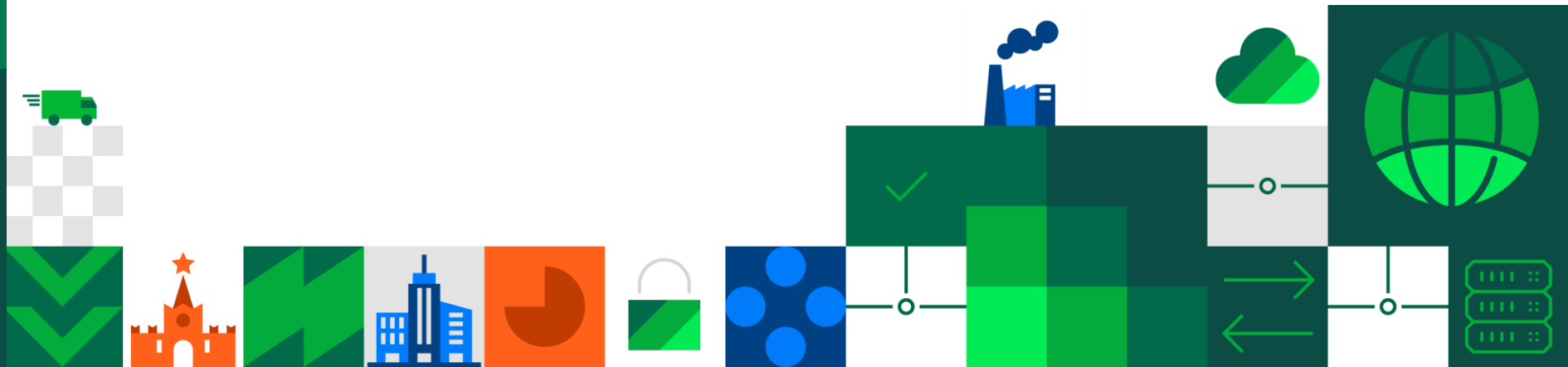
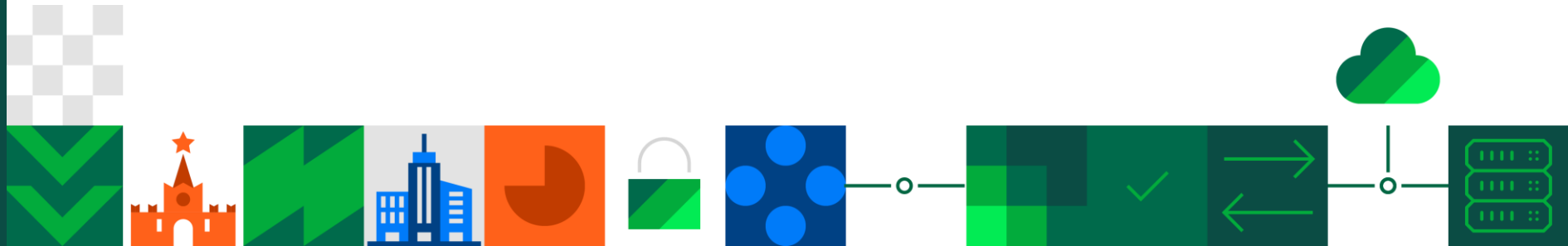
КОД безопасности

Континент 3



КОД безопасности

О продукте



КОД безопасности

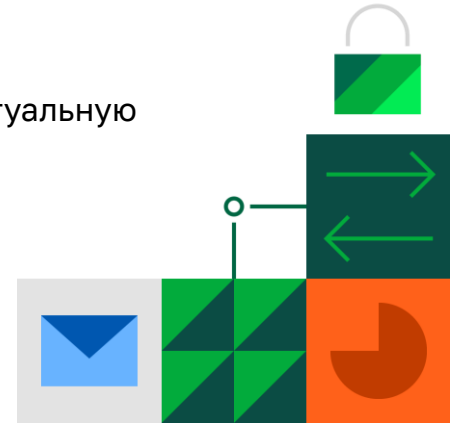
О продукте

Континент 3.9

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

Сертификация

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 УЗ1 включительно
- АС до класса 1Г включительно

КОД безопасности

Архитектура Континент 3.9

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

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

Сервер доступа

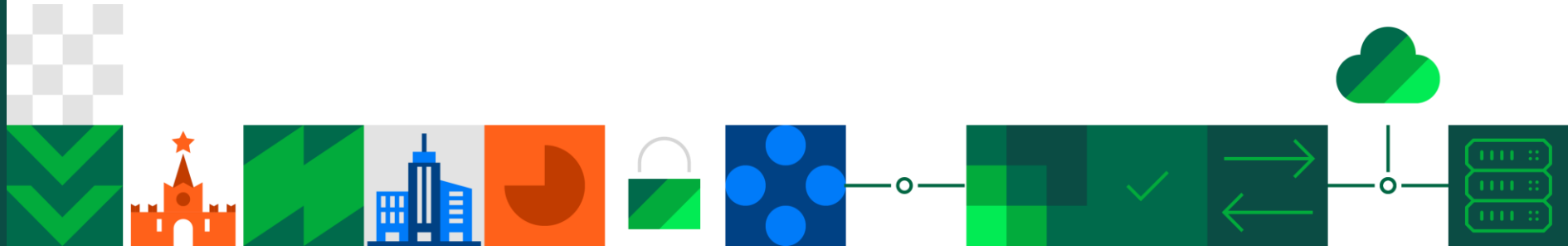
Аппаратно-программный комплекс, предназначенный для организации защищенного удаленного доступа с помощью VPN-клиента Континент АП.

СКЗИ Континент АП

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

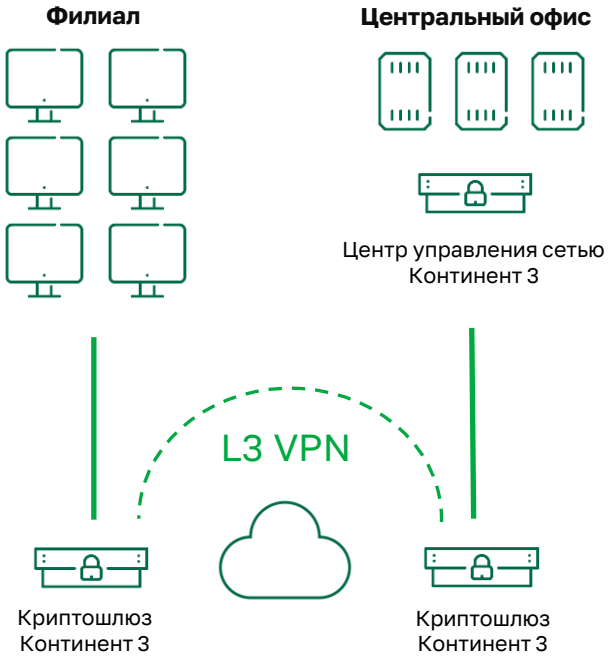
КОД безопасности

Варианты применения



КОД безопасности

Объединение филиалов в единую сеть



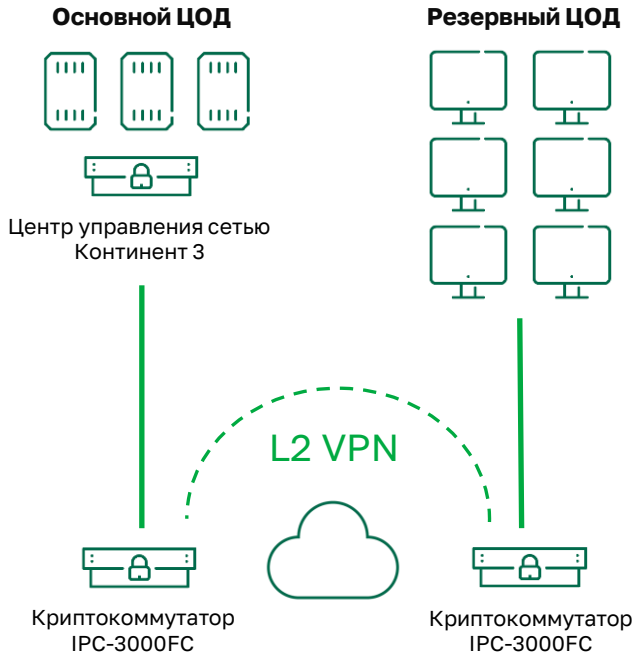
Задачи

- 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

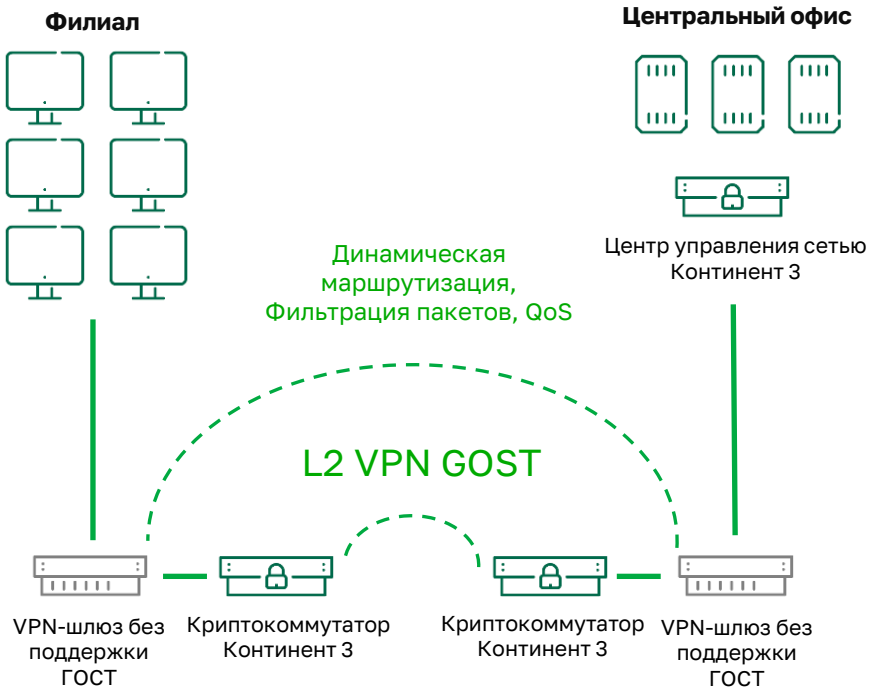
- Защита канала между основным и резервным ЦОД
  - Репликация СХД
  - Кластеризация серверов приложений
- Обеспечение низкой задержки и показателя Round Trip Time

Компоненты

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

КОД безопасности

Наложенный ГОСТ



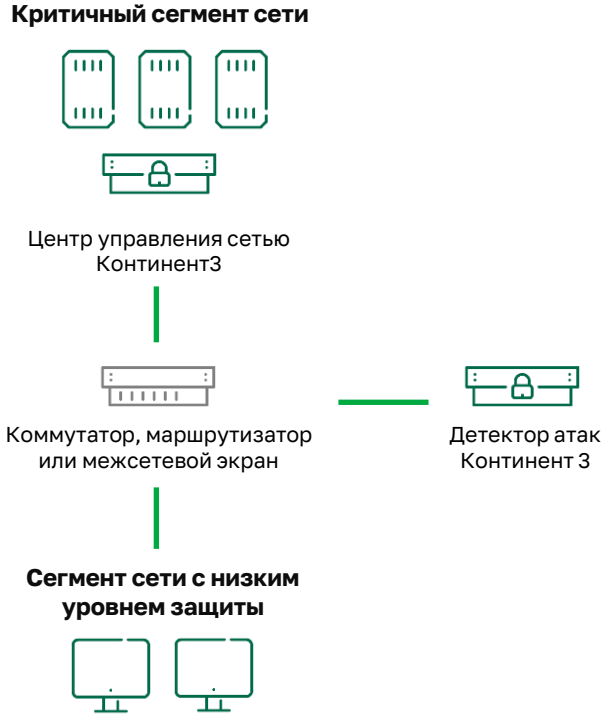
Задачи

- 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

КОД безопасности

Удаленный доступ

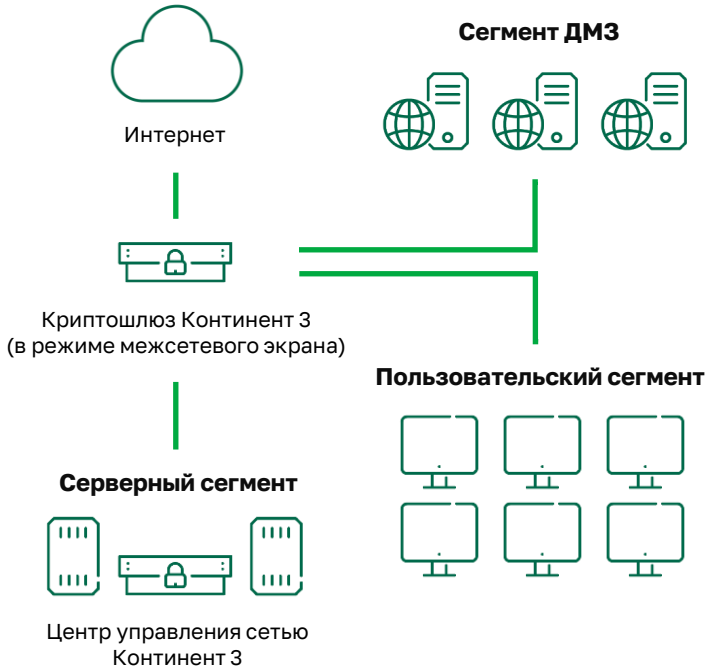
Задачи

- 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

Межсетевое экранирование



Задачи

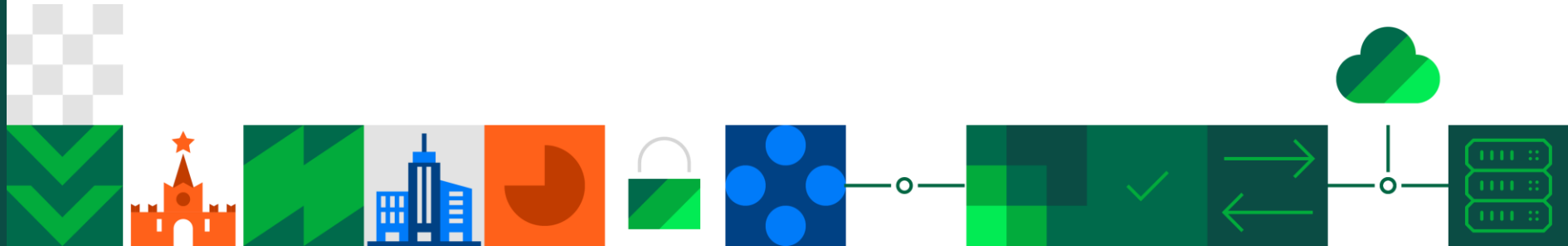
- Защита периметра сети
  - Контроль сетевых приложений
  - URL - фильтрация
- Единая база правил фильтрации и сетевых объектов для всех межсетевых экранов

Компоненты

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

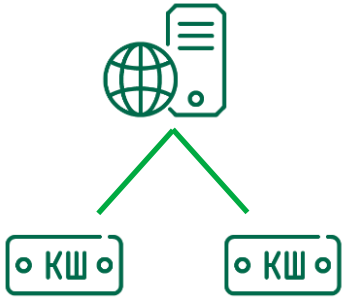
КОД безопасности

Компоненты



КОД безопасности

Управление инфраструктурой Континент 3



Центр управления сетью

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

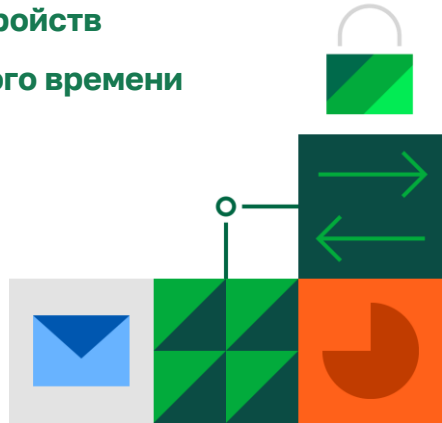
Централизованное управление

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

Централизованное обновление ПО устройств

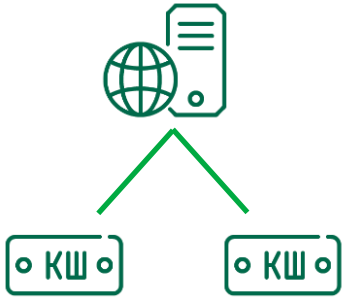
Мониторинг событий в режиме реального времени

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

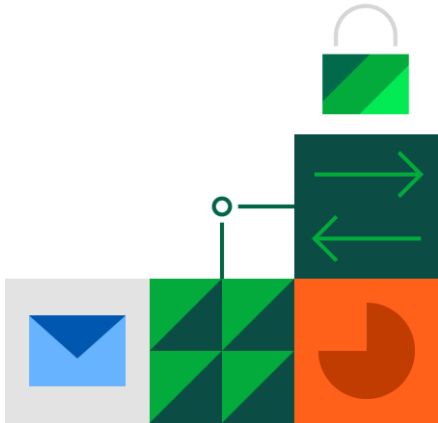
КОД безопасности

Межсетевое экранирование и VPN

Криптошлюз

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

- **Детальный контроль HTTP и FTP**
- **Инспекция внутри SSL-туннеля**
- **Профили усиленной фильтрации**
- **Идентификация и аутентификация пользователей**
- **Поддержка технологии Stateful Inspection**



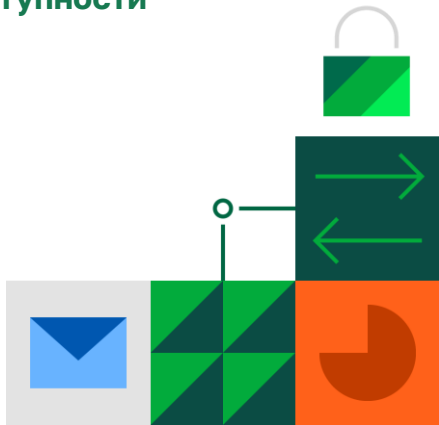
КОД безопасности

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**
- **Резервирование каналов связи**
- **Поддержка IPv6 для WAN**
- **Поддержка Multicast-маршрутизации**
- **Поддержка VLAN**
- **Работа в режиме кластера высокой доступности**



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

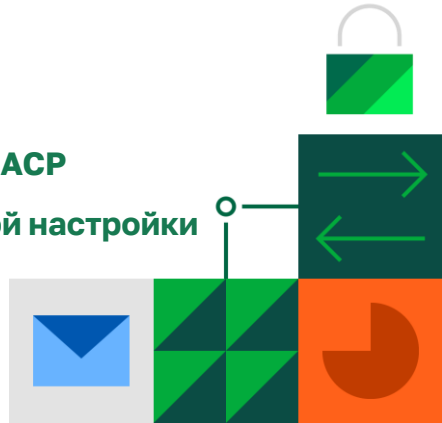
- Source NAT
- Destination NAT

Возможность работы КШ за NAT

Доступ к сети за несколькими КШ

Агрегация интерфейсов по протоколу LACP

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



КОД безопасности

Межсетевое экранирование и VPN

Криптокоммутатор

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

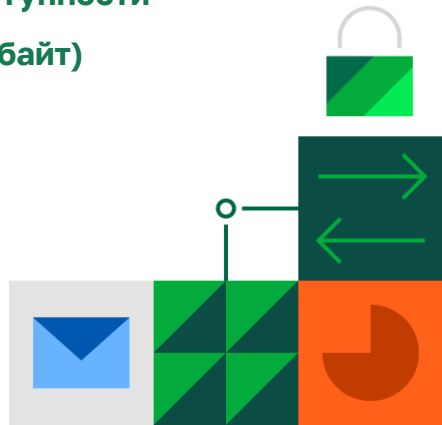
Шифрование данных в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью

Алгоритм имитозащиты данных – ГОСТ 28147–89 в режиме выработки имитовставки

Работа в едином адресном пространстве

Работа в режиме кластера высокой доступности

Поддержка Jumbo-frame (MTU до 9000 байт)



КОД безопасности

Межсетевое экранирование и VPN

Криптокоммутатор

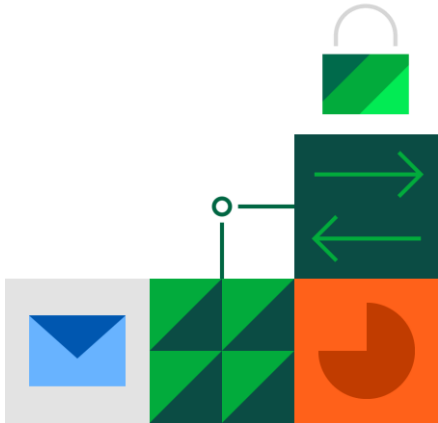
Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне

Туннелирование MPLS-трафика

512 портов виртуального коммутатора

Линейное увеличение производительности

Классификация трафика по ToS



КОД безопасности

Обнаружение вторжений

Детектор атак

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

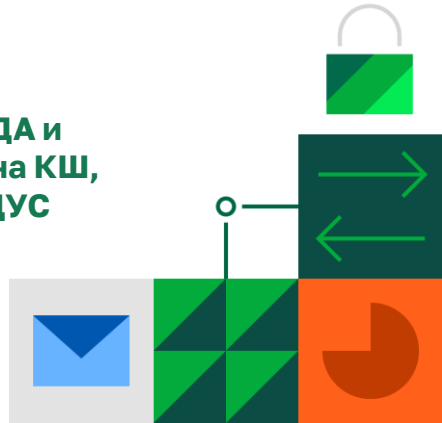
Регулярное обновление сигнатур (базы решающих правил, БРП)

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



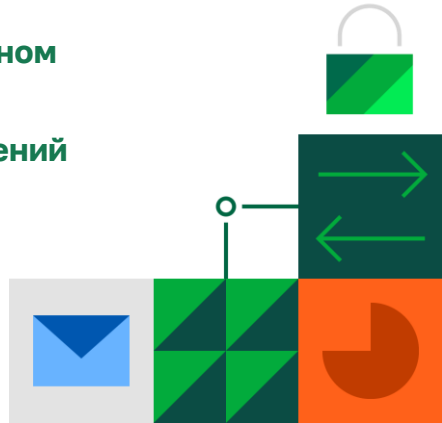
КОД безопасности

Удаленный доступ

Сервер доступа **Континент АП**

Аппаратно-программный комплекс и клиентское ПО, установленное на персональное устройство, предназначенные для криптографической защиты передаваемого трафика

- **Клиентские приложения для всех популярных платформ**
- **Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26)**
- **Поддержка различных ключевых носителей**
- **Возможность установки VPN-соединения до регистрации пользователя в ОС**
- **Объединённый TLS и VPN клиенты в одном инсталляторе**
- **Режим запрета незащищенных соединений**



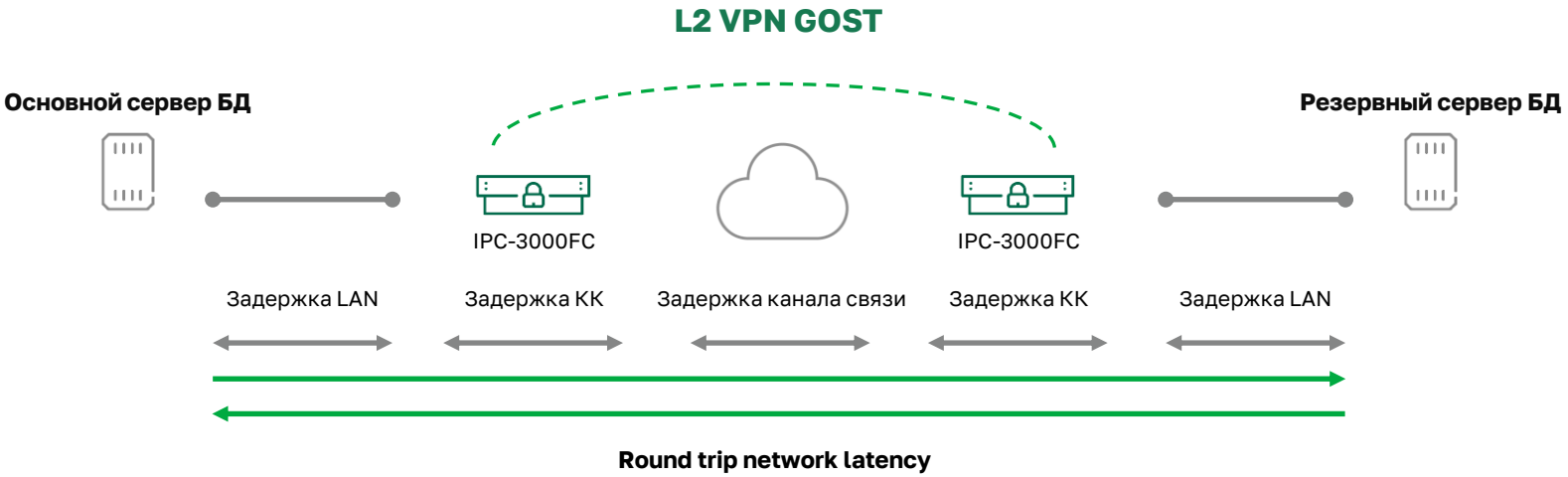
КОД безопасности

Высокопроизводительное шифрование

Формфактор	Семейство специализированных аппаратных платформ для построения защищённого VPN-канала
Производительность шифрования	20 Гбит/с 40 Гбит/с
Особенности	Минимизация задержек при передаче трафика На обычной платформе показатель задержки минимум в два раза больше, а чаще всего – на порядок
Модельный ряд	IPC-3000FC IPC-3000FC-H IPC-3000FC-40G

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