

Безопасность коммуникаций

Как мы защищаем системы ВКС
от внешних угроз



Олег Кривонос

Директор по ИБ



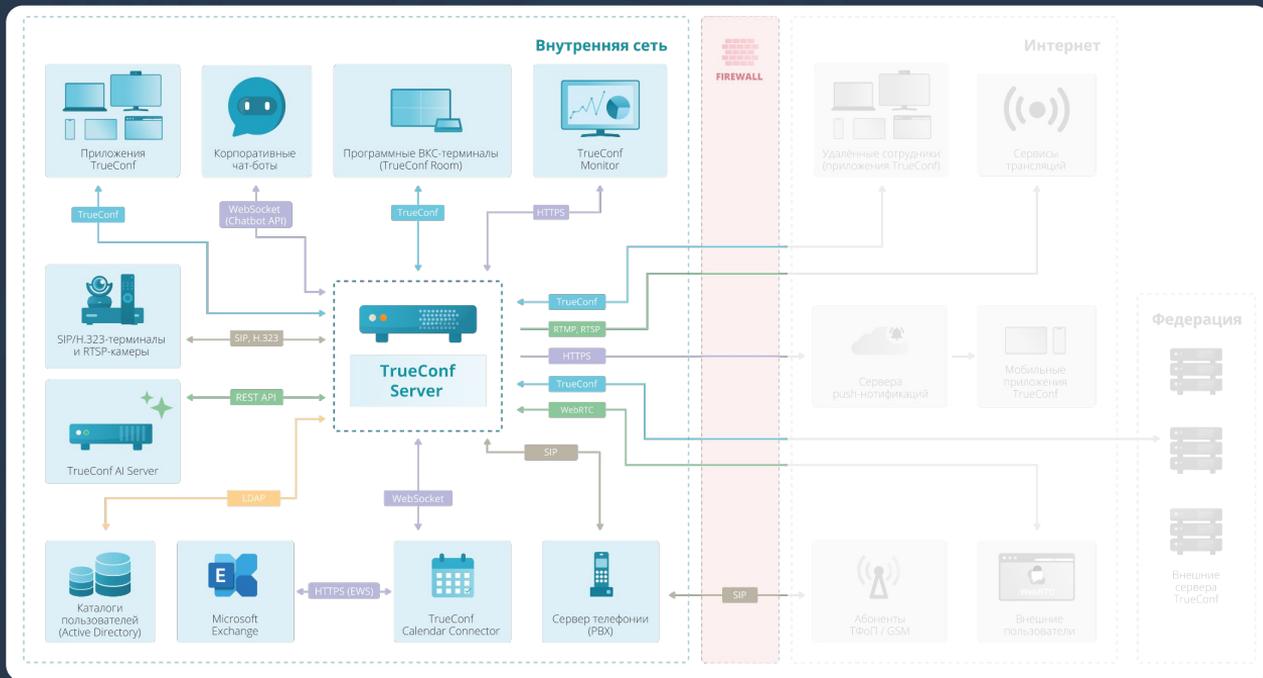
Лев Якупов

Директор по маркетингу



Рекомендация №2.

Архитектура. Оффлайн эксплуатация.



НИ ОДНА уязвимость
в БДУ не коснулась
оффлайн инсталляций

Рекомендация №2. Архитектура. Свой протокол.



TrueConf Server



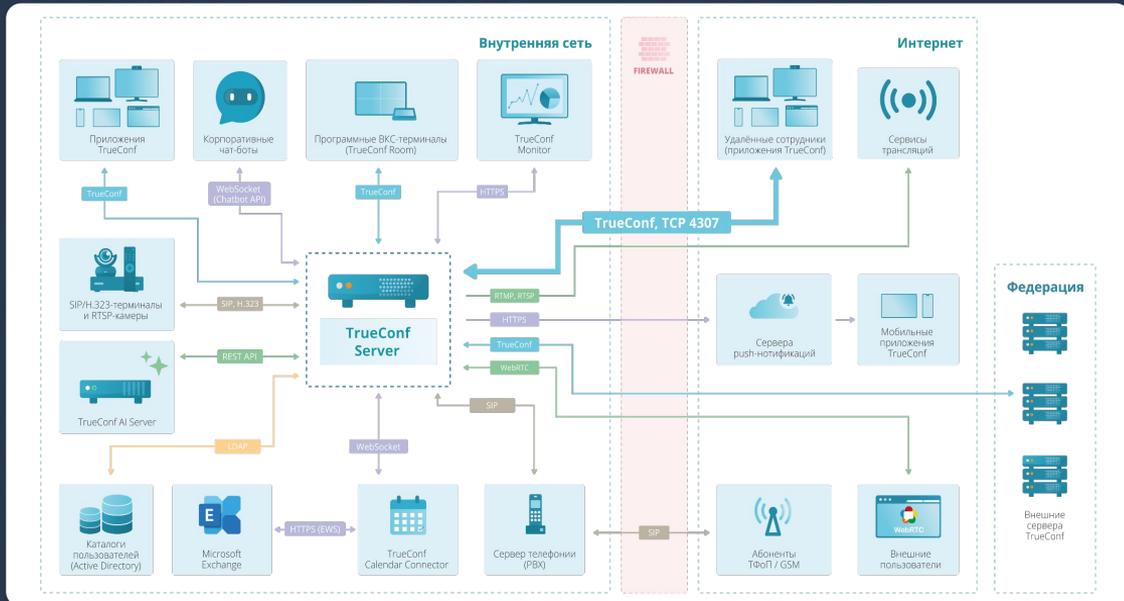
Сеть



Приложение
Труконф

- Все соединения устанавливаются в безопасном режиме
- Все соединения зашифрованы закодированы AES-256
- Внутри свой проприетарный протокол TrueConf

Рекомендация №3. Правильная настройка сети



- Снаружи необходимы только порты **4307** и **443** (не обязательный)
- UDP по умолчанию не используется

Рекомендация №3.

Правильная настройка сети



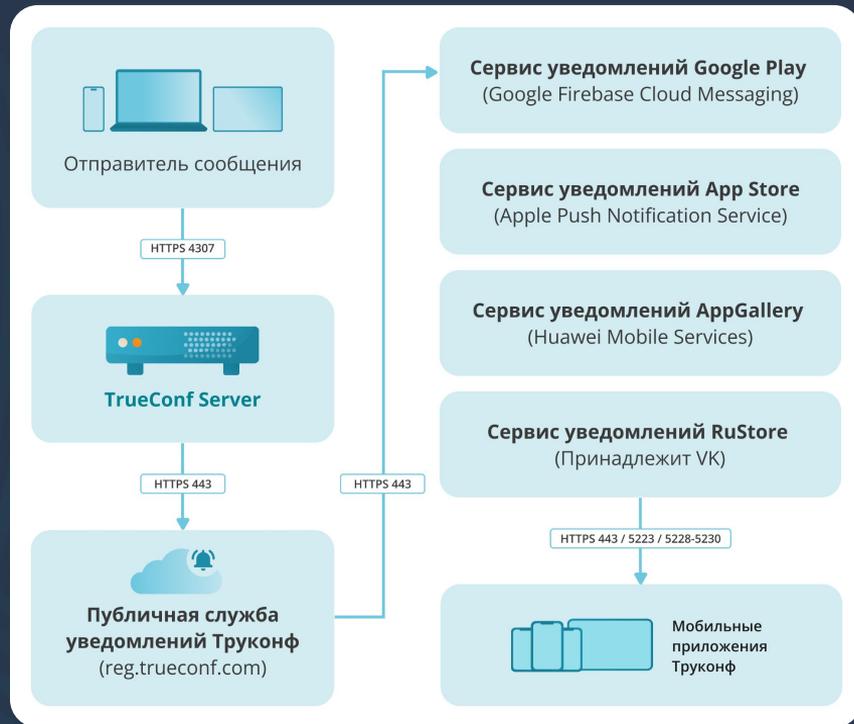
- **4307**: звук, видео, контент, файлы, сигнализация, сообщения чата и всё кроме того, что указано для порта 443.
- **443**: планировщик, личный кабинет, доставка слайдов.
- Все порты можно переназначать.

The image displays two screenshots of the TrueConf web interface. The top screenshot shows the 'Настройки сети' (Network Settings) page for 'video.example.com#vcs'. The 'Использовать все IP-адреса' (Use all IP addresses) checkbox is checked. The internal address field contains '10.110.2.240:4307' and 'fd00:110::14:3e5b]:4307'. The bottom screenshot shows the 'Настройки HTTPS' (HTTPS Settings) page for 'video.example.com#vcs'. The 'Режим работы HTTPS' (HTTPS mode) dropdown is set to 'Использовать самоподписанный сертификат' (Use self-signed certificate). The 'HTTPS порт' (HTTPS port) is set to '443'. The 'Используемые версии протокола TLS' (Used TLS protocol versions) checkboxes for 'TLSv1.2' and 'TLSv1.3' are both checked. A green 'Проверить конфигурацию' (Check configuration) button is visible at the bottom.

Рекомендация №3. Правильная настройка сети

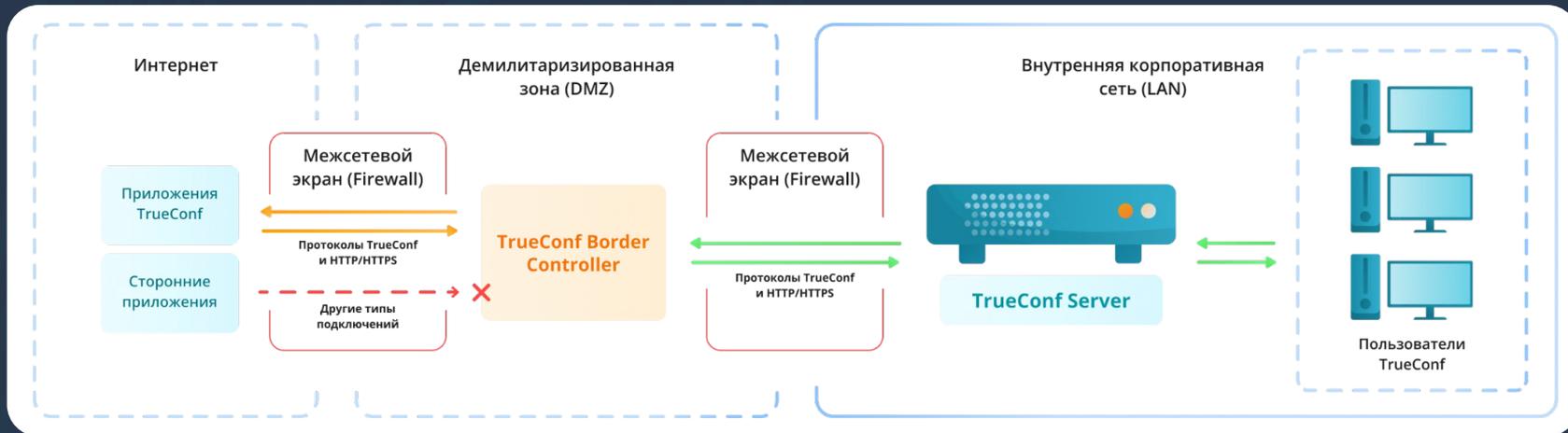


- Для пуш нотификаций необходимо исходящее соединение по **443** до `reg.trueconf.com`
- Все данные зашифрованы.
- Мы их не видим.

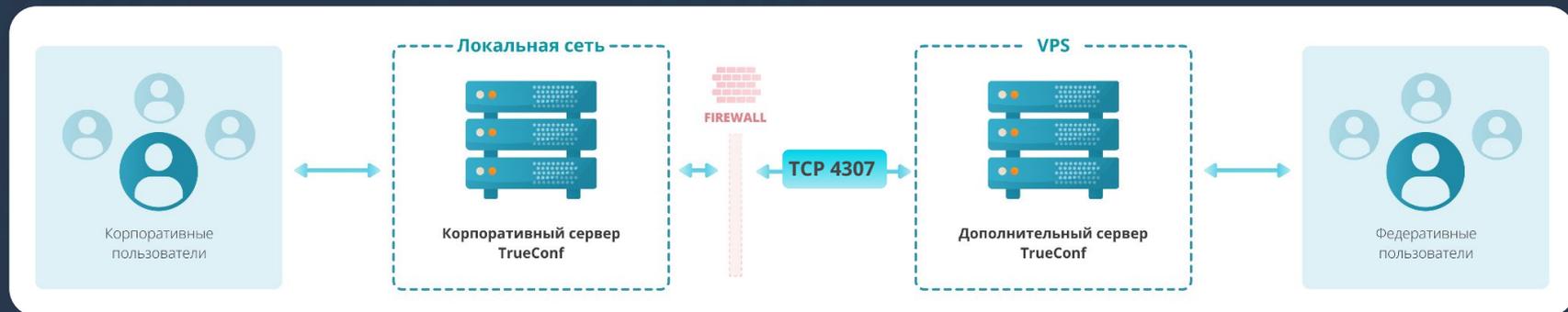
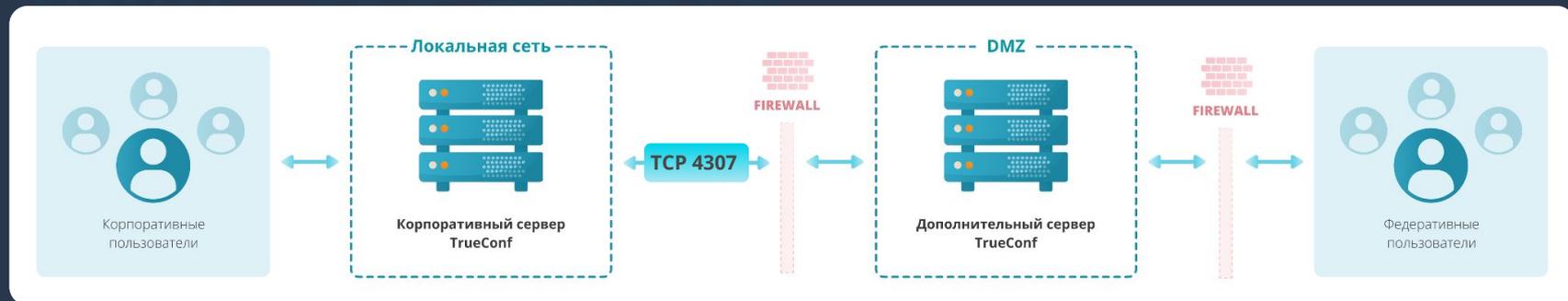


Рекомендация №4.

Использовать контроллер сессий



Рекомендация №5. Второй (федеративный) сервер в DMZ или VPS для гостей





Рекомендация №6. Правильная настройка ОС

- Специальная группа TrueConf Server Admin
- Доступ к панели управления ограничен списком доверенных подсетей

TrueConf video.example.com#vcs Система

Сеть

Настройки сети
SMTP
Федерация

Шлюзы
SIP
H.323
RTP
WebRTC
Транскодирование

Веб
Настройки
Безопасность
HTTPS
Пользователи
Учетные записи

Безопасность веб [Помощь ?](#)

Панель управления

Предоставить административный доступ:

членам локальной группы безопасности **tcadmins**

все пользователи Linux на **localhost**

Разрешить административный доступ с локальных адресов без авторизации

Ограничить доступ к разделу по IP

10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

TrueConf Server до 5.5.2

TrueConf video.example.com#vcs Система

Сеть

Настройки сети
SMTP
Федерация

Шлюзы
SIP
H.323
RTP
WebRTC
Транскодирование

Веб
Настройки
Безопасность
HTTPS
Пользователи
Учетные записи
Группы

Безопасность веб [Помощь ?](#)

Панель управления

Предоставить административный доступ:

членам локальной группы безопасности **TrueConf Server Admin**

все пользователи Windows на **localhost**

Ограничить доступ к разделу по IP

10.0.0.0/8
192.168.0.0/16
172.16.0.0/12

Добавить

TrueConf Server 5.5.2+

Рекомендация №7.

Правильные настройки для групп



TrueConf video.example.com#vcs Система [Помощь ?](#)

Веб

- Настройки
- Безопасность
- HTTPS

Пользователи

- Учетные записи
- Группы**
- Псевдоним
- Аутентификация
- LDAP / Active Directory

Групповые конференции

- Конференции
- Шаблоны
- Трансляции
- Настройки

Чаты

- Опросы
- API
- OAuth2

Группы

Список групп

Название группы [Создать](#)

	Название группы	Адресная книга	Прилож...	Группов... вызов	Права пользователей														
<input type="checkbox"/>																			
<input type="checkbox"/>	IT	Настр...	Настро...	Настро...	<input checked="" type="checkbox"/>	<input type="checkbox"/>													
	<u>Пользователи без группы</u>	Настр...	Настро...		<input checked="" type="checkbox"/>	<input type="checkbox"/>													
	Федеративные пользователи	Настр...	Настро...		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Гостевые пользователи	Настр...	Настро...		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Рекомендация №8.

Правильные настройки для зон сети



The screenshot displays the TrueConf management interface for the domain `video.example.com#vcs`. The interface is divided into several sections:

- Left Sidebar:** A navigation menu with categories like Веб, Пользователи, Группы, and Настройки. The 'Настройки' (Settings) section is expanded, showing options like Аутентификация, which is currently selected.
- Top Header:** Shows the TrueConf logo, the domain name, and a 'Система' dropdown menu.
- Main Content Area:**
 - Аутентификация (Authentication):** A table listing network zones and their authentication methods.

Зоны	Название	Способы аутентификации	Состояние
	Доверенная сеть	Логин и пароль	<input checked="" type="checkbox"/>
	Internet	Логин и пароль, NTLM SSO, AD FS	<input checked="" type="checkbox"/>

Способы аутентификации	Название	Статус	Состояние
	Логин и пароль	Активировано	<input checked="" type="checkbox"/>
	NTLM SSO	Активировано	<input checked="" type="checkbox"/>
	Kerberos SSO	Отключено, Не настроено	<input type="checkbox"/>
	AD FS	Активировано	<input checked="" type="checkbox"/>
	Microsoft Outlook SSO	Отключено, Не настроено	<input type="checkbox"/>
 - Редактирование зоны (Zone Editing):** A form for editing a specific zone. The 'Название' (Name) field contains 'Доверенная сеть'. Below it, the 'МАСКИ ПОДСЕТЕЙ' (Subnet Masks) field contains '10.0.0/8'. There are 'ДОБАВИТЬ' (Add) and 'ОТМЕНА' (Cancel) buttons.
 - СПОСОБЫ АУТЕНТИФИКАЦИИ (Authentication Methods):** A list of authentication methods with checkboxes and status information.
 - Логин и пароль
 - NTLM SSO: Этот способ аутентификации клиентские приложения используют по умолчанию
 - Kerberos SSO: Не настроено. [Перейти в настройки](#)
 - AD FS
 - Microsoft Outlook SSO: Не настроено. [Перейти в настройки](#)

Рекомендация №9. Использование DLP



The image displays the TrueConf web interface for configuring DLP integration. The browser address bar shows `video.example.com#vcs` and the page title is "Система".

Интеграция с DLP-системой

Данное расширение позволяет подключиться к сторонней DLP-системе, используя протокол ICAP (RFC 3507).

Активировать расширение

ICAP-сервер

Хост	Порт	Безопасное подключение
<input type="text" value="dozor.trueconf.loc"/>	<input type="text" value="2344"/>	<input type="text" value="Отсутствует"/>

Статус: DLP-система доступна (Mailfilter ICAP service)

Проверка текстовых сообщений

Включить

ICAP-запрос

```
REQMOD icap://%host:%port/ ICAP/1.0
Host: %host
Allow: 204
Connection: keep-alive
Encapsulated: req-hdr=0, req-body=%body_offset

POST / HTTP/1.1
Host: %server_name
X-Client-IP: %src_ip
```

Действие с нежелательным текстовым сообщением

Заменить текст сообщения на указанный в DLP-системе

Заменить текст сообщения на

Оставить без изменений

Ответы DLP-системы будут проигнорированы

Чаты

Димитрий Зуйков
В сети

Сегодня

Привет! 16:34

ⓧ Подозрительная активность! ⓧ изменено 16:34

Введите сообщение...

Рекомендация №10. Использование SSO



TrueConf
video.example.com#vcs Система

Веб
Настройки
Безопасность
HTTPS
Пользователи
Учетные записи
Группы
Псевдоним
Аутентификация
LDAP / Active Directory
Настройки
Групповые конференции
Конференции
Шаблоны
Трансляции
Настройки
Чаты
Опросы
API
OAuth2
Отчеты
Журнал событий
История звонков

Помощь ?

LDAP

Настройки сервера

Тип сервера: Active Directory

- Active Directory
- OpenLDAP
- 389 Directory Server
- FreeIPA
- ALD Pro
- Выборочно

Домен: example.com

Сервер: Порт: 636

Базовый DN: DC=example,DC=com

Безопасно
 Автоматически
 Ручная настройка

Аутентификация

Текущий пользователь: Имя: Пароль:

Группа с правом авторизации

Данная группа ограничивает список пользователей, которым разрешена авторизация на TrueConf Server.

Путь (distinguishedName): Обзор

Применить

++Дополнительно

MS Active Directory

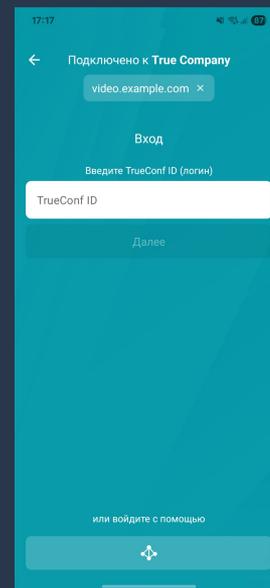
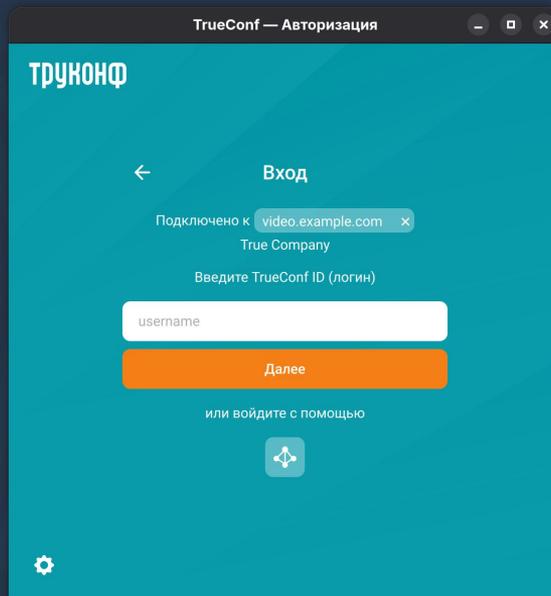
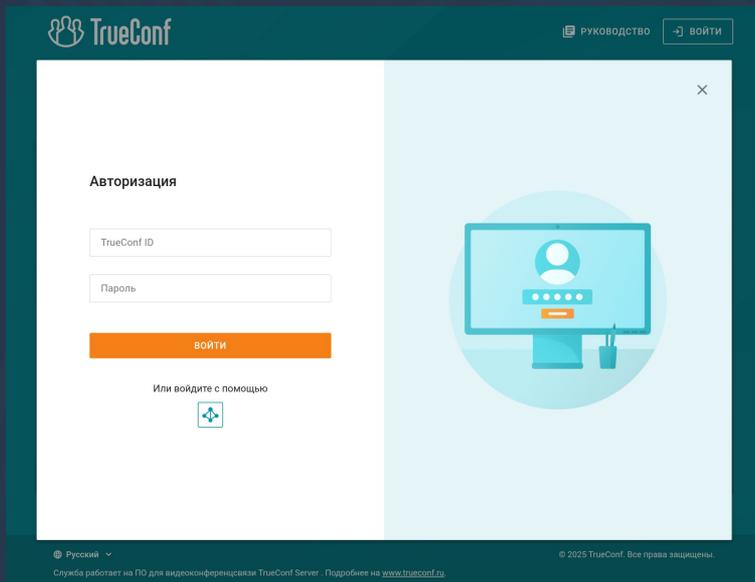
OpenLDAP

389 Directory Server

FreeIPA

ALP Pro

Рекомендация №11. Многофакторная аутентификация



Microsoft AD FS

Keycloak

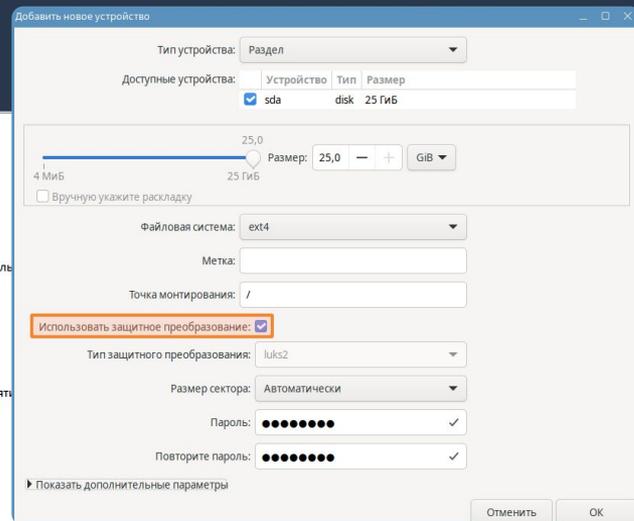
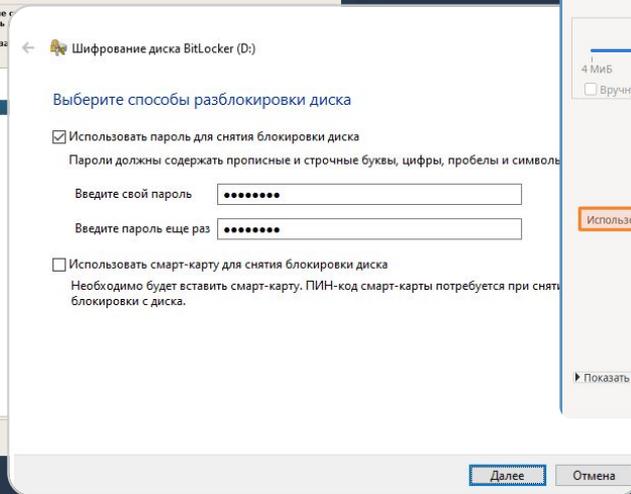
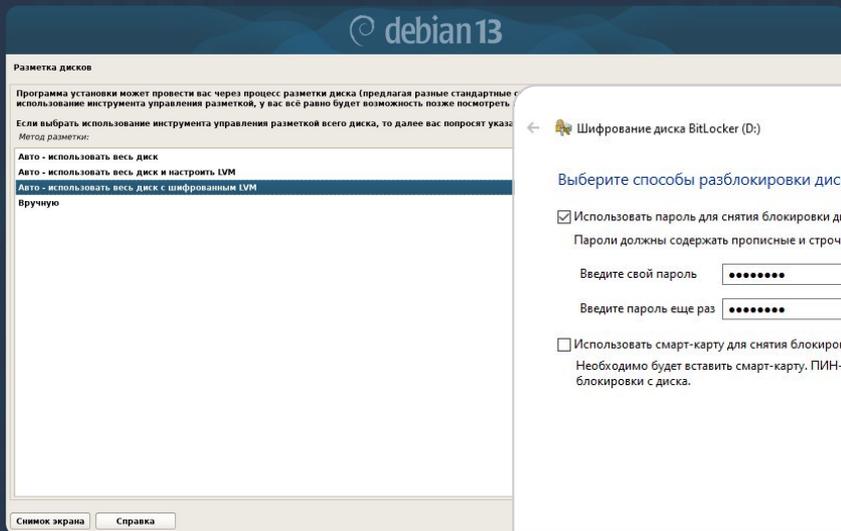
OpenID Connect

Indeed AM

Рекомендация №12.

Шифрование разделов диска

- Шифрование на уровне файловой системы (EncFS, eCryptfs)
- Шифрование блочных устройств



Рекомендация №13.

Ограничение доступа для некоторых ОС



TrueConf video.example.com#vcs Система

Панель управления
Информация о сервере
ПРО-лицензии
Настройки

Сеть
Настройки сети
SMTP
Федерация

Шлюзы
SIP
H.323
RTP
WebRTC
Транскодирование

Веб
Настройки

Приложение

Приложение	Текущая версия	Мин. версия	Последн. версия	Авторизация	URL Установки
TrueConf Android				<input checked="" type="checkbox"/>	https://play.google.com/store/apps/details?id=com.trueconf.videochat&hl=ru
TrueConf iOS	3.8.3	3.0	3.8.3	<input type="checkbox"/>	https://itunes.apple.com/ru/app/trueconf/id536475636
TrueConf Linux				<input checked="" type="checkbox"/>	
TrueConf OS X				<input checked="" type="checkbox"/>	
TrueConf Windows	8.5.2	7.2.1	8.5.2	<input checked="" type="checkbox"/>	https://10.110.2.240/downloads/trueconf_windows_client.exe

Рекомендация №14.

Ограничение на передачу файлов



TrueConf video.example.com#vcs Система

Отчеты

- Журнал событий
- История звонков
- Сообщения чата
- Изменения настроек
- Записи конференций
- Подключения
- Файловое хранилище
- Записи
- Расширения
 - TrueConf Directory
 - Интеграция с DLP
 - Почтовые плагины
 - TrueConf Calendar Connector
 - TrueConf AI Server
- Помощь
- Выйти

Ограничения на отправку файлов

Ограничить отправку файлов по размеру (МБ): 100

Ограничить отправку файлов по расширениям

Черный список

Список расширений файлов

BAS BAT CHM CMD COM CPL DLL EXE HLP JAVA JS LNK PIF REG SCR SHS SS

Расширения перечисляются через пробел и без точки перед ними

Замена заблокированного файла текстовым сообщением

Файл (%file_name) не может быть отправлен!

Применить

TrueConf <Дмитрий Зуйков>

Чаты

Антон Бааджи
был(а) в сети сегодня в 19:08

Сегодня

Привет! 16:34

Выбрано 1 файл

updater.exe
Недопустимый тип файла

Комментарий

Добавить Отмена Отправить

Введите сообщение...

Рекомендация №15.

Правильные настройки конференций



- Приватные быстрые конференции:
 - можно заранее задать список участников
 - закрыть вход после подключения всех нужных абонентов
- Для публичных конференций:
 - использовать ПИН
 - использовать комнату ожидания
- Для публичных комнат:
 - менять ПИН между сессиями

Присоединяйтесь
к сообществу
пользователей
Труконф!

