

Преимущества



Аппаратные платформы, выпускаемые на территории РФ (ТОРП)



Отказоустойчивость серверов управления



Кластер высокой доступности с автоматической синхронизацией конфигураций элементов кластера для криптошлюза и криптокоммутатора



Агрегация сетевых интерфейсов (поддержка протокола 802.2ad)



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
- Защита магистральных каналов связи
- Защита каналов связи между ЦОД
- Создание VPN ГОСТ «поверх» существующей VPN-сети

Компоненты комплекса

◦ L2 ◦

Криптокоммутатор

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

◦ L3 ◦

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).



Центр управления сетью

Аппаратно-программный комплекс, предназначенный для управления и мониторинга всех компонентов Континент 3.М3.

Возможности



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 из защищенных сетей.
- Расширенное журналирование событий на локальном оборудовании.
- Гибкая система отчетов:
 - Экспорт событий в SIEM-систему;
 - Экспорт конфигураций для анализа в Skybox.





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).



Шифрование

- Поддерживаемые криптоалгоритмы:
 - Алгоритм шифрования – ГОСТ 34.12-2018 (Магма) в режиме гаммирования с обратной связью по шифртексту по ГОСТ 34.13-2018;
 - Алгоритм имитозащиты данных – на базе ГОСТ 34.12-2018 (Магма) в режиме выработки имитовставки.
- Варианты работы VPN:
 - Site-to-site VPN – симметричное распределение ключей.
- Централизованное управление криптографическими ключами.
- Поддержка L3 VPN и L2 VPN.



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.



Модельный ряд

IPC-R10 IPC-R50 IPC-R300 IPC-R550 IPC-R800 IPC-R1000 IPC-R3000

Характеристики



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 1000 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

Максимальное количество конкурирующих keep-state сессий

30 000 300 000 350 000 350 000 1 000 000 1 500 000 3 000 000

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 Gigabit 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 резервирования 2x300W с функцией горячего резервирования

Сертификаты



Континент 3.М3

Сертифицирован по требованиям РД ФСБ:

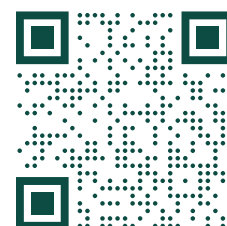
- СКЗИ класса КВ;
- МЭ класса 4.

Комплекс Континент может использоваться для защиты:

- Объектов Критической информационной инфраструктуры до К1 включительно;
- Информационных систем персональных данных до У31 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 (многоканальный)

info@securitycode.ru

www.securitycode.ru