КОД безопасности

Континент 4

Универсальное устройство корпоративного уровня для всесторонней защиты сети (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

Варианты использования

- Защита внешнего периметра корпоративной сети.
- Сегментация внутренней сети.
- Создание защищенной корпоративной сети передачи данных с использованием алгоритмов ГОСТ.
- Защита магистральных каналов связи.
- Защита трафика систем видео-конференц-связи.
- Защищенный удаленный доступ.
- Защита информационных систем персональных данных (ИСПДн).
- Защита государственных информационных систем (ГИС).
- Защита каналов связи между ЦОД.
- Создание VPN ГОСТ «поверх» существующей VPN-сети.
- Защита от сетевых вторжений.

Возможности

Защита от сетевых атак

- Два режима работы:
  - Обнаружение сетевых атак;
  - Предотвращение сетевых атак в режиме реального времени.
- Автоматическое обновление базы решающих правил с серверов «Кода безопасности».
- Сигнатуры IPS, разработанные собственной лабораторией.
- Модуль поведенческого анализа.
- Интеграция с песочницей по ICAP. new
- Потоковый антивирус. new
- Регистрация информации об атаке:
  - Субъект/объект атаки, IP-адрес, номер порта;
  - Возможность загрузки пользовательских сигнатур;
  - 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.
- Преднастроенные URL-категории. new
- Фильтрация по местоположению (GeoIP). new
- Фильтрация по доменным именам. new

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.
- Поддержка VoIP.
- Поддержка протокола LLDP. new
- Возможность изменения всех допустимых опций DHCP согласно RFC 2132. new

Управление и мониторинг

- Централизованное управление:
  - Узлами сети;
  - Настройками маршрутизации;
  - Правилами фильтрации трафика;
  - VPN-сетями.
- 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).
- API для добавления правил. new
- Обновление баз компонентов защиты без применения политики и участия администратора. new
- Уведомление по SMTP при инсталляции политики. new
- Экспорт событий в SIEM-систему:
  - Поддержка SNMP v.2 и v.3;
  - Поддержка Syslog;
  - Поддержка NetFlow и IPFIX.

Защита каналов связи и удаленный доступ

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

Отказоустойчивость

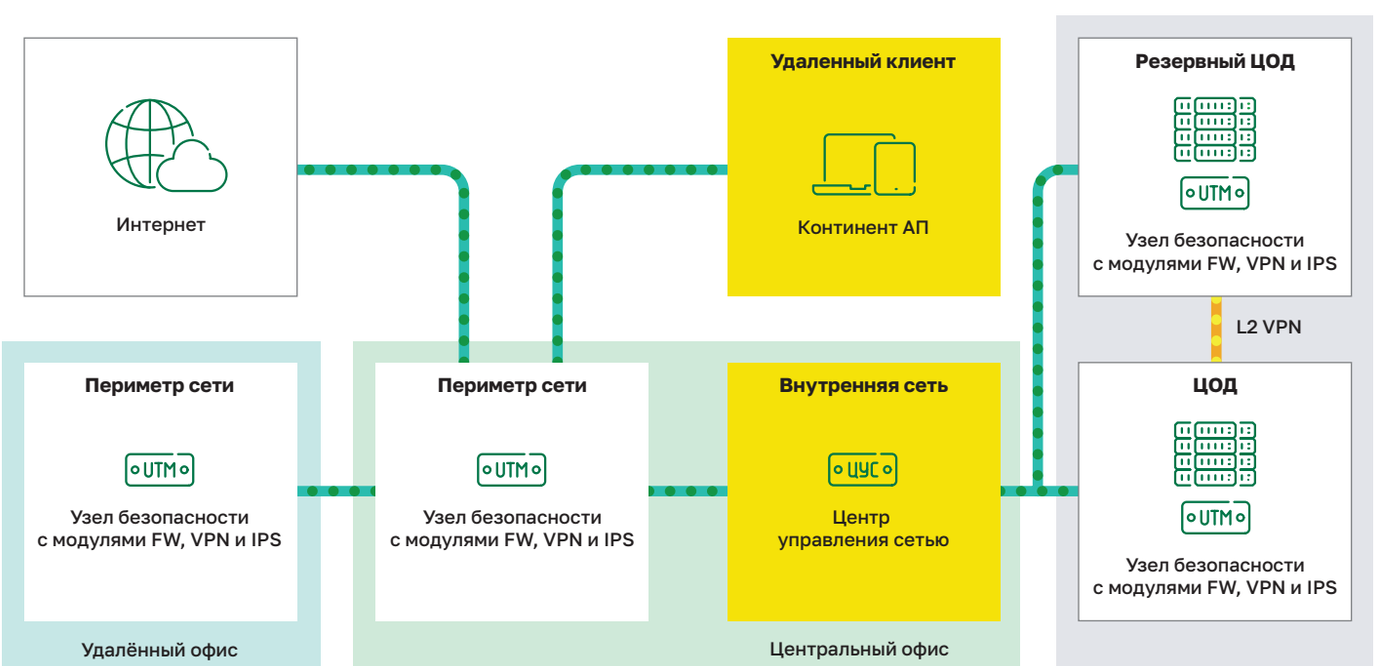
- Использование модулей твердотельной памяти DOM и SSD.
- Режим автоматического переключения на резервный канал связи.
- Режим кластера высокой доступности с автоматической синхронизацией состояния сессий.
- Работа в необслуживаемом режиме 24x7x365.
- Среднее время наработки на отказ – 50 000 часов.

Консолидация механизмов

Узел безопасности (УБ)

FW | IPS | App Control | L2 VPN | L3 VPN | MGMT | Threat Intelligence | Log | URL Filtering

Концепция UTM



Сертификация ФСТЭК России

Сертифицирован:

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

Ожидается сертификация по наборам требований:

- 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)	●	●	●
Расширенный контроль приложений	–	●	●
Система обнаружения вторжений (СОВ)	–	●	●
Модуль блокировки трафика по стране происхождения (GeoIP)	–	●	●
Защита от вредоносных сайтов (Malicious URL)	–	–	●
URL-фильтрация (с преднастроенными URL-категориями)	–	–	●
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**