



КОНТИНЕНТ 4

О ПРОДУКТЕ



КОД БЕЗОПАСНОСТИ





КОНТИНЕНТ 4

КОНТИНЕНТ 4

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

Предназначен для решения следующих задач:

- Централизованная и масштабируемая защита сети или критической информационной инфраструктуры
- Сегментация внутренней сети
- Предотвращение атак
- Анализ сетевых приложений (L7-фильтрация трафика)
- Криптографическая защита информации, передаваемой по открытым каналам связи
- Организация защищенного удаленного доступа



КОД БЕЗОПАСНОСТИ

Криптошлюз (КШ)



Криптокоммутатор (КК)



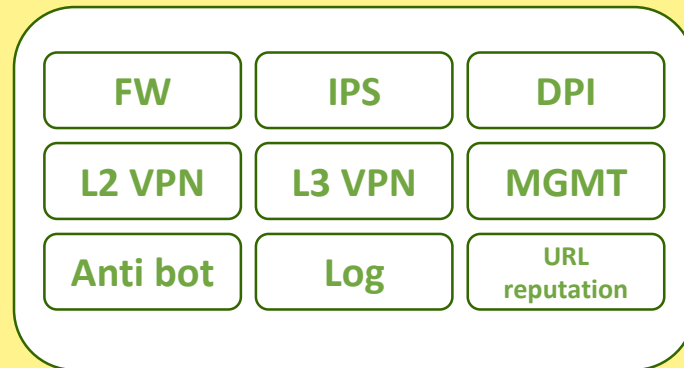
Детектор атак (ДА)

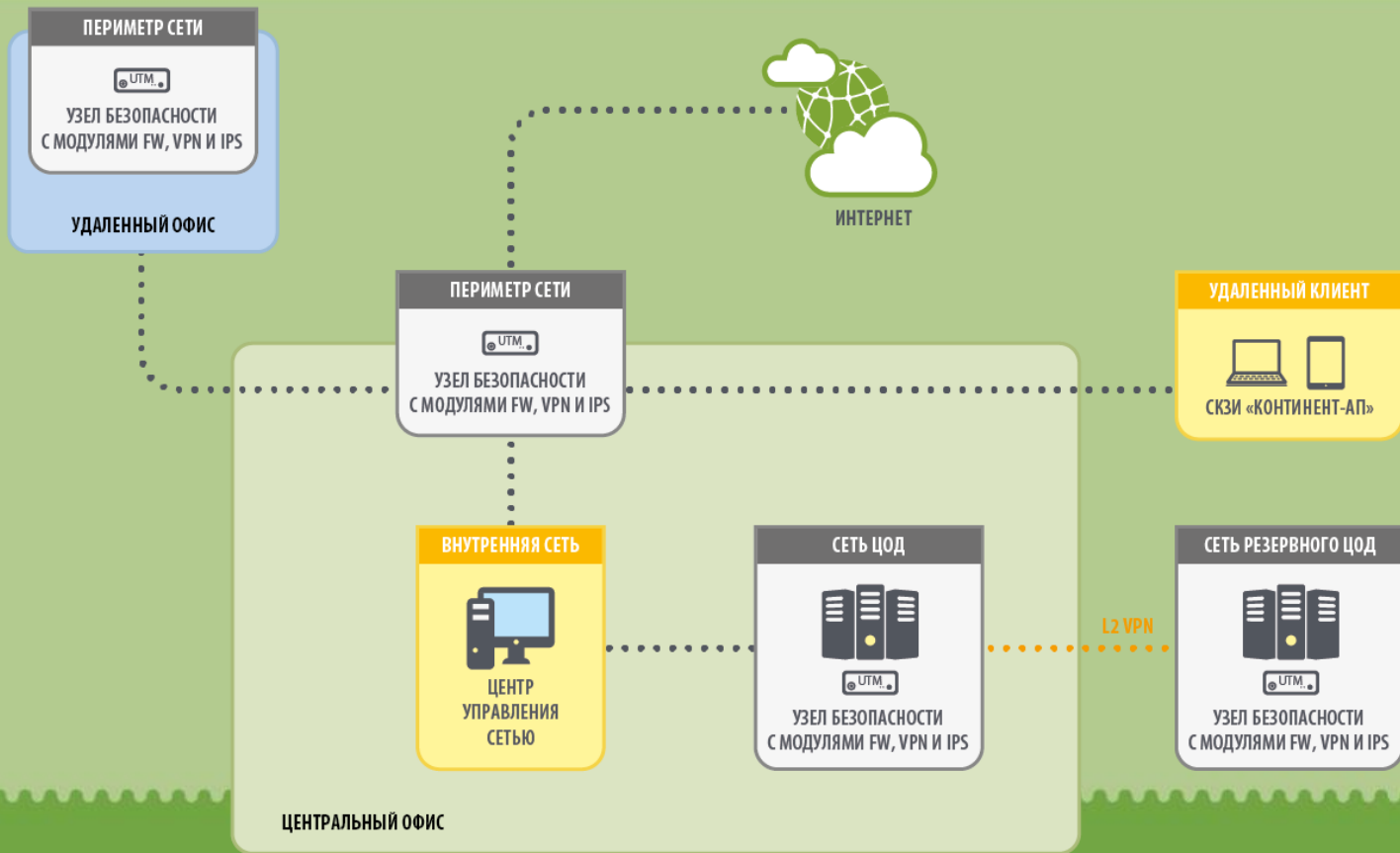


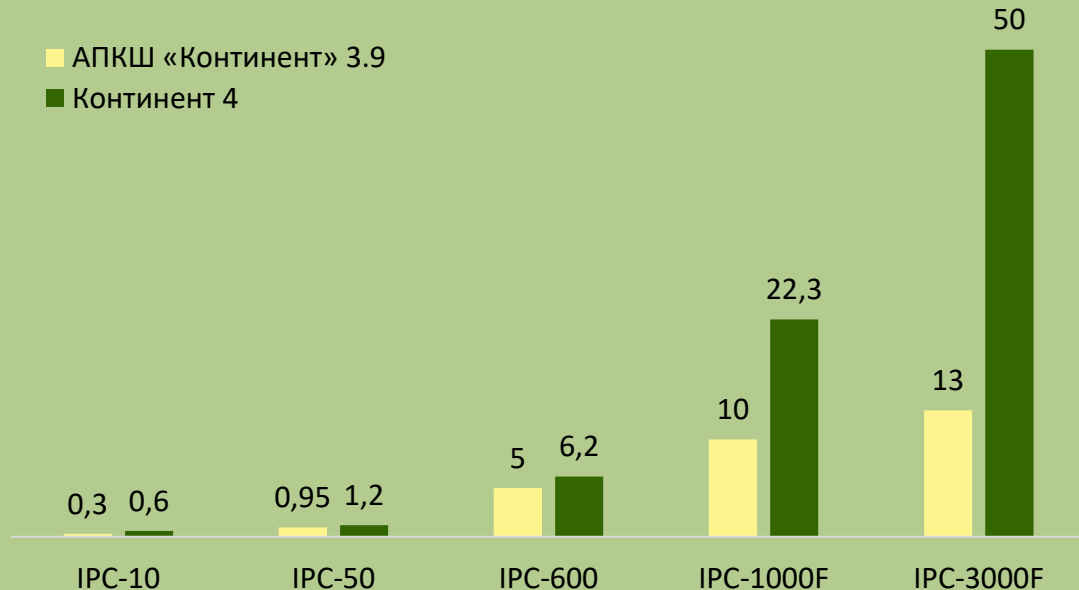
Центр управления сетью (ЦУС)



КОНСОЛИДАЦИЯ МЕХАНИЗМОВ БЕЗОПАСНОСТИ В ЕДИНОМ УСТРОЙСТВЕ





Производительность межсетевого экрана,
Гбит/с

Новый функционал
Одно устройство для всех механизмов безопасности
Управление компонентами из единого интерфейса
Доступ из веб-интерфейса мониторинга к данным в реальном времени из любой точки
Построение сложных VPN топологий уровня «созвездие»
Активация COB для конкретного правила фильтрации
Производительность внутреннего МЭ до 80 Гбит/с
Система машинного обучения в модуле поведенческого анализа



Таблицу с адресами всех объектов из всех подсетей хранит ЦУС. При изменении конфигурации сети и внесении изменений на ЦУСе, новая таблица будет применена на всех узлах безопасности.

Администратору безопасности не придется обновлять конфигурацию сети вручную на каждом узле большой инфраструктуры.

СИСТЕМА УПРАВЛЕНИЯ КОНТИНЕНТ 4





Система распределения трафика по механизмам безопасности позволяет проверять определенными модулями (DPI, IPS, URL reputation) только необходимый трафик.

Распределение трафика экономит вычислительные ресурсы устройства и обеспечивает высокую пропускную способность без необходимости снижения уровня защищенности.





КОД БЕЗОПАСНОСТИ

Все правила фильтрации и другие политики можно применять сразу к общекорпоративному каталогу без дублирования списка пользователей.

Интеграция упрощает процессы администрирования, аудита и логирования.

СИСТЕМА УПРАВЛЕНИЯ КОНТИНЕНТ 4





Централизованное управление настройками всех устройств
Континент в сети: их политиками, правилами маршрутизации и фильтрации трафика, VPN-сетями и криптографическими ключами.

Менеджер конфигурации позволяет администратору управлять всеми настройками в едином, удобном и продуманном интерфейсе.





Детальная настройка COB позволяет проверять трафик только по заданным сигнатурам.

COB не перегружает устройство обработкой всего потока трафика, поэтому пропускная способность не снижается при фильтрации другими модулями безопасности.

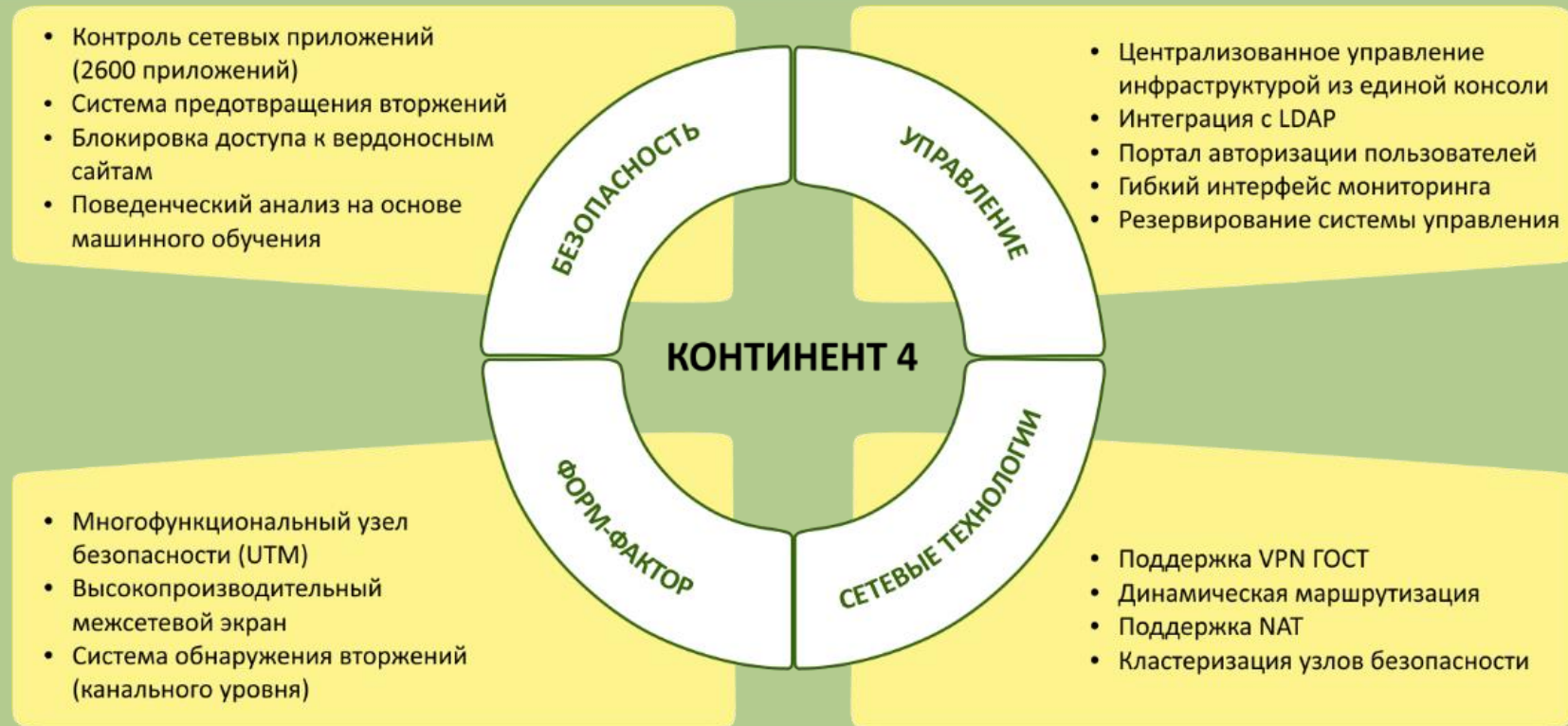




Мониторинг в реальном времени осуществляется в отдельно вынесенном веб-интерфейсе без привязки к консоли ЦУСа.

Мониторинг в реальном времени и из любой точки обеспечивает быстрое реагирование на инциденты.







КОД БЕЗОПАСНОСТИ



КОНТИНЕНТ 4

ПРОХОЖДЕНИЕ СЕРТИФИКАЦИОННЫХ ИСПЫТАНИЙ

По требованиям РД ФСТЭК России

- 4 класс МЭ тип «А»
- 4 класс сетевой СОВ (ИТ.СОВ.С4.ПЗ)

По требованиям РД ФСБ России

- 4 класс МЭ
- СКЗИ класса КС2/КС3

Продукт будет сертифицирован для защиты

- значимых объектов критической информационной инфраструктуры (КИИ) до 1 категории включительно
- государственных информационных систем (ГИС) до К1 включительно
- информационных систем персональных данных (ИСПДн) до УЗ1 включительно
- автоматизированных систем до класса 1Г включительно



КОД БЕЗОПАСНОСТИ

ИННОВАЦИИ ДЛЯ УВЕЛИЧЕНИЯ ПРОИЗВОДИТЕЛЬНОСТИ



Высокопроизводительный МЭ (NF2)

- Производительность до 80 Gbit/s
- Производительность не зависит от количества правил



Оптимизированные IPS сигнатуры

Аппаратный криптоускоритель

- Производительность до 20 Gbit/s
- Минимальные задержки

ВАРИАНТЫ ПРИМЕНЕНИЯ



КОД БЕЗОПАСНОСТИ







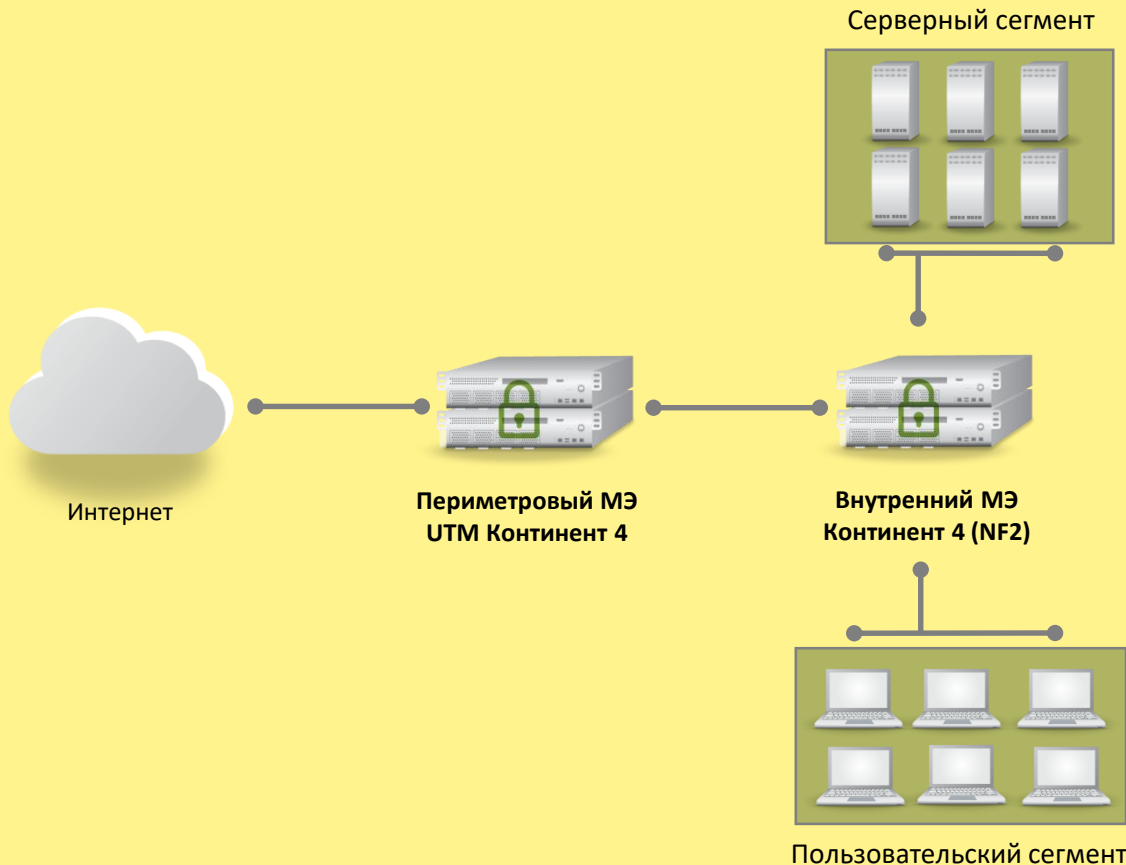
Задачи:

- **Защита взаимодействия с Интернет**

- идентификация пользователей
- обнаружение вторжений
- глубокий анализ трафика
- защита от вредоносных сайтов
- подключение удаленных пользователей
- создание защищенных каналов связи

- **Изоляция сетевых сегментов**

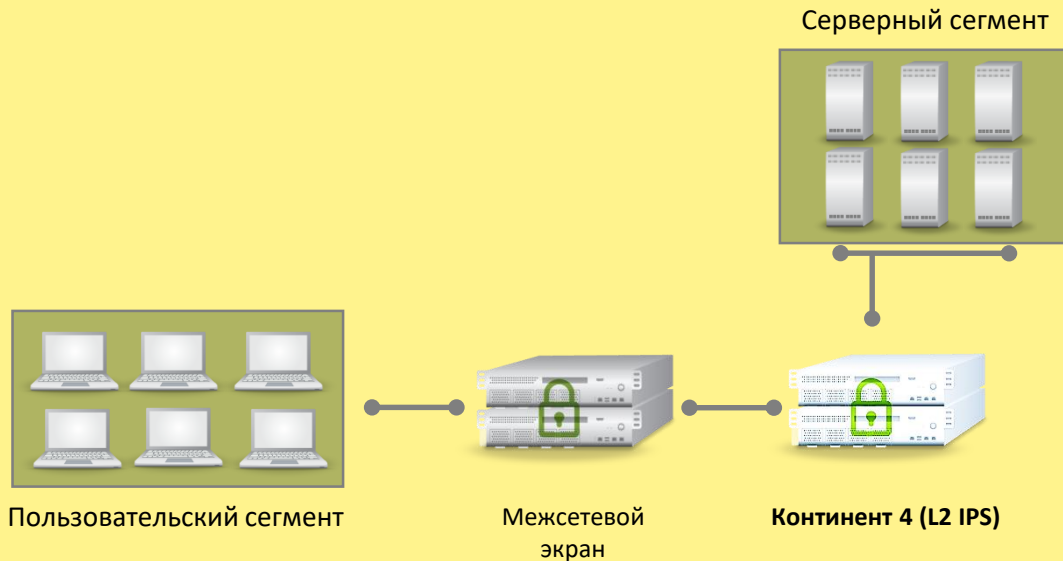
- высокая пропускная способность на любых пакетах
- возможность работать с большой политикой фильтрации трафика
- высокий уровень отказоустойчивости





Задачи:

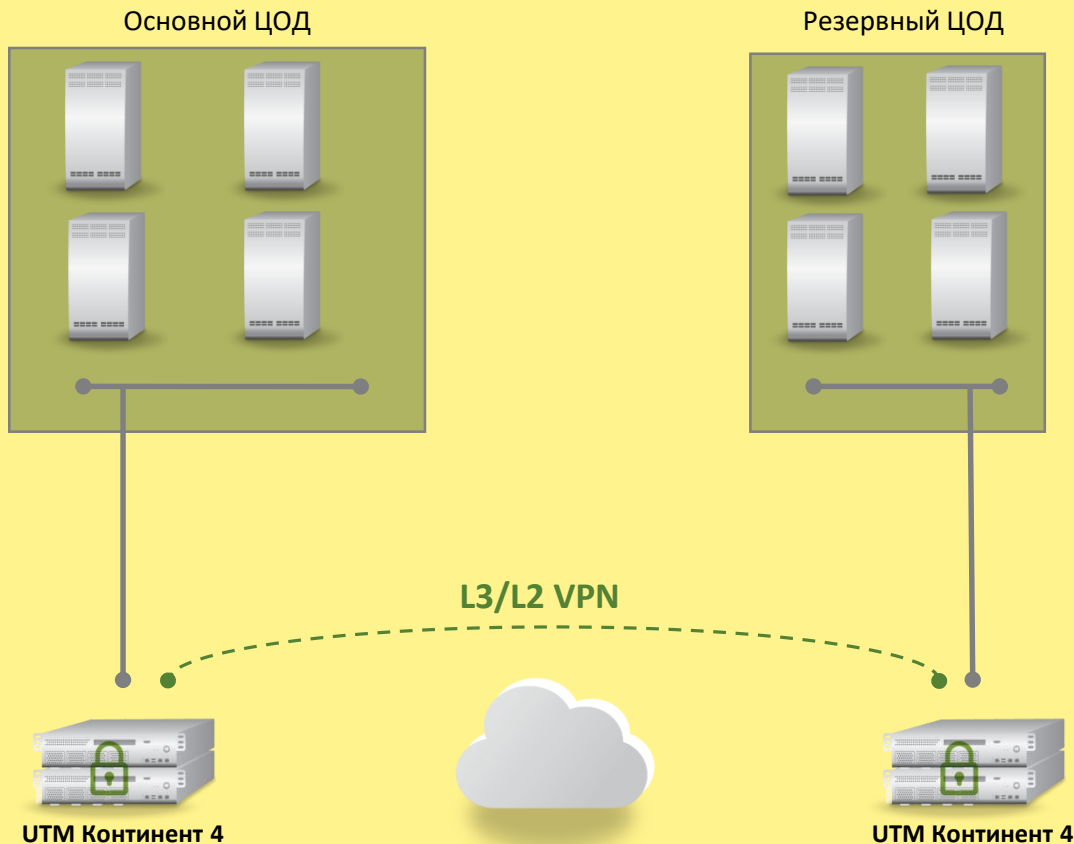
- Обнаружение сетевых угроз
- Выполнение требований приказов ФСТЭК России
 - Приказ № 21 (защита ИСПДн)
 - Приказ № 17 (защита ГИС)
 - Приказ № 239 (защита КИИ)





Задачи:

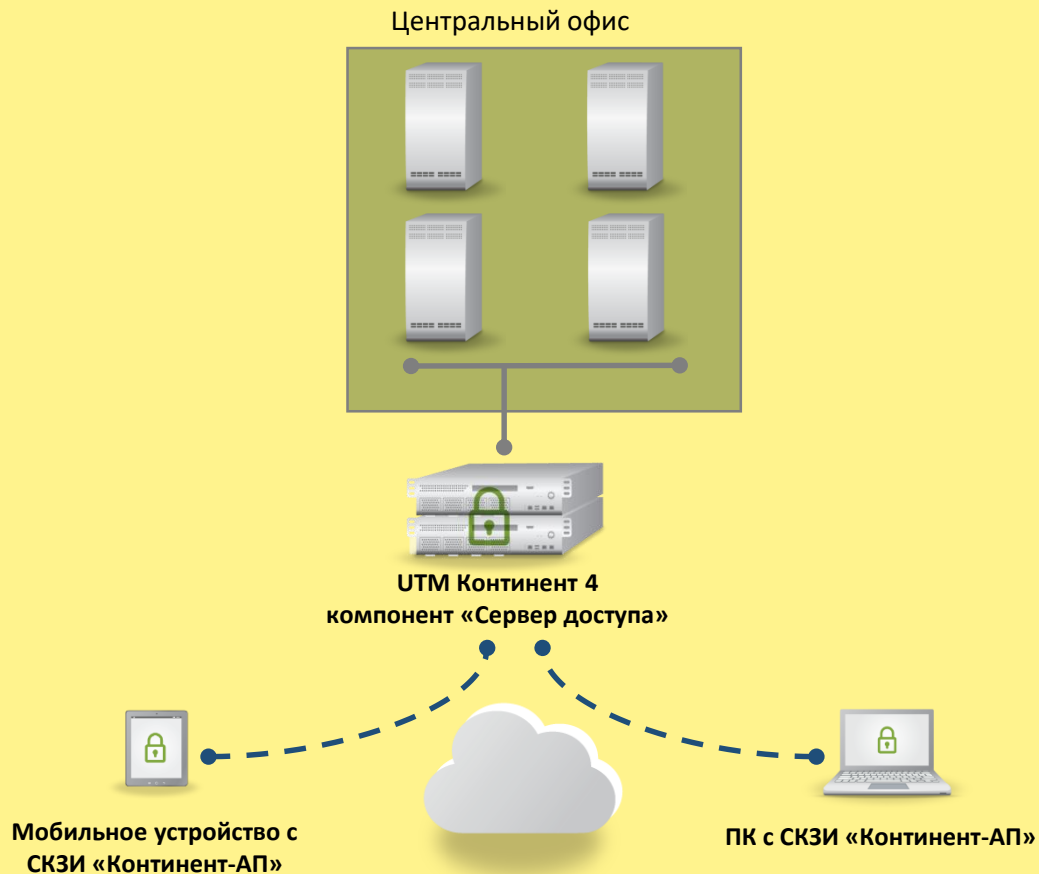
- Защита канала между основным и резервным ЦОД
 - репликация СХД
 - кластеризация серверов приложений
- Обеспечение низкой задержки и показателя Round Trip Time





Задачи:

- Защищенный доступ к корпоративным ресурсам
 - с компьютеров
 - с мобильных устройств
- Защищенный доступ к терминальным серверам/VDI



КОМПОНЕНТЫ



КОД БЕЗОПАСНОСТИ





Централизованное управление:

- Узлами сети
- Настройками маршрутизации
- Правилами фильтрации трафика
- VPN-сообществами
- Криптографическими ключами
- Политикой IPS

Пользователь «в центре» политики

- Интеграция с LDAP
- Captive-портал

Единая база сетевых объектов для политики безопасности

Ролевое управление доступом

Отдельный web-интерфейс мониторинга



Главная Вид

Назад Вперед Правило после Правило до Первое правило Последнее правило Раздел Разкрыть все Свернуть все Раздел Правило Разное Политика

Навигация

Контроль доступа

- Мехсетевой экран
- Web/FTP группы фильтров
- Профили Web/FTP фильтрации
- Трансляция сетевых адресов

Разделы (7), Правила фильтрации (13)

Поиск...

№	Название	Отправитель	Получатель	Сервис	Приложение	Действие	Профиль	COB	Временной интервал
SSH-connect									
1	to SN	192.168.1.0/24 - SMS...	Ек-SN-10.0.10.11	SSH	* Любое	Пропустить	* Не задан	- Выкл	* Всегда
VPN-L3									
2		192.168.1.0/24 - SMS...	192.168.30.0/24 - SN...	* Любой	* Любое	Пропустить	* Не задан	- Выкл	* Всегда
Internet									
3	dns	* Любой	* Любой	DNS DNS	* Любое	Пропустить	* Не задан	- Выкл	* Всегда
4	fpi - web client	192.168.20.0/24-SN-n...	* Любой	* Любой	twitter instagram	Пропустить	* Не задан	- Выкл	* Всегда
5	fpi - thick client	192.168.20.0/24-SN-n...	* Любой	* Любой	steam teamviewer	Пропустить	* Не задан	- Выкл	* Всегда
SSH-inspection									
6	SN-insp	192.168.20.0/24-SN-n...	SSH-server-192.168.1.4	ssh-inspection	* Любое	Пропустить	* Не задан	- Выкл	* Всегда
7	ncc	Ек-SN-10.0.10.11	SSH-server-192.168.1.4	* Любой	* Любое	Пропустить	* Не задан	- Выкл	* Всегда
Remote Access+IPS									

Список объектов ЦУС

Поиск...

Название	Адрес	Маска	Описание
1.1.1.0/24 - Remote net	1.1.1.0	24	
102.1.1.0/24 - protected	102.1.1.0	24	
103.1.1.0/24 - assaulter	103.1.1.0	24	
192.168.1.0/24 - SMS-net	192.168.1.0	24	
192.168.20.0/24-SN-net-2	192.168.20.0	24	
192.168.30.0/24 - SN-net	192.168.30.0	24	
Ек-SN-10.0.10.11	10.0.10.11		
Internet address - SN 100...	100.127.254.101		

Контроль доступа

Виртуальные частные сети

Система обнаружения вторжений

Структура

Администрирование

admin



Структура

Узлы безопасности

Узлы безопасности (2)

С...	Название	Компоненты	Домен	Версия конфигурации	Срок действия сертификата, дней
✓	sgw-1	[Icons]	domain-1	✓ 10421	✓ 276
✓	sgw-2	[Icons]	domain-1	✓ 10426	✓ 304

Узел безопасности - sgw-2

Узел безопасности

- Сертификаты
- Идентификация пользователей
- Сервер доступа
- Интерфейсы
- Статические маршруты
- Динамические маршруты
- Настройки журналирования
 - Локальное хранилище
 - Внешнее хранилище
- DNS
- DHCP
- SNMP
- Дата и время
- Детектор атак
 - Переменные COB

Идентификатор: 2

Название: sgw-2

Описание:

Платформа

Режим: UTM Модель: IPC-100 (MS-S100A)

Компоненты

- ☐ Центр управления сетью
- ☒ Межсетевой экран
 - ☒ Расширенный контроль приложений
 - ☒ Защита от вредоносных веб-сайтов
- ☒ L2VPN
- ☒ L3VPN
- ☒ Детектор атак
- ☒ Сервер доступа
- ☒ Идентификация пользователей
- ☐ Модуль поведенческого анализа

OK Отмена Применить

Идентификатор узла безопасности

Версия политики

Лицензии на компоненты



№	Название	Отправитель	Получатель	Сервис	Приложение	Действие	Профиль	COB	Временной интервал	Лог	Установить
L3VPN											
->DMZ											
2		192.168.10.0/24	web_dmz_10.10.1.1	TCP_1521	oracledb	Пропустить	* Не задан	Вкл	* Всегда	Лог	SG2
Internet											
CAPTIVE PORTAL											
8	Captive ...	i.ivanov m.sidorov	* Любой	tcp_443	* Любое	Пропустить	site1.testers.com_block	Выкл	* Всегда	Лог	SG2
DPI											
9	SSH Bl...	192.168.10.3	* Любой	SSH_inspection	* Любое	Отбросить	* Не задан	Выкл	* Всегда	Лог	SG2
10	VNC Bl...	* Любой	10.0.9.50	* Любой	vnc	Отбросить	* Не задан	Выкл	* Всегда	Лог	SG2
DROP ALL											

Пользователи
LDAPУсловия
фильтрацииЗаблокированный
вредоносный сайт

Включение IPS

Активный
шлюз



Application control (2600 приложений)

- VoIP/messaging: Skype, Oscar (ICQ & AIM), SIP, Skinny, H323, WhatsApp
- Social networking: Facebook, Twitter, MySpace, LinkedIn, Instagram, Tumblr
- P2P/filessharing: BitTorrent, eDonkey, Rapidshare, Uploaded.to, Xunlei
- Streaming: YouTube, Netflix, Hulu, Deezer, MyVideo, Vimeo, QQLive, Youku
- Enterprise: Citrix, Blackberry, SAP, MS Lync, MS Exchange, Lotus Notes, WebEx, etc.

Предотвращение сетевых вторжений

- Сигнатуры собственной разработки
- Возможность работы как на сетевом, так и на канальном уровнях

Блокировка доступа к вредоносным сайтам

- На базе технологий Лаборатории Касперского

SSL-decryption

Анализ сетевого трафика на наличие аномалий

Layer 3 and Layer 2 Network IPS



Система обнаружения вторжений

Политика COB

Профили COB

База решающих правил

Вендорские правила

- Malicious Command Centers
- Phishing
- Potentially dangerous traffic
- CryptoLockers
- Malware for mobile applications
- Backdoors
- Exploits
- Malicious file downloaders

Правила политики COB (1)

Название	Профиль COB	Установить	Описание
New rule	custom_IPS_profile	sgw-2	

Система обнаружения вторжений

Политика COB

Профили COB

База решающих правил

Вендорские правила

- Malicious Command Centers
- Phishing
- Potentially dangerous traffic
- CryptoLockers
- Malware for mobile applications
- Backdoors

Профили COB (6)

Имя	Описание
Full set	A set with a complete selection of rules
IPS_Profile	
IPS_profile	
Optimal set	A set containing a basic selection of rules
Recommended set	A set containing a selection of rules for the most ...
custom_IPS_profile	

Узлы на которые устанавливаются профили IPS

Специализированные профили под определенные типы угроз, в том числе 3 предустановленных профиля



Система обнаружения вто...

- Политика COB
- Профили COB
- База решающих правил
- Вендорские правила
- Пользовательские правила

Правила БРП (67)

Дата последнего обновления вендорской БРП: 03.07.2019 08:33

oracle

Правило БРП					Профили COB			
Важность	Описание	Класс	Ревизия	Идентиф...	Full set	IPS_Profile	Optimal set	Recommended set
Высокая	Successful Oracle/PeopleSoft Phish ...	Фишинг	1	4329393	Блокировать	Блокировать	Отключить	Отключить
Высокая	Oracle Secure Enterprise Search 10.1...	Веб-атаки	5	4109644	Блокировать	Отключить	Отключить	Блокировать
Высокая	Oracle BEA Weblogic Server 10.3 se...	Веб-атаки	5	4109645	Блокировать	Отключить	Отключить	Блокировать
Высокая	SELECT INSTR in URI Possible ORA...	Веб-атаки	4	4110285	Блокировать	Отключить	Отключить	Блокировать
Высокая	Possible Oracle Database Text Comp...	Веб-атаки	2	4110376	Блокировать	Отключить	Блокировать	Ctrl+Shift+B
Средняя	Suspicious inbound to Oracle SQL po...	Сетевые скане...	3	4110937	Оповещать	Отключить	Оповещать	Ctrl+Shift+A
Высокая	Oracle E-Business Suite Financials jtf...	Веб-атаки	2	4111058	Блокировать	Отключить	Пропустить	Ctrl+Shift+P
Высокая	Oracle E-Business Suite Financials jtf...	Веб-атаки	2	4111059	Блокировать	Отключить	Отключено	Ctrl+Shift+O
Высокая	Oracle E-Business Suite Financials jtf...	Веб-атаки	2	4111060	Блокировать	Отключить	Отключить	Блокировать

Информация

tcp \$EXTERNAL_NET any -> \$HOME_NET \$ORACLE_PORTS (msg:"Possible Oracle Database Text Component cbsys.drvxtabc.create_tables Remote SQL Injection Attempt"; flow:established,from_client; content:"cbsys|2E|drvxtabc|2E|create|5F|tables"; nocase; content:"dbms|5F|sql|2E|execute"; nocase; distance:0; pcre:"/cbsys|x2Edrvxtabc|x2Ecreate|x5Ftables.+(SELECT|DELETE|CREATE|INSERT|UPDATE|OUTFILE|si"; reference:url,www.securityfocus.com/bid/36748; reference:cve,2009-1991; classtype:web-application-attack; sid:4110376; rev:2;)



Разделы (0), Правила фильтрации (3)						
Поиск...						
№	Название	Отправитель	Получатель	Сервис	Приложение	Действие
1	Wks access	Net_10.5.5.0_24	Wks_192.168.1.2	* Любой	* Любое	Пропустить
2	Drop Streaming, Tunnel, Voice over IP	Net_10.10.10.0_24	* Любой	HTTP SSL	Streaming Tunnel Voice over IP	Отбросить
3	HTTP_80	Net_10.10.10.0_24	* Любой	HTTP	* Любое	Отбросить

Список объектов ЦУС				
streaming				
Название	Категория	Тип	Описание	
1kxun	Streaming		1kxun	
Sku	Streaming		Sku	
amazon-prime-music	Streaming		Amazon Prime Music	
amazon-prime-video	Streaming		Amazon Prime Video	
anghami	Streaming		Anghami	
apple-music	Streaming		Apple Music	
att-services	Streaming		ATT Services	
audiko	Streaming		Audiko	
audiogalaxy	Streaming		Audiogalaxy	

Группы и категории

Поиск

Список приложений



Узел безопасности - sgw-2

- Узел безопасности
 - Сертификаты
 - Идентификация пользователей
 - Сервер доступа
 - Интерфейсы
 - Статические маршруты
 - Динамические маршруты
- Настройки журналирования
 - Локальное хранилище
 - Внешнее хранилище
- DNS
- DHCP
- SNMP
- Дата и время
- Поведенческий анализ**
 - Шаблоны атак
- Детектор атак
 - Переменные COB

Режим: Постоянное обучение

Время обучения: 48 часов

Действие при обнаружении: Оповещать

Время блокирования: 300 секунд

Интерфейсы

Физические внешние и внутренние интерфейсы: + X

Список известных сетевых атак:

Состояние	Сетевая атака		Область действия		Исключение
	Название	Отправитель	Получатель		
☐	FIN/RST - scan	* Любой	* Любой	— Нет	
☐	Packet Sanity	* Любой	* Любой	— Нет	
☐	FRAGGLE - attack	* Любой	* Любой	— Нет	
☐	DNS max length	* Любой	* Любой	— Нет	
☐	Small Packet MTU	* Любой	* Любой	— Нет	
☐	DNS - mismatch	* Любой	* Любой	— Нет	
☐	SYN - flood	* Любой	* Любой	— Нет	
☐	UDP - scan	* Любой	* Любой	— Нет	

Используется система
машинного обучения



Высокопроизводительный МЭ на платформе Intel DPDK и префиксных деревьях

Шифрование по алгоритмам ГОСТ

L3 и L2 VPN

Автоматическая смена ключей

Динамическая маршрутизация

- OSPF
- BGP

Поддержка Jumbo-frame



Виртуальные частные сети

- L3VPN
- L2VPN
- Удалённый доступ

Виртуальные частные сети (1)

Поиск...

Топология	Состав	Защищаемые ресурсы	Описание
L3 VPN	sgw-1	192.168.1.0/24 - SMS-net	
Полносызкая сеть	sgw-2	192.168.30.0/24 - SN-net	

Список объектов ЦУС

Поиск...

Название	Адрес	Маска	Описание
1.1.1.0/24 - Remote net	1.1.1.0	24	
102.1.1.0/24 - protected	102.1.1.0	24	
103.1.1.0/24 - assaulter	103.1.1.0	24	
192.168.1.0/24 - SMS-net	192.168.1.0	24	
192.168.20.0/24-SN-net-2	192.168.20.0	24	

Управление всеми
схемами VPN

Выбор топологии и типа VPN

Участники VPN

Защищаемые ресурсы



КОД БЕЗОПАСНОСТИ

УДАЛЕННЫЙ ДОСТУП



«Континент-АП»

VPN-клиент для ПК с функциями
персонального межсетевого экрана

Интегрированный в VPN-клиент персональный
межсетевой экран

Поддержка авторизации на HTTP-proxy

Возможность установки VPN-соединения до
регистрации пользователя в ОС

Возможность работы как через TCP так и через UDP

Шифрование каналов связи с помощью алгоритма
ГОСТ 28147-89

Аутентификация пользователей по сертификатам
стандарта X.509

Поддержка различных ключевых носителей

МОДЕЛЬНЫЙ РЯД



КОД БЕЗОПАСНОСТИ

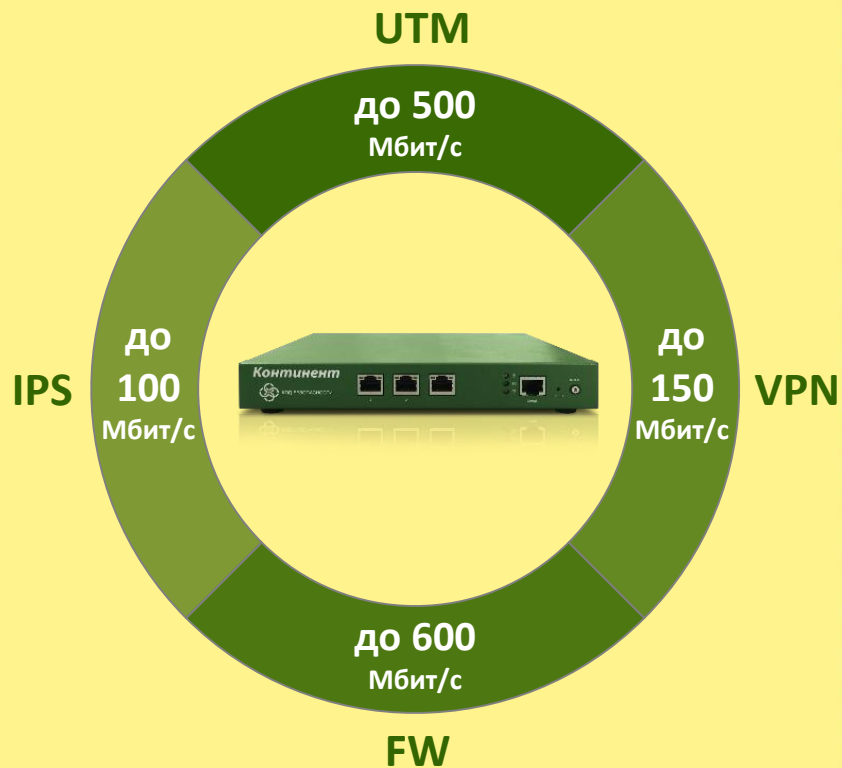




СЕГМЕНТ	КЛЮЧЕВЫЕ ФУНКЦИИ	УСТРОЙСТВА
 Филиал	Точка развертывания: Защита маленькой сети или филиала Форм-фактор: Desktop Интерфейсы: 1G GbE, 1G SFP Производительность: от 600 Мбит/с до 1,2 Гбит/с	IPC-10 IPC-50
 Крупный офис	Точка развертывания: Периметр корпоративной сети Форм-фактор: 1U Интерфейсы: 1G GbE, 1G SFP Производительность: от 2,6 Гбит/с до 11,5 Гбит/с	IPC-500 IPC-500F IPC-600 IPC-800F
 Центр обработки данных	Точка развертывания: Периметр корпоративной сети, внутренняя сеть Форм-фактор: 1U Интерфейсы: 1G GbE, 1G SFP, 10G SFP+ Производительность: 22,3 или 50 Гбит/с Специальные функции: Аппаратный криптоускоритель с низкими задержками обработки трафика	IPC-1000F IPC-3000F IPC-3000FC
 Крупный центр обработки данных	Точка развертывания: Внутренняя сеть Форм-фактор: 1U Интерфейсы: 1G GbE, 1G SFP, 10G SFP+ Производительность: 40 или 80 Гбит/с Специальные функции: высокая производительность на любых типах трафика, производительность не падает при увеличении числа правил фильтрации	IPC-1000NF2 IPC-3000NF2



Режимы работы:



Сетевые интерфейсы:

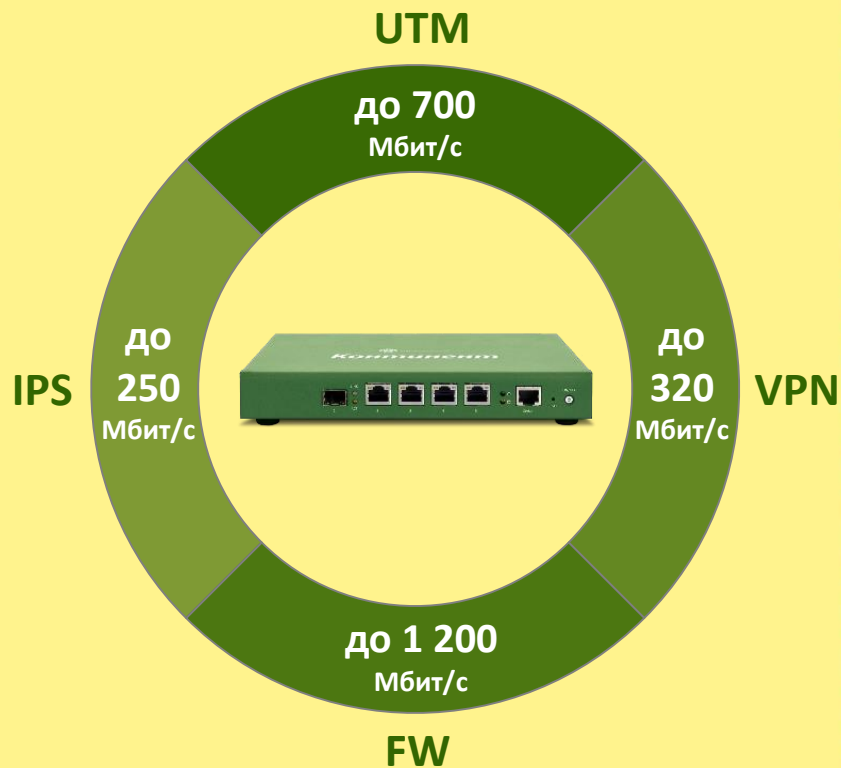
- 3x Ethernet 10/100/1000

Центр управления сетью:

- до 2 управляемых устройств



Режимы работы:



Сетевые интерфейсы:

- 4x Ethernet 10/100/1000
- 1x Gigabit Ethernet Fiber SFP

Центр управления сетью:

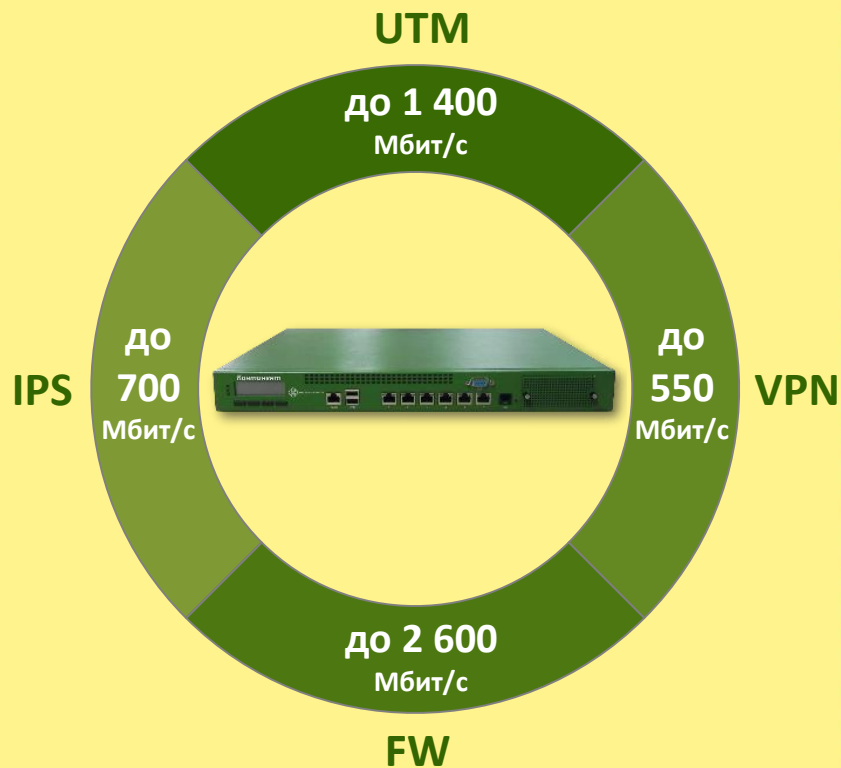
- до 5 управляемых устройств

Сервер доступа:

- до 25 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 6x Ethernet 10/100/1000

Центр управления сетью:

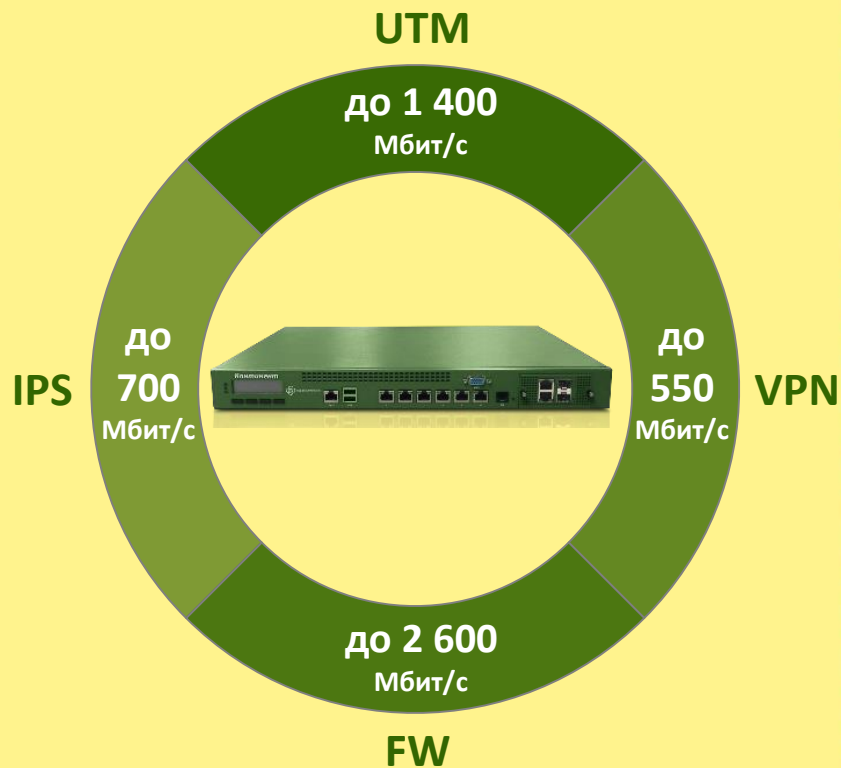
- до 50 управляемых устройств

Сервер доступа:

- до 100 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 6x Ethernet 10/100/1000
- 2x Gigabit Ethernet Fiber SFP

Центр управления сетью:

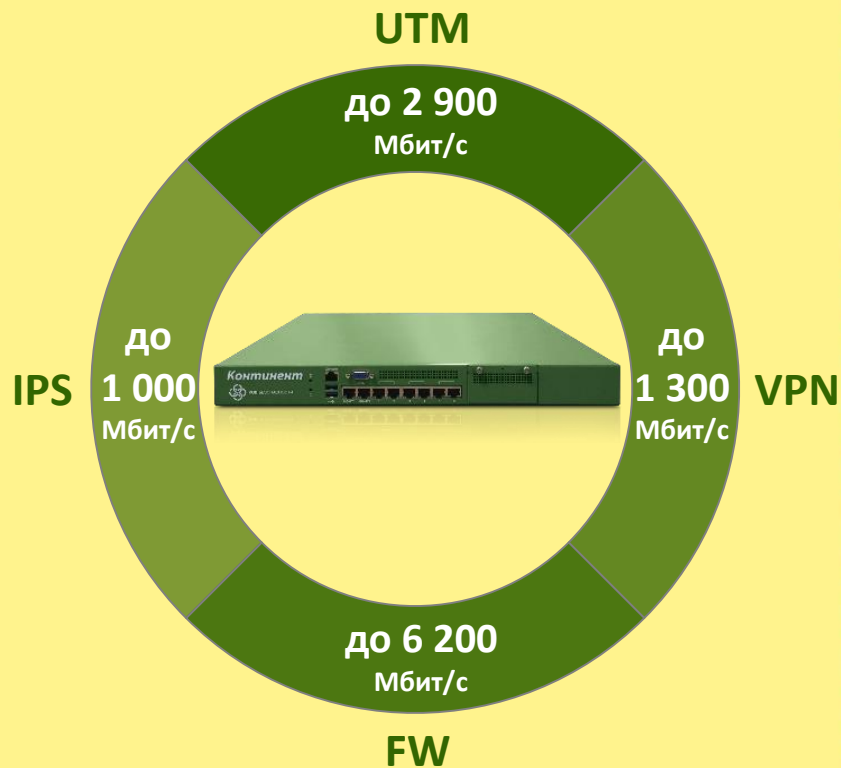
- до 50 управляемых устройств

Сервер доступа:

- до 100 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 8x Ethernet 10/100/1000

Центр управления сетью:

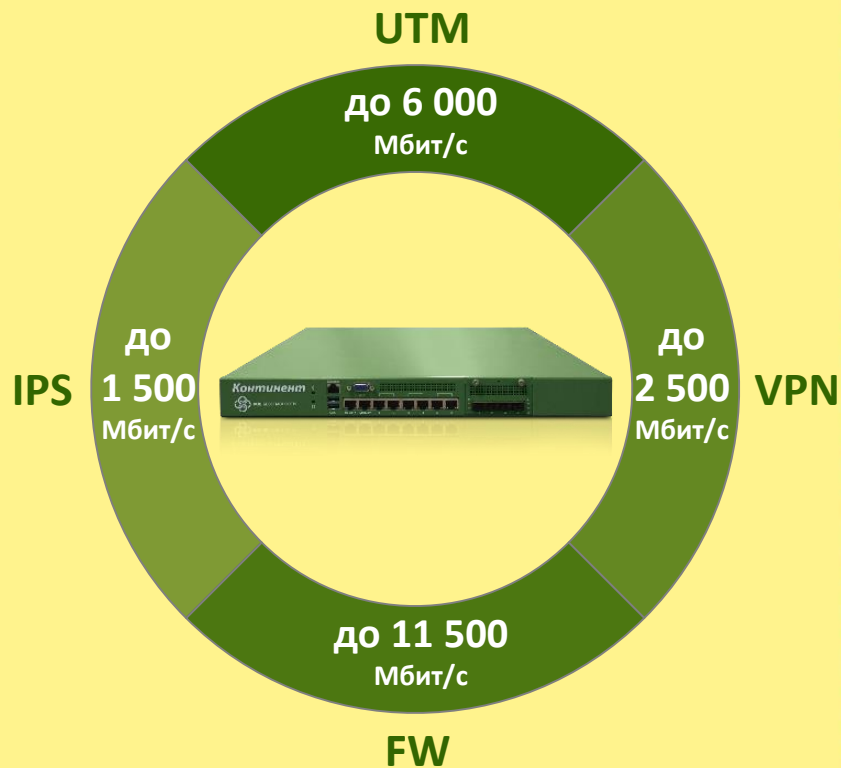
- до 100 управляемых устройств

Сервер доступа:

- до 200 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 8x Ethernet 10/100/1000
- 4x Gigabit Ethernet Fiber SFP

Центр управления сетью:

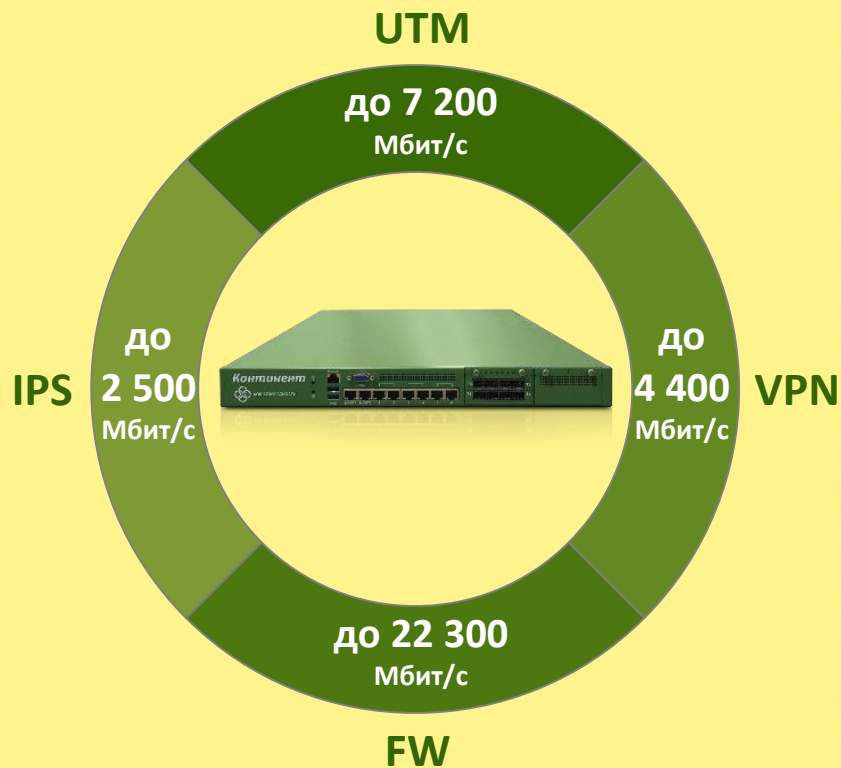
- до 100 управляемых устройств

Сервер доступа:

- до 500 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 8x Ethernet 10/100/1000
- 8x Gigabit Ethernet Fiber SFP

Центр управления сетью:

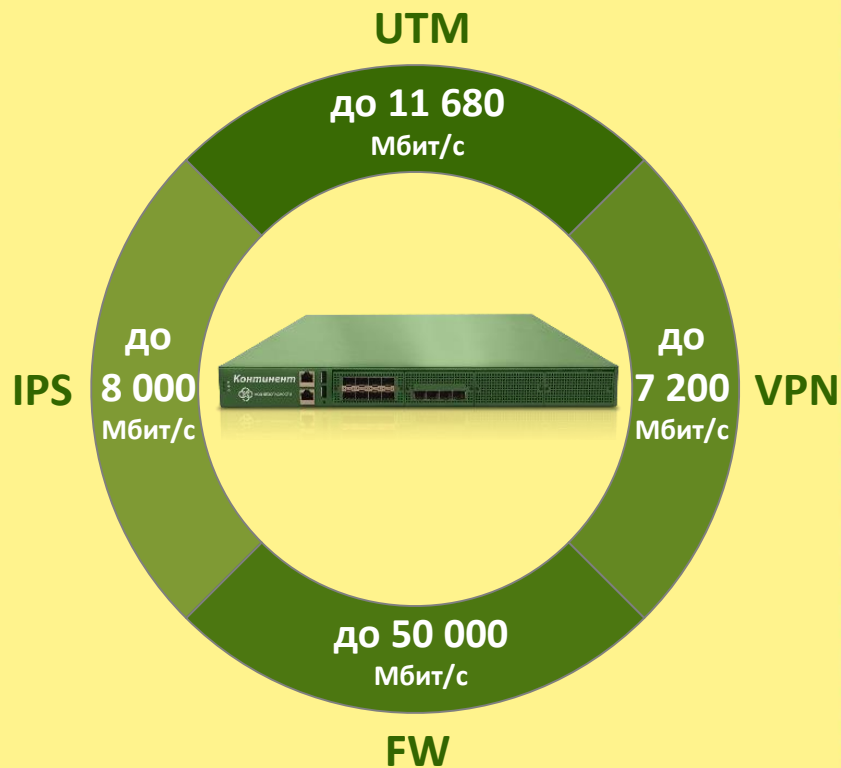
- до 200 управляемых устройств

Сервер доступа:

- до 1000 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 1x Ethernet 10/100/1000
- 8x Gigabit Ethernet Fiber SFP
- 4x 10 Gigabit SFP+

Центр управления сетью:

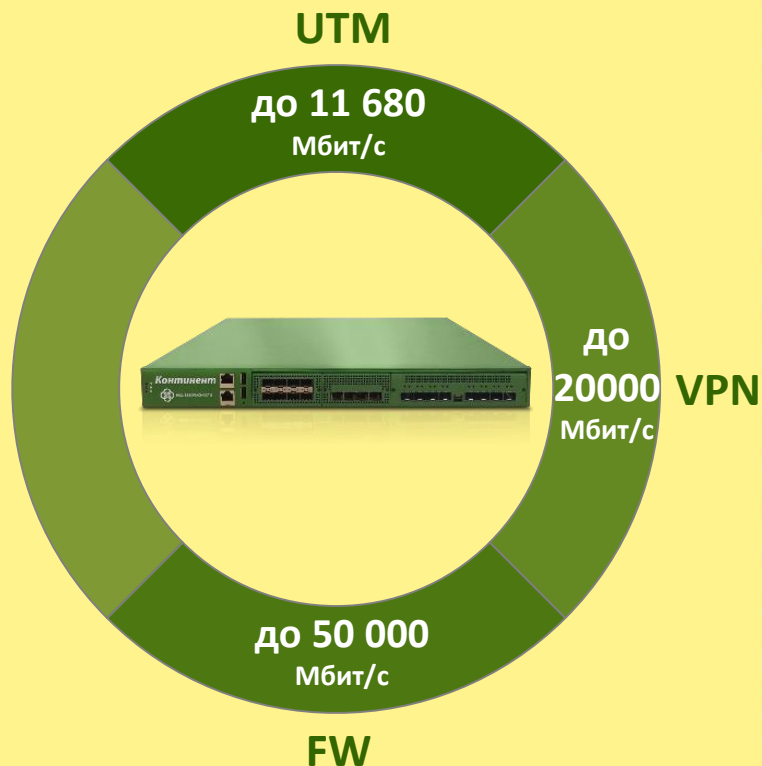
- до 300 управляемых устройств

Сервер доступа:

- до 3000 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 1x Ethernet 10/100/1000
- 8x Gigabit Ethernet Fiber SFP
- 8x 10 Gigabit SFP+

Центр управления сетью:

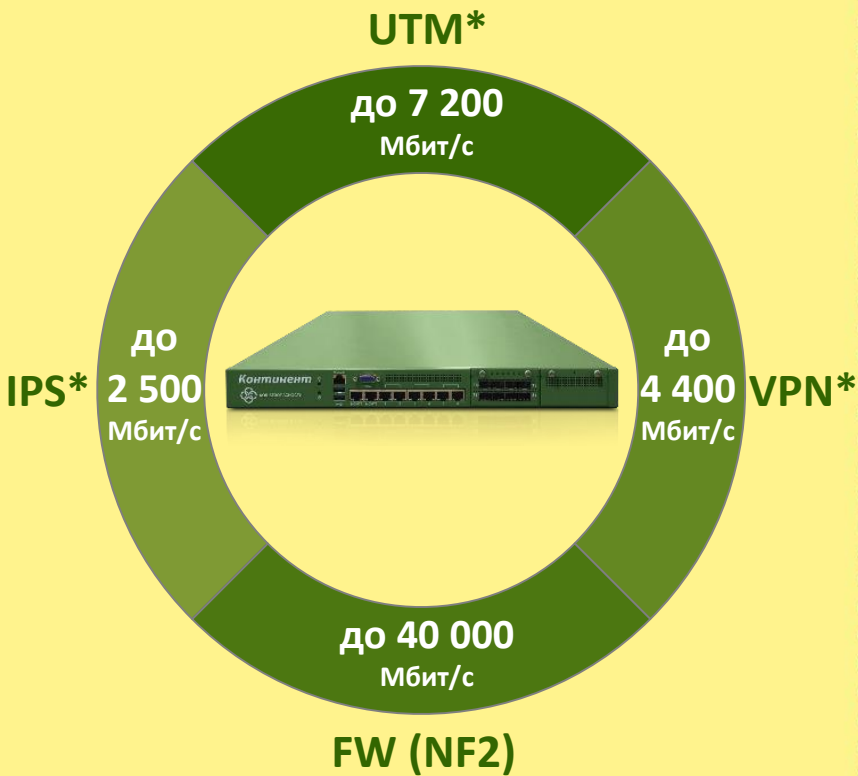
- до 300 управляемых устройств

Сервер доступа:

- до 3000 одновременных подключений СКЗИ «Континент-АП»



Режимы работы:



Сетевые интерфейсы:

- 8x Ethernet 10/100/1000
- 8x Gigabit Ethernet Fiber SFP
- 4x 10 Gigabit SFP+

Центр управления сетью:

- до 200 управляемых устройств

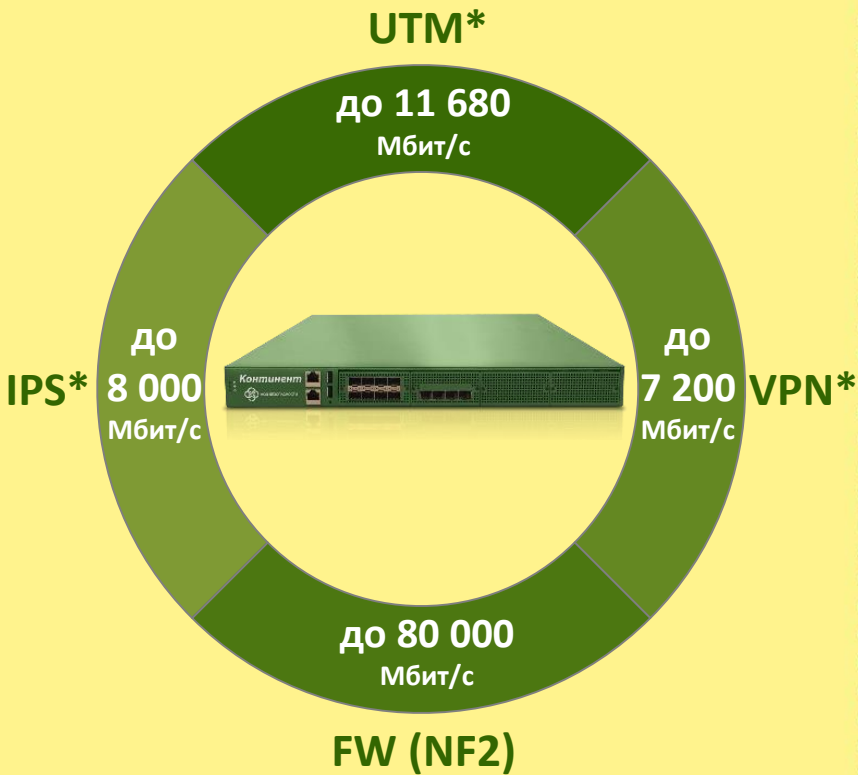
Сервер доступа:

- до 1000 одновременных подключений СКЗИ «Континент-АП»

* Режимы становятся активны при отключении высокопроизводительного межсетевого экрана (NF2)



Режимы работы:



Сетевые интерфейсы:

- 9x Ethernet 10/100/1000
- 8x 10 Gigabit SFP+

Центр управления сетью:

- до 300 управляемых устройств

Сервер доступа:

- до 3000 одновременных подключений СКЗИ «Континент-АП»

* Режимы становятся активны при отключении высокопроизводительного межсетевого экрана (NF2)

СВОДНАЯ ТАБЛИЦА ХАРАКТЕРИСТИК
ПЛАТФОРМ

ХАРАКТЕРИСТИКИ	IPC-10	IPC-50	IPC-500	IPC-500F	IPC-600	IPC-800F	IPC-1000F	IPC-3000F	IPC-3000FC	IPC-1000NF2	IPC-3000NF2
Производительность МЭ, Мбит/с	до 600	до 1 200	до 2 600	до 2 600	до 6 200	до 11 500	до 22 300	до 50 000	до 50 000	до 40 000	до 80 000
Производительность UTM, Мбит/с	До 500	до 700	до 1 400	до 1 400	до 2 900	до 6 000	до 7 200	до 11 680	до 11 680	до 7 200	до 11 680
Производительность L2 IPS, Мбит/с	до 100	до 250	до 700	до 700	до 1 000	до 1 500	до 2 500	до 8 000	---	до 2 500	до 8 000
Производительность VPN, Мбит/с	до 150	до 320	до 550	до 550	до 1 300	до 2 500	до 4 400	до 7 200	до 20 000	до 4 400	до 7 200
Производительность Сервера доступа (одновременные подключения СКЗИ «Континент-АП»)	---	до 25	до 100	до 100	до 200	до 500	до 1 000	до 3 000	до 3 000	до 1 000	до 3 000
Производительность ЦУС (количество управляемых устройств)	до 2	до 5	до 50	до 50	до 100	до 100	до 200	до 300	до 300	до 200	до 300
Сетевые интерфейсы	3x Ethernet 10/100/1000	4x Ethernet 10/100/1000 1x 1000BASE-X SFP	6x Ethernet 10/100/1000	6x Ethernet 10/100/1000 2x 1000BASE-X SFP	8x Ethernet 10/100/1000	8x Ethernet 10/100/1000 4x 1000BASE-X SFP	8x Ethernet 10/100/1000 8x 1000BASE-X SFP	1x Ethernet 10/100/1000 8x 1000BASE-X SFP 4x 10 Gigabit SFP+	1x Ethernet 10/100/1000 8x 1000BASE-X SFP 8x 10 Gigabit SFP+	8x Ethernet 10/100/1000 8x 1000BASE-X SFP 4x 10 Gigabit SFP+	9x Ethernet 10/100/1000 8x 10 Gigabit SFP+

СПАСИБО!

КОНТАКТЫ:

+7 (495) 982-30-20

info@securitycode.ru

www.securitycode.ru



КОД БЕЗОПАСНОСТИ

