



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 более 4000 сетевых приложений



Патент на высокопроизводительный межсетевой экран



VPN-шлюз с поддержкой алгоритмов ГОСТ



Линейное увеличение производительности с использованием специализированного брокера сетевых пакетов



Виртуальные исполнения для VMware и KVM

Сценарии использования:

- Защита внешнего периметра корпоративной сети.
- Защита центров обработки данных (ЦОД).
- Защита геораспределенной инфраструктуры.
- Защита малого и среднего бизнеса.
- 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.
- Добавление фидов Threat Intelligence от ФинЦентр в группу Кода Безопасности. **new**
- TLS/SSL-инспекция.
- Интеграция со сторонними песочницами по ICAP.
- Поточковый антивирус.
 - Возможность добавления пользовательских сигнатур в базу поточного антивируса.
- URL-фильтрация без вскрытия TLS/SSL-трафика (по Server Name Indication) **new**
- 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.
- 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).

Сетевые возможности

- WAN-канал с поддержкой policy based routing.
- 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.
- Поддержка VoIP.
- Поддержка протокола LLDP.
- Возможность использования расширенного набора опций DHCP согласно RFC 2132.

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).
- Импорт сетевых объектов, правил МЭ и NAT из Континент 3.9.2 и Check Point.
- 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

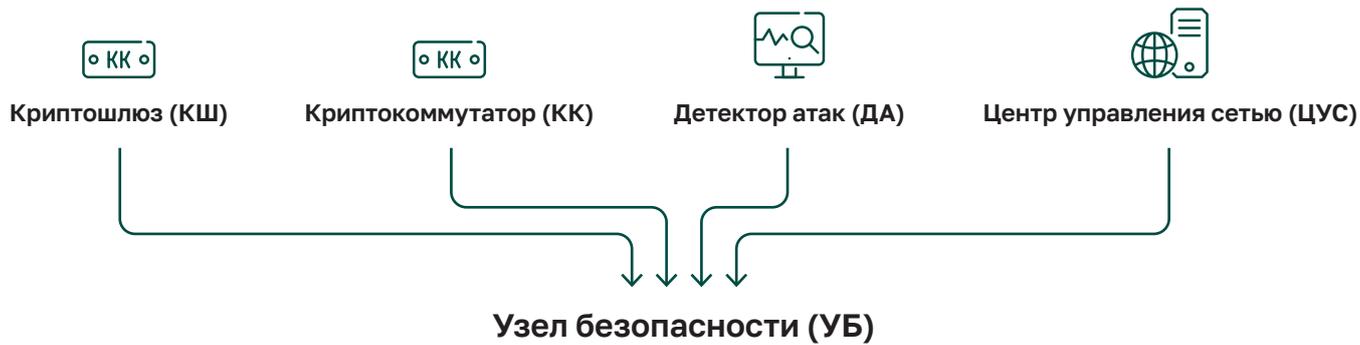
- Поддержка криптоалгоритмов ГОСТ.
- Поддержка L3 VPN и L2 VPN.
- Поддержка клиентских ОС:
 - Windows;
 - Linux;
 - Android;
 - iOS;
 - Аврора.
- Контроль целостности установленного ПО перед подключением к серверу доступа.
- Разные подсети для разных групп удаленных пользователей (Office mode).
- Методы аутентификации удаленных пользователей:
 - Сертификат;
 - Логин/пароль;
 - Многофакторная аутентификация с помощью сервиса Multifactor.ru.

Отказоустойчивость

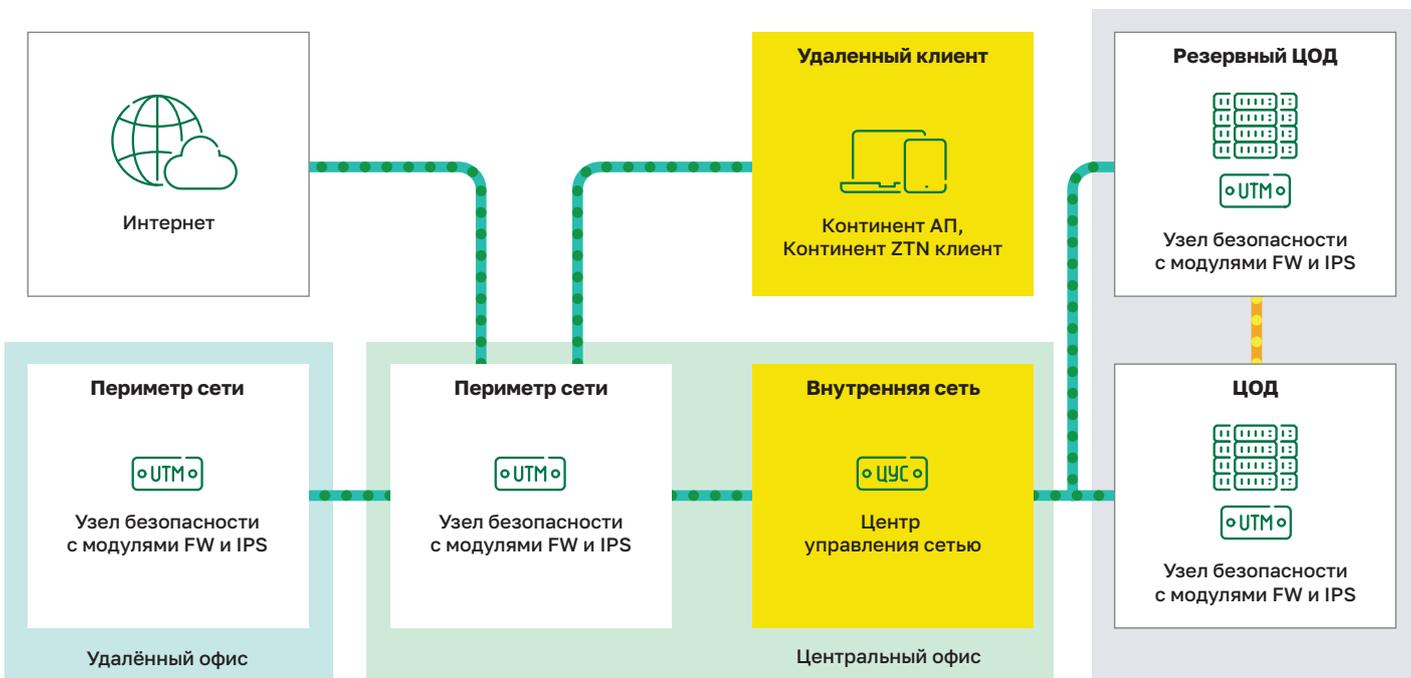
- Использование модулей твердотельной памяти DOM и SSD.
- Режим автоматического переключения на резервный канал связи.
- Режим кластера высокой доступности с автоматической синхронизацией состояния сессий.
- Возможность использования резервных ЦУС.
- Работа в необслуживаемом режиме 24x7x365.
- Среднее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



Консолидация механизмов



Концепция UTM





Сертификация по наборам требований:

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

Лицензирование

Модуль	УБ	UTM базовый	UTM Расширенный
Центр управления сетью (ЦУС)	●	●	●
Межсетевой экран (МЭ)	●	●	●
Шифрование L3VPN	●	●	●
Сервер доступа (СД)	●	●	●
Контроль приложений (300 приложений и протоколов)	●	●	●
URL-фильтрация	●	●	●
Модуль поведенческого анализа	●	●	●
Отказоустойчивый кластер	●	●	●
Расширенный контроль приложений (4000 приложений и протоколов)	-	●	●
Система обнаружения вторжений	-	●	●
Модуль блокировки трафика по стране происхождения	-	●	●
Защита от вредоносных сайтов	-	-	●
Преднастроенные URL-категории	-	-	●
Потоковый антивирус	-	-	●
NF2	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		
L2VPN	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 (многоканальный)

info@securitycode.ru

www.securitycode.ru