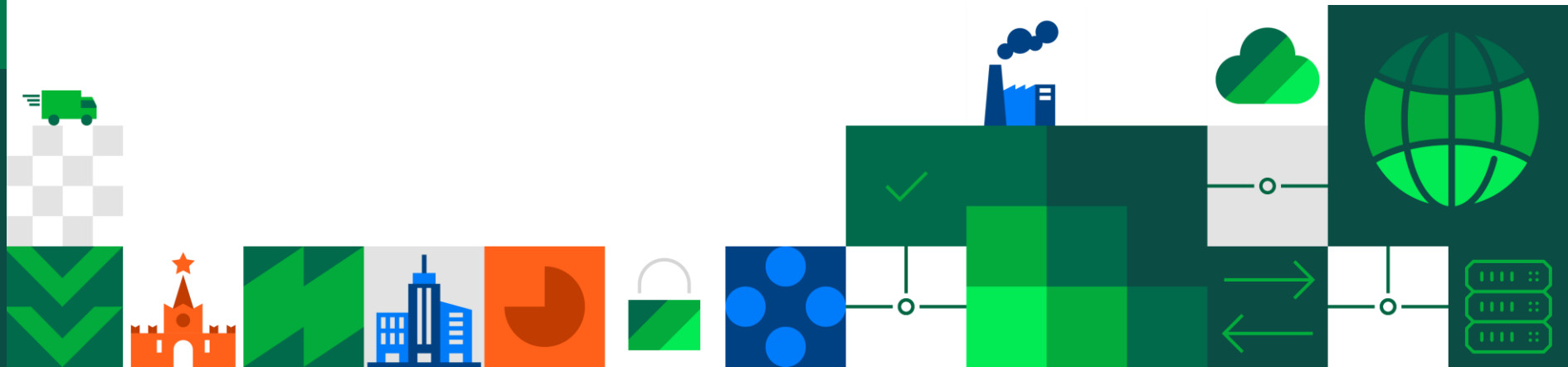
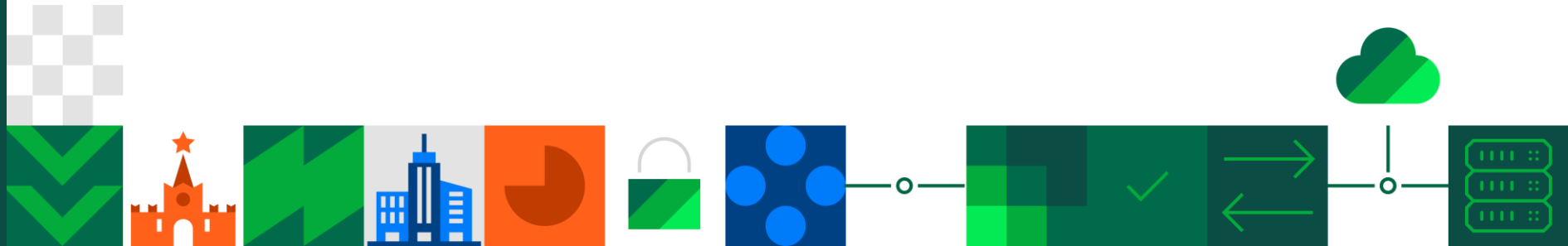
КОД безопасности

Континент 3.9.3 КС



КОД безопасности

О продукте



КОД безопасности

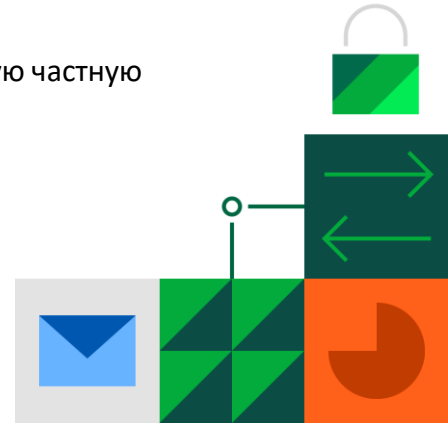
О продукте

Континент 3.9.3 КС

Централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов ГОСТ

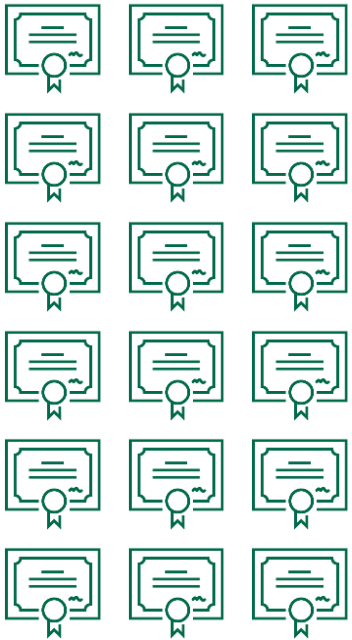
Предназначен для решения следующих задач:

- Криптографическая защита информации, передаваемой по открытым каналам связи
- Объединение филиалов организации в виртуальную частную сеть (VPN)
- Централизованная защита периметра корпоративной сети
- Защищенный удаленный доступ
- Обнаружение вторжений



КОД безопасности

Планы по сертификации



ФСТЭК России

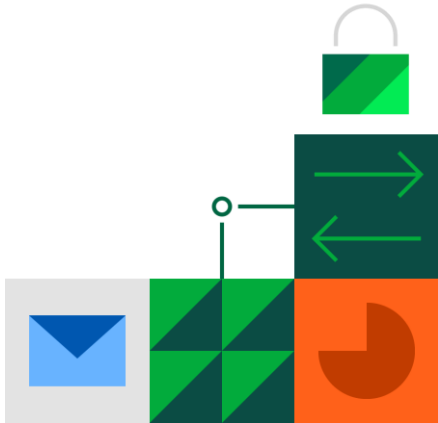
- 3-й класс защиты МЭ типа «А»
- 3-й класс защиты СОВ уровня сети
- 3-й уровень доверия

ФСБ России

- СКЗИ класса КС2/КС3
- Межсетевой экран 4 класса

Сертифицирован для защиты

- КИИ до 1 категории включительно
- ГИС до 1 класса защищенности включительно
- ИСПДн до класса У31 включительно
- АС до класса 1Г включительно



КОД безопасности

Архитектура Континент 3.9.3

Криптошлюз

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на сетевом уровне (создании L3 VPN-сети).

Криптокоммутатор

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне (создании L2 VPN-сети).

Детектор атак

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения в нем угроз безопасности.

Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент 3.

СКЗИ Континент АП/ZTN

VPN-клиент для подключения персональных компьютеров на базе Windows и Linux к Серверу доступа.

Сервер доступа

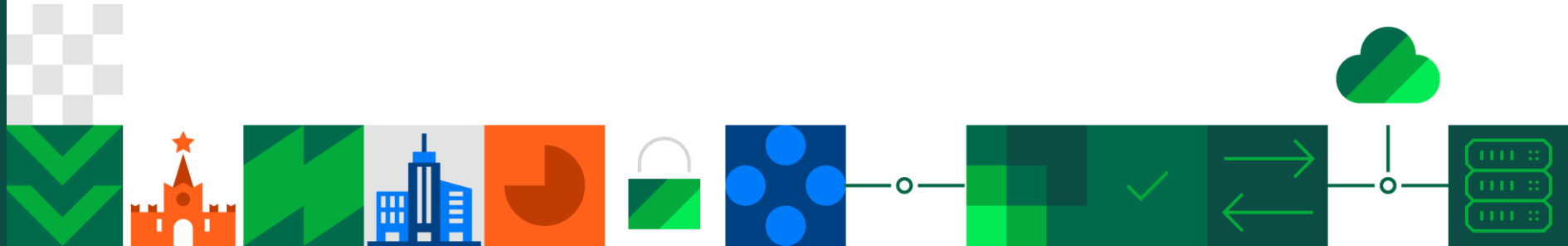
Аппаратно-программный комплекс, предназначенный для организации защищенного удаленного доступа с помощью VPN-клиента Континент АП/ZTN.

СКЗИ Континент АП/ZTN

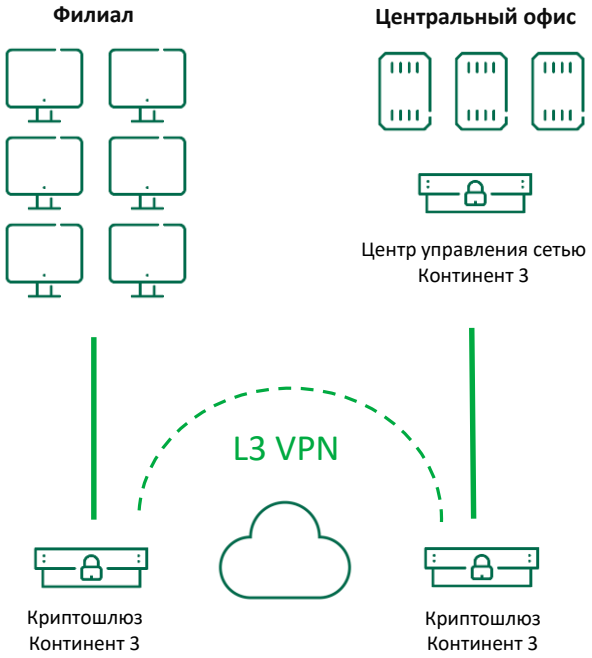
VPN-клиент для подключения мобильных устройств на базе Android, iOS/iPadOS и ОС Аврора к Серверу доступа.

КОД безопасности

Варианты применения



Объединение филиалов в единую сеть



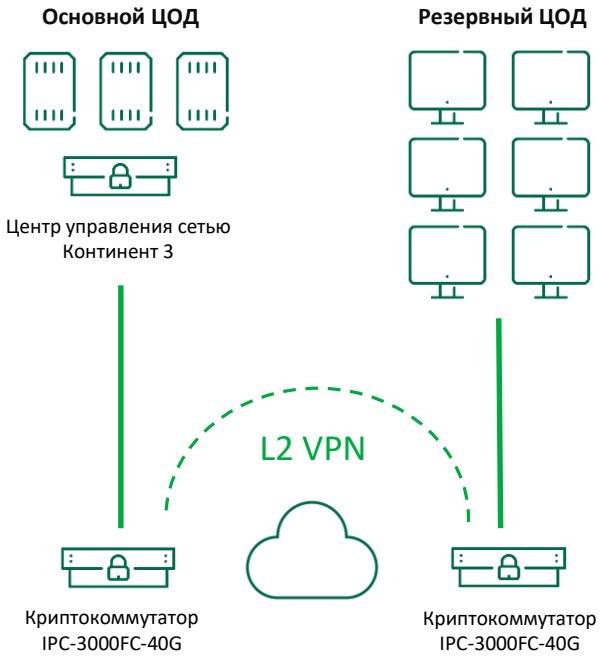
Задачи

- Защита доступа филиалов к ресурсам центрального офиса
- Защита трафика систем ВКС
- Подключение к СМЭВ
- Защита трафика ИСПДн, ГИС и СОПКА

Компоненты

- Центр управления сетью
- Криптошлюз

Защита канала между ЦОД



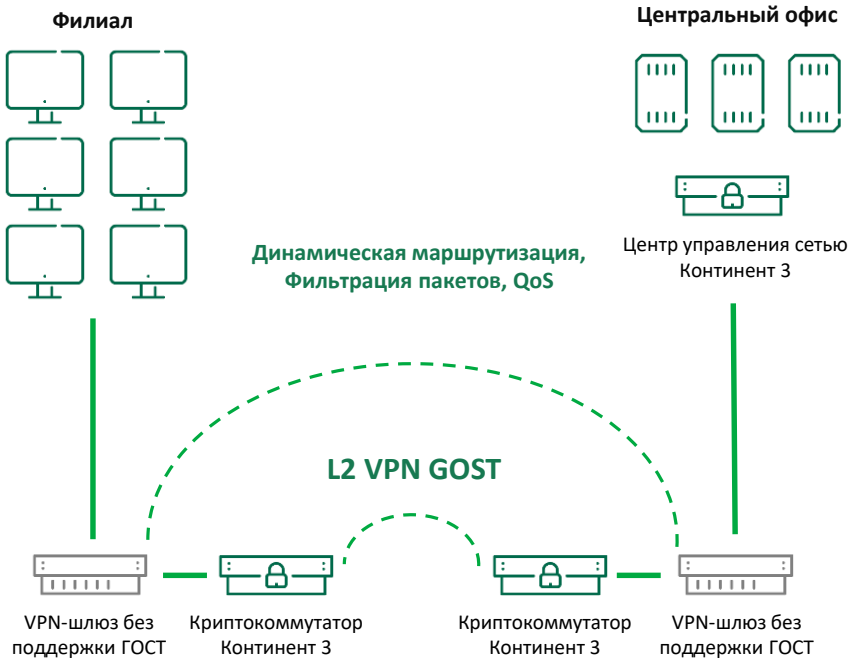
Задачи

- Защита канала между основным и резервным ЦОД
  - Репликация СХД
  - Кластеризация серверов приложений
- Обеспечение низкой задержки и показателя Round Trip Time

Компоненты

- Центр управления сетью
- Специализированный криптокоммутатор IPC-3000FC-40G

Наложенный ГОСТ



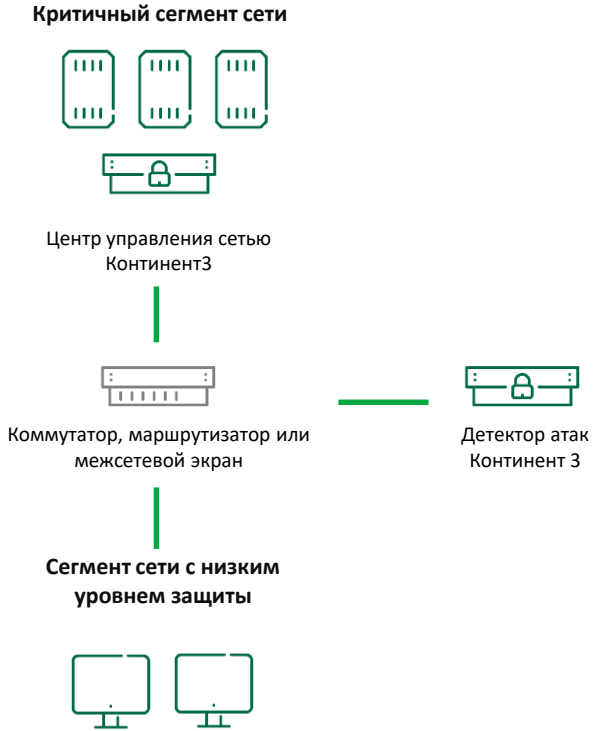
Задачи

- Развертывание VPN ГОСТ на существующей VPN-сети
- «VPN ГОСТ как услуга» для клиентов операторов связи

Компоненты

- Центр управления сетью
- Криптокоммутатор

Обнаружение вторжений



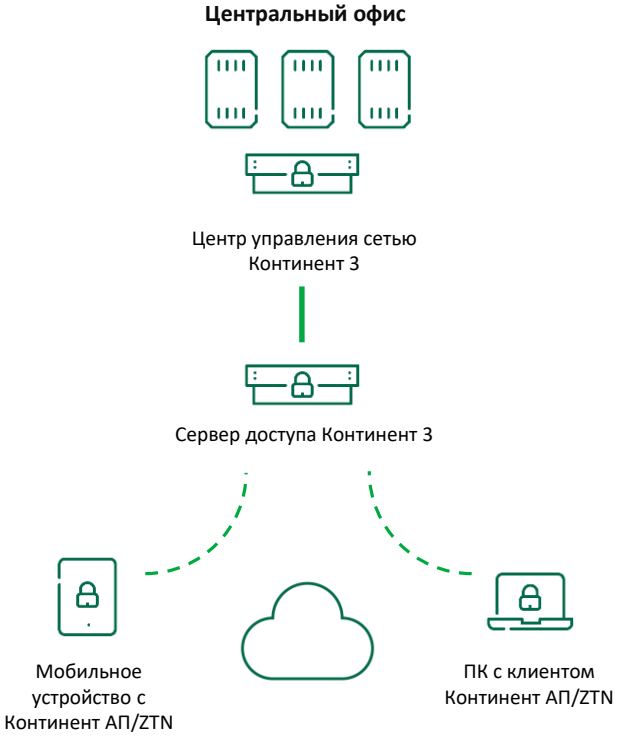
Задачи

- Обнаружение сетевых угроз
- Выполнение требований приказов ФСТЭК России
  - Приказ №21 (Защита ИСПДн)
  - Приказ №17 (Защита ГИС)
  - Приказ №239 (Защита КИИ)

Компоненты

- Центр управления сетью
- Детектор атак

Удаленный доступ



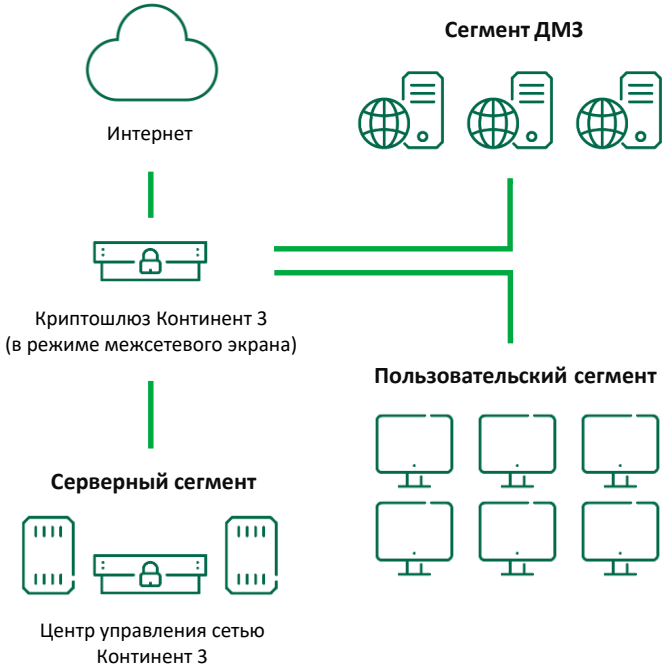
Задачи

- Защищенный доступ к корпоративным ресурсам
  - С компьютеров
  - С мобильных устройств
- Защищенный доступ к терминальным серверам/VDI

Компоненты

- Центр управления сетью
- Сервер доступа
- VPN-клиент Континент АП/ZTN клиент

Межсетевое экранирование



Задачи

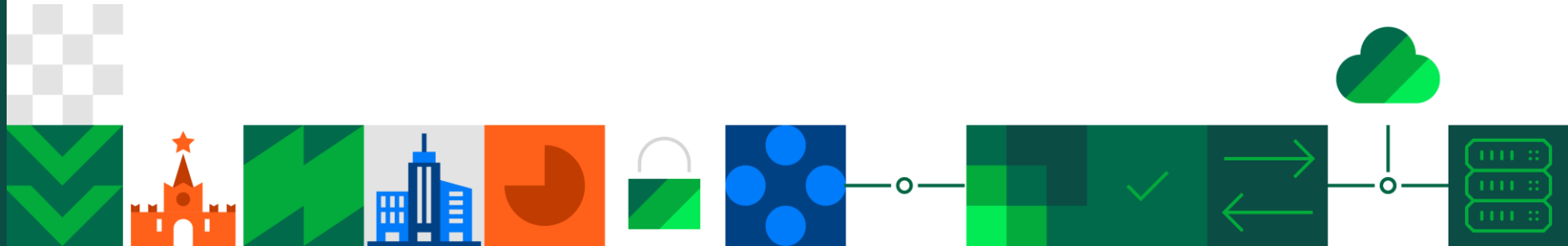
- Защита периметра сети
  - Контроль сетевых приложений
  - URL - фильтрация
- Единая база правил фильтрации и сетевых объектов для всех межсетевых экранов

Компоненты

- Центр управления сетью
- Криптошлюз (в режиме межсетевого экрана)

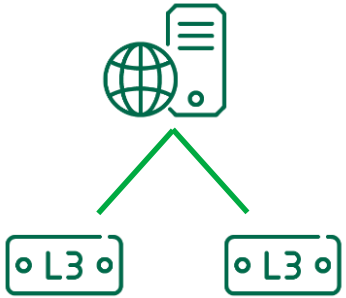
КОД безопасности

Компоненты



КОД безопасности

Управление инфраструктурой Континент 3



Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент 3

Централизованное управление

- Узлами сети
- Настройками маршрутизации
- Правилами фильтрации трафика
- VPN - связями
- Криптографическими ключами
- Параметрами SNMP

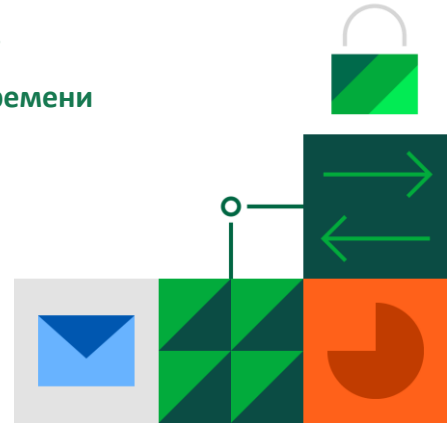
Утилиты для развертывания сетей new

Подключение устройств предыдущих версий new

Централизованное обновление ПО устройств

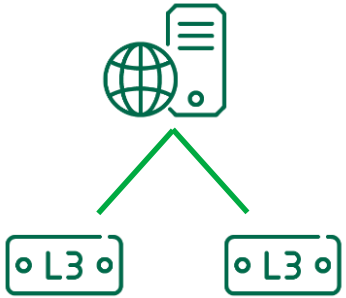
Мониторинг событий в режиме реального времени

Групповые операции над узлами



КОД безопасности

Управление инфраструктурой Континент 3



Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов Континент 3

Централизованный сбор и хранение журналов

Расширенная диагностика инфраструктуры

- Централизованный сбор отладочной информации узлов Континент 3
- Доступ к консоли узлов по протоколу SSH
- Удаленное создание локальных пользователей на узлах Континент 3

Интеграция с системами мониторинга сетевой инфраструктуры (SNMP)

Интеграция с системами мониторинга ИБ (SIEM)

Отказоустойчивость серверов управления

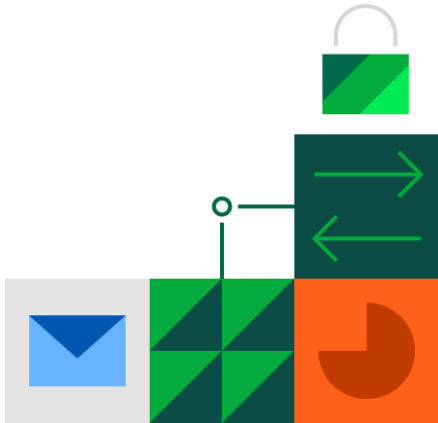
Просмотр статуса соединения с ЦУС из локального меню new

Межсетевое экранирование и VPN

Криптошлюз

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче
на сетевом уровне

- Детальный контроль HTTP и FTP
- Управление исключениями в HTTPS инспекции new
- Инспекция внутри SSL-туннеля
- Профили усиленной фильтрации
- Идентификация и аутентификация пользователей
- Поддержка технологии Stateful Inspection
- Проверка NTP-сервера new



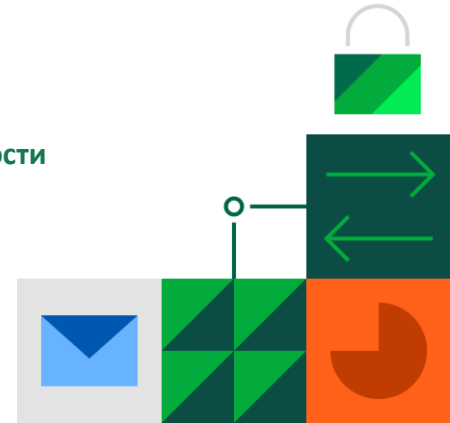
КОД безопасности

Межсетевое экранирование и VPN

Криптошлюз

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче
на сетевом уровне

- Поддержка QoS, ToS и Traffic shaping
- Работа с метками ToS new
- Резервирование каналов связи
- Резервирование полосы пропускания для управляющего трафика new
- Поддержка IPv6 для WAN
- Поддержка Multicast-маршрутизации
- Поддержка VLAN
- Работа в режиме кластера высокой доступности
- Адаптация к изменению MTU new



КОД безопасности

Межсетевое экранирование и VPN

Криптошлюз

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче
на сетевом уровне

Маршрутизация трафика

- Статическая
- Динамическая
  - RIP
  - OSPF
  - BGP

Поддержка NAT

- Source NAT
- Destination NAT

Возможность работы КШ за NAT

Доступ к сети за несколькими КШ new

Агрегация интерфейсов по протоколу LACP

Встроенный DHCP-сервер с поддержкой настройки provisioning server и DHCP-relay

Расширенные настройки на DHCP-сервере

КОД безопасности

Межсетевое экранирование и VPN

Криптокоммутатор

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне

Шифрование данных в соответствии с ГОСТ 34.12-2018 (Магма) в режиме гаммирования с обратной связью

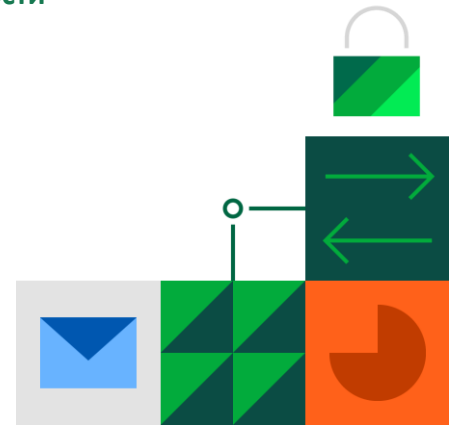
Защита данных от искажения осуществляется по ГОСТ 34.12-2018 (Магма) в режиме выработки имитовставки

Работа в едином адресном пространстве

Работа в режиме кластера высокой доступности

Поддержка Jumbo-frame (MTU до 9000 байт)

Адаптация к изменению MTU new

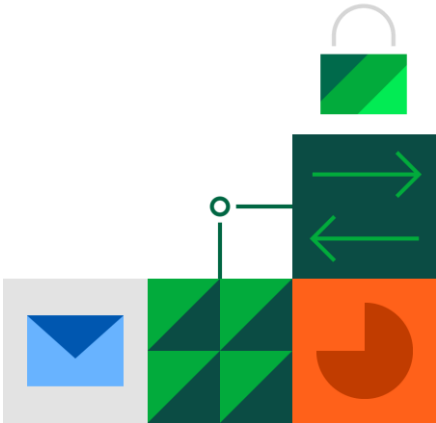


Межсетевое экранирование и VPN

Криптокоммутатор

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне

- **Туннелирование MPLS-трафика**
- **Линейное увеличение производительности**
- **Классификация трафика по ToS**
- **Резервирование полосы пропускания для управляющего трафика** new



КОД безопасности

Обнаружение вторжений

Детектор атак

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения в нем угроз безопасности

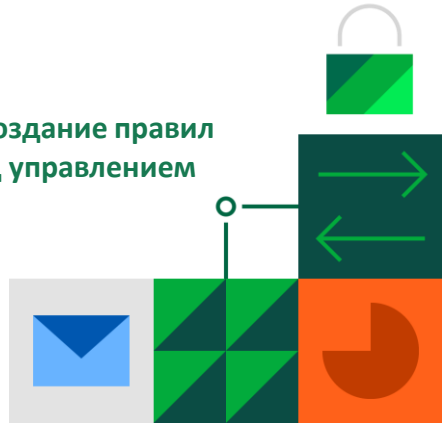
Регулярное обновление сигнатур (базы решающих правил, БРП)

Сочетание сигнатурного и эвристического методов анализа трафика

Поддержка протоколов различных уровней

- Транспортного уровня
- Сетевого уровня
- Сеансового уровня
- Прикладного уровня

Автоматическое получение данных от ДА и создание правил блокировки трафика на КШ, работающих под управлением одного ЦУС



КОД безопасности

Удаленный доступ

Сервер доступа **Континент АП/ZTN**

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче
на сетевом уровне

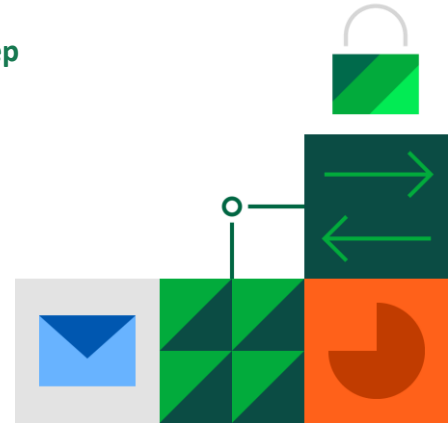
Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26)

Аутентификация пользователей по сертификатам стандарта X.509

Поддержка различных ключевых носителей

Возможность установки VPN-соединения до регистрации пользователя в ОС

Возможность работы через HTTP-proxy сервер



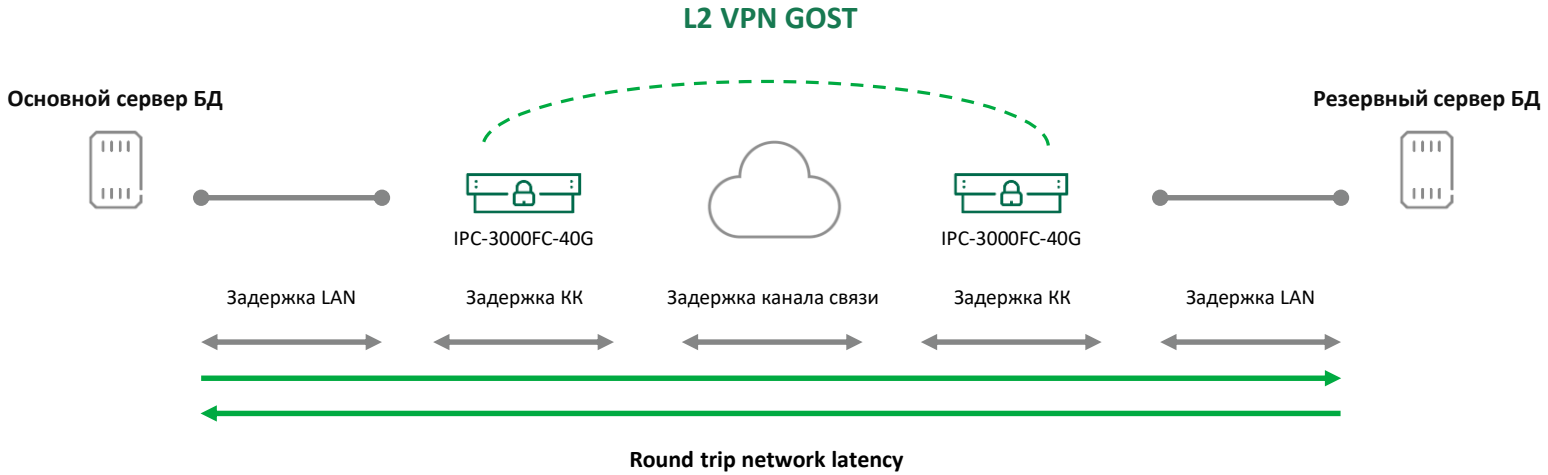
КОД безопасности

Высокопроизводительное шифрование

Платформа	**IPC-3000FC-40G**
Формфактор	Специализированная аппаратная платформа для построения защищённого VPN-канала
Производительность шифрования	40 Гбит/с с минимизацией задержек при передаче трафика

КОД безопасности

Важность задержки при резервировании СУБД



Round trip network latency
время затраченное на передачу пакета плюс время до получения пакета-подтверждения.

Он состоит из:

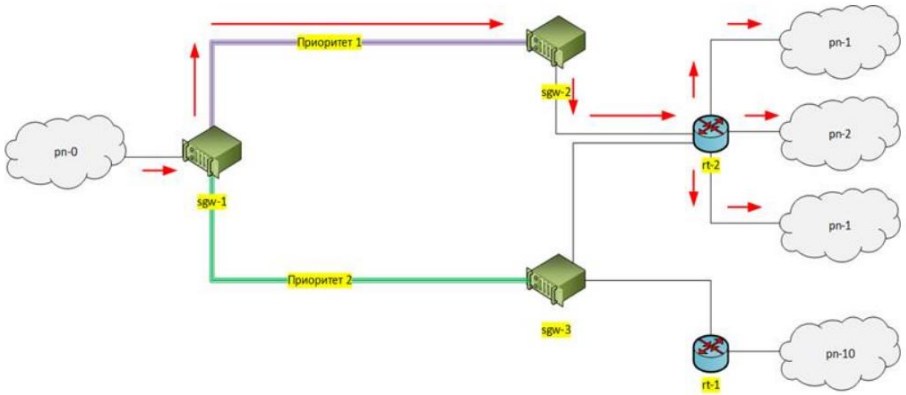
- задержка криптокоммутатора
- задержка локальной сети
- задержка канала связи

Задержка криптокоммутатора должна минимально влиять на общую задержку передачи данных

КОД безопасности

Функции Континент 3.9.3 для защиты территориально распределенных сетей

Защита объекта за разными КШ new

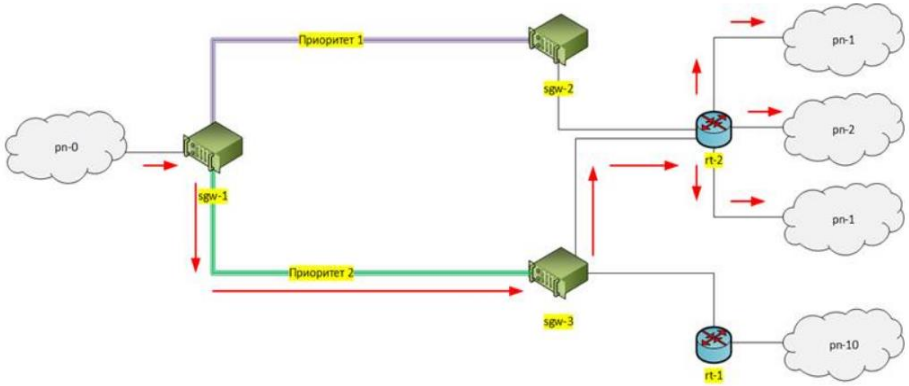


- Возможность доступа к одной защищаемой сети через несколько криптошлюзов, без переконфигурирования всей сети вручную
- Отказоустойчивое подключение
- Балансировка нагрузки
- Упрощение и удешевление развертывания

КОД безопасности

Функции Континент 3.9.3 для защиты территориально распределенных сетей

Защита объекта за разными КШ new



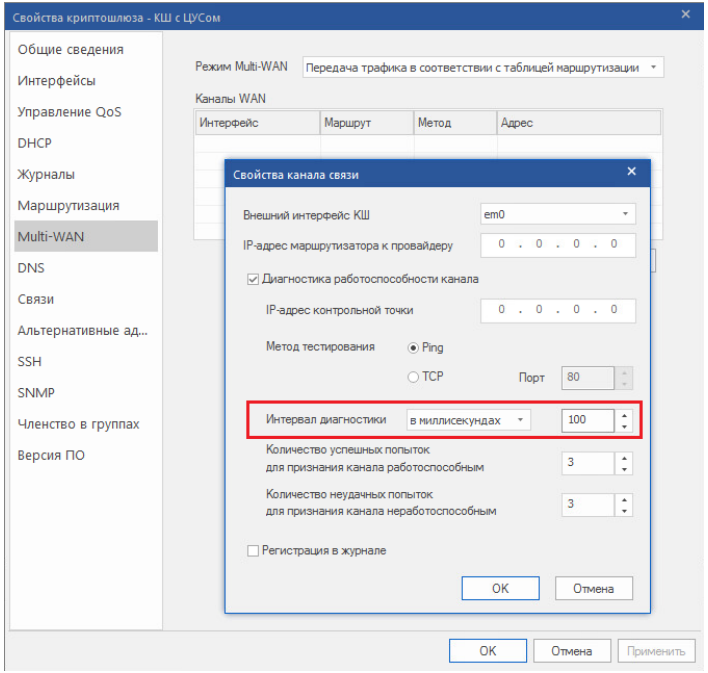
Организация доступа к ЗС pn-1 и pn-2 через КШ sgw-3, если доступ к приоритетному КШ sgw-2 отсутствует

- Возможность доступа к одной защищаемой сети через несколько криптошлюзов, без переконфигурирования всей сети вручную
- Отказоустойчивое подключение
- Балансировка нагрузки
- Упрощение и удешевление развертывания

КОД безопасности

Функции Континент 3.9.3 для защиты территориально распределенных сетей

Быстрый Multi-WAN



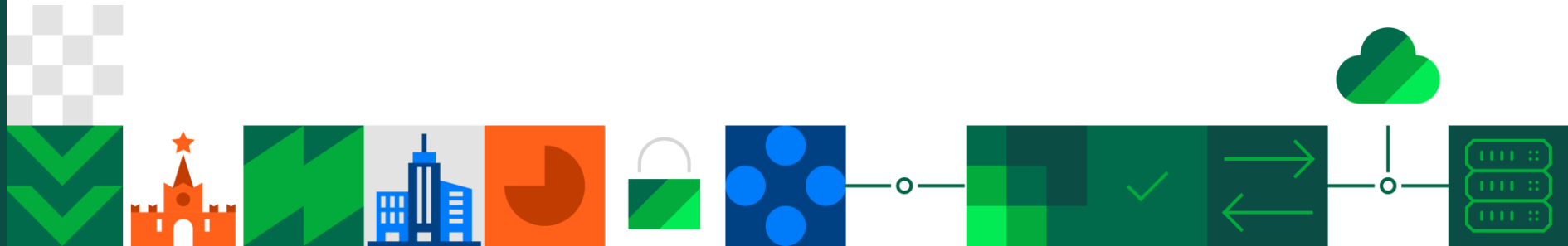
Снижение интервала диагностики работоспособности канала до 100 миллисекунд

Быстрое переключение на резервный канал без разрыва соединения

Бесперебойная видео-конференц-связь

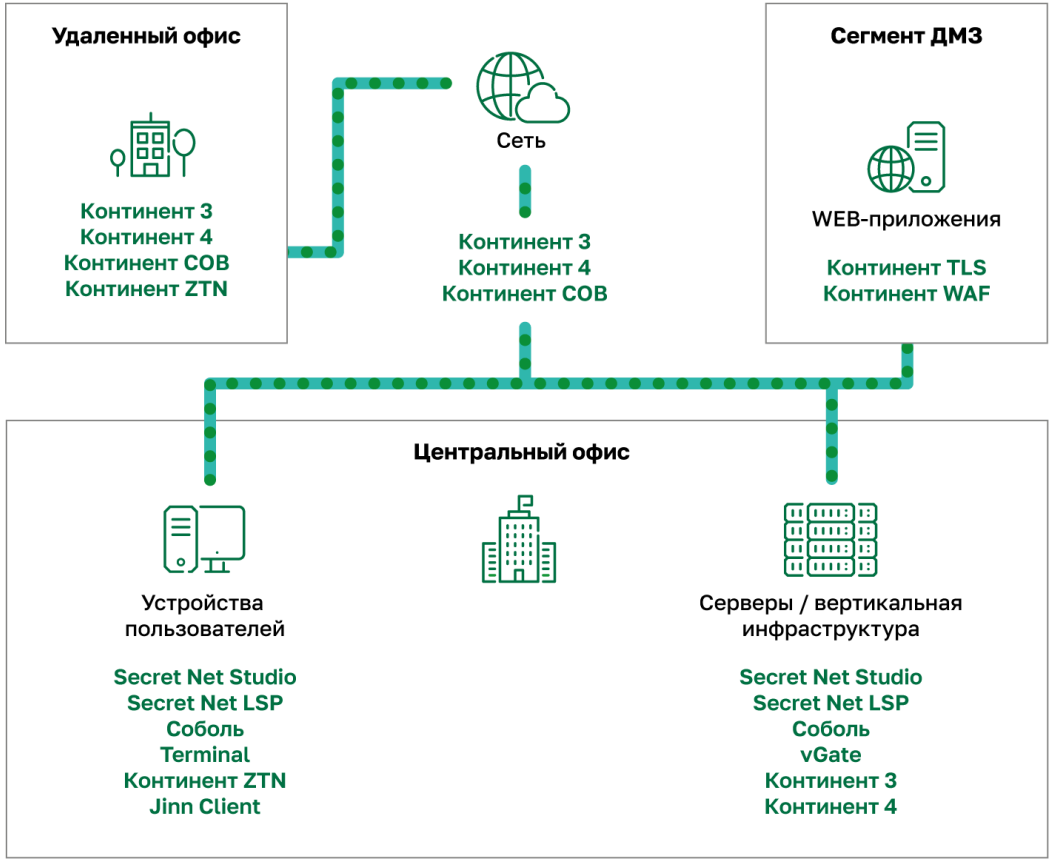
КОД безопасности

О компании



КОД безопасности

Комплексный подход к защите инфраструктуры



КОД безопасности

Факты о компании

«Крупнейшие производители высокотехнологичного оборудования»

«Крупнейшие разработчики ПО»

«Крупнейшие ИТ-компании России»

- Более **30 лет** на страже безопасности крупнейших предприятий России
- **9 лицензий** ФСТЭК, ФСБ и Минобороны России
- **3 центра разработки:** Москва, Санкт-Петербург, Пенза
- Более **800 квалифицированных специалистов R&D**, имеющих уникальные компетенции
- Более **50 разработанных СЗИ и СКЗИ**
- Более **60 сертификатов** соответствия
- Обеспечена безопасность **3 000 000 компьютеров** в **50 000 организаций**
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров**

КОД безопасности

Нам доверяют

Государственные организации:

- Федеральное казначейство России
- Федеральная налоговая служба России
- Федеральная таможенная служба России
- Федеральный Фонд обязательного медицинского страхования
- Центральная избирательная комиссия Российской Федерации
- Министерство юстиции Российской Федерации

Силовые структуры:

- Министерство внутренних дел Российской Федерации
- Министерство обороны Российской Федерации
- Федеральная служба безопасности Российской Федерации
- Федеральная служба охраны Российской Федерации

Телекоммуникационные компании:

- ПАО «Ростелеком»
- ПАО «МГТС»
- ГК «АКАДО Телеком»
- АО «Военателеком»

Финансовые организации:

- ПАО «Сбербанк»
- Центральный банк Российской Федерации
- ГК «Внешэкономбанк»
- АО «Газпромбанк»
- ПАО «Промсвязьбанк»
- Банк ВТБ (ПАО)
- ПАО «Московский кредитный банк»
- АО «АЛЬФА-БАНК»

Промышленные предприятия:

- ГК «Ростех»
- АО «Российские космические системы»
- ПАО «ГМК «Норильский никель»

Предприятия ТЭК:

- ГК «Росатом»
- ПАО «Газпром»
- ПАО «АК «Транснефть»
- ПАО «НК «Роснефть»»
- ПАО «Россети»

КОД безопасности

info@securitycode.ru
www.securitycode.ru