КОД безопасности

Континент 4

Многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ

- Единая панель управления всеми механизмами защиты
- Выделенный интерфейс для мониторинга инфраструктуры в реальном времени
- Сигнатуры IPS, разработанные собственной лабораторией
- Контроль сетевых приложений и протоколов
- Патент на высокопроизводительный межсетевой экран
- VPN-шлюз с поддержкой алгоритмов ГОСТ и RSA/AES
- Линейное увеличение производительности с использованием специализированного брокера сетевых пакетов
- Виртуальные исполнения для VMware и KVM

Сценарии использования:

- Защита внешнего периметра корпоративной сети.
- Защита внутренней сети предприятия.
- Защита центров обработки данных (ЦОД).
- Защита георасределенной инфраструктуры.
- Защита технологических сетей.

Возможности

Защита от сетевых атак

- Два режима работы:
  - Обнаружение сетевых атак (IDS);
  - Предотвращение сетевых атак в режиме реального времени (IPS).
- Автоматическое обновление базы решающих правил с серверов «Кода безопасности».
- Сигнатуры IPS, разработанные собственной лабораторией:
  - Возможность загрузки пользовательских сигнатур.
- Модуль поведенческого анализа.
- Фиды Threat Intelligence (индикаторы компрометации):
  - Код Безопасности;
  - Лаборатория Касперского;
  - ФинЦерт;
  - Технологии киберугроз/RST-cloud
- TLS/SSL-инспекция.
- Прокси-сервер:
  - Прозрачный режим (Transparent);
  - Явный режим (Explicit).
- Интеграция со сторонними песочницами по ICAP.
- Потоковый антивирус:
  - Возможность добавления пользовательских сигнатур в базу поточного антивируса.
- URL-фильтрация без вскрытия TLS/SSL-трафика (по Server Name Indication).
- Регистрация информации об атаке:
  - Субъект/объект атаки, IP-адрес, номер порта;
  - Время и дата события;
  - Тип атаки;
  - Копия подозрительного трафика.
- Оперативное уведомление об атаке:
  - Оповещение в консоли мониторинга;
  - Оповещение по электронной почте;
  - Оповещение по SNMP.

Межсетевое экранирование

- Поддержка технологии Stateful Inspection.
- Контроль сетевых приложений (Application Control).
- Защита от доступа к вредоносным сайтам.
- Возможность управления всеми механизмами защиты в рамках одного правила.
- Интеграция с внешними каталогами пользователей:
  - LDAP(S);
  - RADIUS. new
- Разграничение доступа пользователей на основе данных:
  - Локальной базы пользователей;
  - MS Active Directory.
- Аутентификация пользователей с помощью:
  - Captive-портал;
  - Локального агента аутентификации;
  - Браузерная аутентификация SSO в AD Windows.
- Преднастроенные URL-категории.
- Фильтрация по местоположению (GeoIP).
- Фильтрация по доменным именам (FQDN).

Отказоустойчивость

- Использование модулей твердотельной памяти DOM и SSD.
- Режим автоматического переключения на резервный канал связи.
- Режим кластера высокой доступности с автоматической синхронизацией состояния сессий.
- Возможность использования резервных ЦУС.
- Работа в необслуживаемом режиме 24x7x365.
- Среднее время наработки на отказ – 50 000 часов.

Управление и мониторинг

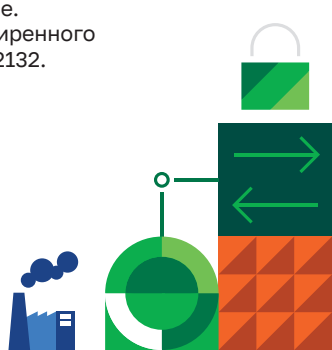
- Централизованное управление всеми механизмами комплекса.
- Мониторинг событий в режиме реального времени.
- Ролевая модель доступа администраторов.
- Высокопроизводительная система хранения и обработки событий безопасности.
- Дистанционное обновление компонентов комплекса (системного ПО и базы решающих правил).
- Инструменты автоматизации работы администраторов:
  - Инструменты API;
  - Конвертация конфигурации сторонних МСЭ в Континент 4.
- Уведомление по SMTP при инсталляции политики.
- Экспорт событий в SIEM-систему:
  - Поддержка SNMP v.2 и v.3;
  - Поддержка Syslog;
  - Поддержка Netflow v5, Netflow v9, Netflow v10 (IPFIX).
- Управление списком подключения к ЦУС.

Защита каналов связи и удаленный доступ

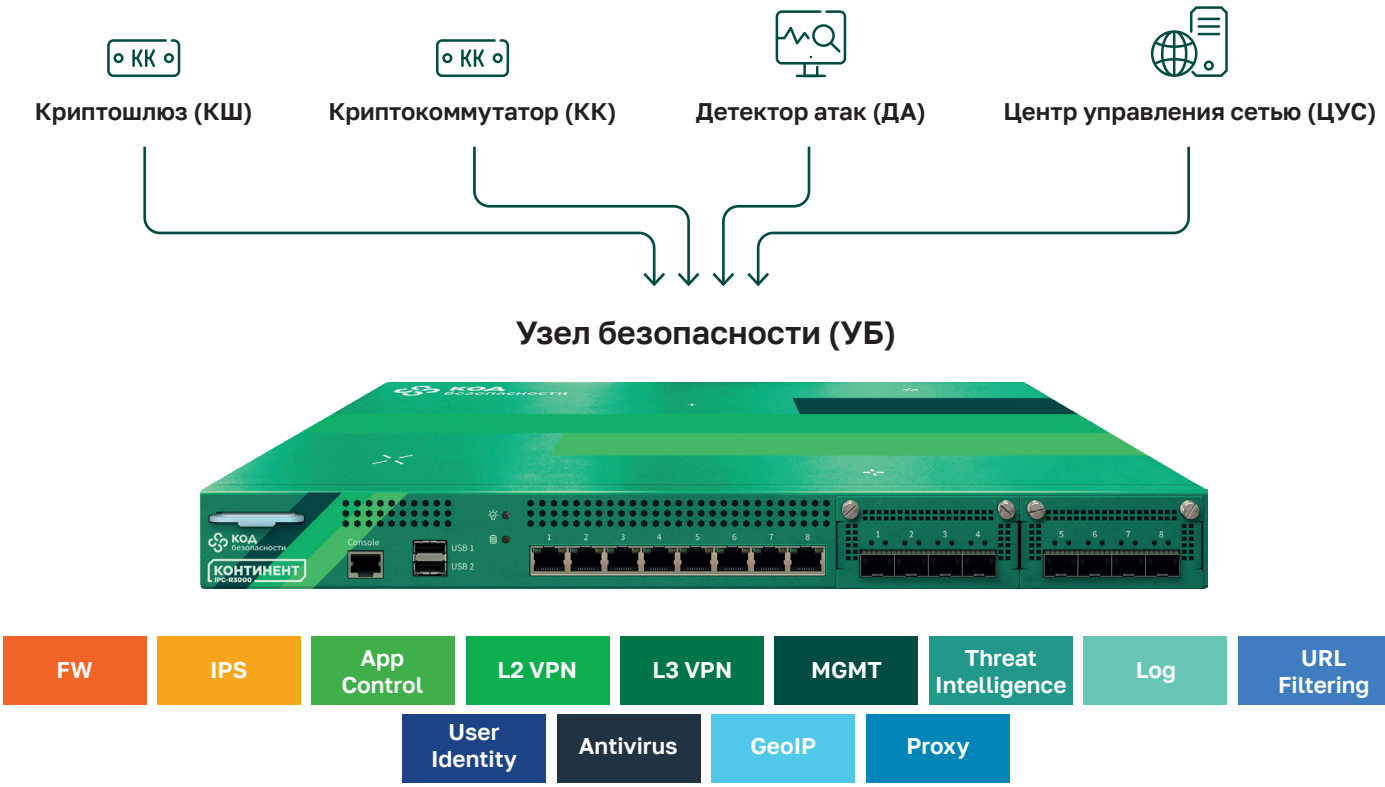
- Поддержка набора протоколов IPSec: new
  - Криптоалгоритмы ГОСТ;
  - Криптоалгоритмы RSA/AES. new
- Поддержка L3 VPN и L2 VPN.
- Поддержка удаленного доступа (Remote Access VPN)
- Поддержка клиентских ОС:
  - Windows;
  - Linux;
  - Android;
  - iOS;
  - MacOS;
  - Аврора.
- Поддержка GeoIP для ограничения подключения удаленных пользователей. new
- Контроль целостности установленного ПО перед подключением к серверу доступа.
- Разные подсети для разных групп удаленных пользователей (Office mode).
- Методы аутентификации удаленных пользователей:
  - Сертификат;
  - Логин/пароль;
  - Усиленная аутентификация через токен;
  - Многофакторная аутентификация с помощью сервисов Multifactor.ru и Avanpost MFA.

Сетевые возможности

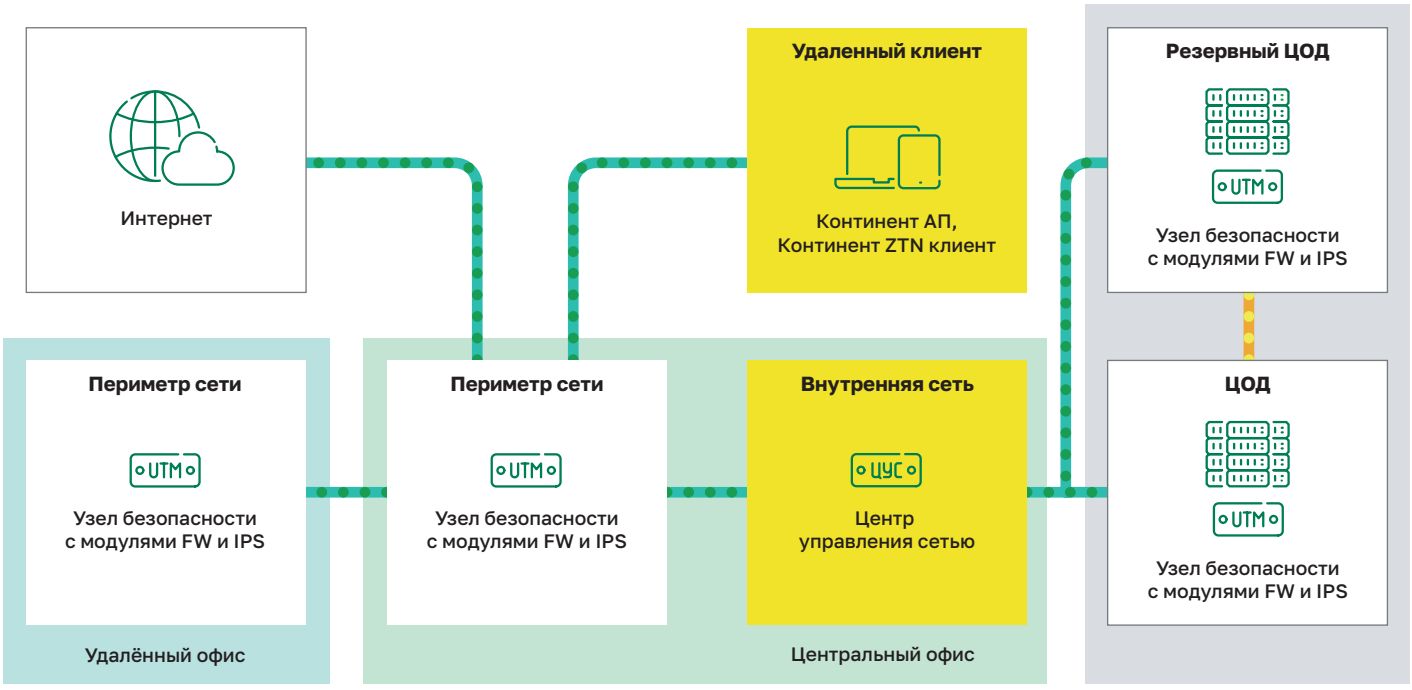
- Виртуальные маршрутизаторы (VRF).
- WAN-канал с поддержкой policy based routing (PBR).
- Поддержка протоколов динамической маршрутизации:
  - OSPF;
  - BGP.
- Агрегация интерфейсов по протоколу LACP (802.3ad).
- Поддержка приоритизации трафика (QoS).
- Поддержка подключения к нескольким каналам провайдера (Multi-WAN).
- Поддержка технологии VLAN (IEEE802.1Q).
- Поддержка технологии NAT:
  - Source NAT;
  - Destination NAT.
- NAT-трансляция внутри VPN.
- Встроенный DHCP-сервер с поддержкой режима DHCP-relay, в том числе на кластере.
- Возможность использования расширенного набора опций DHCP согласно RFC 2132.
- Поддержка VoIP.
- Поддержка протокола LLDP.
- Поддержка протокола BFD.



Консолидация механизмов



Концепция UTM



Сертификаты

Планируется сертификация по наборам требований:

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

ФСБ России
- МЭ класса 4

Сертифицирован по набору требований:

ФСБ России
- СКЗИ класса КС2

Лицензирование

Модуль	Узел Безопасности (УБ)	UTM базовый	UTM Расширенный
Центр управления сетью (ЦУС)	●	●	●
Межсетевой экран (МЭ)	●	●	●
Сервер доступа (СД)	●	●	●
URL-фильтрация	●	●	●
Модуль поведенческого анализа (МПА)	●	●	●
Контроль приложений		●	●
Система обнаружения вторжений	–	●	●
Модуль блокировки трафика по стране происхождения (GeoIP)	–	●	●
Защита от вредоносных сайтов	–	–	●
Преднастроенные категории URL	–	–	●
Потоковый антивирус	–	–	●
Высокопроизводительный межсетевой экран (NF2)	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		
L2 VPN	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		

О компании «Код Безопасности»

Компания «Код Безопасности» – лидирующий российский разработчик сертифицированных программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов.

+7 (495) 982-30-20 **info@securitycode.ru** **www.securitycode.ru**