КОД безопасности

Комплексная защита сети от «Кода Безопасности»

Рынок сетевой безопасности

Доли рынка

Сетевая безопасность от «Кода Безопасности»:

1. **Континент 3:**
   - КС – VPN-шлюз / Криптошлюз для защиты каналов связи по классу КС
   - КВ – VPN-шлюз / Криптошлюз для защиты каналов связи по классу КВ
2. **Континент 4:**
   - NGFW – многофункциональный межсетевой экран
   - IDS/IPS – детектор атак (система обнаружения/предотвращения вторжений)
3. **Континент TLS – TLS-шлюз**
4. **Континент АП/ZTN Клиент – VPN-клиенты для удаленного доступа**
5. **Континент WAF – межсетевой экран уровня приложений**

Преимущества «Кода Безопасности»

	Преимущество:	Чем лучше конкурентов:	Ценность для заказчика:
1 **Единое управление сетевой безопасностью**	Уменьшаем простои вследствие ошибок конфигурирования	✓ Неотъемлемая и сертифицированная часть продукта ✓ Единое управление NGFW, криптошлюзами, прокси, IDS/IPS, МСЭ	✓ Экономия на обучении сотрудников ✓ Снижение операционных и капитальных затрат
2 **Опыт защиты сетей федерального уровня**	Понимаем специфику реализации крупных проектов	✓ 20 лет защиты сетей федерального уровня ✓ Набор проектной документации	Снижение рисков по несвоевременным окончаниям проектов
3 **Надежный сервис-провайдер**	✓ Большой штат опытных специалистов ✓ Обслуживание крупных федеральных сетей 24/7	✓ Документированный SLA ✓ Подключение к SOC «Кода Безопасности»	✓ Сокращение времени внедрения ✓ Сокращение времени простоя и ущерба от инцидентов ИБ

Континент 4

Континент 4

NGFW «Континент 4»

FW | IPS | App control | L2 VPN | L3 VPN | MGMT

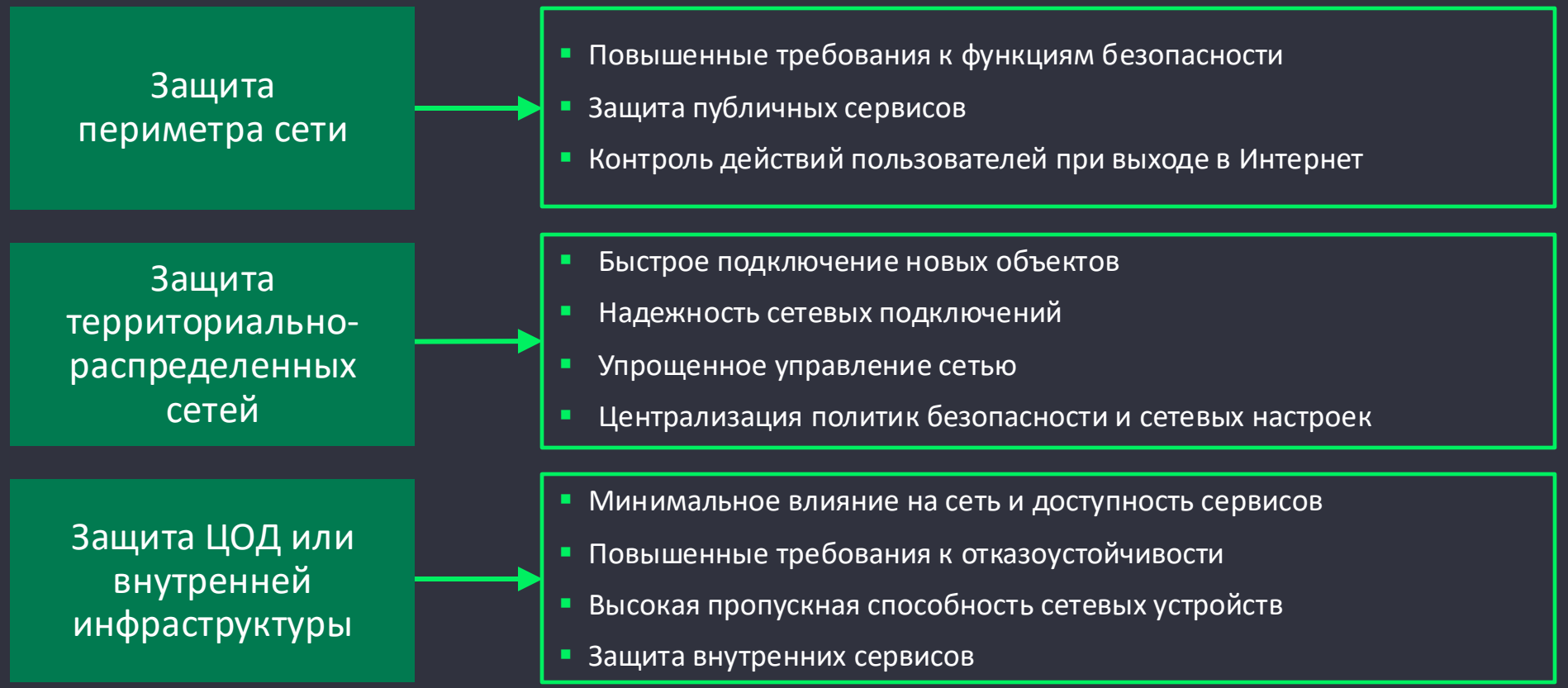
Threat Intelligence | Log | URL Filtering | User Identity | Antivirus | GeoIP | Proxy

Континент 4 – многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ

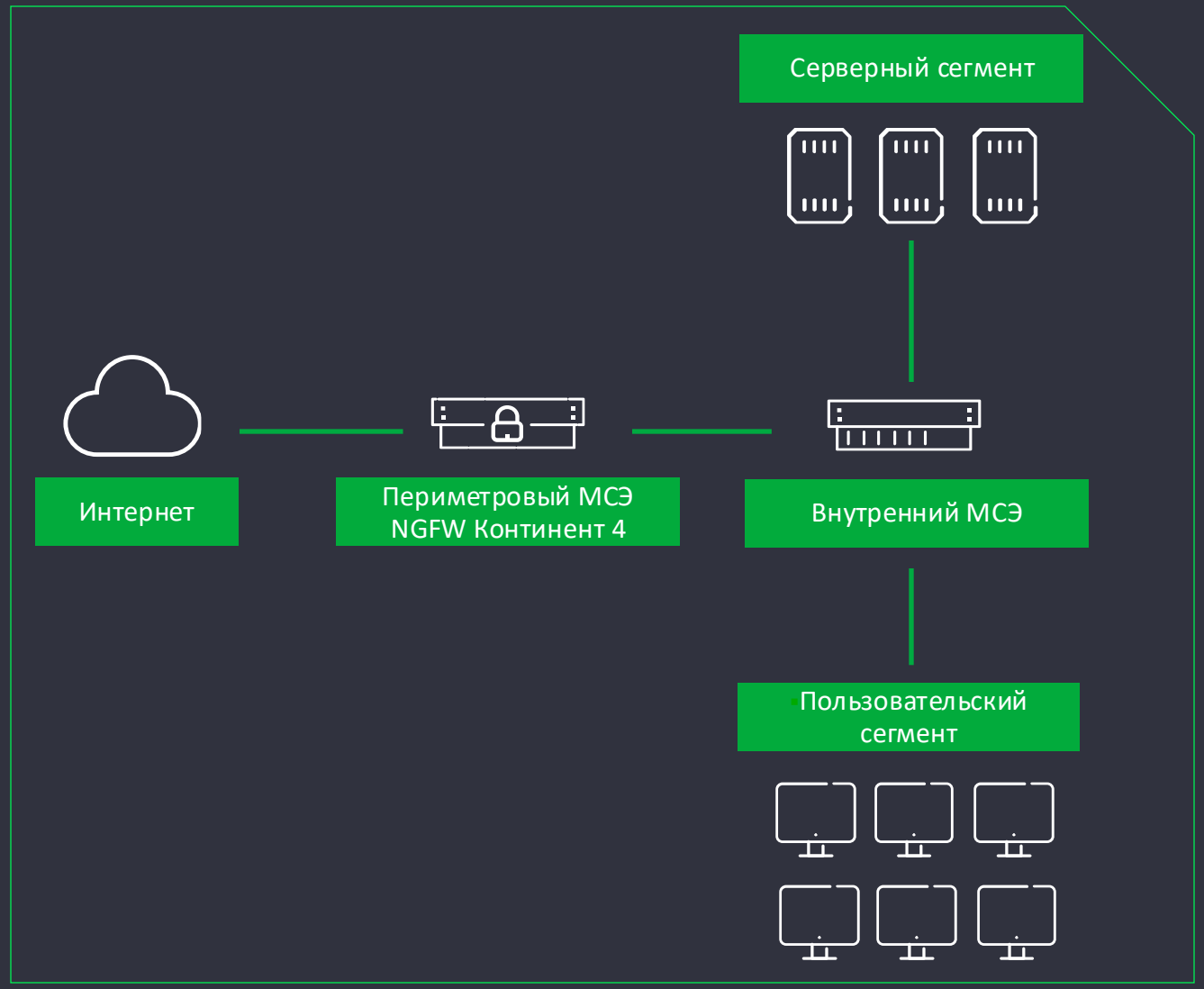
Предназначен для решения следующих задач:

- Централизованная защита периметра корпоративной сети
- Контроль доступа пользователей в Интернет
- Предотвращение сетевых вторжений
- Организация защищенного удаленного доступа

Сценарии использования Континент 4



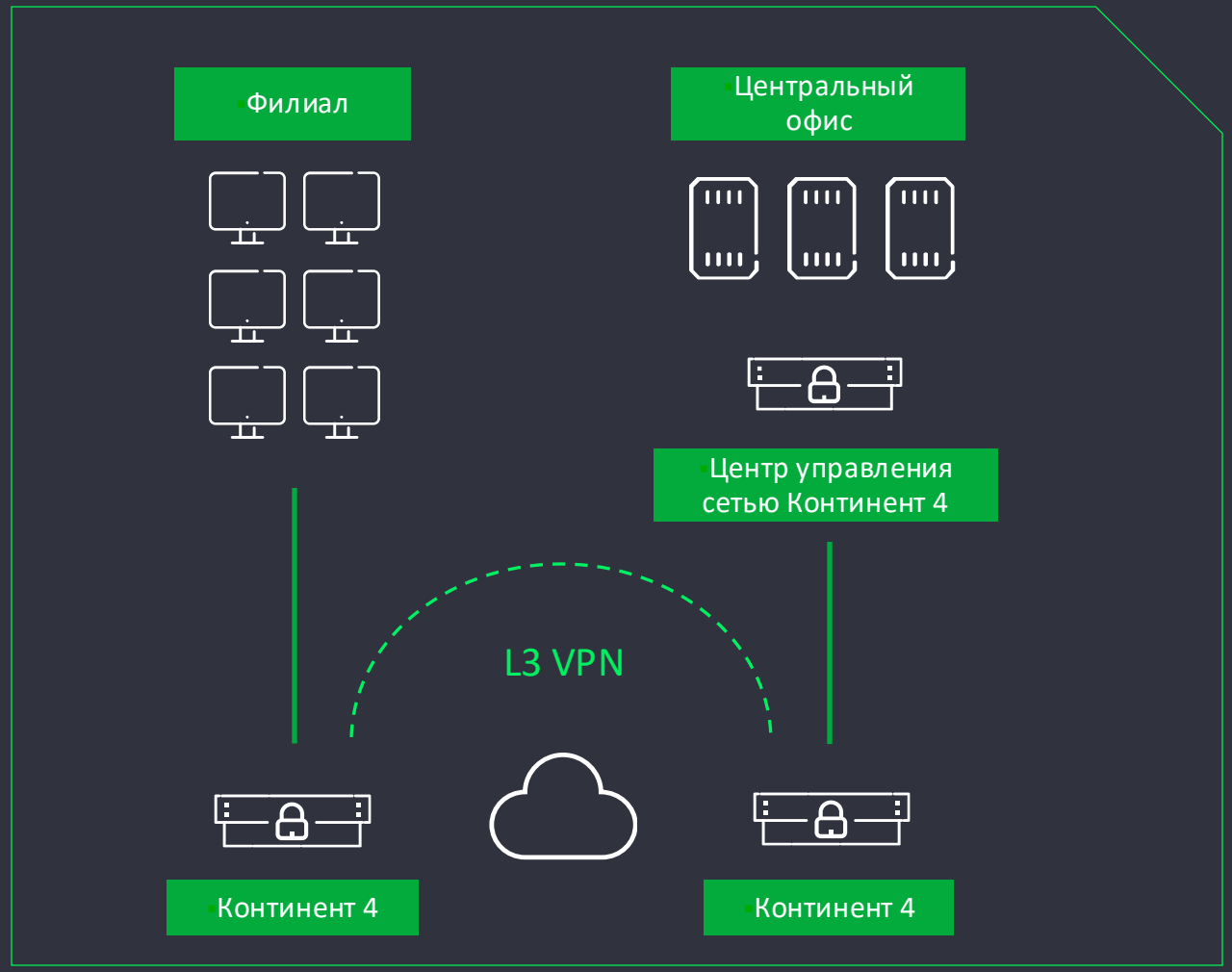
Защита периметра сети: преимущества



Основные преимущества:

- Контроль приложений
- Система обнаружения/предотвращения вторжений
- Индикаторы компрометации (IoC) от нескольких поставщиков:
  - Код Безопасности
  - Лаборатория Касперского
  - ФинЦЕРТ (ЦБ РФ)
  - Технологии киберугроз
- Явный прокси
- Модуль поведенческого анализа на базе машинного обучения (защита от DoS-атак, аномалий в трафике, атак сканирования)

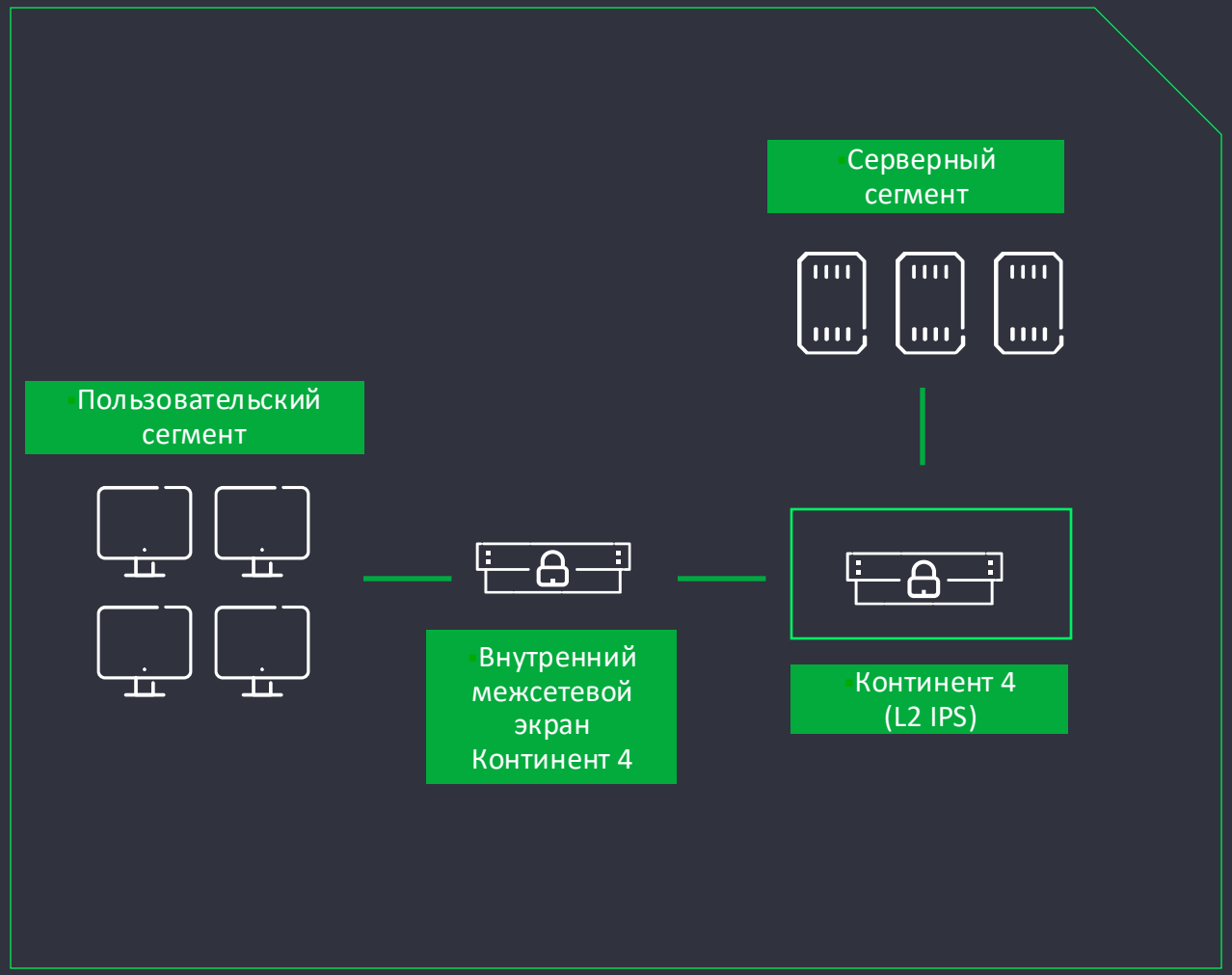
Защита территориально-распределенных сетей: преимущества



Основные преимущества:

- Централизованное управление и мониторинг
- Сервисы массового разворачивания устройств (Zero-touch provisioning)
- Защита каналов связи с ГОСТ-шифрованием (Site-to-Site VPN и Remote Access VPN)
- Резервирование сетевых подключений (Multi-WAN)
- Приоритизация трафика (QoS)

Защита ЦОД или внутренней инфраструктуры: преимущества



Основные преимущества:

- Работа в прозрачном режиме (L2 IDS/IPS)
- Производительность NGFW 50+ Гб/сек
- Поэтапный процесс миграции:
  - Обнаружение атак в прозрачном режиме
  - Предотвращение атак в прозрачном режиме
  - Сегментация сети
  - NGFW уровня ЦОД

Отличие Континент 4 от конкурентов – повышенный уровень защищенности

Технологическое преимущество

Развитый Threat Intelligence (IoC) для обнаружения и блокировки вредоносного трафика:

IoC в Континент 4

- Хэши вредоносных файлов
- Вредоносные домены
- Вредоносные URL

Встроенные базы

- Фиды Кода Безопасности
- Фиды Лаборатории Касперского
- Фиды Центрального банка
- Фиды Технологий киберугроз (RST-cloud)

Интегрированные базы

- Threat Intelligence Platform Security Vision
- Threat Intelligence Platform R-Vision
- Пользовательские

Модуль поведенческого анализа (используется машинное обучение) для обнаружения и блокирования атак типа «отказ в обслуживании» и других аномалий в трафике

Организация безопасного удаленного доступа с реализацией концепции Zero Trust Networking с клиентами для всех основных операционных систем (Windows, Linux, Mac OS, iOS, Android, Аврора)

Сертификаты Континент 4

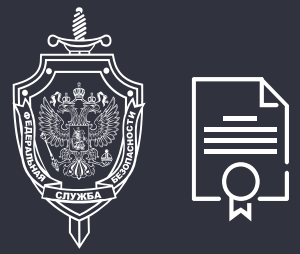
Сертифицирован ФСТЭК России:

- 4-й класс защиты МЭ типа «А»
- 4-й класс защиты МЭ типа «Б»
- 4-й класс защиты МЭ типа «Д»
- 4-й класс защиты СОВ уровня сети
- 4-й уровень доверия

Позволяет применять **Континент 4** для защиты значимых объектов КИИ до 1 категории, ИСПДн до 1 уровня, ГИС до 1 класса и АС до класса 1Г включительно

Планируется сертификация ФСТЭК России:

- Многофункциональный межсетевой экран (NGFW)



Планируется сертификация ФСБ России:

- КС1/КС2
- МЭ4

Позволит применять **Континент 4** как СКЗИ

Независимые тестирования

НА РЫНКЕ >20 NGFW

**Как в таком многообразии NGFW понять,
где правда, а где только маркетинг?**

Мы за независимые тестирования:

1. **Функциональное тестирование**
   от компании Инфосистемы Джет
2. **Тестирование механизмов безопасности**
   от компании ТС Солюшен
3. **Тестирование производительности**
   от компании BI.ZONE

Экспертиза в Континент 4 подтверждена экспертами рынка

КиберАльянс

Многофакторная аутентификация

MULTIFACTOR
Avanpost
Аладдин
КОМПАНИЯ ИНДИД
КОМПАНИЯ АКТИВ

Удаленный доступ

MacOS
iOS
АВРОРА

Комплаенс-контроль

Континент ZTN клиент
Сакура
Secret Net Studio

Защита виртуализации

vGate

Анализ правил

EFROS
DEFENCE OPERATIONS
Нетхаб
SPACE-BIT

Балансировка нагрузки

ЦИФРОВЫЕ РЕШЕНИЯ

Песочницы

AVSOFT
positive technologies
kaspersky

Индикаторы компрометации

kaspersky
Security Vision
CyberThreatTech
R-Vision
BI.ZONE

Континент 3

Континент 3

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

Сертификаты Континент 3

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

Архитектура Континент 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 Аврорак Серверу доступа.

Континент АП/ZTN Клиент

Удаленный доступ

Континент АП/ZTN

VPN-клиент для мобильных устройств и ПК

- Клиентские приложения для всех популярных платформ
- Методы аутентификации удаленных пользователей:
  - Сертификат
  - Логин/пароль
  - Многофакторная аутентификации с помощью сервиса multifactor.ru*
  - Многофакторная аутентификации с помощью Avanpost MFA*
- Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26)
- Поддержка различных ключевых носителей
- Возможность установки VPN-соединения до регистрации пользователя в ОС
- Режим запрета незащищенных соединений
- Разделение пулов ip-адресов удаленных пользователей

* необходима проверка функциональности в пилотных проектах

Континент ZTN Клиент: новое поколение клиентов удаленного доступа

Платформы:

- Windows
- Linux
- Aurora
- Android
- IOS
- MACOS (M1+M2)

- **Единый криптографический клиент под все платформы**
- **Контроль соответствия рабочей станции пользователя установленным политикам безопасности и контроль установленных приложений перед подключением**
- **Подключение к ряду решений:**
  - Континент 4
  - Континент TLS
  - Континент 3.9.1
- **Единая лицензия с Континент-АП**
- **Единая лицензия для любой клиентской ОС**

Континент TLS

О продукте

Континент TLS

Система комплексной защиты веб-приложений

(SSL VPN + WAF*)

Предназначен для решения следующих задач:

- Защищенный удаленный доступ к корпоративным ресурсам (RA VPN)
- Защищенный доступ к интернет-порталам с шифрованием по ГОСТ и RSA/AES (SSL VPN)
- Публикация веб-приложений через аутентификацию на шлюзе
- Защита веб-приложений от атак (WAF)

* Модуль WAF добавлен в версии 2.7

Сценарии использования

SSL VPN и RA VPN

- ГОСТ VPN
- Поддержка всех ОС для ГОСТ VPN
- RSA VPN
- Безагентский доступ для иностранной криптографии

Защиты веб-приложений (WAF)

- Публикация веб-приложений
- Защита веб-приложений от атак (OWASP, DDoS и др)

Защита приложений по Zero Trust

- Публикация корпоративных и/или облачных веб-приложений через аутентификацию на шлюзе
- Защита корпоративных веб-приложений от атак (OWASP, DDoS и др)

Платформы «Континент»

Российские платформы

Малые

IPC-R10

IPC-R50

Средние

IPC-R300

IPC-R550

IPC-R800

Старшие

IPC-R1000

IPC-R3000

IPC-R5000

КОД безопасности

Спасибо за внимание!

info@securitycode.ru
www.securitycode.ru

Все соцсети