TrueConf

TrueConf Border Controller

Руководство администратора

Оглавление

1. Описание

В комплексное решение TrueConf Enterprise входит расширение TrueConf Border Controller для предоставления защищённого доступа к серверам видеосвязи внешним (находящимся вне зоны корпоративной среды) пользователям.

TrueConf Border Controller — отдельное расширение, выполняющее роль пограничного контроллера и предназначенное для установки в DMZ (демилитаризованной зоне) корпоративной сети и пропускающее только безопасный трафик от приложений Труконф.

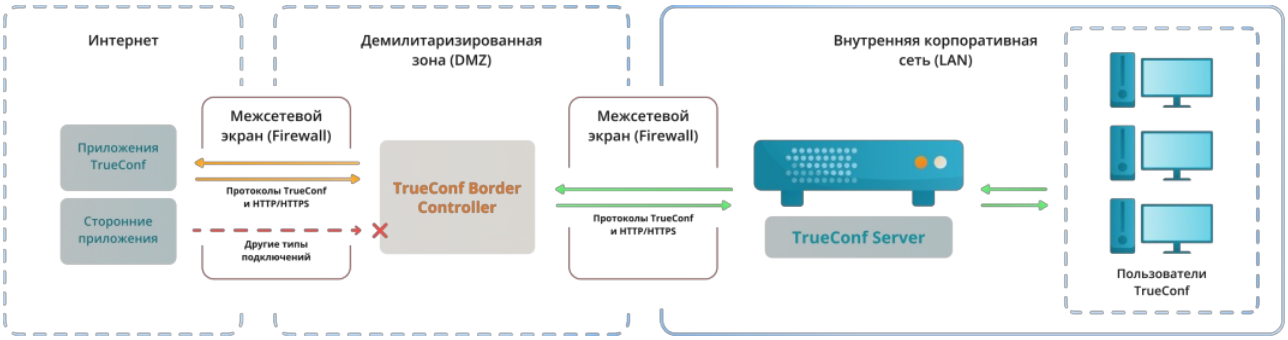
1.1. Состав решения

Расширение состоит из двух компонентов, которые валидируют трафик соответственно по протоколам Труконф и HTTP/HTTPS.

> *i* Рекомендуется использовать HTTPS на TrueConf Server, т.к. это повышает безопасность доступа к веб-ресурсам сервера, а также обеспечивает работу планировщика, расширенного управления конференцией, подключение к вашим мероприятиям из браузера и возможность перехода в личный кабинет пользователя.

Каждый из компонентов TrueConf Border Controller настраивается отдельно и работает независимо друг от друга, то есть можно настроить только пропуск трафика Труконф, но не HTTPS.

Схема работы TrueConf Border Controller:



1.2. Принцип работы

1. В DMZ установлено расширение TrueConf Border Controller.
2. Расширение проверяет протоколы поступающего на него из внешней сети трафика.
3. Если трафик пришёл не по протоколам Труконф или HTTPS, то он просто отбрасывается.
4. Если же расширение детектирует трафик от приложения Труконф или HTTPS, то соединение принимается и создаётся новое в направлении от TrueConf Border Controller к указанному TrueConf Server или TrueConf Enterprise. После установки соединения получаемые от приложения пакеты передаются по новому соединению на сервер видеосвязи, допускается трафик по протоколам Труконф и HTTPS. Это обеспечивает не только отправку медиапотоков, но и работу планировщика, доступ к веб-страницам сервера видеосвязи, работу федерации и пр.
5. Доступно опциональное шифрование трафика от TrueConf Border Controller к серверу видеосвязи с помощью множества симметричных алгоритмов, в том числе с использованием PSK (Pre-Shared Key) .
6. Расширение не производит дополнительных операций с трафиком помимо шифрования, таких как: анализ, сохранение, передача на сторонние службы и т.д.

Таким образом, защита установленного внутри корпоративной сети сервера видеосвязи основана на том, что:

- TrueConf Border Controller не создаёт нового подключения к TrueConf Server, пока не убедится, что пакеты приходят от приложения Труконф или по безопасному протоколу HTTPS;
- в принципе в сторону сервера видеосвязи TrueConf Border Controller не направляет никакой сторонний трафик, в том числе SIP/H.323/RTP и пр. Например, подключиться снаружи сети к TrueConf Server смогут только клиентские приложения Труконф;
- скрывается IP сервера видеосвязи внутри корпоративной сети и для него требуется только наличие связи с DMZ, но не выхода в Интернет. При этом следует учесть, что если не будет связи с Интернет, то не будет возможности участвовать в федерации;
- дополнительно возможно шифрование трафика, передаваемого по протоколу Труконф.

Каждый компонент расширения представляет собой исполняемый файл, не требующий установки. Поддерживается запуск из консоли или добавление в качестве службы на Windows или демона (daemon) на Linux.

2. Системные требования

Мы рекомендуем устанавливать TrueConf Border Controller на отдельный физический или виртуальный сервер в DMZ, который отвечает следующим минимальным требованиям (из расчёта анализа около 800 Мбит/с транзитного трафика):

Параметр	Значение
Операционная система	Выделенная или виртуальная 64-битная операционная система: • Microsoft Windows Server 2008 R2/2012/2016/2019/2022 (в том числе редакции Core) с установленными последними версиями обновлений • Debian 10 / 11 / 12 • CentOS Stream 9 • Astra Linux CE 2.12 • Astra Linux SE 1.6 / 1.7 • Альт Сервер 9 / 10 • РЕД ОС 7.3
Процессор	Любой процессор с количеством физических ядер не менее 4
Оперативная память	4 ГБ
Жёсткий диск	Свободное место для сохранения лог-файлов работы расширения (если активировано)

Подробнее требования в зависимости от желаемого числа параллельно работающих на одной машине экземпляров каждого из компонентов TrueConf Border Controller и предполагаемого объёма трафика уточняйте у нашей технической поддержки.

Далее мы покажем вам, как настроить запуск компонентов на ОС Windows и ОС семейства Linux.

При возникновении любых вопросов по настройке TrueConf Border Controller вам поможет наша техническая поддержка.

3. Компонент для протокола TrueConf

Предоставляется в виде установщиков для Windows и всех поддерживаемых ОС Linux. Настройки для работы компонента указываются в файле конфигурации `tc_bc.cfg`, который создаётся автоматически при установке. Пример файла конфигурации смотрите после перечисления параметров.

После установки компонента в ОС автоматически появится соответствующая служба:

- на ОС Windows с названием **TrueConf Border Controller** и id **tc_bc**, путь к исполняемому файлу `C:\Program Files\TrueConf\Border Controller\tc_bc.exe`
- на ОС Linux: **trueconf-bc**, путь к исполняемому файлу `/opt/trueconf/border-controller/bin/tc_bc`

3.1. Список параметров

При установке компонента будет создан файл конфигурации для указания параметров работы:

- на ОС Windows: `C:\Program Files\TrueConf\Border Controller\etc\tc_bc.cfg`
- на ОС Linux: `/opt/trueconf/border-controller/etc/tc_bc.cfg`

Компонент поддерживает следующие параметры (в скобках для некоторых представлены альтернативные варианты вызова).

3.1.1. Общие параметры

- `--Debug <level>` — уровень логирования от **0** (отключен) до **4**;
- `--LogDirectory <path>` — путь к сохранению лог-файлов по работе расширения;
- `--LogToConsole` — вывод логов в консоль вместо лог-файла;
- `--Daemonize <path to the PID lock-file>` **(только для Linux)** — запуск в виде демона (daemon) с указанием пути сохранения PID-файла;
- `--Service` **(только для Windows)** — запуск в виде службы;
- `--R` — автоматический перезапуск службы при ошибке.

3.1.2. Параметры маршрутизации

- `-D <id>/<host>:<port>` (`--Destination <id>/<host>:<port>`) — адрес или FQDN TrueConf Server или TrueConf Enterprise для перенаправления трафика. Здесь:
  - `<id>` — (опционально) уникальная строка идентификатора для объединения опций (если требуется работа одного TrueConf Border Controller с несколькими правилами перенаправления, **не рекомендуется**);
  - `<host>` — IPv4, IPv6 или FQDN (IPv6 должен быть указан в квадратных скобках `[IPv6]`);
  - `<port>` — (опционально) порт, может быть опущен если равен значению по-умолчанию **4307**;
- `-L <id>/<host>:<port>` (`--Listen <id>/<host>:<port>`) — сетевой интерфейс для получения входящего трафика, опции совпадают с таковыми для параметра `-D`;
- `-E <id>/<cipher>:<flags>:<key>` (`--Encryption <id>/<cipher>:<flags>:<key>`) — шифрование пакетов от TrueConf Border Controller к серверу видеосвязи. Здесь:
  - `<id>` — (опционально) уникальная строка идентификатора для объединения опций;
  - `<cipher>` — используемый шифр, принимает значения `None` (без шифрования, по-умолчанию), `ChaCha20`, `AES-256-CTR`, `AES-256-OFB`, `AES-192-CTR`, `AES-192-OFB`,

`AES-128-CTR`, `AES-128-OFB`, `xoshiro256++`, `xoshiro256**`;

- `<key>` — ключ для шифрования (в 16-ричном виде), может быть опущен, чтобы использовалось случайно сгенерированное значение (не совместимо с режимом PSK);
- `<flags>` — если имеется и равен `PSK`, значит, используется шифрование с использованием Pre-Shared Key. Тогда требуется его настройка на стороне сервера видеосвязи.

3.1.3. Параметры командной строки для запуска из терминала (консоли)

Вы можете запустить исполняемый файл компонента из терминала с некоторыми параметрами, которые нельзя использовать в файле конфигурации:

- `-h` (`--help`) — вывод встроенной помощи со списком параметров и примерами;
- `-c <path>` (`--ConfigFile <path>`) — путь `<path>` к файлу конфигурации;
- `-v` (`--version`) — версия компонента.

Например, вызов справки для ОС Linux:

```sh
sudo /opt/trueconf/border-controller/bin/tc_bc -h
```

3.1.4. Пример файла конфигурации

```
LogDirectory=/opt/trueconf/border-controller/var/log
Listen=10.140.10.123
Destination=10.110.10.10
Encryption=ChaCha20
```

3.2. Запуск компонента

После настройки файла конфигурации можно запустить компонент.

3.2.1. На ОС Windows

Для управления службами на ОС Windows можно использовать как графический интерфейс так и командную строку (терминал).

Чтобы быстро открыть окно управления службами, запустите командную строку (терминал) или PowerShell и выполните команду `services.msc`. В открывшемся окне вы сможете выбрать в списке службу **TrueConf Border Controller** и запустить её, а также настроить её автозапуск при старте ОС.

Для управления службами полностью с помощью терминала используется утилита `sc.exe`. Все команды выполняются от имени администратора ОС. Например, чтобы запустить службу, выполните:

```sh
sc start tc_bc
```

Чтобы добавить службу в автозапуск, выполните:

```sh
sc config tc_bc start=auto
```

3.2.2. На ОС Linux

Управление службами (которые в терминологии Linux называются *демонами*, от англ. *daemon*) осуществляется с помощью утилиты `systemctl`.

Чтобы запустить демон **trueconf-bc**, выполните:

```sh
sudo systemctl start trueconf-bc
```

Чтобы демон **trueconf-bc** запускался при старте ОС, выполните:

```sh
sudo systemctl enable trueconf-bc
```


4. Компонент для протокола HTTPS

Предоставляется в виде установщиков для Windows и всех поддерживаемых ОС Linux. Настройки для работы компонента указываются в файле конфигурации `webproxy.toml` как показано далее.

После установки компонента в ОС автоматически появится соответствующая служба:

- на ОС Windows с названием **TrueConf Border Controller htpps** и id **tc_bchttps**, путь к исполняемому файлу `C:\Program Files\TrueConf\Border Controller\tc_bchttps.exe`
- на ОС Linux: **trueconf-bchttps**, путь к исполняемому файлу `/opt/trueconf/border-controller/bin/tc_bchttps`

Запуск компонента настраивается так же, как и для рассмотренного ранее компонента для трафика Труконф, но с рядом отличий:

- надо предварительно настроить работу с сертификатами;
- параметры работы настраиваются в конфигурационном файле **webproxy.toml**.

4.1. Настройка сертификатов

1. Если на стороне TrueConf Server настроен самоподписанный сертификат, то скачайте его (по ссылке **Скачать ca.crt** в блоке **Самоподписанный сертификат**) и добавьте его в доверенные корневые сертификаты на машине с TrueConf Border Controller. Как это сделать, читайте в документации к вашей ОС.

Например, **на ОС Debian**:

- скопируйте файл сертификата в хранилище сертификатов в каталог `usr/local/share/ca-certificates/` :

```sh
sudo cp ca.crt /usr/local/share/ca-certificates/
```

- обновите хранилище сертификатов командой:

```sh
sudo update-ca-certificates -v
```

* Если вы получите ошибку что команда не найдена, то установите пакет из репозитория:

```sh
sudo apt install -y ca-certificates
```

- для проверки, что ваша ОС доверяет сертификату, выполните:

```sh
openssl verify /usr/local/share/ca-certificates/ca.crt
```

2. На ОС Linux после копирования файлов сертификатов убедитесь, что у них владелец `trueconf` (иначе не будет корректно запускаться служба TrueConf Border Controller). Для проверки выполните команду:

```sh
ls -l /usr/local/share/ca-certificates/ca.crt
```

В выводе должно быть `trueconf trueconf` во 2 и 3 столбцах. Если это не так, то выполните команду:

```sh
sudo chown trueconf:trueconf /usr/local/share/ca-certificates/ca.crt
```

3. В панели управления TrueConf Server перейдите в раздел **Веб →Настройки** и в поле **Внешний**

адрес веб страницы TrueConf Server укажите адрес машины с TrueConf Border Controller.

4. Создайте сертификат для машины с TrueConf Border Controller. Если нет коммерческого, можно создать самоподписанный как показано в нашей базе знаний.

5. Полученные на шаге 3 сертификат и ключ скопируйте в каталог `<path_to_border_controller>\etc\crt\`, где `<path_to_border_controller>` — путь к исполняемому файлу компонента на вашей ОС.

6. Переименуйте файлы сертификата и ключа в виде `<guid>.crt` и `<guid>.key` где `<guid>` — одинаковый для обоих файлов 128-битный идентификатор GUID. Его можно сгенерировать, например, с помощью онлайн-сервиса UUID Generator.

4.2. Настройка файла конфигурации

При установке компонента будет создан файл конфигурации `webproxy.toml`:

- на ОС Windows: `C:\Program Files\TrueConf\Border Controller\etc\webproxy.toml`
- на ОС Linux: `/opt/trueconf/border-controller/etc/webproxy.toml`

Файл конфигурации по-умолчанию содержит такие строки:

```
[certificate]
cert_extension = '.crt'
key_extension = '.key'

[dir]
executable_relative = false
installation = '/opt/trueconf/border-controller'

[file]
configname = 'webproxy'

[interfaces]
[interfaces.list]
[interfaces.list.0]
Address = '[::]:80'
EnableTLS = false
ReadTimeout = 0
TLSConfigID = ''
TargetID = ''

[proxy]
trust_client_headers = false

[targets]
[targets.list]

[tls]
[tls.list]
```

Для настройки работы компонента для протокола HTTPS укажите следующие значения:

- в разделе `[dir]`:
  - `installation` — путь к исполняемому файлу компонента;
- в разделе `[interfaces.list.0]`:
  - `Address` — порт для HTTPS если отличается от стандартного **443**;

- `TLSConfigID` — имя файлов сертификата и ключа, полученное на шаге 5;
- `TargetID` — GUID для идентификации блока настроек HTTPS из раздела `[targets]`;

- в разделе `[interfaces.list.1]`:
  - `Address` — порт для доступа к панели управления по HTTP если отличается от стандартного **80**;
  - `TargetID` — GUID для идентификации блока настроек HTTP из раздела `[targets]`;
- для каждого из блоков `[targets.list.<guid>]` в разделе `[targets]`:
  - сгенерируйте уникальные GUID и добавьте их в названиях вместо `<guid>`;
  - `address` — IP-адрес или FQDN TrueConf Server и порт для передачи трафика от компонента;
  - `is_secure` — если для параметра `address` текущего блока `[targets.list.<guid>]` был указан HTTPS порт, то значение `true`, иначе `false`;
- в разделе `[tls]`:
  - для названия блока `[tls.list.<guid>]` замените `<guid>` на значение `TLSConfigID` (оно же название файла сертификата из шага 5);
  - `CertificateID` и `ID` — значение `TLSConfigID`.

7. Сохраните файл `webproxy.toml` и запустите компонент.

4.3. Запуск компонента на ОС Windows

Как и компонент для протокола Труконф запуск службы на Windows можно произвести из оснастки `services.msc` либо из терминала с помощью утилиты `sc.exe`. Например:

```sh
sc start tc_bchttps
```

Аналогичным образом компонент добавляется в автозапуск, например:

```sh
sc config tc_bchttps start=auto
```

4.4. Запуск компонента на ОС Linux

Для управления компонентом используйте утилиту `systemctl` как было показано для **trueconf-bc**. Например, для запуска выполните:

```sh
sudo systemctl start trueconf-bchttps
```