КОД безопасности

Континент 3.9

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)
- Контроль сетевых приложений

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

VPN-клиент для персональных компьютеров и мобильных устройств.

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 и мониторинг

- 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

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
- Приоритизация трафика (QoS)
  - Защита от перегрузок
  - Управление очередями
  - Перенос полей ToS
- 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
- Поддержка Jumbo frame (MTU до 9000 байт)

Шифрование

- Поддерживаемые криптоалгоритмы:
  - Шифрование данных производится в соответствии с ГОСТ 28147-89 в режиме гаммирования с обратной связью
  - 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
- Режим автоматического переключения на резервный канал связи как при доступности, так и недоступности ЦУСа
- 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

Характеристики	IPC-10	IPC-R10	IPC-25	IPC-R50	IPC-100	IPC-500	IPC-500F	IPC-600
								
Форм-фактор	Mini-ITX	Настольный	Mini-ITX	Настольный	1U	1U	1U	1U
Производительность								
Пропускная способность L3 VPN и L2 VPN, Мбит/с	до 120	до 140	до 100	до 350	до 410	до 500	до 500	до 1 100
Пропускная способность МЭ, Мбит/с	до 300	до 700	до 700	до 1 200	до 2 100	до 2 100	до 2 100	до 5 000
Пропускная способность детектора атак, Мбит/с	–	–	до 25	до 200	до 260	до 500	до 500	до 550
Максимальное количество конкурирующих keep-state сессий	30 000	250 000	250 000	250 000	350 000	350 000	350 000	1 000 000
Производительность Сервера Доступа (количество одновременных подключений Континент АП)	–	–	до 25	до 50	до 100	до 100	до 100	до 200
Производительность ЦУС (количество КШ под управлением ЦУС)	до 5	до 5	до 10	до 70	до 100	до 200	до 200	до 250
Производительность ЦУС в режиме VPN Full Mesh (количество КШ под управлением ЦУС)	–	–	–	до 20	до 50	до 70	до 70	до 100
Сетевые интерфейсы								
Общее количество сетевых интерфейсов	3x Gigabit Ethernet	5x Gigabit Ethernet	5x Gigabit Ethernet	5x Gigabit Ethernet	8x Gigabit Ethernet	6x Gigabit Ethernet	10x Gigabit Ethernet	8x Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	3x 1000BASE-T RJ45	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	6x 1000BASE-T RJ45	6x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45
Оптические интерфейсы	нет	1x 1G SFP	1x 1G SFP	1x 1G SFP	2x 1G SFP	нет	2x 1G SFP	нет
Подключение внешнего 3G USB модема	да	нет	да	нет	нет	нет	нет	нет
Порт RS232 для подключения Dial-UP модема	да	нет	да	нет	да	нет	нет	нет
Отказоустойчивость и надежность								
Режим кластера высокой доступности (горячее резервирование)	нет	нет	нет	да	да	да	да	да
Блок питания	Внешний адаптер 12V 40W	Внешний адаптер 12V 36W	Внешний адаптер 12V 40W	Внешний адаптер 12V 36W	1x 270W	1x 150W	1x 150W	1x 250 W

Характеристики	IPC-R300	IPC-R550	IPC-800F	IPC-1000F	IPC-1000NF2	IPC-3000F	IPC-3000NF2
							
Форм-фактор	Настольный	Настольный	1U	1U	1U	1U	1U
Производительность							
Пропускная способность L3 VPN и L2 VPN, Мбит/с	до 500	до 900	до 2 300	до 4 400	до 4 400	до 6 400	до 6 400
Пропускная способность МЭ, Мбит/с	до 3 100	до 4 000	до 7 000	до 10 000	до 10 000	до 13 000	до 13 000
Пропускная способность детектора атак, Мбит/с	до 400	до 500	до 800	до 900	до 900	до 960	до 960
Максимальное количество конкурирующих keep-state сессий	1 000 000	1 000 000	1 000 000	1 500 000	1 500 000	3 000 000	3 000 000
Производительность Сервера Доступа (количество одновременных подключений Континент АП)	до 100	до 150	до 500	до 1 000	до 1 000	до 3 000	до 3 000
Производительность ЦУС (количество КШ под управлением ЦУС)	до 200	до 200	до 350	до 800	до 800	до 900	до 900
Производительность ЦУС в режиме VPN Full Mesh (количество КШ под управлением ЦУС)	до 70	до 70	до 200	до 250	до 250	до 500	до 500
Сетевые интерфейсы							
Общее количество сетевых интерфейсов	6x Gigabit Ethernet 2x 10 Gigabit Ethernet	6x Gigabit Ethernet 2x 10 Gigabit Ethernet	12x Gigabit Ethernet	16x Gigabit Ethernet	16x Gigabit Ethernet 4x 10 Gigabit Ethernet	9x Gigabit Ethernet 4x 10 Gigabit Ethernet	9x Gigabit Ethernet, 8x 10 Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	4x 1000BASE-T RJ45	4x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45	1x 1000BASE-T RJ45	9x 1000BASE-T RJ45
Оптические интерфейсы	2x Combo SFP/RJ45 2x 10G SFP+	2x Combo SFP/RJ45 2x 10G SFP+	4x 1G SFP	8x 1G SFP	8x 1G SFP 4x 10G SFP+	8x 1G SFP 4x 10G SFP+	8x 10G SFP+
Подключение внешнего 3G USB модема	нет	нет	нет	нет	нет	нет	нет
Порт RS232 для подключения Dial-UP модема	нет	нет	нет	нет	нет	нет	нет
Отказоустойчивость и надежность							
Режим кластера высокой доступности (горячее резервирование)	да	да	да	да	да	да	да
Блок питания	Внешний адаптер 12V, 36W	Внешний адаптер 12V, 36W	1x 250 W	2x 300W с горячей заменой	2x 300W с горячей заменой	2x 300W с горячей заменой	2x 300W с горячей заменой

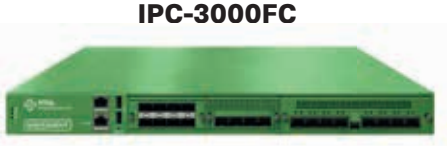
IPC-3000FC/FC-H/FC-40G

Формфактор: специализированная аппаратная платформа для построения защищённого VPN-канала

Производительность шифрования: от 20 до 40 Гбит/с с минимизацией задержек при передаче трафика

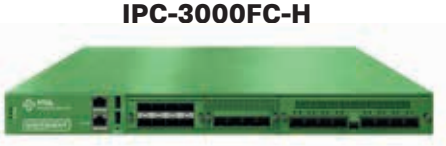
Сетевые интерфейсы:

IPC-3000FC



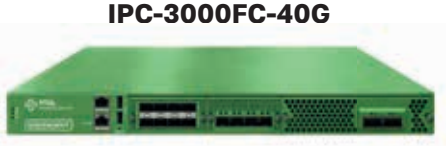
1x 1000BASE-T RJ45
8x 1G SFP
8x 10G SFP+

IPC-3000FC-H



1x 1000BASE-T RJ45
8x 1G SFP
4x 10G SFP+
8x 10G SFP+
специального назначения
(подключаются 2 кабелями
Breakout с выходами на 40G QSFP)

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 (многоканальный) **info@securitycode.ru** **www.securitycode.ru**