TrueConf

TrueConf Border Controller

Руководство администратора

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

Оглавление

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

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 TrueConf.

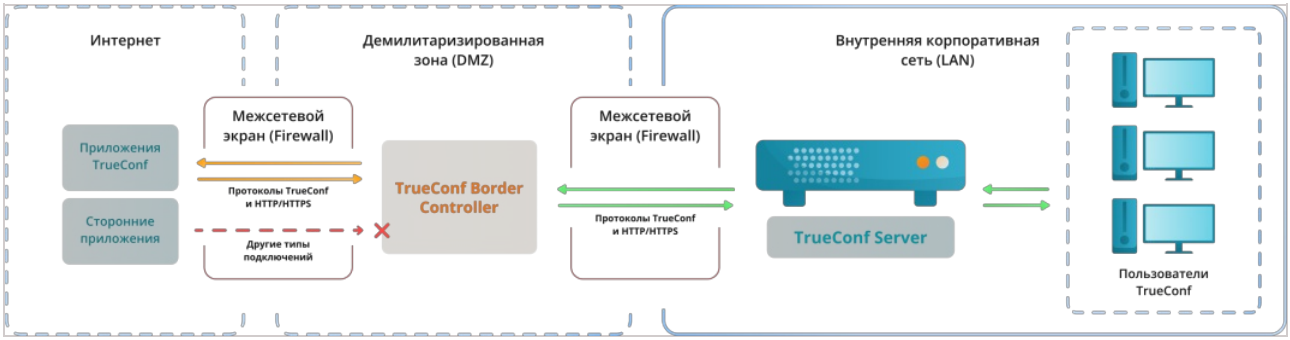
1.1. Состав решения

Расширение состоит из двух компонентов, которые валидируют трафик соответственно по протоколам TrueConf 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 TrueConf, 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 TrueConf или HTTPS, то он просто отбрасывается.
4. Если же расширение детектирует трафик от приложения TrueConf 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 TrueConf 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

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

на том, что:

- TrueConf Border Controller не создаёт нового подключения к TrueConf Server, пока не убедится, что пакеты приходят от приложения TrueConf 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 TrueConf;
- 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 TrueConf.

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.

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

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 • 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.

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

3. Компонент для протокола TrueConf

Представляет собой исполняемый файл с именем **tc_bc**. Настройки для работы компонента можно указать в списке параметров запуска после пути к исполняемому файлу или в подключаемом файле конфигурации (с помощью параметра `-c`). Пример файла конфигурации смотрите после перечисления параметров.

3.1. Запуск из консоли

Для запуска компонента как консольного приложения перейдите в терминал и выполните команду:

```sh
<path_to_border_controller> <parameters>
```

где `<path_to_border_controller>` — путь к исполняемому файлу, `<parameters>` — список параметров (см. далее).

Например, запуск на **Windows** с минимально необходимым параметром `-d` (адрес TrueConf Server):

```sh
"C:\Program Files\TrueConf\tc_bc.exe" -d 10.110.10.10
```

Запуск на **Linux** с минимально необходимым параметром `-d`:

```sh
"/opt/trueconf/enterprise/etc/bc/tc_bc" -d 10.110.10.10
```

3.2. Добавление как службы или демона

Данный способ удобнее по ряду причин:

- процесс может быть запущен автоматически от имени системной учётной записи ОС (не требуется входа в сеанс пользователя), при этом остаётся возможность его управлением вручную;
- в пределах ОС можно сделать разные службы/демоны на базе одного приложения для направления трафика на несколько экземпляров TrueConf Server, не разворачивая множество виртуальных или физических серверов в DMZ;
- в журнале событий ОС будут записи о старте и остановке службы/демона, сообщения в случае проблем в работе и пр.

3.2.1. Добавление службы на Windows

Чтобы добавить компонент в список служб Windows, можно воспользоваться командой `New-Service` в PowerShell или утилитой **sc.exe** .

При этом для большей гибкости в дальнейшей поддержке расширения рекомендуем указать параметры не в списке после пути к исполняемому файлу, а в подключаемом файле конфигурации (смотрите параметр `-c`).

Создание службы с помощью **PowerShell**:

1. Запустите PowerShell от имени администратора.
2. Выполните команду вида:

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

```sh
$params = @{
  Name = "TrueConf Border Controller"
  BinaryPathName = "c:\trueconf\tc_bc.exe -c c:\trueconf\tc_bc.cfg --service"
  DisplayName = "TrueConf Border Controller"
  StartupType = "Automatic"
  Description = "This is a TrueConf Border Controller service."
}
new-service @params
```

где в параметре `BinaryPathName` укажите ваш путь к `tc_bc.exe` и расположение файла конфигурации. Обратите внимание, что наличие параметра `--service` является **обязательным**.

* Если путь, например, к файлу конфигурации, содержит пробелы, то его следует заключить в двойные кавычки " и экранировать их с помощью символа ` (обратная одинарная кавычка), например:

  ```sh
  `"c:\trueconf\trueconf\tc_bc.cfg`"
  ```

  Подробнее об этом читайте в документации PowerShell .

Создание службы с помощью утилиты **sc** через **cmd** (терминал):

1. Запустите **cmd** от имени администратора.
2. Выполните команду вида:

```sh
sc create TrueConf_Border_Controller binPath= ""C:\TrueConfBorderController\tc_bc.exe"
--service --ConfigFile C:\TrueConfBorderController\tc_bc.cfg"
DisplayName=TrueConf_Border_Controller type=own start=auto
```

3.2.2. Добавление демона на Linux

Для добавления демона на Linux надо создать для него файл запуска (называемый ***юнит***) в каталоге `/etc/systemd/system`. Например, для запуска от имени **root** с чтением файла конфигурации **tc_bc.cfg**:

1. В одной директории, например, `/opt/trueconf/enterprise/etc/bc/`, разместите исполняемый файл компонента **tc_bc** и конфигурационный файл **tc_bc.cfg**. Список параметров для файла конфигурации представлен ниже.
2. Создайте файл юнита, например, **tbc.service**, с помощью команды:

```sh
sudo nano /etc/systemd/system/tbc.service
```

3. Сохраните в файле следующее содержимое:

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

```sh
[Unit]
Description=TrueConf Border Controller
After=network.target

[Service]
ExecStart=/usr/bin/tbc.sh
Restart=always
RestartSec=3

[Install]
WantedBy=multi-user.target
```

4. По пути из параметра `ExecStart` разместить скрипт `tbc.sh`, в котором укажите команду запуска в виде:

```sh
#!/bin/bash
/opt/trueconf/enterprise/etc/bc/tc_bc -c /opt/trueconf/enterprise/etc/bc/tc_bc.cfg
```

5. Для обновления конфигурации в подсистеме **systemd** выполните команду:

```sh
sudo systemctl daemon-reload
```

6. Для ручного запуска демона выполните команду:

```sh
sudo systemctl start tbc.service
```

7. Проверить статус работы демона можно с помощью команды:

```sh
sudo systemctl status tbc.service
```

Созданный демон будет запускаться автоматически при старте системы и успешной проверке конфигурации сети.

* Подробнее о создании демона Linux читайте в документации к вашей версии ОС, или в общих руководствах, например на Linux Handbook.

3.3. Список параметров

Компонент TrueConf Border Controller для перенаправления трафика TrueConf поддерживает следующие параметры запуска (в скобках для некоторых представлены альтернативные варианты вызова).

3.3.1. Параметры командной строки (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.

3.3.2. Общие параметры

- `--Debug <level>` — уровень логирования от **0** (отключен) до **4**;

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

- `--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.

3.3.3. 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.

3.4. Пример файла конфигурации:

```
LogDirectory=/opt/trueconf/enterprise/etc/bc/logs/
Listen=10.140.10.123
Destination=10.110.10.10
Encryption=ChaCha20
```

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

4. Компонент для протокола HTTPS

Представляет собой исполняемый файл с именем **webproxy_windows_amd64** для Windows или **webproxy_linux_amd64** для Linux. Настройки для работы компонента указываются в файле конфигурации `webproxy.toml` как показано далее.

Компонент поддерживает три варианта запуска: из консоли, как служба Windows или демон Linux. Они настраиваются так же, как и для рассмотренного выше компонента для трафика TrueConf, но с рядом отличий:

- надо предварительно настроить работу с сертификатами;
- требуется рядом с исполняемым файлом создать конфигурационный файл **webproxy.toml**;
- файл запускается с параметром **run** (ниже подробнее использование на Windows и Linux).

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. 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.

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

4. 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.

5. 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. Создание файла конфигурации

В каталоге с исполняемым файлом компонента создайте файл конфигурации `webproxy.toml`

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

вида:

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

[dir]
executable_relative = true
installation = 'C:\TrueConf Border Controller'

[file]
configname = 'webproxy'

[interfaces]
[interfaces.list]
[interfaces.list.0]
Address = '[::]:443'
EnableTLS = true
ReadTimeout = 0
TLSConfigID = 'd25ceb20-f473-41dc-8db9-37f4dec1a3d1'
TargetID = 'a824b5cb-c92d-4a52-a5cc-434fecaba6a8'

[interfaces.list.1]
Address = '[::]:80'
EnableTLS = false
ReadTimeout = 0
TLSConfigID = ''
TargetID = '2f0dbf86-8378-41fc-9c5a-89a43728a0b7'

[proxy]
trust_client_headers = true

[targets]
[targets.list.a824b5cb-c92d-4a52-a5cc-434fecaba6a8]
address = '10.110.2.82:443'
is_secure = true

[targets.list]
[targets.list.2f0dbf86-8378-41fc-9c5a-89a43728a0b7]
address = '10.110.2.82:80'
is_secure = false

[tls]
[tls.list]
[tls.list.d25ceb20-f473-41dc-8db9-37f4dec1a3d1]
CertificateID = 'd25ceb20-f473-41dc-8db9-37f4dec1a3d1'
CertificateType = 'user-provided'
DisplayName = 'My TLS configuration'
ID = 'd25ceb20-f473-41dc-8db9-37f4dec1a3d1'
```

где укажите следующие значения:

- в разделе `[dir]`:
  - `installation` — путь к исполняемому файлу компонента;
- в разделе `[interfaces.list.0]`:

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru

- `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

Для запуска компонента из консоли выполните команду:

```sh
<path_to_border_controller> run
```

где `<path_to_border_controller>` — путь к исполняемому файлу. Например:

```sh
c:\Program Files\TrueConf\webproxy_windows_amd64.exe run
```

Создание службы аналогично рассмотренным для компонента **tc_bc** инструкциям, только в качестве пути к файлу (параметры `BinaryPathName` или `binPath`) надо указать `c:\Program Files\TrueConf\webproxy_windows_amd64.exe run`.

4.4. Запуск компонента на ОС Linux

Для запуска компонента из терминала выполните команду:

```sh
<path_to_border_controller> run
```

где `<path_to_border_controller>` — путь к исполняемому файлу. Например:

```sh
/opt/trueconf/enterprise/etc/bc/webproxy_linux_amd64 run
```

© 2010-2023 АО «ТКС». Все права защищены. www.trueconf.ru