КОД безопасности

Континент 3.9.3 КС

Централизованный комплекс для защиты сетевой инфраструктуры и создания VPN-сетей с использованием алгоритмов шифрования ГОСТ

Преимущества

- Аппаратные платформы, выпускаемые на территории РФ (ТОРП)
- Специализированная аппаратная платформа с производительностью VPN ГОСТ до 40 Гбит/с
- Отказоустойчивость серверов управления
- Кластер высокой доступности с автоматической синхронизацией конфигураций элементов кластера для криптошлюза и криптокоммутатора
- Агрегация сетевых интерфейсов (поддержка протокола 802.2ad)
- Защита георасределенных кластеров ЦОДов

Варианты использования

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

Компоненты комплекса

Криптокоммутатор

Аппаратно-программный комплекс, предназначенный для криптографической защиты трафика при его передаче на канальном уровне (позволяет создавать L2 VPN-сети).

Криптошлюз

Аппаратно-программный комплекс, предназначенный для маршрутизации сетевого трафика, межсетевого экранирования и криптографической защиты трафика при его передаче на сетевом уровне (создании L3 VPN-сети).

Детектор атак

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика для выявления и предотвращения сетевых атак.

Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга всех компонентов Континент 3.9.

Континент АП/ZTN

Клиентское приложение для защищенного доступа в корпоративную сеть с удаленных персональных компьютеров и смартфонов сотрудников.

Сервер доступа

Аппаратно-программный комплекс, предназначенный для обеспечения защищенного подключения удаленных пользователей.

Возможности

Обнаружение сетевых атак

- Сочетание сигнатурного и эвристического методов анализа трафика.
- Автоматическое обновление базы решающих правил с серверов «Кода Безопасности».
- Сигнатуры детектора атак, разработанные собственной лабораторией.
- Регистрация информации об атаке:
  - Субъект/объект атаки, IP-адрес, номер порта;
  - Время и дата события;
  - Тип атаки.
- Оперативное уведомление об атаках:
  - Оповещение в консоли ЦУС;
  - Оповещение по электронной почте.

Межсетевое экранирование

- Поддержка технологии Stateful Inspection.
- Контроль сетевых приложений.
- Инспекция внутри SSL-туннеля.
- Фильтрация трафика по:
  - IP-адресу, группам IP-адресов или диапазону;
  - IP-адресов источника и назначения;
  - Номерам портов;
  - Типам протоколов;
  - Типам и кодам сообщений ICMP;
  - Направлению пакетов;
  - Клиенту или серверу в TCP-соединении;
  - Расписанию.
- Идентификация и аутентификация пользователей МЭ:
  - С использованием клиентского ПО.
- Управление исключениями в HTTPS инспекции.new

Управление и мониторинг

- Утилиты для развертывания сетей.new
- Централизованное управление:
  - Узлами сети;
  - Настройками маршрутизации;
  - Правилами фильтрации трафика;
  - VPN-сетями;
  - Криптографическими ключами;
  - Параметрами SNMP.
- Мониторинг событий в режиме реального времени.
- Ролевая модель доступа администраторов.
- Автоматическое реагирование на события с использованием скриптов.
- Централизованное управление локальными администраторами устройств.
- Групповые операции над узлами.
- Доступ к платформам по SSH.
- Расширенное журналирование событий на локальном оборудовании.
- Гибкая система отчетов:
  - Экспорт событий в SIEM-систему;
  - Экспорт конфигураций для анализа в Skybox.

Шифрование

- Поддерживаемые криптоалгоритмы:
  - Шифрование данных производится в соответствии с ГОСТ 34.12-2018 (МАГМА) в режиме гаммирования с обратной связью по шифротексту при инициализации ЦУС с ПАК «Соболь»;
  - Шифрование данных производится в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью по шифротексту при инициализации ЦУС с ключевого носителя РДП-006;
  - Защита данных от искажения осуществляется по ГОСТ 28147-89 в режиме имитовставки.
- Варианты работы VPN:
  - Site-to-site VPN – симметричное распределение ключей;
  - Remote Access VPN – открытое распределение ключей.
- Централизованное управление криптографическими ключами.
- Поддержка L3 VPN и L2 VPN.
- Аппаратное ускорение шифрования L2 и L3 VPN.
- Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26).

Отказоустойчивость

- Использование модулей твердотельной памяти DOM и SSD.
- Просмотр статуса соединения с ЦУС из локального меню.new
- Режим автоматического переключения на резервный канал связи как при доступности, так и недоступности ЦУСа.
- Быстрое переключение на резервный канал без разрыва соединения.new
- Резервирование ЦУС.
- Режим кластера высокой доступности для криптошлюза и криптокоммутатора с автоматической синхронизацией конфигураций элементов кластера.
- Работа в необслуживаемом режиме 24x7x365.
- Среднее время наработки на отказ – 50 000 часов.

Сетевые технологии

- Поддержка IPv6.
- Поддержка режима Multi-WAN.
- Резервирование WAN-канала.
- Резервирование VPN-канала.
- Режим балансировки открытого трафика между WAN-портами.
- Поддержка протоколов динамической маршрутизации:
  - RIP;
  - OSPF;
  - BGP.
- Объединение криптокоммутаторов с помощью протокола LACP без дополнительного оборудования.
- Защита объекта за несколькими КШ.new
- Приоритизация трафика (QoS):
  - Защита от перегрузок;
  - Управление очередями;
  - Резервирование полосы пропускания для управляющего трафика;new
  - Перенос полей ToS;
  - Работа с метками ToS:
    - Приоритизация трафика на основе меток ToS;new
    - Фильтрация трафика на основе меток ToS.new
- Классификация трафика. До 32-х классов.
- Управление трафиком:
  - Резервирование;
  - Ограничение полосы пропускания трафика.
- Поддержка технологии VLAN (IEEE802.1Q).
- Поддержка технологии NAT:
  - Source NAT;
  - Destination NAT.
- Возможность работы КШ за NAT.
- Встроенный DHCP-сервер с поддержкой настройки provisioning server и DHCP-relay.
- Режим зеркалирования трафика:
  - Настраиваемый SPAN-порт.
- Возможность работы с виртуальными IP-адресами:
  - NAT-трансляция внутри VPN. Позволяет создавать VPN между сетями с пересекающимися диапазонами IP-адресов.
- Адаптация к изменению MTU.new
- Поддержка Jumbo frame (MTU до 9000 байт).

Модельный ряд

Характеристики	IPC-R10	IPC-R50	IPC-R300	IPC-R550	IPC-R800	IPC-R1000	IPC-R3000
							
Форм-фактор	Настольный	Настольный	Настольный	Настольный	1U	1U	1U
Производительность							
Пропускная способность L3 VPN и L2 VPN, Мбит/с	до 140	до 350	до 500	до 1000	до 2500	до 5000	до 8000
Пропускная способность МЭ, Мбит/с	до 1000	до 1200	до 4000	до 7000	до 12 000	до 15 000	до 25 000
Пропускная способность детектора атак, Мбит/с	-	до 200	до 400	до 500	до 850	до 950	до 1000
Максимальное количество конкурирующих keep-state сессий	30 000	300 000	350 000	350 000	1 000 000	1 500 000	3 000 000
Производительность Сервера Доступа (количество одновременных подключений Континент АП)	-	до 50	до 100	до 150	до 500	до 1200	до 2500
Производительность ЦУС (количество КШ под управлением ЦУС)	до 5	до 70	до 200	до 200	до 350	до 850	до 900
Производительность ЦУС в режиме VPN Full Mesh (количество КШ под управлением ЦУС)	-	до 20	до 70	до 70	до 200	до 300	до 500
Сетевые интерфейсы							
Общее количество сетевых интерфейсов	5x Gigabit Ethernet	5x Gigabit Ethernet	6x Gigabit Ethernet 2x 10 Giga-bit Ethernet	6x Gigabit Ethernet 2x 10 Gigabit Ethernet	8x Gigabit Ethernet 4x 10 Gigabit Ethernet	8x Gigabit Ethernet 4x 10 Gigabit Ethernet	8x Gigabit Ethernet 8x 10 Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45
Оптические интерфейсы	1x 1G SFP	1x 1G SFP	2x Combo SFP/RJ45 2x 10G SFP+	2x Combo SFP/ RJ45 2x 10G SFP+	4x 10GSFP+	4x 10G SFP+	8x 10GSFP+
Отказоустойчивость и надежность							
Режим кластера высокой доступности (горячее резервирование)	нет	да	да	да	да	да	да
Блок питания	Внешний адаптер 12V 36W	Внешний адаптер 12V 36W	Внешний адаптер 12V 36W	Внешний адаптер 12V 36W	1x 250W	2x300W с функцией горячего резерви-рования	2x300W с функцией горячего резерви-рования

IPC-3000FC-40G

Формфактор: специализированная аппаратная платформа для построения защищённого VPN-канала

Производительность шифрования: до 40 Гбит/с с минимизацией задержек при передаче трафика

Сетевые интерфейсы:

IPC-3000FC-40G

1x 1000BASE-T RJ45
8x 1G SFP
4x 10G SFP+
2x 40G QSFP

Сертификаты

Континент 3.9

Сертифицирован по требованиям РД ФСТЭК:
- 3-й класс защиты МЭ типа «А»;
- 3-й класс защиты СОВ уровня сети;
- 3-й уровень доверия.

Сертифицирован по требованиям РД ФСБ:
- СКЗИ класса КС2/КС3;
- МЭ класса 4.

Комплекс Континент может использоваться для защиты:
- Объектов Критической информационной инфраструктуры до К1 включительно;
- Информационных систем персональных данных до УЗ1 включительно;
- Государственных информационных систем до К1 включительно;
- Автоматизированных систем до класса 1В включительно.

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**