Код безопасности

АПКШ «Континент» — IPC-100 (S102)

Май 2015

АПКШ «Континент» — IPC-100 (S102)

Назначение

АПКШ «Континент» обеспечивает криптографическую защиту информации (в соответствии с ГОСТ 28147–89), передаваемой по открытым каналам связи, между составными частями VPN, которыми могут являться локальные вычислительные сети, их сегменты и отдельные компьютеры.

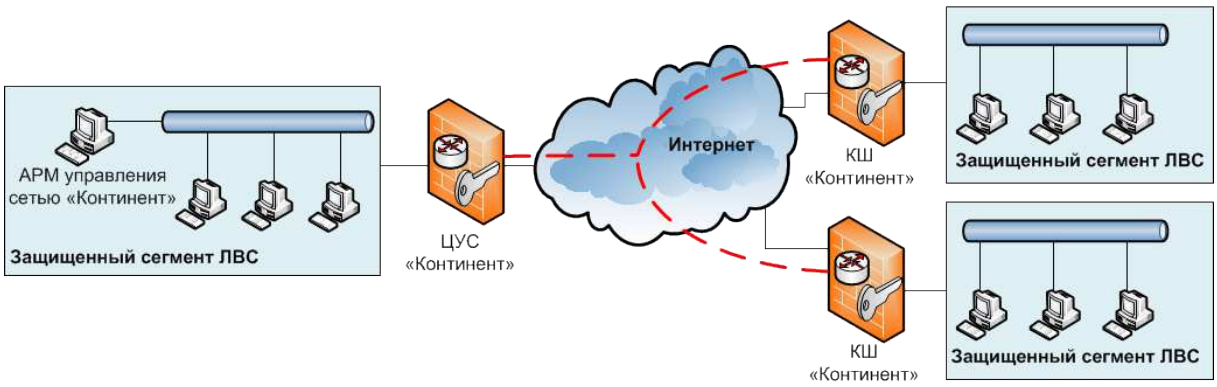
Современная ключевая схема, реализуя шифрование каждого пакета на уникальном ключе, обеспечивает гарантированную защиту от возможности дешифрации перехваченных данных.

Для защиты от проникновения со стороны сетей общего пользования АПКШ «Континент» обеспечивает фильтрацию принимаемых и передаваемых пакетов по различным критериям (адресам отправителя и получателя, протоколам, номерам портов, дополнительным полям пакетов и т.д.). Осуществляет поддержку VoIP, видеоконференций, GPRS, 3G, LTE, ADSL, Dial-Up и спутниковых каналов связи, технологии NAT/PAT для сокрытия структуры сети.

Область применения

- Защита внешнего периметра сети от вредоносного воздействия со стороны сетей общего пользования.
- Создание отказоустойчивой VPN-сети между территориально распределенными сетями.
- Защита сетевого трафика в мультисервисных сетях (VoIP, Video conference).
- Разделение сети на сегменты с различным уровнем доступа.
- Организация защищенного удаленного доступа к сети для мобильных сотрудников.
- Защита беспроводных сегментов сетей.
- Организация защищенного межсетевого взаимодействия между конфиденциальными сетями.

Пример VPN-сети «Континент»



Основные возможности

Надежная криптозащита

Шифрование трафика по ГОСТ 28147–89 с современной ключевой схемой обеспечивает гарантированную криптостойкость VPN-сети.

Межсетевое взаимодействие

Организация защищенного соединения между КШ, принадлежащими разным криптографическим сетям и управляемыми разными ЦУС. Для установления доверительных отношений между ЦУС используется собственная инфраструктура открытых ключей. Генерацию ключевой пары и издание сертификата открытого ключа для своей сети выполняет ЦУС.

Межсетевой экран

Высокопроизводительный межсетевой экран на основе технологии SPI с поддержкой технологии NAT/PAT для защиты периметра и сегментации внутренней сети.

Маршрутизация трафика

АПКШ «Континент» обеспечивает балансирование нагрузки между каналами связи и маршрутизацию трафика по протоколам динамической/статической маршрутизации.

Управление трафиком

АПКШ «Континент» обеспечивает работу критически важных приложений при помощи механизмов управления трафиком QoS и Traffic shaping.

Высокая доступность

АПКШ «Континент» обеспечивает функционирование отказоустойчивых защищенных сетей с горячим резервированием каналов связи и VPN-устройств.

Технические характеристики

Характеристики аппаратной платформы

Форм-фактор	1U для монтажа в 19" стойку
Габариты (ВхШхГ)	45 x 437 x 417 мм
Процессор	Intel Pentium G3420
Оперативная память	4Gb DDR-3
Сетевые интерфейсы	6x 1000BASE-T Ethernet 10/100/1000 RJ45
	2x 1000BASE-X оптический Gigabit Ethernet SFP
	(выполнены в виде легко заменяемых модулей)
Накопители оптические	нет
Жесткие диски	SATA SSD модуль 4Gb
Блок питания	270W
Считыватель	Touch Memory
Персональные идентификаторы Touch Memory iButton DS1992L	2шт.
Встроенный модуль АПМДЗ	ПАК «Соболь» 3.0 (mini-PCIe)
USB-flash drive	не менее 1 Гб
Упаковка	индивидуальная картонная коробка
Вес	7,5 кг
Уровень акустического шума при 100% загрузке (методика измерения ISO7779)	60 dBA
Встроенная операционная система	Continent OS – усовершенствованная ОС с усиленной безопасностью на основе ядра FreeBSD

Производительность обработки трафика

Производительность VPN (шифрования+ фильтрация МЭ)	до 300 Мбит/с
Производительность МЭ (открытый трафик)	до 400 Мбит/с
Максимальное количество обрабатываемых конкурирующих TCP сессий (keep-state)	250 000

Характеристики криптографической подсистемы

Поддерживаемые криптоалгоритмы	Шифрование ГОСТ 28147-89 (256 бит), имитозащита, хеширование ГОСТ Р 34.11-2012
Ключевая схема	• Site-to-site VPN – симметричное распределение ключей. • Mobile user VPN – открытое распределение ключей
Протокол туннелирования	Технология «Континент», шифрование и инкапсуляция IP-трафика в UDP (L3 VPN)
Количество защищенных соединение (VPN тоннелей)	Не ограничено

Межсетевое экранирование

Поддержка технологии Stateful Packet Inspection	Да
Защита от DOS атак	Да (контроль фрагментированных пакетов, антиспуфинг)
Фильтрация	• Фильтрация по IP-адресу источника и назначения (или диапазону IP-адресов), номерам портов и типам протоколов, типам и кодам сообщений ICMP, направлению пакетов, клиенту или серверу в TCP-соединении. • Фильтрация в соответствии с настраиваемым расписанием
Идентификация и аутентификация пользователей МЭ	Да (Позволяет применять правила МЭ к группам пользователей)

Сетевые возможности

Поддержка протокола сетевого взаимодействия IPv6	Да (возможность организации VPN связей через IPv6-сети провайдеров)
Поддержка режима мульти-WAN	Да
Резервирование WAN канала (WAN-failover)	Да
Резервирование VPN канала (VPN-failover)	Да
Режим балансировки исходящего открытого трафика между WAN портами	Да
Маршрутизация на основе политик, через разные WAN интерфейсы	Да
Поддержка протоколов динамической маршрутизации	OSPF, BGP, RIP
Поддержка multicast-маршрутизации	Да

Приоритизация трафика QoS	Да (защита от перегрузок, управление очередями, перенос полей ToS)
Классификация трафика	Да (до 32-х определяемых классов)
Управление трафиком (Traffic shaping)	Да (резервирование, ограничение полосы пропускания трафика)
Поддержка технологии VLAN (IEEE802.1Q)	Да (тагирование до 4096 VLAN)
Поддержка технологии NAT	NAT, DNAT, PAT, NAT 1:1
Возможность работы КШ за NAT	Да
Наличие встроенного сервера IP адресов	Да (DHCP сервер, DHCP relay)
Возможность получения динамически настраиваемого IP адреса	Да
Поддержка VoIP	Да
Поддержка режима зеркалирования трафика	Настраиваемый SPAN порт
Возможность работы с виртуальными IP-адресами	Да, NAT трансляция внутри VPN (позволяет создавать VPN связи между сетями с пересекающимися диапазонами IP-адресов)

Управление и мониторинг

Управление и настройка	• ЦУС - интегрированная централизованная система управления всеми узлами сети, настройками маршрутизации, межсетевого экранирования, VPN связями, криптографическими ключами. • Возможность создания и управления политиками. • Возможность группировки объектов и применения к ним глобальных политик
Средства управления	Графическая консоль управления ПУ ЦУС
Мониторинг	• Вывод событий и состояния сети в реальном времени на графическую консоль управления ПУ ЦУС. • Поддержка SNMP trap для удаленного оповещения о событиях
Обновление версии ПО узлов сети	Централизованное, дистанционное обновление версии ПО всех узлов сети
Подсистема журналирования	• Централизованный сбор и хранение журналов во внешней СУБД MS SQL Serve.r • Возможность регистрации всех пакетов
Возможность экспорта журналов и событий во внешние системы	Модуль ArcSight коннектор позволяет выполнять автоматическую выгрузку и конвертацию журналов в формат xml
Синхронизация системного времени узлов сети	Автоматическая синхронизация системного времени КШ с ЦУС • Возможность синхронизации времени ЦУС с NTP-серверами точного времени

Доступность и надежность

Надежность	• Использование в качестве дисковой подсистемы модулей твердотельной памяти DOM и SSD. • Отсутствие необходимости установки защищенной сессии между узлами сити, IP-пакеты шифруются и отправляются сразу после получения (IP-шифратор). • Файловая система с защитой от сбоев
Защита от сбоев канала связи	Режимы автоматического переключения на резервный канал связи WAN-failover, VPN-failover
Обеспечение высокой доступности	Поддержка режима кластера высокой доступности (HA) с автоматической синхронизацией конфигураций элементов кластера
Работа в необслуживаемом режиме	24x7x365
Среднее время наработки на отказ (MTBF)	40 000 часов

Сертификаты

- соответствие руководящих документов ФСТЭК России по 2-му уровню контроля на отсутствие НДВ и 2-му классу защищенности для межсетевых экранов. Может использоваться для создания автоматизированных систем до класса защищенности 1Б включительно и при создании информационных систем персональных данных до 1-го класса включительно;
- соответствие требованиям ФСБ России к устройствам типа межсетевой экран по 4 классу защищенности;
- соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС3 и возможность применения для криптографической защиты информации не содержащей сведений, составляющих государственную тайну;
- Минкомсвязи России – о соответствие установленным требованиям к оборудованию маршрутизации пакетов информации и возможности применения на сетях связи общего пользования в качестве оборудования коммутации и маршрутизации пакетов информации.

Код Безопасности

Почтовый адрес: 105318, Россия, Москва, а/я 101.

Адрес офисов в Москве:
ул. Щербаковская, д. 3.
ул. Большая Семеновская, д. 32, стр. 1
Тел.: +7 (495) 982 30 20 (многоканальный).
Факс: +7 (495) 974 60 34.

Адрес офиса в Санкт-Петербурге:
Пискаревский пр-т, д.2, корп.3, лит. А, БЦ «Бенуа».
Тел.: +7 (812) 313 80 28

E-mail: info@securitycode.ru

Запрос дополнительной информации о продуктах: info@securitycode.ru

По вопросам стоимости и покупки продуктов buy@securitycode.ru

По вопросам партнерства и сотрудничества info@securitycode.ru

Вы можете узнать подробную информацию о продуктах на сайте www.securitycode.ru

Также с помощью онлайн-калькулятора можно рассчитать стоимость решения.

О компании «Код Безопасности»

Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих безопасность информационных систем, а также их соответствие требованиям международных и отраслевых стандартов. Продукты «Код Безопасности» применяются во всех областях информационной безопасности, таких как защита конфиденциальной информации, персональных данных, коммерческой и государственной тайны, а также среды виртуализации. «Код Безопасности» стремится предоставить клиентам качественные решения для любых задач информационной безопасности, как традиционных, так и появляющихся в процессе развития высоких технологий.

ООО «Код Безопасности» ведет свою деятельность на основании лицензий ФСТЭК России и ФСБ России.