КОД БЕЗОПАСНОСТИ

АПКШ «КОНТИНЕНТ» 3.7

Многофункциональный комплекс сетевой безопасности

ПРЕИМУЩЕСТВА

Масштабируемость и отказоустойчивость компонентов системы безопасности.

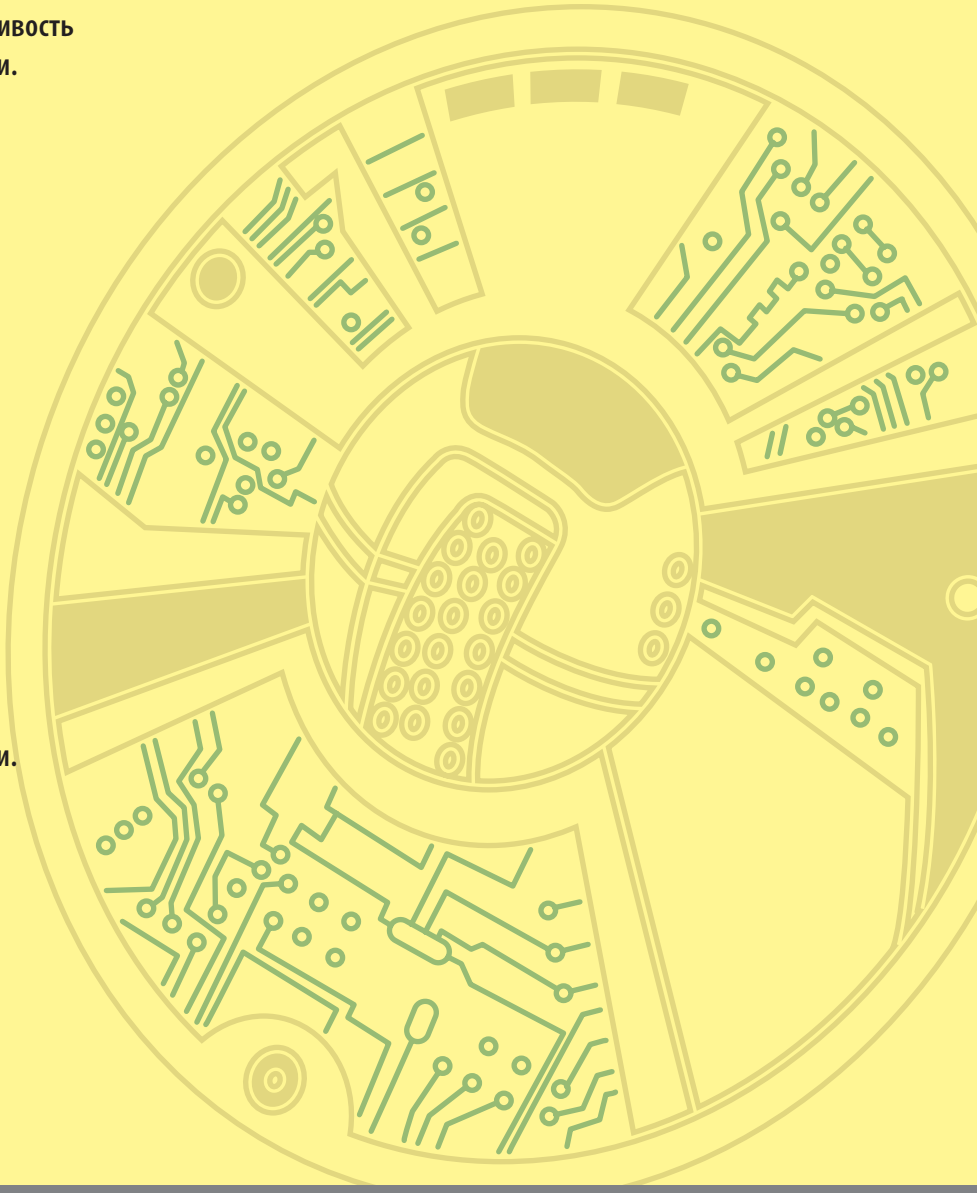
Работа программного VPN-клиента на различных ОС

Централизованное управление всеми компонентами системы защиты.

Централизованное обновление ПО криптошлюзов и базы решающихправил (БРП) системы обнаружения вторжений.

Простота внедрения и эксплуатации.

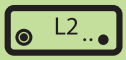
Широкий модельный ряд.



ВАРИАНТЫ ИСПОЛЬЗОВАНИЯ

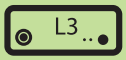
- Создание защищенной корпоративной сети связи на базе интернета
- Защита ИТ-инфраструктуры предприятия от сетевых угроз
- Защита трафика систем видео-конференц-связи и IP-телефонии
- Защита сетей банкоматов и платежных терминалов
- Подключение к системе межведомственного электронного взаимодействия (СМЭВ)
- Защищенный удаленный доступ, в том числе с мобильных устройств
- Защита систем виртуализации рабочих мест (VDI)
- Защита информационных систем персональных данных (ИСПДн)
- Защита государственных информационных систем (ГИС)
- Объединение распределенных сетей без изменения адресного пространства
- Защита канала между ЦОД
- Внедрение технических мер для приведения ИТ-систем в соответствие требованиям приказов ФСТЭК России №17, 21 и 31

КОМПОНЕНТЫ КОМПЛЕКСА



КРИПТОКОММУТАТОР

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



КРИПТОШЛЮЗ

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

ДЕТЕКТОР АТАК

Аппаратно-программный комплекс, предназначенный для анализа сетевого трафика и обнаружения в нем угроз безопасности.

ЦЕНТР УПРАВЛЕНИЯ СЕТЬЮ

Аппаратно-программный комплекс, предназначенный для управления и мониторинга состояния компонентов АПКШ «Континент».

СКЗИ «КОНТИНЕНТ-АП»

VPN-клиент для персональных компьютеров, выполняющий функции персонального межсетевого экрана.

СЕРВЕР ДОСТУПА

Аппаратно-программный комплекс, предназначенный для организации защищенного удаленного доступа с помощью VPN-клиента СКЗИ «Континент АП».

КОНТИНЕНТ Т-10

Планшетный компьютер со встроенным VPN-клиентом СКЗИ «Континент-АП».

ВОЗМОЖНОСТИ

ОБНАРУЖЕНИЕ СЕТЕВЫХ ВТОРЖЕНИЙ

- Сочетание сигнатурного и эвристического методов анализа сетевого трафика
- Регистрация информации об атаке
  - Субъект/объект атаки, IP-адрес, номер порта
  - Время и дата события
  - Тип атаки
- Обновление базы решающих правил (БРП)
  - Автоматически
  - Вручную
- Поддержка широкого списка протоколов
  - Сетевого уровня: ICMPv4, ICMPv6, IPv4, IPv6
  - Транспортного уровня: TCP, UDP, SCTP
  - Канального уровня: PPPoE, PPP
  - Прикладного уровня: FTP, HTTP, SMB, SSH, SMTP
  - Сеансового уровня: SSL, DCE/RPC
- Оперативное уведомление об атаках
  - Оповещение в консоли ЦУС
  - Оповещение по электронной почте
- Интеграция в существующую сетевую инфраструктуру
  - Подключение к SPAN-порту

УПРАВЛЕНИЕ И МОНИТОРИНГ

- Централизованная система управления:
  - Узлами сети
  - Настройками маршрутизации
  - Правилами фильтрации трафика
  - VPN-связями
  - Криптографическими ключами
- Графическая консоль управления
- Мониторинг состояния сети и событий НСД в реальном времени
- Поддержка SNMP-trap
- Централизованное обновление версии ПО всех узлов сети
- Централизованный сбор и хранение журналов во внешней СУБД
- Возможность регистрации каждого пакета
- Интеграция с SIEM HP ArcSight
  - Выгрузка и конвертация журналов в формат XML
- Синхронизация системного времени
  - Автоматическая синхронизация системного времени криптошлюзов с центром управления сетью
  - Синхронизация системного времени ЦУС с NTP-серверами

МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ

- Контроль состояния сетевых соединений
- Защита от DoS-атак
- 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
  - В соответствии с расписанием
- Идентификация и аутентификация пользователей МЭ

СЕТЕВЫЕ ВОЗМОЖНОСТИ

- Поддержка IPv6
- Резервирование WAN-канала
- Резервирование VPN-канала
- Поддержка протоколов динамической маршрутизации
  - RIP
  - OSPF
  - BGP
- Поддержка Multicast-маршрутизации
- Приоритизация трафика (QoS)
  - Защита от перегрузок
  - Управление очередями
  - Перенос полей ToS
- Резервирование и ограничение полосы пропускания трафика
- Поддержка технологии VLAN (IEEE802.1Q)
- Поддержка технологии NAT
  - Source NAT
  - Destination NAT
  - Bidirectional NAT
- Возможность работы КШ за NAT
- Встроенный сервер IP-адресов
  - DHCP-сервер
  - DHCP-relay
- NAT-трансляция внутри VPN. Позволяет создавать VPN между сетями с пересекающимися диапазонами IP-адресов

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
- Ключевая схема:
  - Site-to-site VPN – симметричное распределение ключей
  - Remote Access VPN – открытое распределение ключей
- Управление криптографическими ключами производится централизованно
- Протокол туннелирования
  - Шифрование и инкапсуляция IP-трафика в UDP (L3 VPN)
  - Шифрование и инкапсуляция Ethernet-кадров в UDP (L2 VPN)

ОТКАЗОУСТОЙЧИВОСТЬ

- Использование модулей твердотельной памяти DOM и SSD
- Режим автоматического переключения на резервный канал связи
- Режим кластера высокой доступности с автоматической синхронизацией конфигураций элементов кластера
- Работа в необслуживаемом режиме 24x7x365
- Среднее время наработки на отказ – 40 000 часов

ХАРАКТЕРИСТИКИ АППАРАТНЫХ ПЛАТФОРМ

МОДЕЛЬ	IPC-10	IPC-25	IPC-100	IPC-400
				
Форм-фактор	Mini-ITX		1U	2U
ПРОИЗВОДИТЕЛЬНОСТЬ				
Пропускная способность VPN, мбит/с	до 10	до 50	до 300	до 500
Пропускная способность L2VPN (для крипто-коммутатора), мбит/с	до 10	до 50	до 300	до 500
Пропускная способность МЭ, мбит/с	до 100	до 100	до 400	до 1000
Максимальное количество конкурирующих keep-state сессий	5 000	10 000	250 000	350 000
Пропускная способность детектора атак на 1 интерфейс, мбит/с	до 10	до 25	до 260	до 500
Производительность Сервера Доступа (количество одновременных подключений Континент АП)	не поддерживается	до 25	до 500	до 1000
Производительность ЦУС (количество КШ под управлением ЦУС)	не поддерживается	до 10	до 500	до 1000
КОНФИГУРАЦИЯ СЕТЕВЫХ ИНТЕРФЕЙСОВ				
Общее количество сетевых интерфейсов	3x Ethernet	5x Gigabit Ethernet	8x Gigabit Ethernet	6x Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	3x Ethernet 10/100	4x Ethernet 10/100/1000	6x Ethernet 10/100/1000	6x Ethernet 10/100/1000
Интерфейсы оптические	нет	1x 1000BASE-X SFP	2x 1000BASE-X SFP	нет
Подключение внешнего 3G USB модема	да	да	нет	нет
Порт RS232 для подключения Dial-UP модема	да	да	да	нет
ОТКАЗОУСТОЙЧИВОСТЬ И НАДЕЖНОСТЬ				
Режим кластера высокой доступности (горячее резервирование)	Нет		Да	
Блок питания	Внешний адаптер 19V 40W		1 x 270W	1 x 680W

МОДЕЛЬ	IPC-1000	IPC-1000F	IPC-1000F2	IPC-3000F	IPC-3034	IPC-3034F
						
Форм-фактор	2U					
ПРОИЗВОДИТЕЛЬНОСТЬ						
Пропускная способность VPN, мбит/с	до 950	до 950	до 950	до 2500	до 2500	до 2500
Пропускная способность L2VPN (для крипто-коммутатора), мбит/с	до 950	до 950	до 950	до 3000	до 3000	до 3000
Пропускная способность МЭ, мбит/с	до 1000	до 1000	до 1000	до 3500	до 3500	до 3500
Максимальное количество конкурирующих keep-state сессий	1 000 000	1 000 000	1 000 000	3 000 000	3 000 000	3 000 000
Пропускная способность детектора атак на 1 интерфейс, мбит/с	до 600	до 600	до 600	до 660	до 660	до 660
Производительность Сервера Доступа (количество одновременных подключений Континент АП)	до 1000	до 1000	до 1000	до 3000	до 3000	до 3000
Производительность ЦУС (количество КШ под управлением ЦУС)	до 3000	до 3000	до 3000	до 3000	до 3000	до 3000
КОНФИГУРАЦИЯ СЕТЕВЫХ ИНТЕРФЕЙСОВ						
Общее количество сетевых интерфейсов	10x Gigabit Ethernet	10x Gigabit Ethernet	18x Gigabit Ethernet	14x Gigabit Ethernet	34x Gigabit Ethernet	34x Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	10x Ethernet 10/100/1000	6x Ethernet 10/100/1000	10x Ethernet 10/100/1000	10x Ethernet 10/100/1000	34x Ethernet 10/100/1000	2x Ethernet 10/100/1000
Интерфейсы оптические	нет	4x 1000BASE-X SFP	8x 1000BASE-X SFP	4x 10 Gigabit SFP+	нет	32x 1000BASE-X SFP
Подключение внешнего 3G USB модема	нет	нет	нет	нет	нет	нет
Порт RS232 для подключения Dial-UP модема	нет	нет	нет	нет	нет	нет
ОТКАЗОУСТОЙЧИВОСТЬ И НАДЕЖНОСТЬ						
Режим кластера высокой доступности (горячее резервирование)	Да					
Блок питания	2 x 680W с горячей заменой					

СЕРТИФИКАТЫ

ФСТЭК России.

АПКШ «Континент»: МЭ 2/ СОВ 3/ НДВ2.
МЭ – для защиты АС до класса 1Б включительно (гостайна с грифом «совершенно секретно»)
и СОВ для защиты АС до класса 1В включительно. Для защиты ИСПДн до УЗ1, ГИС до К1
и АСУ ТП до К1 включительно.
СКЗИ «Континент-АП»: МЭ 3/НДВ 3 для защиты АС до класса 1В включительно, ИСПДн до УЗ1, ГИС до К1 и АСУ ТП до К1 включительно.

ФСБ России.

АПКШ «Континент»: СКЗИ КС3/ МЭ 4/ СОА В.
СКЗИ «Континент-АП»: СКЗИ КС 1/ КС 2/ МЭ 4.
АПКШ «Континент» 3.М: КВ 2/МЭ 4
для применения в ИТС
органов государственной власти РФ.

Сертификаты Минобороны РФ и Минкомсвязи России.

ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Техническая поддержка продуктов линейки «Континент» может осуществляться как напрямую, силами специалистов «Код-Безопасности», так и через авторизованных партнеров.
В случае технической поддержки через партнера, партнер обеспечивает первую линию технической поддержки, а в случае сложных вопросов обращается в службу технической поддержки вендора.
Существует несколько пакетов технической поддержки:

Базовый | Стандартный | Расширенный | VIP

КАТАЛОГ УСЛУГ	ПАКЕТ ПОДДЕРЖКИ			
	БАЗОВЫЙ	СТАНДАРТНЫЙ	РАСШИРЕННЫЙ	VIP
Доступность услуги	8x5, e-mail, телефон		24x7, e-mail, телефон	
Приоритет	Низкий	Средний	Высокий	Первоочередной
Количество обращений	Не ограничено			
Консультирование по установке и использованию продукта	●	●	●	●
Доступ на форум по продукту и к базе знаний	●	●	●	●
Доступ к пакетам обновлений	●	●	●	●
Личный кабинет на веб-портале	●	●	●	●
Прием предложений по улучшению продукта	●	●	●	●
Регистрация обращений на веб-портале		●	●	●
Консультирование по дополнительному функционалу продукта			●	●
Выделенный инженер (для проведения работ)				●
Присутствие инженера на площадке заказчика				●

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