

Континент 4

Универсальное устройство корпоративного уровня для всесторонней защиты сети (UTM) с поддержкой алгоритмов ГОСТ



Преимущества



Единая панель управления всеми механизмами защиты



Выделенный интерфейс для мониторинга инфраструктуры в реальном времени



Сигнатуры IPS, разработанные собственной лабораторией



Контроль более 4000 сетевых приложений



Патент на высокопроизводительный межсетевой экран



VPN-шлюз с поддержкой алгоритмов ГОСТ



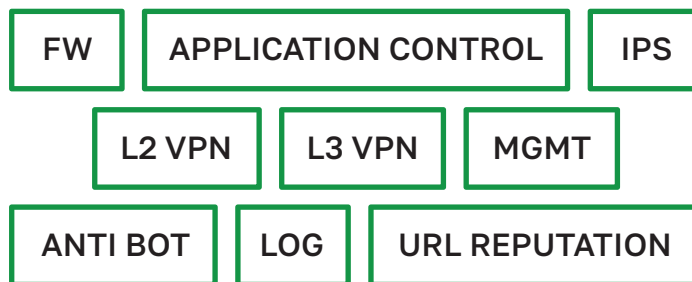
Визуализация данных мониторинга



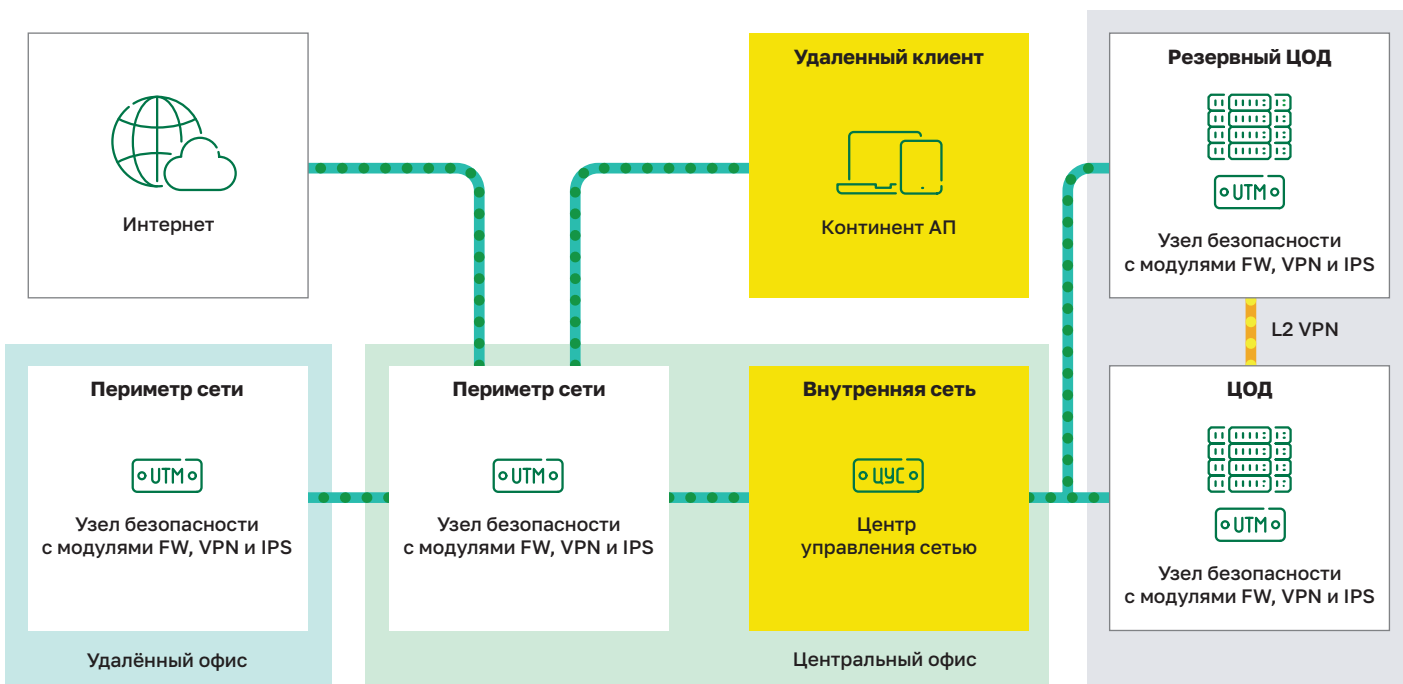
Варианты использования

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

Консолидация механизмов



Концепция UTM



Возможности



Защита от сетевых атак

- Два режима работы:
 - Обнаружение сетевых атак
 - Предотвращение сетевых атак в режиме реального времени
- Автоматическое обновление базы решающих правил с серверов «Кода безопасности»
- Сигнатуры IPS, разработанные собственной лабораторией
- Регистрация информации об атаке
 - Субъект/объект атаки, IP-адрес, номер порта
 - Возможность загрузки пользовательских сигнатур
 - Время и дата события
 - Тип атаки
 - Копия подозрительного трафика
- Оперативное уведомление об атаке
 - Оповещение в консоли мониторинга
 - Оповещение по электронной почте
 - Оповещение по SNMP



Управление и мониторинг

- Централизованное управление:
 - Узлами сети
 - Настройками маршрутизации
 - Правилами фильтрации трафика
 - VPN-сетями
- Мониторинг событий в режиме реального времени
- Ролевая модель доступа администраторов
- Высокопроизводительная система хранения и обработки событий безопасности
- Дистанционное обновление компонентов комплекса (системного ПО и базы решающих правил)
- Экспорт событий в SIEM-систему:
 - Поддержка SNMP v.2 и v.3
 - Поддержка Syslog
 - Поддержка NetFlow и IPFIX



Межсетевое экранирование

- Поддержка технологии Stateful Inspection
- Контроль сетевых приложений (Application Control)
- Защита от доступа к вредоносным сайтам
- Модуль поведенческого анализа
- Возможность управления всеми механизмами защиты в рамках одного правила
- Возможность идентификации и аутентификации пользователей (из локальной базы пользователей ЦУС и/или из MS Active Directory), работающих на компьютерах в защищаемой сети Узла Безопасности, с помощью Агентов аутентификации, установленных на компьютерах пользователей и/или Captive Portal





Сетевые возможности

- WAN-канал с поддержкой policy based routing
- Поддержка протоколов динамической маршрутизации
 - OSPF
 - BGP
- Агрегация интерфейсов по протоколу LACP (802.3ad)
- Поддержка приоритизации трафика (QoS)
- Поддержка подключения к нескольким каналам провайдера (Multi-WAN)
- Поддержка технологии VLAN (IEEE802.1Q)
- Поддержка технологии NAT
 - Source NAT
 - Destination NAT
- NAT-трансляция внутри VPN
- Встроенный DHCP-сервер с поддержкой режима DHCP-relay
- Поддержка VoIP



Шифрование

- Поддержка криптоалгоритмов ГОСТ
- Поддержка L3 VPN и L2 VPN



Отказоустойчивость

- Использование модулей твердотельной памяти DOM и SSD
- Режим автоматического переключения на резервный канал связи
- Режим кластера высокой доступности с автоматической синхронизацией состояния сессий
- Работа в необслуживаемом режиме 24x7x365
- Среднее время наработки на отказ – 50 000 часов



Модельный ряд

IPC-10

IPC-50M

IPC-500

IPC-500F

IPC-600

IPC-800F

Характеристики



Производительность

Производительность МЭ, Мбит/с	до 800	до 1 700	до 3 800	до 3 800	до 8 000	до 10 200
Производительность УТМ, Мбит/с	до 250	–	до 400	до 400	до 2 900	до 5 600
Производительность IPS, Мбит/с	до 100	–	до 1 750	до 1 750	до 1 500	до 3 000
Производительность VPN, Мбит/с	до 150	до 300	до 500	до 500	до 2 000	до 2 500
Максимальное число одновременных сессий МЭ	1 000 000	1 000 000	3 000 000	3 000 000	3 000 000	3 000 000
Производительность сервера доступа, Количество одновременных подключений	–	до 25	до 100	до 100	до 200	до 500
Производительность ЦУС, Количество устройств под управлением	–	–	до 20	до 20	–	–
Производительность выделенной аппаратной платформы управления, Количество устройств под управлением	–	до 20	IPC-500M до 80	–	IPC-600M до 400	–

Сетевые интерфейсы

Общее количество сетевых интерфейсов	3x Gigabit Ethernet	5x Gigabit Ethernet	6x Gigabit Ethernet	10x Gigabit Ethernet	8x Gigabit Ethernet	12x Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	3x 1000BASE-T RJ45	4x 1000BASE-T RJ45	6x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45	8x 1000BASE-T RJ45
Оптические интерфейсы	нет	1x 1G SFP	нет	2x 1G SFP	нет	4x 1G SFP

Отказоустойчивость и надежность

Режим кластера высокой доступности (горячее резервирование)	нет	–	да	да	да	да
Блок питания	Внешний адаптер 12V 40W	Внешний адаптер 12V 40W	1 x 150W	1 x 150W	1x250 W	1x250 W

IPC-1000F

IPC-3000F

IPC-3000FC

IPC-1000NF2

IPC-3000NF2

Характеристики



Производительность

Производительность МЭ, Мбит/с	до 22 300	до 40 000	–	до 40 000*	до 80 000*
Производительность UTM, Мбит/с	до 6 000	до 7 000	–	до 6 000	до 7 000
Производительность IPS, Мбит/с	до 6 500	до 10 000	–	до 6 500	до 10 000
Производительность VPN, Мбит/с	до 4 500	до 8 000	до 20 000	до 4 500	до 8 000
Максимальное число одновременных сессий МЭ	10 000 000	10 000 000	10 000 000	10 000 000	10 000 000
Производительность сервера доступа, Количество одновременных подключений	до 1 000	до 3 000	–	до 1 000	до 3 000
Производительность ЦУС, Количество устройств под управлением	до 50	до 100	–	до 50	до 100
Производительность выделенной аппаратной платформы управления, Количество устройств под управлением	IPC-1000FM до 1 000	–	–	–	–

Сетевые интерфейсы

Общее количество сетевых интерфейсов	16x Gigabit Ethernet	9x Gigabit Ethernet 4x 10 Gigabit Ethernet	9x Gigabit Ethernet 8x 10 Gigabit Ethernet	16x Gigabit Ethernet 4x 10 Gigabit Ethernet	9x Gigabit Ethernet 8x 10 Gigabit Ethernet
Интерфейсы RJ-45 (медь UTP)	8x 1000BASE-T RJ45	1x 1000BASE-T RJ45	1x 1000BASE-T RJ45	8x 1000BASE-T RJ45	9x 1000BASE-T RJ45
Оптические интерфейсы	8x 1G SFP	8x 1G SFP 4x 10G SFP+	8x 1G SFP 8x 10G SFP+	8x 1G SFP 4x 10G SFP+	8x 10G SFP+

Отказоустойчивость и надежность

Режим кластера высокой доступности (горячее резервирование)	да	да	да	да	да
Блок питания	2 x 300W с горячей заменой	2 x 300W с горячей заменой	2 x 300W с горячей заменой	2 x 300W с горячей заменой	2 x 300W с горячей заменой

* При использовании в режиме высокопроизводительного межсетевого экрана

IPC-3000FC



Формфактор: специализированная аппаратная платформа для построения защищённого VPN-канала

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

Сетевые интерфейсы: 1x 1000BASE-T RJ45
8x 1G SFP
4x 10G SFP+



Сертификация ФСТЭК России

Сертифицирован:

- 4 класс защищенности межсетевых экранов типа «А», 4 класс защиты СОВ уровня сети и 4 уровень доверия.

Планируется по наборам требований:

- 4 класс защищенности межсетевых экранов типа «Б», 4 класс защиты СОВ уровня сети и 4 уровень доверия.
- 3 класс защищенности межсетевых экранов типа «А», 3 класс защиты СОВ уровня сети и 3 уровень доверия.
- 3 класс защиты СОВ уровня сети и 3 уровень доверия.

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