

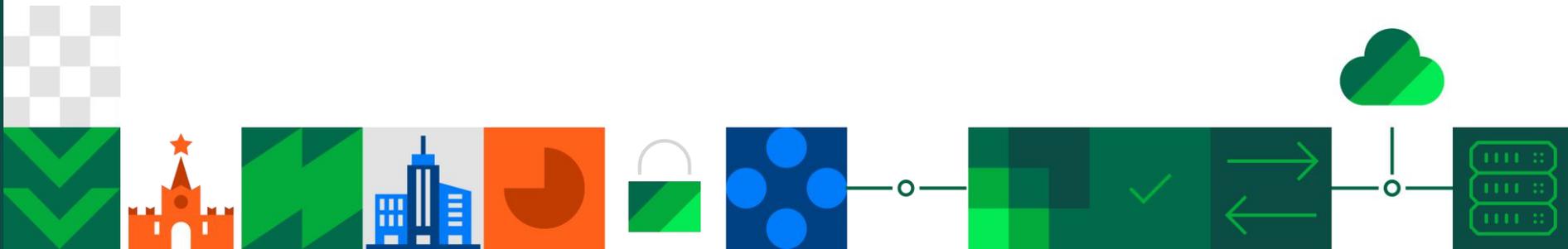


Континент 4





О продукте



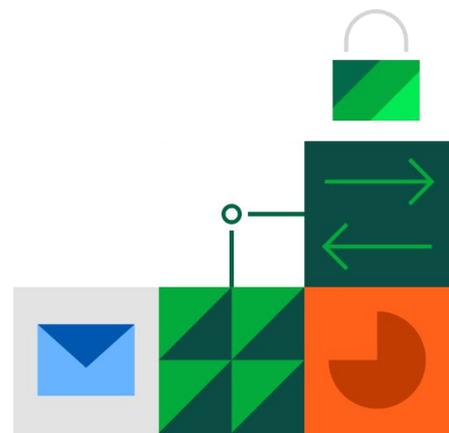


Континент 4

Многофункциональный межсетевой экран (NGFW/UTM) с поддержкой алгоритмов ГОСТ

Предназначен для решения следующих задач:

- ✓ Централизованная защита периметра корпоративной сети
- ✓ Контроль доступа пользователей в Интернет
- ✓ Предотвращение сетевых вторжений
- ✓ Организация защищенного удаленного доступа



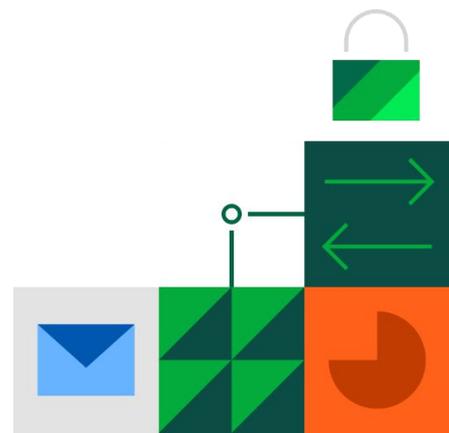
Сертифицирован ФСТЭК России:

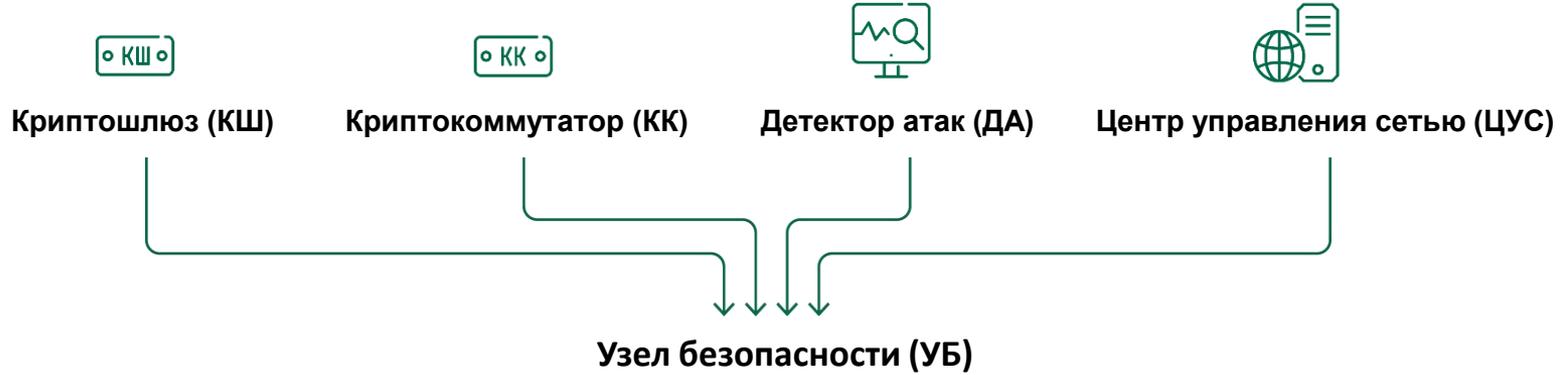
- 4-й класс защиты МЭ типа «А»
- 4-й класс защиты МЭ типа «Б»
- 4-й класс защиты СОВ уровня сети
- 4-й уровень доверия



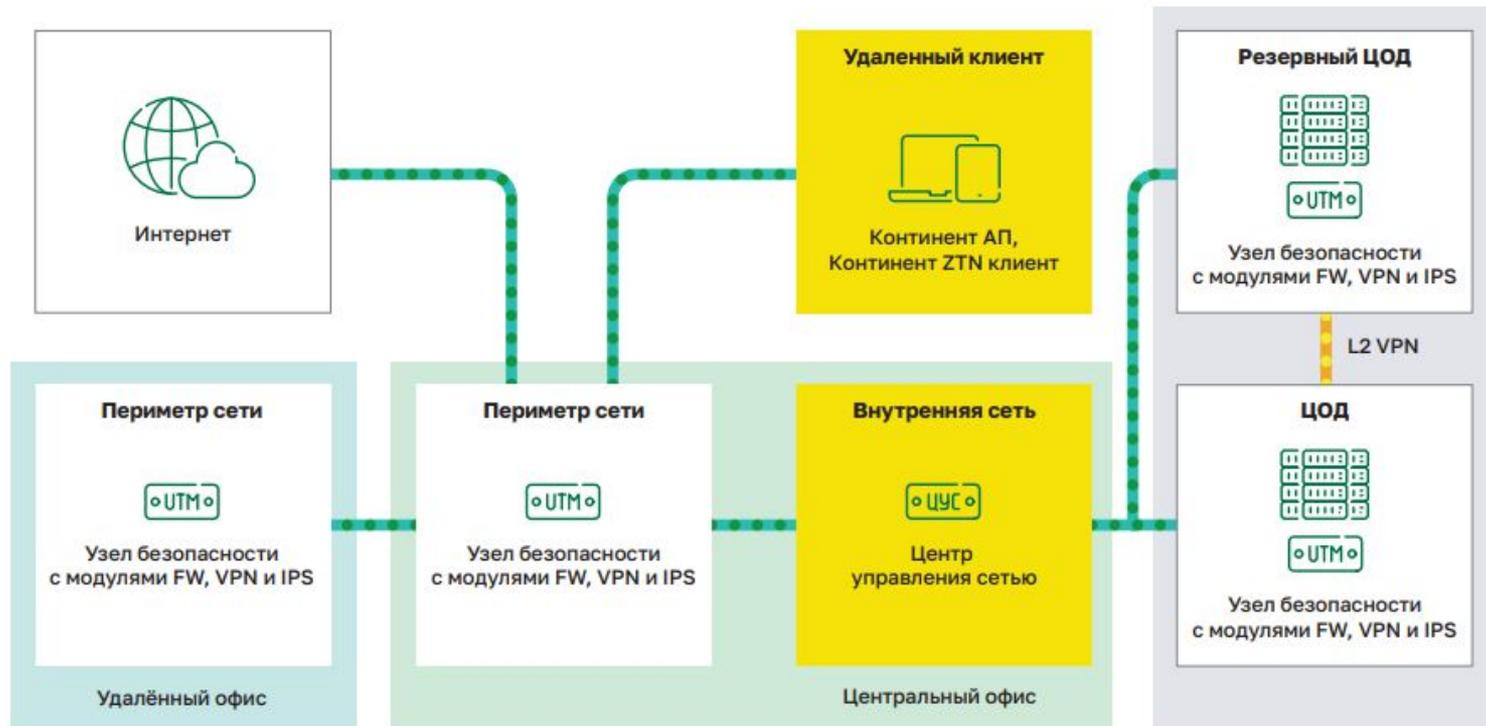
Сертификат ФСТЭК России № 4496 (действует до 14.12.2026) распространяется на:

- Континент 4.1.0.2825
- Континент 4.1.0.3070
- Континент 4.1.0.3175
- Континент 4.1.5.2475
- Континент 4.1.7.1325
- Континент 4.1.7.1395



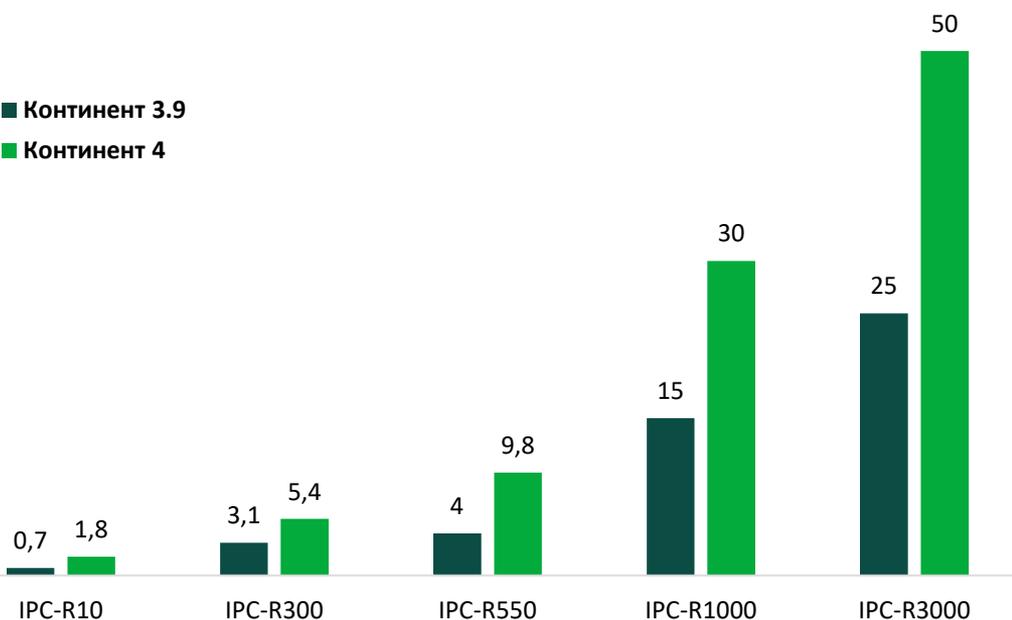


- FW
- IPS
- App control
- L2 VPN
- L3 VPN
- MGMT
- Threat Intelligence
- Log
- URL Filtering
- User Identity
- Antivirus
- GeoIP



Производительность межсетевого экрана, Гбит/с

■ Континент 3.9
■ Континент 4



НОВЫЙ ФУНКЦИОНАЛ

Одно устройство для всех механизмов безопасности

Новые механизмы безопасности (контроль приложений, фиды Threat Intelligence, URL-категоризация, антивирус)

Идентификация пользователей из Active Directory

Мониторинг с веб-интерфейсом

Активация COV для конкретного правила фильтрации

Производительность внутреннего МЭ до 80 Гбит/с

Самообучающийся модуль поведенческого анализа для защиты от DoS-атак

Новая операционная система ContinentOS



Единая база сетевых объектов хранится на ЦУС.

Любой объект из базы ЦУС может быть использован в правилах фильтрации.

Для каждого правила могут быть выбраны узлы, на которые оно будет установлено.

Администратору безопасности не придется вручную настраивать каждый узел при внесении изменений в корпоративную сеть.



Система распределения трафика по механизмам безопасности позволяет проверять определенными модулями (Контроль приложений, IPS, URL reputation) только выбранный трафик.

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



Группы пользователей из общего корпоративного каталога можно добавлять в правила фильтрации в качестве источника.

Прозрачная аутентификация SSO через протокол Kerberos.

Интеграция упрощает процессы администрирования, аудита и логирования.

Нет необходимости заводить новых пользователей локально.



Централизованное управление настройками всех устройств Континент в сети: их политиками, правилами маршрутизации и фильтрации трафика.

Массовое развёртывание узлов безопасности.

Импорт политик со сторонних МСЭ/Миграция.

Планировщик обновлений.

Централизованная настройка и управление устройствами упрощает администрирование и аудит.



Детальная настройка COB позволяет проверять трафик только по заданным сигнатурам.

COB не перегружает устройство обработкой всего потока трафика по всем сигнатурам, что позволяет освободить ресурсы для других механизмов защиты и снизить нагрузку на устройство.



Мониторинг осуществляется из независимого от консоли управления веб-интерфейса.

Отправка логов в сторонние системы для анализа по протоколам syslog, NetFlow, SNMP.

Получение оповещений об установке политик.

Мониторинг позволяет обеспечить быстрое реагирование на инциденты.



Безопасность

- Контроль сетевых приложений (4000 приложений)
- Система предотвращения вторжений
- Блокировка доступа к вредоносным сайтам (Threat Intelligence)
- URL-фильтрация по категориям
- Фильтрация трафика по принадлежности IP-адреса к стране
- SSL-инспектирование трафика
- Поведенческий анализ на основе машинного обучения
- Поддержка VPN ГОСТ



Управление

- Централизованное управление инфраструктурой из единой консоли
- Интеграция с LDAP
- Портал и агент аутентификации пользователей, SSO
- Гибкий интерфейс мониторинга
- Резервирование системы управления



Форм-фактор

- Многофункциональный узел безопасности (UTM)
- Высокопроизводительный межсетевой экран
- Система обнаружения вторжений (L2 IPS)
- Выделенная платформа управления

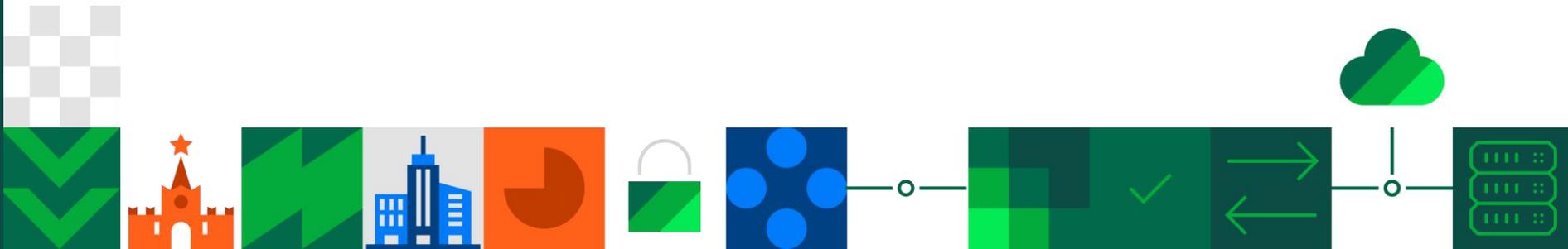


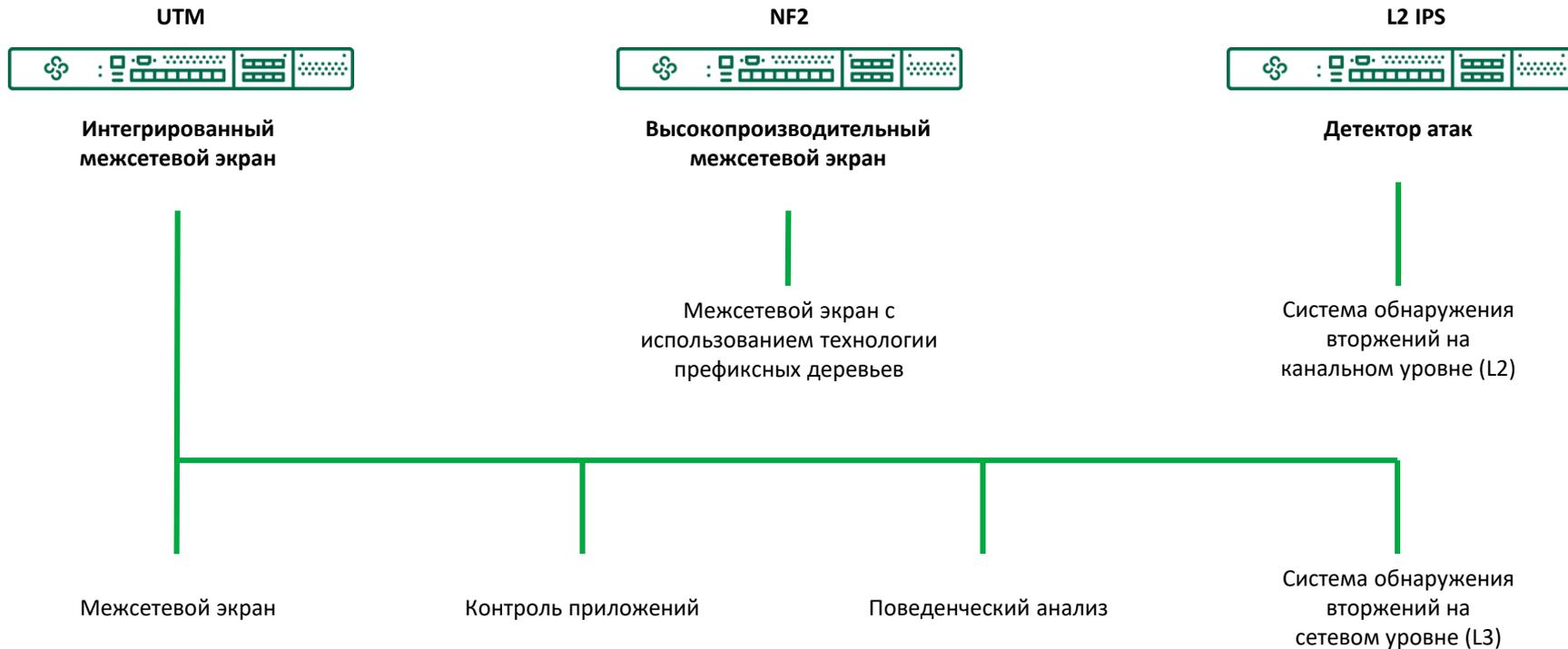
Сетевые технологии

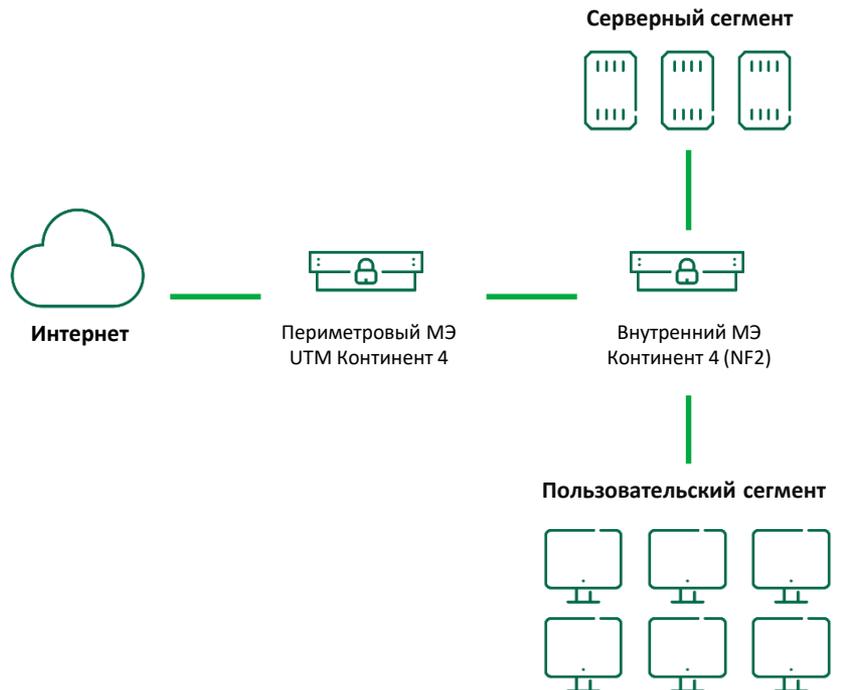
- Динамическая маршрутизация
- Поддержка NAT
- Multi-WAN
- QoS
- Кластеризация узлов безопасности (переключение менее 1 секунды)



Варианты применения







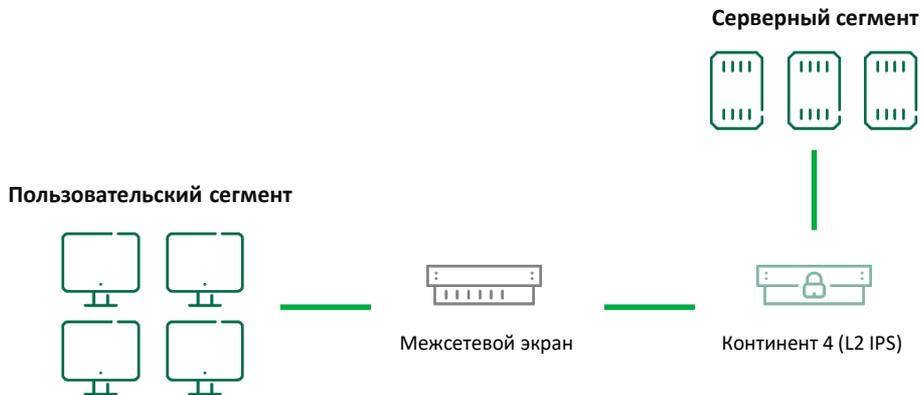
Задачи

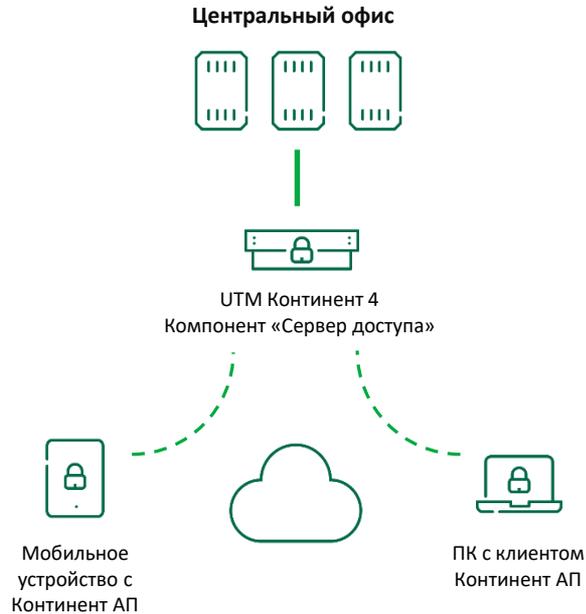
- Защита взаимодействия с Интернет
 - идентификация пользователей
 - обнаружение вторжений
 - контроль приложений
 - URL-фильтрация
 - подключение удаленных пользователей
 - создание защищенных каналов связи
- Изоляция сетевых сегментов
 - высокая пропускная способность на любых пакетах
 - возможность 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)





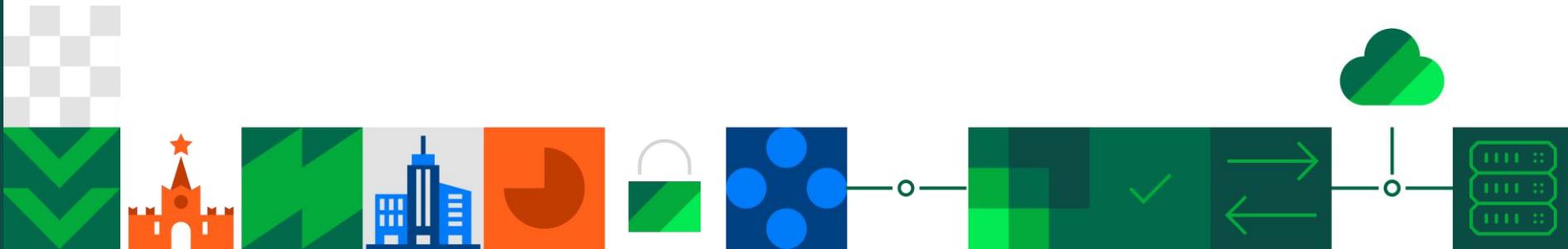
Задачи

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





Компоненты



Централизованное управление

- Узлами сети
- Настройками маршрутизации
- Правилами фильтрации трафика
- VPN-сообществами

Идентификация и аутентификация пользователей локальной базы ЦУС и/или Active Directory с помощью:

- SSO через Kerberos
- Captive-портал
- С помощью агентов аутентификации

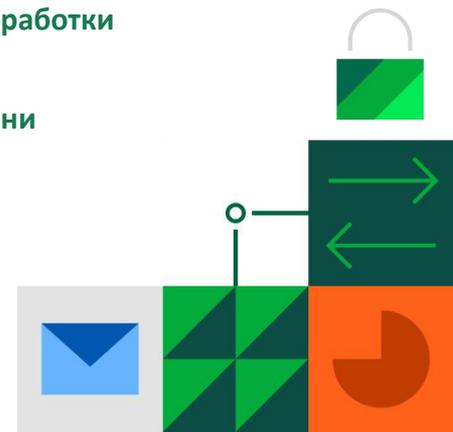
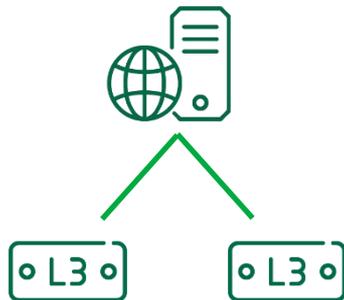
Высокопроизводительная система хранения и обработки событий безопасности

Мониторинг событий в режиме реального времени

Ролевая модель доступа администраторов

Многофакторная аутентификация удаленных пользователей:

- Сертификаты на USB-токенах
- Сервис Multifactor.ru

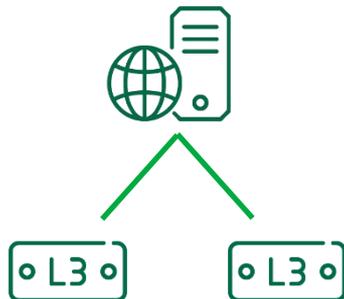


Автоматизированные инструменты миграции:^{new}

- Миграция с Check Point
- Миграция с FortiGate
- Миграция с Cisco
- Миграция с Континент 3

Автоматизация работы администратора через API:^{new}

- Генерация правил МСЭ и NAT
- Экспорт конфигурации УБ в сторонние системы
- Экспорт конфигурации УБ в сторонние ЦУС
- Установка политики по расписанию
- Создание бэкапов по расписанию



Встроенный администратор

Назад Вперед Главная Вид

Навигация

Правило после Правило до Создать

Раздел

Раскрыть все Свернуть все

Вверх Вниз

Копировать

Правило

Разное

Политика

Пропустить

Отбросить

Удалить

Обновить

Установить

Навигация

- Межсетевой экран
 - Группы Web/FTP-фильтров
 - ICAP-серверы
 - ECAP-сервисы
 - Профили Web/FTP-фильтрации
 - Исключения Web/FTP-фильтрации
- Трансляция сетевых адресов
- Приоритизация трафика
 - Профили приоритизации трафика
- Контроль доступа
- Виртуальные частные сети
- Система обнаружения вторжений
- Структура
- Администрирование

Разделы (5), Правила фильтрации (13)

Поиск...

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	COB	Временной интервал	Лог	Установить	Описание
SSH-connect												
1	To SN	192.168.1.0/24-SMS-net	Ext-SN-10.0.10.11	SSH	* Любое	Пропустить	* Не задан	- Выкл	* Всегда	Лог	* Везде	
VPN-L3												
2	VPN	192.168.1.0/24-SMS-net	192.168.20.0/24-SN-net-2	DNS ICMP	DNS RDP FTP SSH HTTP TLS	Пропустить	* Не задан	- Выкл	* Всегда	Лог	* Везде	
Internet												
3	DNS	192.168.1.0/24-SMS-net 192.168.20.0/24-SN-net-2 192.168.30.0/24-SN-net	* Любой	DNS	dns	Пропустить	* Не задан	- Выкл	* Всегда	- Нет	* Везде	
4	Application Control Access	192.168.20.0/24-SN-net-2	* Любой	* Любой	anydesk telegram	Пропустить	* Не задан	- Выкл	* Всегда	- Нет	NGFW	
5	Application Control Deny	* Любой	* Любой	* Любой	anydesk telegram tor	Отбросить	* Не задан	- Выкл	* Всегда	- Нет	NGFW	
6	Web Access For Users	192.168.20.0/24-SN-net-2 192.168.30.0/24-SN-net	* Любой	TLS	* Любое	Фильтровать	HTTPS-profile for Users	- Выкл	* Всегда	Лог	NGFW	
DPI												
Название	Адрес	Маска	Описание									
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										
Ext-SN-10.0.10.11	10.0.10.11											
Gey_192	192.168.0.0	16										
Internet address-SN-100.12...	100.127.254.101											
LAN	192.168.144.0	24										

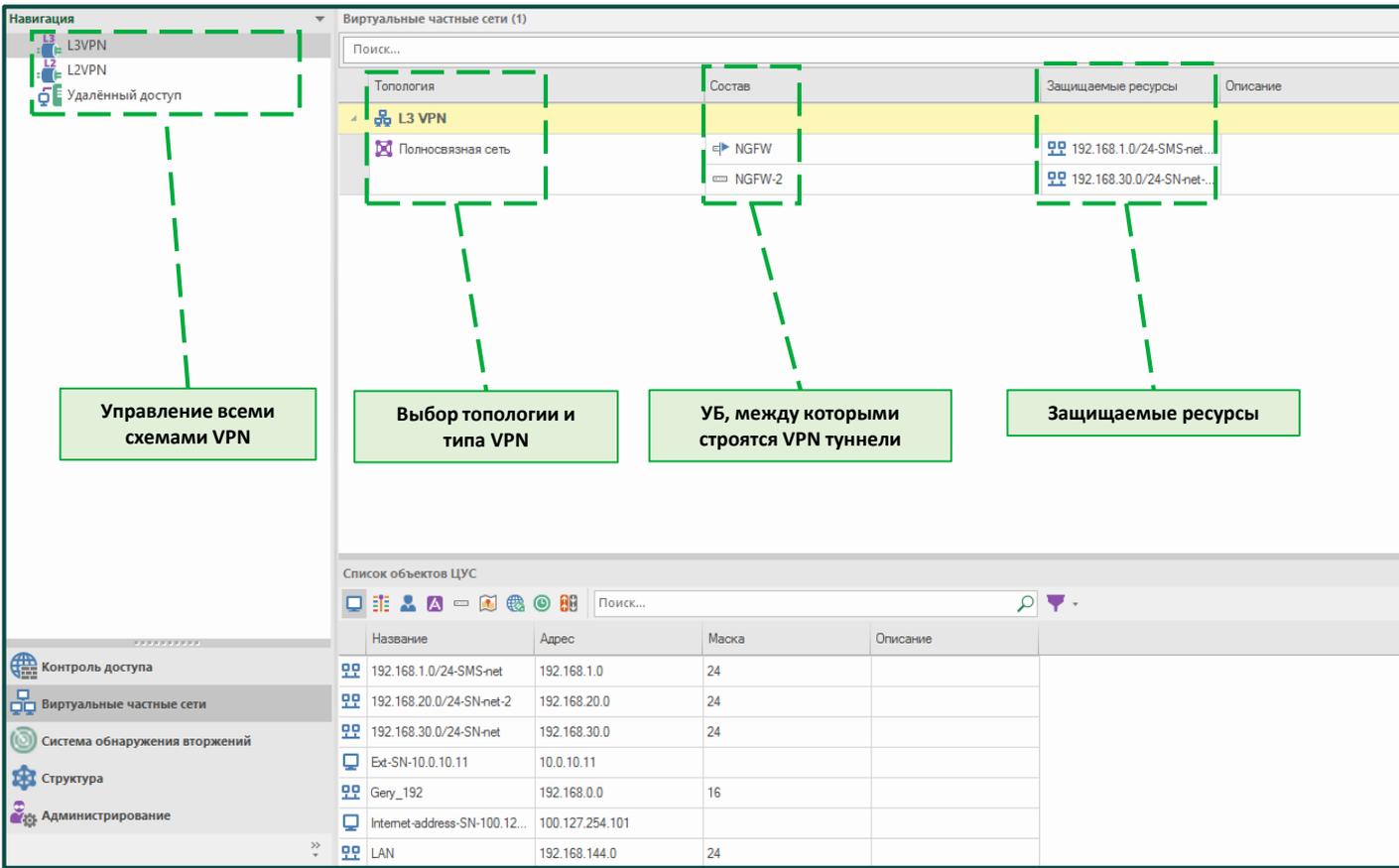
The screenshot displays a web-based management interface for security nodes. At the top, a navigation pane shows 'Узлы безопасности (2)'. Below it is a table with columns for 'Статус', 'Название', 'Компоненты', 'Версия конфигурации', 'Состояние', 'Срок действия сертификата, дней', and 'Описание'. The first row shows a 'Подключен' status, 'NGFW' name, and '10146' configuration version. A second row is partially visible with 'Нет информации' and 'NGFW-2'. A modal window titled 'Узел безопасности - NGFW' is open, showing a tree view of components on the left and a configuration panel on the right. The configuration panel includes fields for 'Идентификатор' (1111), 'Название' (NGFW), and 'Описание'. Under the 'Устройство' section, 'Режим' is set to 'UTM' and 'Платформа' is 'Custom platform'. The 'Компоненты' section has several checked items: 'Центр управления сетью', 'Межсетевой экран', 'Расширенный контроль протоколов и приложений', 'Защита от вредоносных веб-сайтов', 'URL-фильтрация по категориям', 'Антивирус', 'Модуль GeoProtection', 'Система обнаружения вторжений', and 'Идентификация пользователей'. There are also unchecked items like 'Приоритизация трафика', 'L2VPN', 'L3VPN', 'Сервер доступа', and 'Модуль поведенческого анализа'. Buttons for 'OK', 'Отмена', and 'Применить' are at the bottom of the modal.

Статус	Название	Компоненты	Версия конфигурации	Состояние	Срок действия сертификата, дней	Описание
Подключен	NGFW	[Icons]	10146	[Icon]	347	
Нет информации	NGFW-2	[Icon]				

Наименование узла безопасности

Компоненты

Версия политики



The screenshot shows the VPN management interface with several callouts explaining key features:

- Управление всеми схемами VPN**: Points to the navigation menu on the left, which includes options for L3VPN, L2VPN, and Remote Access.
- Выбор топологии и типа VPN**: Points to the 'Топология' (Topology) and 'Полноязычная сеть' (Full network) options in the 'L3 VPN' configuration table.
- УБ, между которыми строятся VPN туннели**: Points to the 'Состав' (Composition) column, showing 'NGFW' and 'NGFW-2' as the protected resources.
- Защищаемые ресурсы**: Points to the 'Защищаемые ресурсы' (Protected resources) column, showing IP ranges like '192.168.1.0/24-SMS-net'.

Виртуальные частные сети (1)

Топология	Состав	Защищаемые ресурсы	Описание
L3 VPN	<ul style="list-style-type: none"> NGFW NGFW-2 	<ul style="list-style-type: none"> 192.168.1.0/24-SMS-net... 192.168.30.0/24-SN-net... 	

Список объектов ЦУС

Название	Адрес	Маска	Описание
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	
Ext-SN-10.0.10.11	10.0.10.11		
Gery_192	192.168.0.0	16	
Internet-address-SN-100.127.254.101	100.127.254.101		
LAN	192.168.144.0	24	



Высокопроизводительный МЭ на платформе Intel DPDK и технологии префиксных деревьев

Шифрование по алгоритмам ГОСТ

L3 VPN и L2 VPN

NAT-трансляция внутри VPN

Динамическая маршрутизация

- OSPF
- BGP

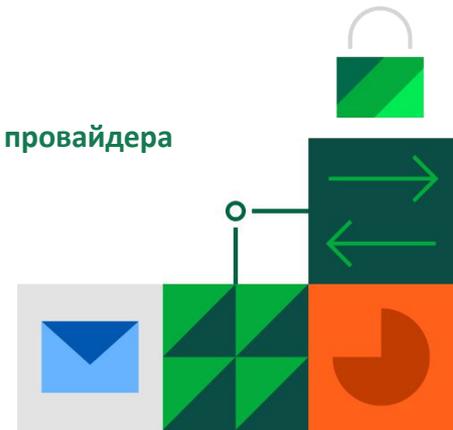
Поддержка приоритизации трафика (QoS)

Поддержка подключения к нескольким каналам провайдера (Multi-WAN)

Поддержка технологии VLAN (IEEE802.1Q)

Поддержка Jumbo-frame

Поддержка LLDP





Определение приложений в сетевом трафике

- Базовый движок – 300 приложений
- Продвинутый движок – 4000 приложений

URL-фильтрация

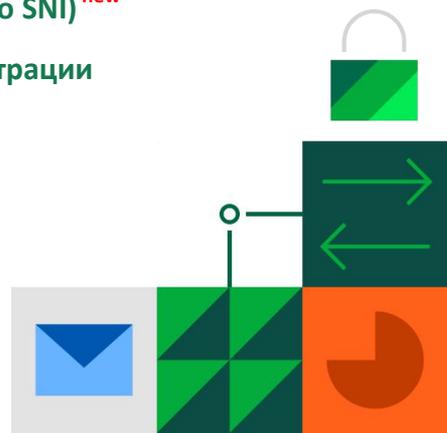
- На базе собственных черных и белых списков
- На базе predetermined categories of sites

URL-фильтрация через инспектирование TLS/SSL-трафика

URL-фильтрация без вскрытия TLS/SSL-трафика (по SNI) ^{new}

Использование доменных имен в правилах фильтрации

Фильтрация трафика на основе стран (GeoIP)



№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	COB	Временной интервал	Лог	Установить
SSH-connect											
1	To SN	192.168.1.0/24-SMS-net	ssh.mycompany.com	SSH	* Любое	Пропустить	* Не задан	Выкл	* Всегда	Лог	Везде
DMZ											
2	To DMZ	Россия	WEB-server-192.168.80...	HTTP ICMP TLS	* Любое	Пропустить	* Не задан	Вкл	* Всегда	Лог	NGFW
VPN-L3											
Internet											
4	DNS	192.168.1.0/24-SMS-net 192.168.20.0/24-SN-net-2 192.168.30.0/24-SN-net	* Любой	DNS DNS	dns	Пропустить	* Не задан	Выкл	* Всегда	Нет	Везде
5	Application Control Access	192.168.20.0/24-SN-net-2	* Любой	* Любой	anydesk telegram telegram	Пропустить	* Не задан	Выкл	* Всегда	Нет	NGFW
6	Application Control Deny	* Любой	* Любой	* Любой	anydesk telegram telegram tor tor	Отбросить	* Не задан	Выкл	* Всегда	Нет	NGFW
7	Web Access For Admins	admins@testlab.local a.porov	* Любой	TLS	* Любое	Фильтровать	HTTPS-profile for Users	Выкл	* Всегда	Лог	NGFW
DPI											
8	SN-inspection	192.168.20.0/24-SN-net-2	SSH-server-192.168.1.4	SSH	ssh	Пропустить	* Не задан	Выкл	* Всегда	Нет	Везде
9	WEB-Inspection	* Любой	WEB-server-192.168.80...	HTTP TLS	http ssl	Пропустить	* Не задан	Выкл	* Всегда	Нет	Везде

Страны (отправитель: Россия)
IP-адреса (отправитель: 192.168.1.0/24-SMS-net)
Доменные имена (получатель: ssh.mycompany.com)
Включение IPS (COB: Вкл)
Шлюз, на который устанавливается политика (Установить: NGFW)
Пользователи локальные или LDAP-групп (отправитель: admins@testlab.local, a.porov)
Условия фильтрации (сервис: SSH, протокол: http, ssl)
Профиль URL-фильтрации (действие: Фильтровать, профиль: HTTPS-profile for Users)

Разделы (4), Правила фильтрации (12)

Поиск...

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие
Block App and Trash						
1	Block bad site	* Любой	* Любой	* Любой	Агрессия, расизм, терроризм Блокировка по предписанию Ботнеты Криптомайнинг Наркотики Порнография и секс Прокси и анонимайзеры Реестр запрещенных сайтов Сайты для взрослых Сайты, распространяющие вирусы Социальные сети Торренты и P2P-сети Федеральный список Менюста Фишинг	Отбросить
2	Block App	* Любой	* Любой	* Любой	bit bit duckduckgo openvpn osupdate teamviewer telegram telegram tor tor whatsapp whatsapp windows-store	Отбросить

Список объектов ЦУС

Название	Категория	Тип	Комплект	Родитель
1-clickshare-com	Sharehosting	Приложение	Расширенный	
1clickshare-net	Sharehosting	Приложение	Расширенный	
1fichier-com	Sharehosting	Приложение	Расширенный	
1xun	Streaming	Протокол	Базовый	
1xun	Streaming	Приложение	Расширенный	
1-upload-com	Sharehosting	Приложение	Расширенный	1-upload-com
1-upload-to	Sharehosting	Приложение	Расширенный	1-upload-to
2chaanel	Social	Приложение	Расширенный	2chaanel

Все
 Группы протоколов/приложений
 Приложения
 Протоколы
 Базовый комплект
 Расширенный комплект
 Базовый для Высокопроизводительного МЭ

Применить

Группы, прикладные протоколы, категории, приложения

Список приложений



Предотвращение сетевых вторжений

- Сигнатуры IPS, разработанные собственной лабораторией
- Возможность работы как на сетевом, так и на канальном уровнях

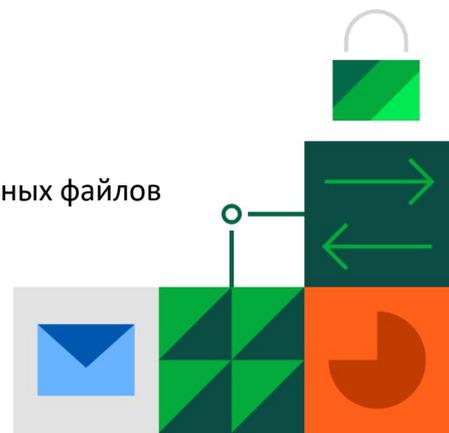
Блокировка доступа к вредоносным сайтам

- На базе технологий Лаборатории Касперского
- На базе технологий Кода Безопасности – Threat Intelligence

Анализ сетевого трафика на наличие аномалий

Антивирусная проверка трафика

- Поточковый антивирус
- Взаимодействие с песочницами по ICAP
- Добавление собственных хэшей вредоносных файлов



Навигация

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

Правила БРП (30 891)

Поиск...

Правило БРП							Профили COB				
Важность	Описание	Уязвимость	Дата создания	Дата обновления	Класс	Идент...	IPS-profile	Оптимальный н...	Полный набор	Рекомендованн...	
Высокая	Likely CryptoWall .onion Proxy DNS lo...	Отсутствует	27.06.2014	01.09.2020	Криптолокеры	4118610	Блокировать	Оповещать	Оповещать	Оповещать	
Высокая	Android Adups Firmware DNS Query	Отсутствует	16.11.2016	17.09.2020	Вредоносное ПО для моб...	4123516	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Mobile Device Posting Phone Number	Отсутствует	06.07.2011	11.08.2020	Вредоносное ПО для моб...	4113209	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Possible Mobile Malware POST of IMS...	Отсутствует	25.05.2011	12.08.2020	Вредоносное ПО для моб...	4112850	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Android.Plankton/Tonclank Successfu...	Отсутствует	16.06.2011	28.10.2020	Вредоносное ПО для моб...	4113044	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup	Отсутствует	07.04.2022	02.05.2022	Вредоносное ПО для моб...	4135866	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup (arab...	Отсутствует	06.04.2022	02.05.2022	Вредоносное ПО для моб...	4135783	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup	Отсутствует	07.04.2022	02.05.2022	Вредоносное ПО для моб...	4135869	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Possible Pegasus Related DNS Looku...	Отсутствует	13.01.2022	13.01.2022	Вредоносное ПО для моб...	4134919	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup	Отсутствует	07.04.2022	07.04.2022	Вредоносное ПО для моб...	4135864	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup (akh...	Отсутствует	06.04.2022	02.05.2022	Вредоносное ПО для моб...	4135775	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Pegasus Domain in DNS Lookup (akh...	Отсутствует	06.04.2022	02.05.2022	Вредоносное ПО для моб...	4135774	Отключить	Отключить	Оповещать	Оповещать	
Высокая	Observed DNS Query to Pegasus Dom...	Отсутствует	13.01.2022	13.01.2022	Вредоносное ПО для моб...	4134921	Отключить	Отключить	Оповещать	Оповещать	

Информация

Pegasus Domain in DNS Lookup (akhbar-islamyah .com)

Детально	Ссылки
Идентификатор: 4135775	https://citizenlab.ca/2022/04/peace-through-pegasus-jordanian-human-rights-defenders-and-journalists-hacked-with-pegasus-spyware/
Важности: Высокая	
Уязвимости: Отсутствует	
Дата создания: 06.04.2022	
Дата обновления: 02.05.2022	
Класс: Вредоносное ПО для мобильных приложений	

Навигация

- Политика COB
- Профили COB
- База решающих правил
- Вендорские правила
 - DoS-атаки
 - АСУТП
 - Бэкдоры
 - Веб-атаки
 - Вредоносное ПО для мобильных устройств
 - Вредоносные командные центры
 - Криптолокеры
 - Криптомайнеры

Правила политики COB (1)

Поиск...

Название	Профиль COB	Установить	Описание
Новое правило	IPS-profile	NGFW	

Узлы, на которые устанавливаются профили IPS

Навигация

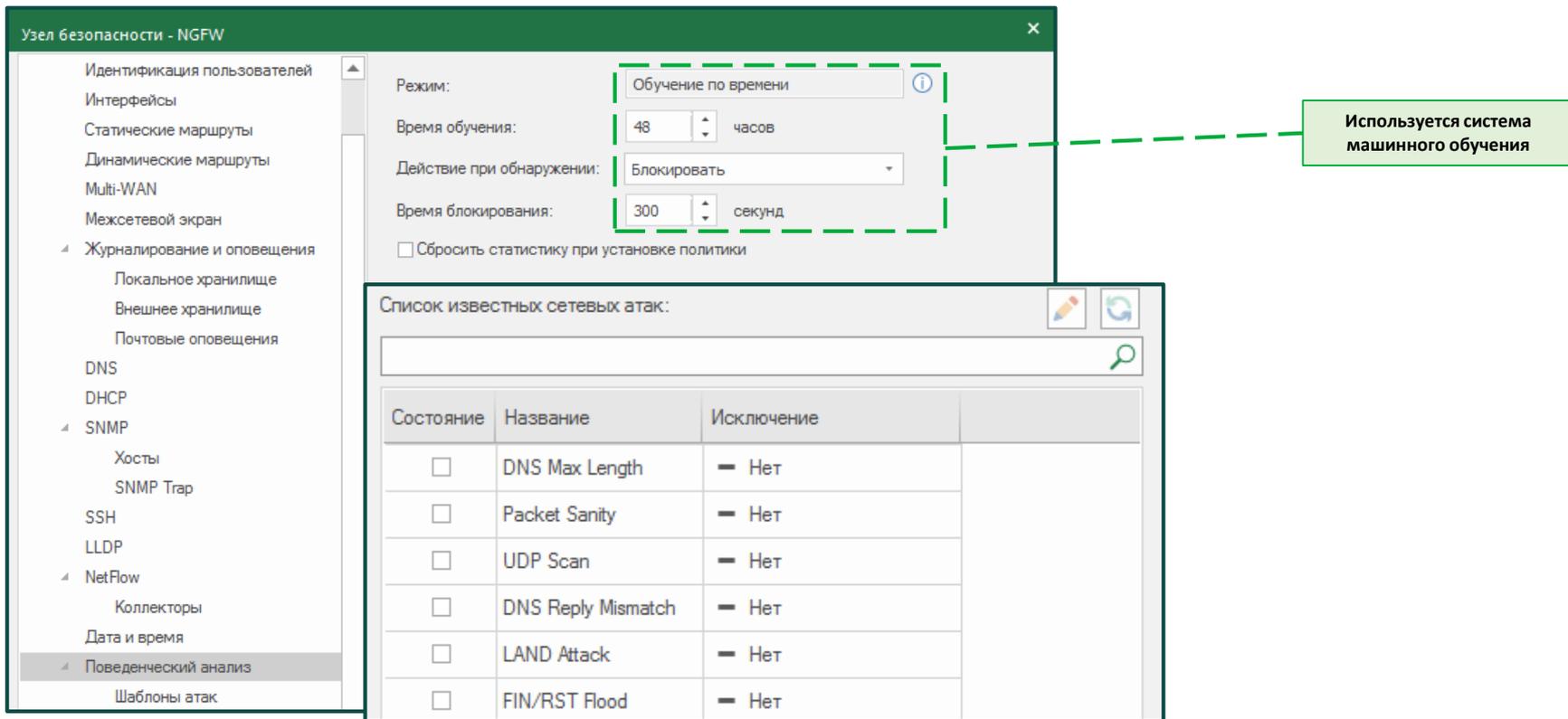
- Политика COB
- Профили COB
- База решающих правил
- Вендорские правила
 - DoS-атаки
 - АСУТП
 - Бэкдоры
 - Веб-атаки
 - Вредоносное ПО для мобильных устройств
 - Вредоносные командные центры

Профили COB (4)

Поиск...

Имя	Категория	Описание
Оптимальный набор	Вендорский	Набор, содержащий базовую выборку правил
Полный набор	Вендорский	Набор, содержащий полную выборку правил
Рекомендованный набор	Вендорский	Набор, содержащий выборку правил на наиболее распространенные угрозы
IPS-profile	Пользовательский	

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



Узел безопасности - NGFW

Идентификация пользователей
Интерфейсы
Статические маршруты
Динамические маршруты
Multi-WAN
Межсетевой экран
Журналирование и оповещения
Локальное хранилище
Внешнее хранилище
Почтовые оповещения
DNS
DHCP
SNMP
Хосты
SNMP Trap
SSH
LLDP
NetFlow
Коллекторы
Дата и время
Поведенческий анализ
Шаблоны атак

Режим: Обучение по времени ⓘ
Время обучения: 48 часов
Действие при обнаружении: Блокировать
Время блокирования: 300 секунд
 Сбросить статистику при установке политики

Используется система машинного обучения

Список известных сетевых атак:

Состояние	Название	Исключение
<input type="checkbox"/>	DNS Max Length	— Нет
<input type="checkbox"/>	Packet Sanity	— Нет
<input type="checkbox"/>	UDP Scan	— Нет
<input type="checkbox"/>	DNS Reply Mismatch	— Нет
<input type="checkbox"/>	LAND Attack	— Нет
<input type="checkbox"/>	FIN/RST Flood	— Нет



Континент АП/ZTN

VPN-клиент для мобильных устройств и ПК

Клиентские приложения для всех популярных платформ

Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (TK26)

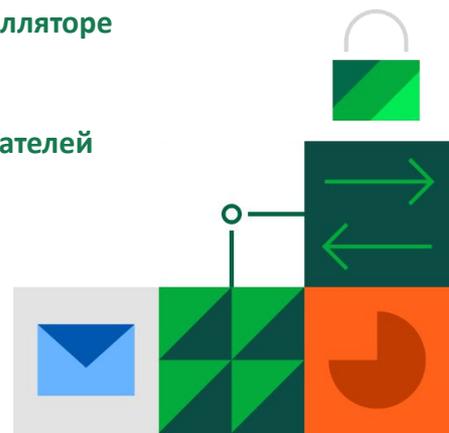
Поддержка различных ключевых носителей

Возможность установки VPN-соединения до регистрации пользователя в ОС

Объединённый TLS и VPN клиенты в одном инсталляторе

Режим запрета незащищенных соединений

Разделение пулов IP-адресов удаленных пользователей





Единый криптографический клиент под все платформы
Контроль установленных приложений перед подключением

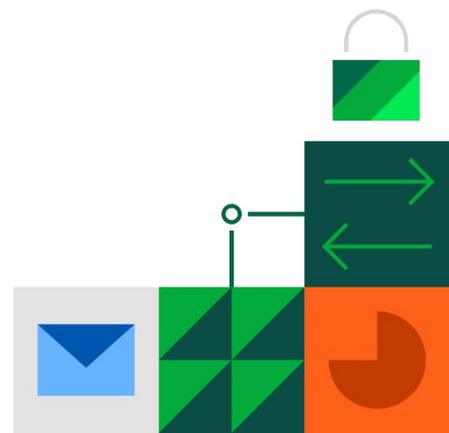
Подключение к ряду решений:

- Континент 4
- Континент TLS
- Континент 3.9.1

Единая лицензия с Континент-АП
Единая лицензия для любой клиентской ОС

Платформы:

- Windows
- Linux
- Aurora
- Android
- IOS
- MACOS (M1+M2)



Малые



- IPC-R10
- IPC-R50

Средние



- IPC-R300
- IPC-R550
- IPC-R800

Старшие



- IPC-R1000
- IPC-R3000

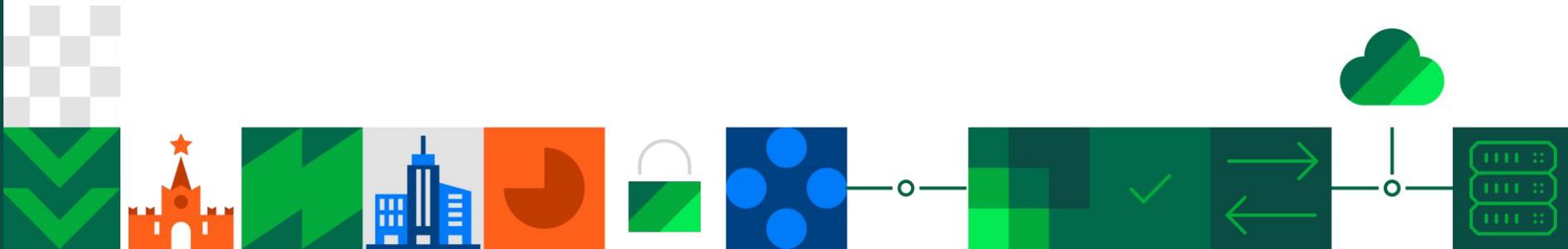
Название	Число ядер	МЭ, Мбит/с	UTM, Мбит/с	L2 IPS, Мбит/с
SOHO	2	4 000	700	1 000
SMB	4	12 000	2 500	2 000
ENT	8	16 000	6 000	5 500

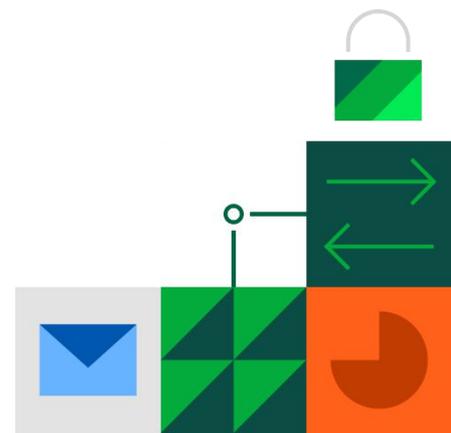
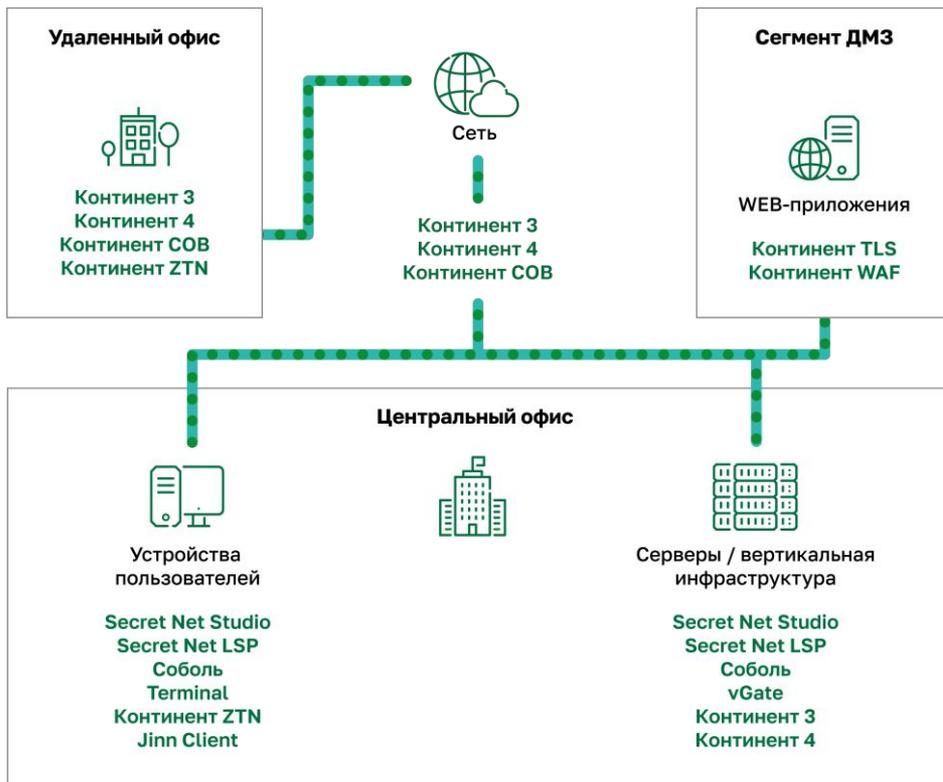


Модуль	Узел Безопасности (УБ)	UTM Базовый	UTM Расширенный
Центр управления сетью (ЦУС)	✓	✓	✓
Межсетевой экран (МЭ)	✓	✓	✓
Сервер Доступа (СД)	✓	✓	✓
Контроль приложений (300 приложений и протоколов)	✓	✓	✓
URL-фильтрация	✓	✓	✓
Расширенный контроль приложений (4000 приложений и протоколов)		✓	✓
Система обнаружения вторжений		✓	✓
Модуль блокировки трафика по стране происхождения (GeoIP)		✓	✓
Защита от вредоносных сайтов			✓
Преднастроенные категории URL			✓
Потоковый антивирус			✓
Высокопроизводительный межсетевой экран (NF2)	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		
L2 VPN	Не входит в состав УБ/UTM, приобретается отдельно. Срок действия лицензии - бессрочно.		



О компании





Компания «Код Безопасности» – российский разработчик программных и аппаратных средств, обеспечивающих защиту информационных систем, а также их соответствие требованиям международным и отраслевым стандартам.

- **Более 20 лет** на страже безопасности крупнейших предприятий России.
- Ведет свою деятельность на основании **9 лицензий ФСТЭК, ФСБ и Минобороны России.**
- Технологии защиты обеспечивают безопасность **3 000 000 компьютеров** в **50 000 организаций.**
- **3 центра разработки:** Москва, Санкт-Петербург, Пенза.
- Более **800 квалифицированных специалистов R&D**, имеющих уникальные компетенции.
- Более **50 разработанных СЗИ и СКЗИ.**
- Более **60 действующих сертификатов** соответствия подтверждают высокое качество продуктов.
- Партнерская сеть компании насчитывает более **1000 авторизованных партнеров.**

Компетентность «Кода Безопасности» подтверждена независимыми аналитиками:

- «Крупнейшие производители высокотехнологичного оборудования»: №1 («Эксперт РА»), №3 («Коммерсант»).
- «Крупнейшие разработчики программного обеспечения»: №7 («Эксперт РА»), №9 («Коммерсант»).
- «Крупнейшие ИТ-компании России»: №30 («Коммерсант»), №47 (TAdviser).

Государственные организации:



Федеральное казначейство
России



Федеральная налоговая
служба России



Федеральная таможенная служба
России



Федеральный Фонд
обязательного
медицинского
страхования



Центральная избирательная
комиссия Российской
Федерации



Министерство юстиции Российской
Федерации



Министерство внутренних дел
Российской Федерации



Федеральная служба
безопасности Российской
Федерации



Министерство обороны
Российской Федерации



Федеральная служба охраны
Российской Федерации

Телекоммуникационные компании:



ПАО «Ростелеком»



ПАО «МГТС»



ГК «АКАДО Телеком»



АО «Воентелеком»

Финансовые организации:



ПАО «Сбербанк»



Центральный банк
Российской Федерации



ГК «Внешэкономбанк»



АО «Газпромбанк»



ПАО «Промсвязьбанк»



Банк ВТБ (ПАО)



ПАО «Московский кредитный
банк»



АО «АЛЬФА-БАНК»

Промышленные предприятия:



ГК «Ростех»



АО «Российские
космические системы»



ПАО «ГМК «Норильский
никель»



ГК «Росатом»



ПАО «Газпром»



ПАО «АК «Транснефть»



ПАО «НК «Роснефть»



ПАО «Россети»

Предприятия ТЭК:



КОД безопасности

info@securitycode.ru
www.securitycode.ru

