



Континент ZTN-клиент

Клиентское приложение для защищенного доступа в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников

 Единый криптографический клиент под все платформы: Windows, Linux, Аврора, Android, iOS, MacOS, iPadOS

 Подключение к Континент 3.9, Континент 4, Континент TLS

 Контроль внешней среды

Варианты использования

- Удаленный доступ пользователей к ресурсам защищаемой сети по шифрованному алгоритмами ГОСТ каналу.
- Защищенный доступ к корпоративным ресурсам:
 - С компьютеров;
 - С мобильных устройств.
- Поддержка браузеров при подключении к Континент TLS:
 - Яндекс
 - Google Chrome
 - Microsoft Edge
- Подключение удаленных небольших филиалов к корпоративной инфраструктуре.
- Обмен трафиком с защищенными сегментами сети для любых прикладных приложений .
- Проведение защищенных видеоконференций и обмен голосовыми сообщениями.
- Защищенный доступ к терминальным серверам/VDI.

Возможности

- Схемы аутентификации:
 - по логину и паролю;
 - по сертификатам ГОСТ 2012 (ТК26).
- Алгоритмы шифрования:
 - ГОСТ 28147-89;
 - ГОСТ Р 34.12-2015.
- Двусторонняя аутентификация с использованием сертификатов X.509v3.
- Поддержка различных ключевых носителей.
- Возможность установки VPN-соединения до регистрации пользователя в ОС.
- Возможность работы через HTTP-проxy сервер.
- Режим запрета незащищенных соединений.
- Режим перенаправления всего трафика в VPN туннель.

Контроль внешней среды

Контроль установленного ПО

Контроль целостности среды функционирования и файлов ZTN осуществляется:

- в начале работы Клиента;
- в ходе регламентного контроля;
- в момент установления соединения с сервером доступа;
- в момент установки соединения с защищенным ресурсом (режим TLS).

Контроль установленного ПО компании «Код Безопасности»:

- Secret Net Studio (версии 8.4.0.0 и новее);
- МСЭ SNS;
- Соболь (версии 3.0 и новее);
- Secret Net Studio - Antivirus (версии 8.4.0.0 или новее).

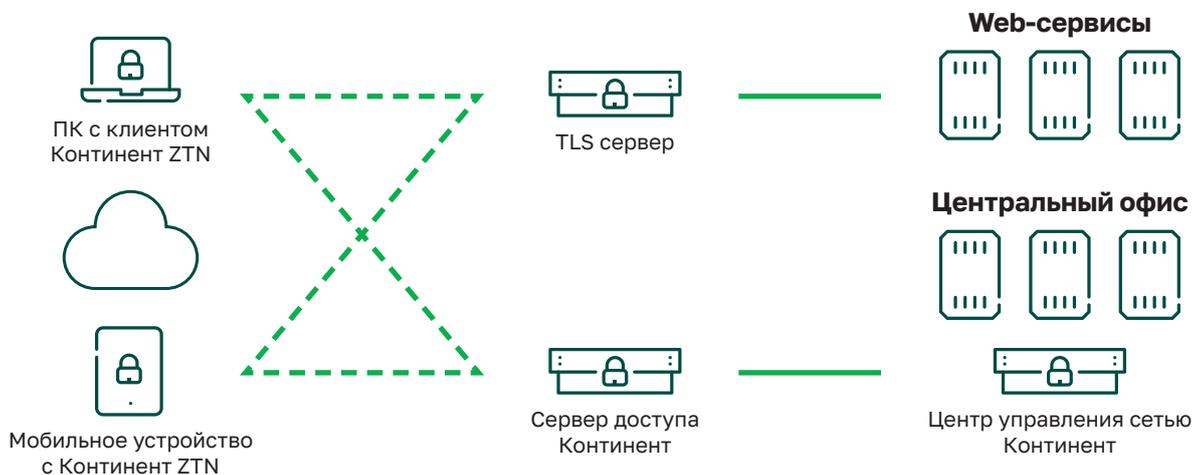
Контроль установленного стороннего ПО:

- Для пользовательских ОС:
 - Kaspersky Endpoint Security 10.0.0.0 или новее;
 - Kaspersky Internet Security 18.0.0.0 или новее;
 - Dr. Web Security Space 10.0.0.0 или новее;
 - Symantec Endpoint Protection 14.0.0.0 или новее;
 - ESET Security 11.1.0.0 или новее;
 - McAfee Total Protection 16.0.0.0 или новее;
 - Avast Internet Security 11.2.0.0 или новее.
- Для серверных ОС:
 - Kaspersky Endpoint Security 10.0.0.0 или новее;
 - Kaspersky Small Office Security 20.0.0.0 или новее;
 - Kaspersky Security 10.0.0.0 или новее;
 - Avira Antivirus 15.0.0.0 или новее;
 - Avast Business Security 19.0.0.0 или новее;
 - ESET File Security 6.5.0.0 или новее;
 - Платформа McAfee Endpoint Security 10.7.0.0 или новее;
 - Dr.Web Agent 11.0.0.0 или новее.

Поддерживаемые ОС:

- Windows:
 - Windows 8.1 x86/x64;
 - Windows 10 x86/x64 (не ниже версии 1909);
 - Windows 11 x64;
 - Windows Server 2012 R2 x64;
 - Windows Server 2016 x64;
 - Windows Server 2019 x64.
- Linux:
 - Astra Linux Special Edition «Смоленск» 1.6 x86_64 Desktop;
 - Astra Linux Common Edition «Орел» 2.12.43 x86_64 Desktop;
 - РЕД ОС 7.3 МУРОМ x86_x64 Server, Desktop;
 - Ubuntu 20.04.3 LTS x86_64 Server, Desktop;
 - Альт Рабочая станция 9.2 x86_64 Desktop;
 - ОС специального назначения Astra Linux SE «Смоленск» (исп. 1) (КСЗ).
- Аврора:
 - 3.2.3;
 - 4.0.1;
 - 4.0.3.
- Android:
 - Android 6 Marshmallow;
 - Android 7 Nougat;
 - Android 8 Oreo;
 - Android 9 Pie;
 - Android 10;
 - Android 11;
 - Android 12;
- IOS;
- MACOS (M1+M2).

Архитектура



Планы по сертификации

- Континент ZTN Клиент для Windows – СКЗИ класса КС1/КС2/КС3;
- Континент ZTN Клиент для Linux – СКЗИ класса КС1/КС2/КС3;
- Континент ZTN Клиент для Аврора – СКЗИ класса КС1;
- Континент ZTN Клиент для Android – СКЗИ класса КС1.

Лицензирование

- Клиентская часть отдельно не лицензируется;
- Используются лицензии для подключения к Серверу Доступа Континент или Континент TLS серверу;
- Лицензии на подключение не зависят от клиентской ОС

