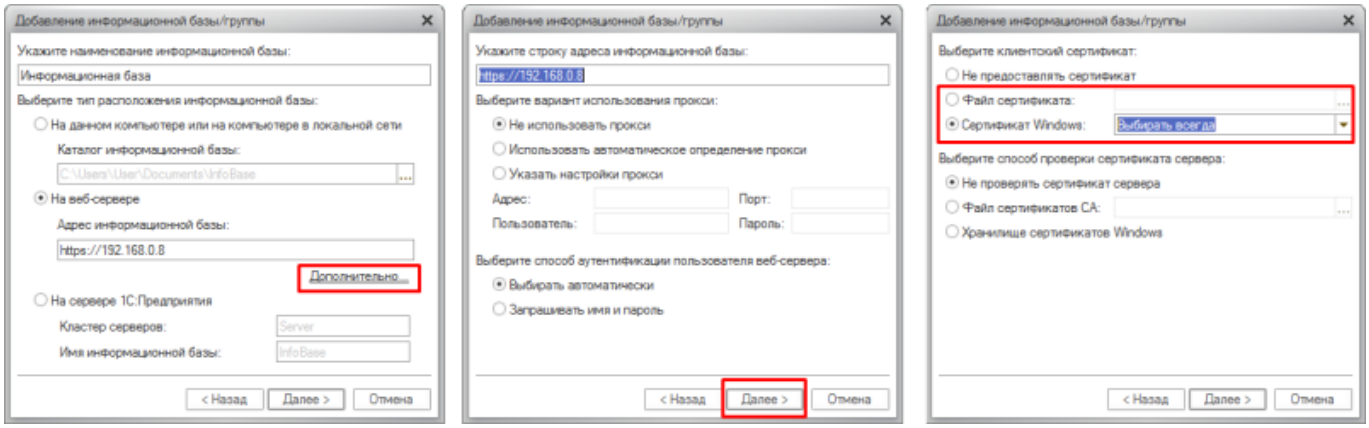
    # Прочие настройки из инструкции

        # SSL
        SSLEngine on
        SSLProtocol all -SSLv2
        SSLCertificateFile    /etc/ssl/certs/myserver.pem
        SSLCertificateKeyFile /etc/ssl/private/myserver.key

        SSLCACertificateFile /etc/ssl/ca.crt  # путь к сертификату CA
        SSLCARevocationFile /etc/ssl/ca.crl   # путь к списку отозванных
сертификатов
        <Directory /var/www/html>             # путь к DocumentRoot или к
каталогу публикации ИБ 1С
            SSLVerifyClient require
        </Directory>

    # Прочие настройки из инструкции
</VirtualHost>
```

На стороне клиента можно установить клиентский сертификат в хранилище сертификатов, или же просто указать файл сертификата в настройке подключения информационной базы 1С:Предприятие.



Использование подписанных сертификатов сервера

Для безопасного обмена информацией в Интернет важно, что бы не только сервер был уверен, что клиент именно тот, за кого он себя выдает, но и клиент мог удостовериться, что он соединился именно с тем сервером, который ему нужен, и что передаваемую между ними зашифрованную информацию никто другой не прочитает. Помогают в этом удостоверяющие центры, англ. Certification Authority (CA).

Принцип работы CA можно сравнить с печатью в паспорте. Сервер предъявляет паспорт - публичный сертификат, в паспорте есть печать - он подписан CA, печать легко проверяется и ее невозможно подделать.

При настройке HTTPS в Apache мы сами себе сделали ключ и сертификат, и подписали сертификат этим же ключом. Такие сертификаты называются *самоподписанными*, они вполне годятся для шифрования трафика в SSL протоколе, но они не дают гарантии, что сайт который их использует именно тот, за кого он себя выдает, о чем браузер обязательно предупредит пользователя.

Проводя аналогию с паспортом, такой сертификат можно сравнить с документом, напечатанным на принтере, где нет даже подписи, которую кто-нибудь смог бы опознать как нашу, вместо подписи в документе напечатано «Администрация».

Если мы хотим, что бы пользователи могли удостовериться, что они имеют дело именно с нашим сервером, сертификат сервера нужно заверить в CA.

Важный вопрос безопасности: можно ли доверять документу, на котором стоит простая подпись человека, может даже и синяя печать какого-нибудь ООО, или все-таки можно доверять только документу, заверенному у нотариуса? В жизни бывает так и так, в интернете тоже.

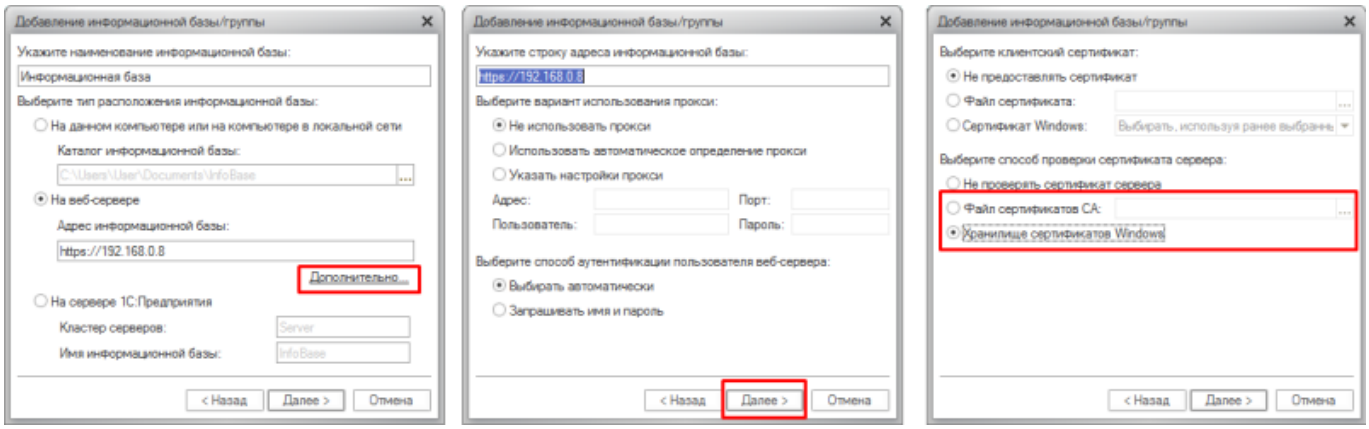
Вы можете сделать свой собственный CA, раздать его корневой сертификат Вашим пользователям и договориться, что этим сертификатом они будут проверять, действительно ли они подключаются к Вашему серверу, а не к злоумышленнику, имитирующему его в целях хищения конфиденциальной информации. Если пользователей устроит такой вариант - отлично, на OpenSSL собственный CA делается совершенно бесплатно.

Роль «нотариуса» в Интернете выполняют т.н. *доверенные* удостоверяющие центры. Корневые сертификаты таких CA по-умолчанию установлены в браузеры, и браузеры по-умолчанию доверяют сайтам, предъявляющим сертификаты, подписанные доверенными CA.

Вы можете получить такой сертификат для своего сайта. Это платная услуга, Вы подаете заявку в удостоверяющий центр, прилагаете требуемые документы, удостоверяющий центр проводит проверку, что Вы это Вы, что сайт, для которого запрашивается сертификат действительно принадлежит Вам и если не возникает никаких подозрений, Вам выдается подписанный сертификат сроком действия 1 год. Через год процедуру и оплату нужно повторить.

Когда Вы установите такой сертификат себе на сервер, браузеры сразу будут считать Ваш сайт безопасным.

В веб-клиенте 1С:Предприятия есть настройка проверки сертификата сервера.



Здесь имеется ввиду корневой сертификат CA, а не сертификат сервера. С самоподписными сертификатами такая проверка не работает.

Так же как и в случае с клиентским сертификатом есть вариант установить его в хранилище сертификатов или предъявить в виде файла.

В SSL применяется два типа файлов: приватный ключ, он обычно имеет расширение .key и публичный сертификат, он обычно имеет расширение .cer

Никогда ни при каких обстоятельствах не передавайте посторонним приватный ключ.

Если остались вопросы, или Вы хотите получить дополнительную консультацию, обращайтесь, будем рады помочь.

- Twitter
- Facebook
- Google+
- LinkedIn
- Pinterest
- Tumblr
- Reddit
- Taringa
- StumbleUpon
- Telegram
- Hacker News
- Xing
- Vk

- Email

From:
https://wiki.lineris.ru/ - **ЛИНЕРИС**

Permanent link:
https://wiki.lineris.ru/web_security?rev=1492594410

Last update: **2017/04/19 09:33**