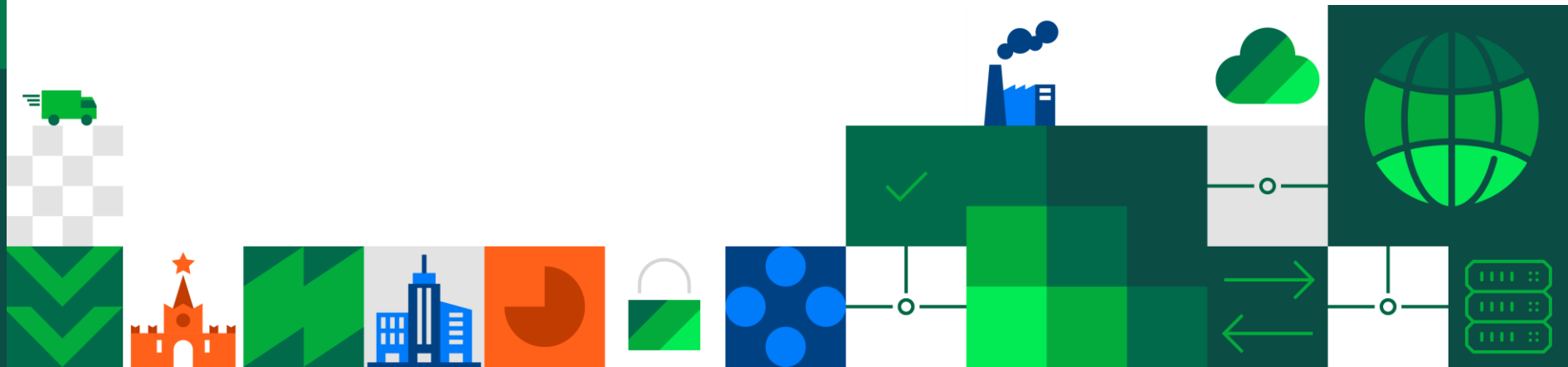
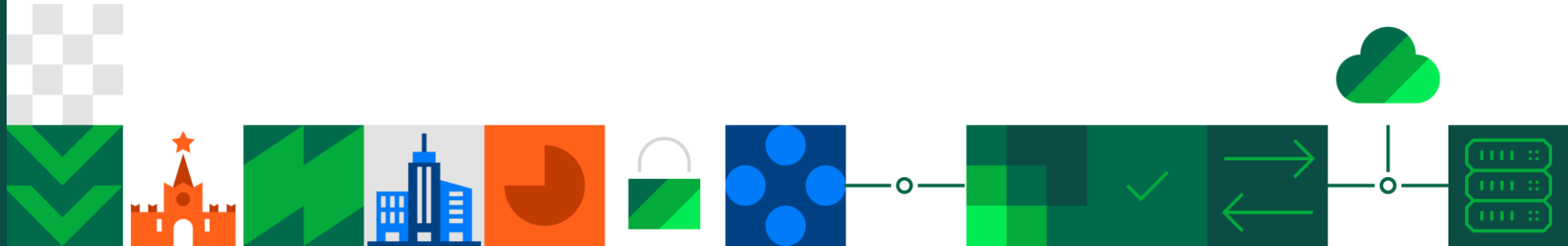
КОД безопасности

Континент 4



КОД безопасности

О продукте



КОД безопасности

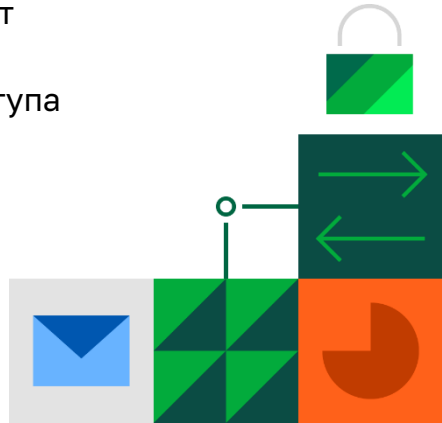
О продукте

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

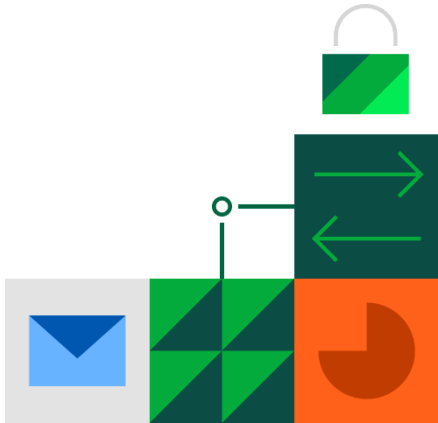


КОД безопасности

Прохождение сертификационных испытаний

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



КОД безопасности

Континент 4

КШ — Криптошлюз (КШ)

КК — Криптокоммутатор (КК)

Детектор атак (ДА)

Центр управления сетью (ЦУС)

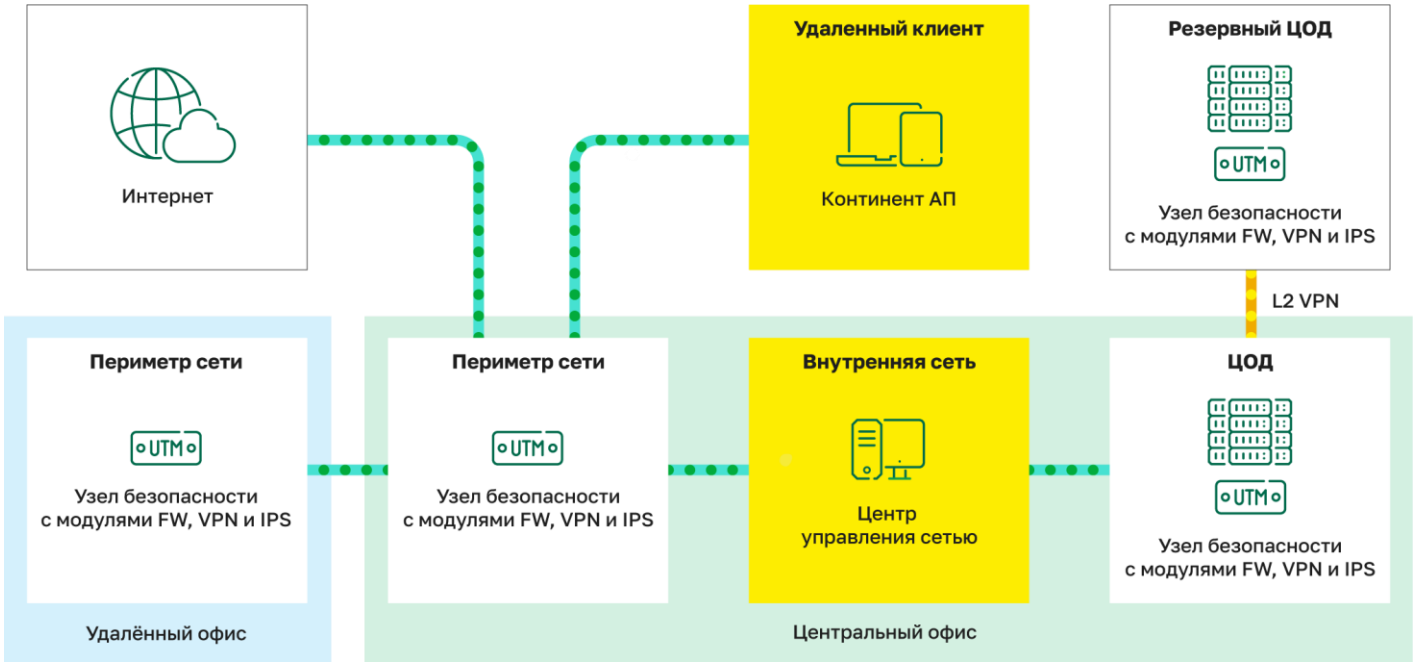
Узел безопасности (УБ)

FW | IPS | App control | L2 VPN | L3 VPN | MGMT | Threat Intelligence | Log | URL Filtering | User Identity

Antivirus | GeoIP

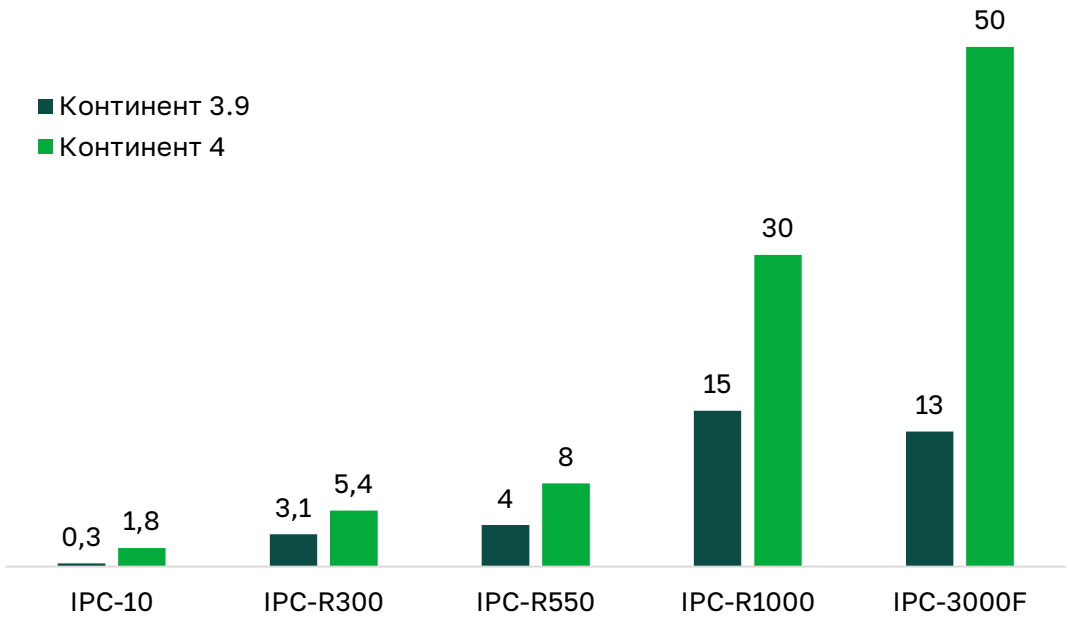
КОД безопасности

Архитектура Континент 4



Изменения по сравнению с Континент 3

Производительность межсетевого экрана, Гбит/с



НОВЫЙ ФУНКЦИОНАЛ

- Одно устройство для всех механизмов безопасности
- Управление компонентами из единой консоли
- Мониторинг с веб-интерфейсом
- Активация СОВ для конкретного правила фильтрации
- Производительность внутреннего МЭ до 80 Гбит/с
- Самообучающийся модуль поведенческого анализа для защиты от DoS-атак

КОД безопасности

Система управления Континент 4

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.

КОД безопасности

Система управления Континент 4

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.

КОД безопасности

Система управления Континент 4

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.

Система управления Континент 4

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.

Система управления Континент 4

Детальная настройка СОВ позволяет проверять трафик только по заданным сигнатурам.

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

КОД безопасности

Система управления Континент 4

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.

Архитектура Континент 4

Безопасность

- Контроль сетевых приложений (4000 приложений)
- Система предотвращения вторжений
- Блокировка доступа к вредоносным сайтам
- 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

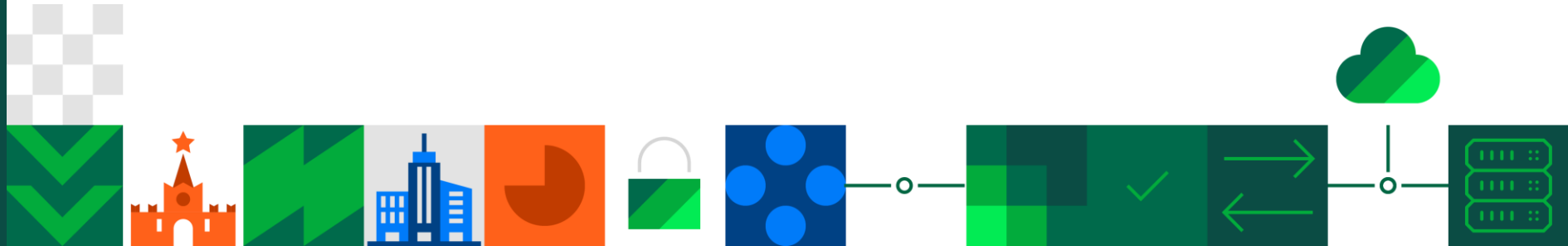
- Многофункциональный узел безопасности (UTM)
- Высокопроизводительный межсетевой экран
- Система обнаружения вторжений (L2 IPS)
- Выделенная платформа управления

Сетевые технологии

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

КОД безопасности

Варианты применения



КОД безопасности

Режимы работы

UTM

Интегрированный межсетевой экран

- Межсетевой экран
- Контроль приложений
- Поведенческий анализ
- Система обнаружения вторжений на сетевом уровне (L3)

NF2

Высокопроизводительный межсетевой экран

- Межсетевой экран с использованием технологии префиксных деревьев

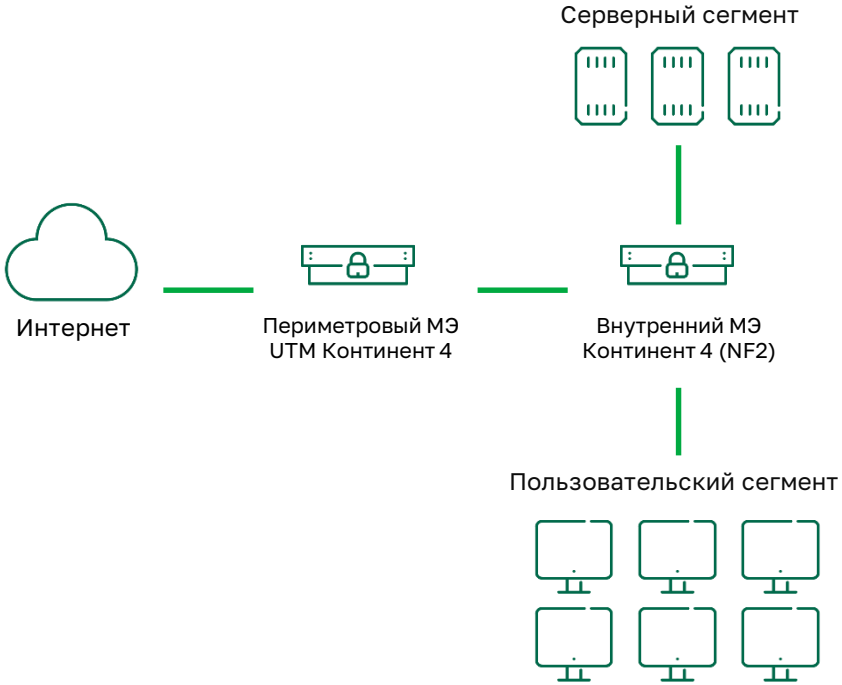
L2 IPS

Детектор атак

- Система обнаружения вторжений на канальном уровне (L2)

КОД безопасности

Межсетевое экранирование

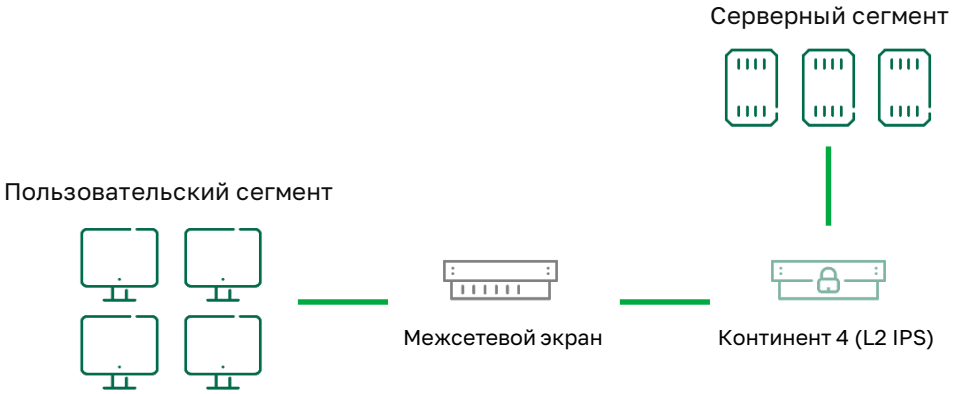


Задачи

- 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

КОД безопасности

Обнаружение вторжений

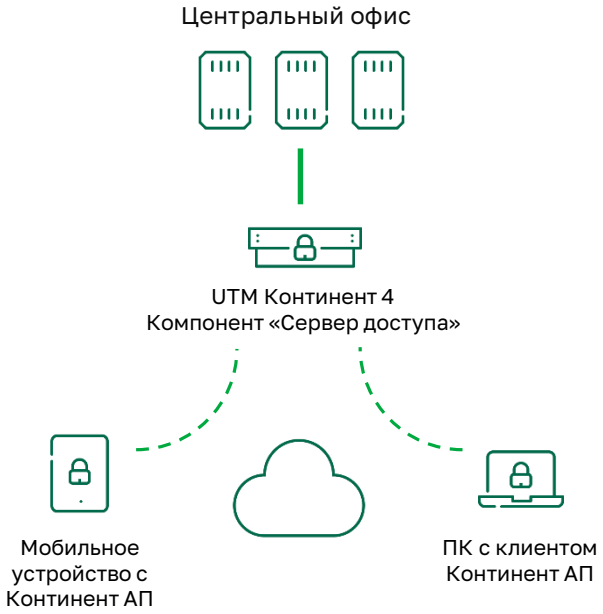


Задачи

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

КОД безопасности

Удаленный доступ

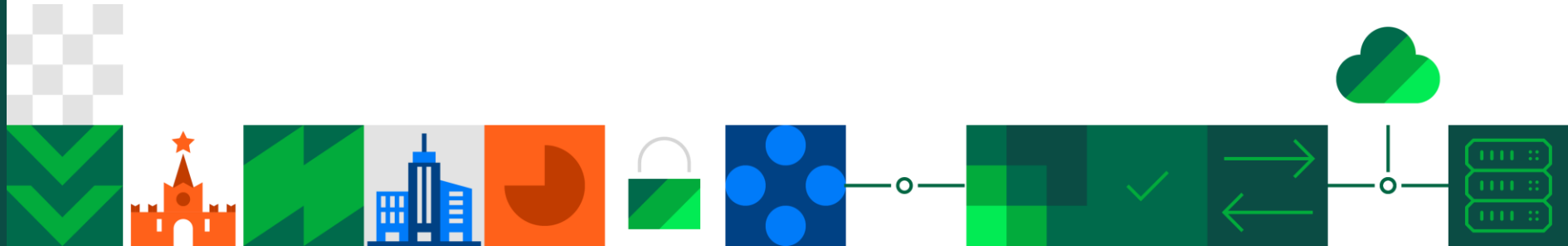


Задачи

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

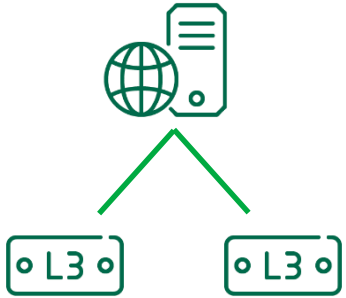
КОД безопасности

Компоненты



КОД безопасности

Управление инфраструктурой



Централизованное управление

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

Идентификация и аутентификация пользователей

- Из локальной базы ЦУС и/или Active Directory
- С помощью агентов аутентификации
- Captive-портал
- SSO через Kerberos new

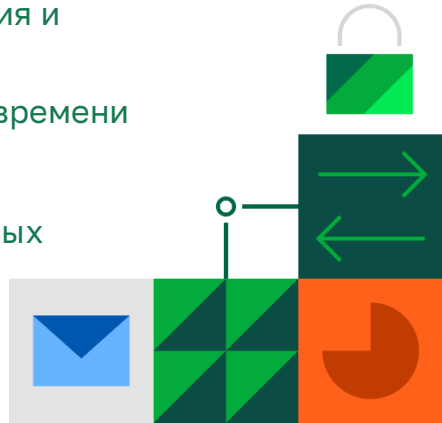
Высокопроизводительная система хранения и обработки событий безопасности

Мониторинг событий в режиме реального времени

Ролевая модель доступа администраторов

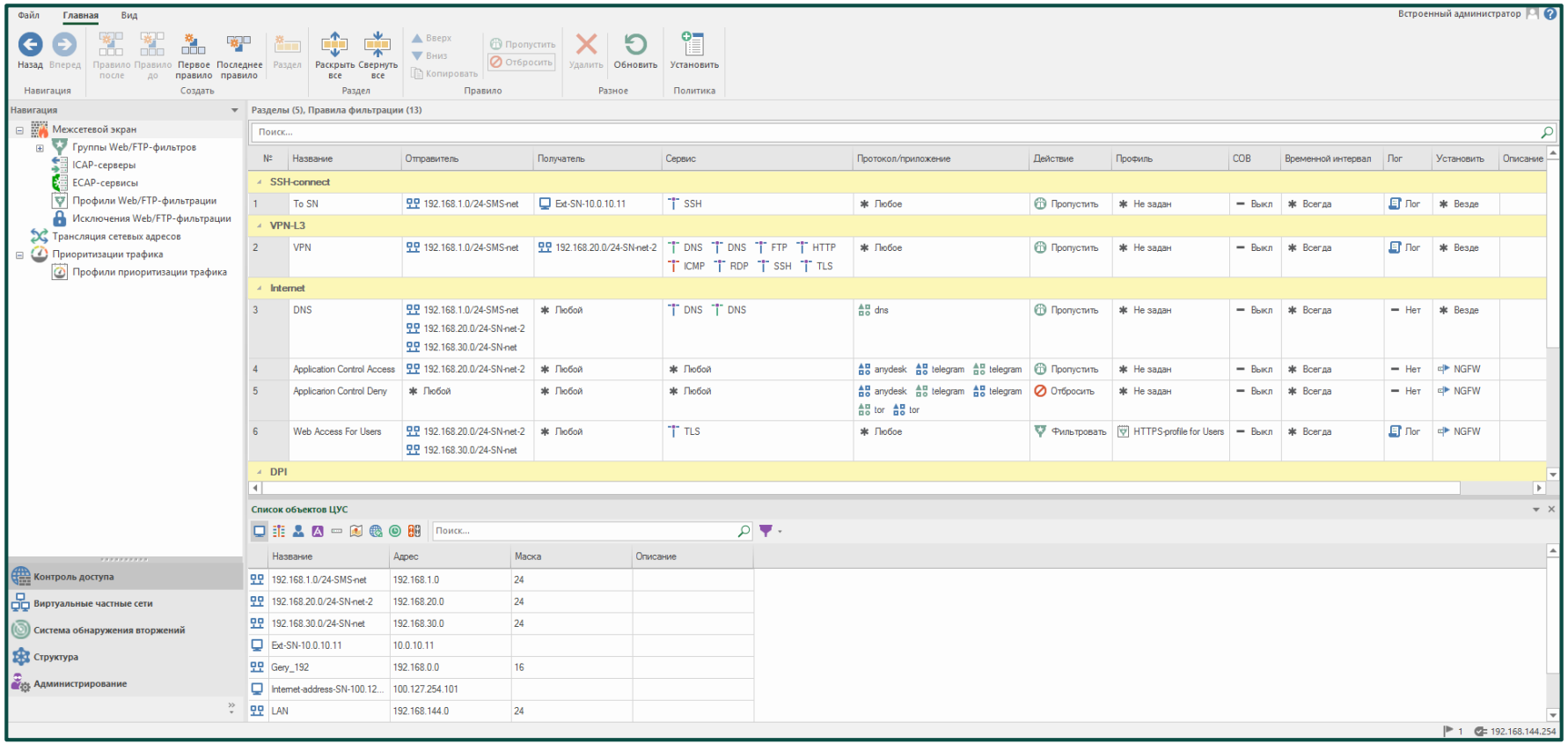
Многофакторная аутентификация удаленных пользователей:

- Сертификаты на USB-токенах
- Сервис Multifactor.ru



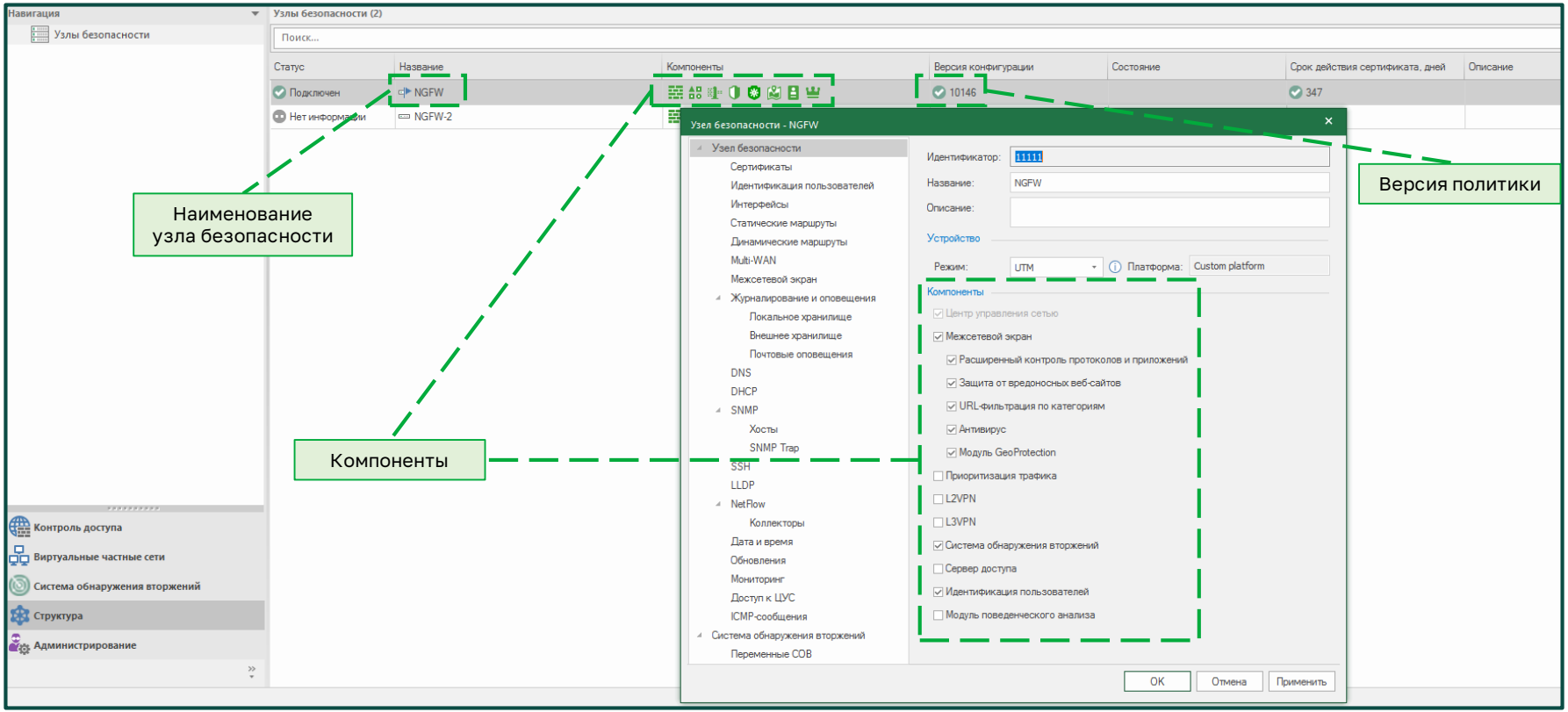
КОД безопасности

Интерфейс управления Континент 4



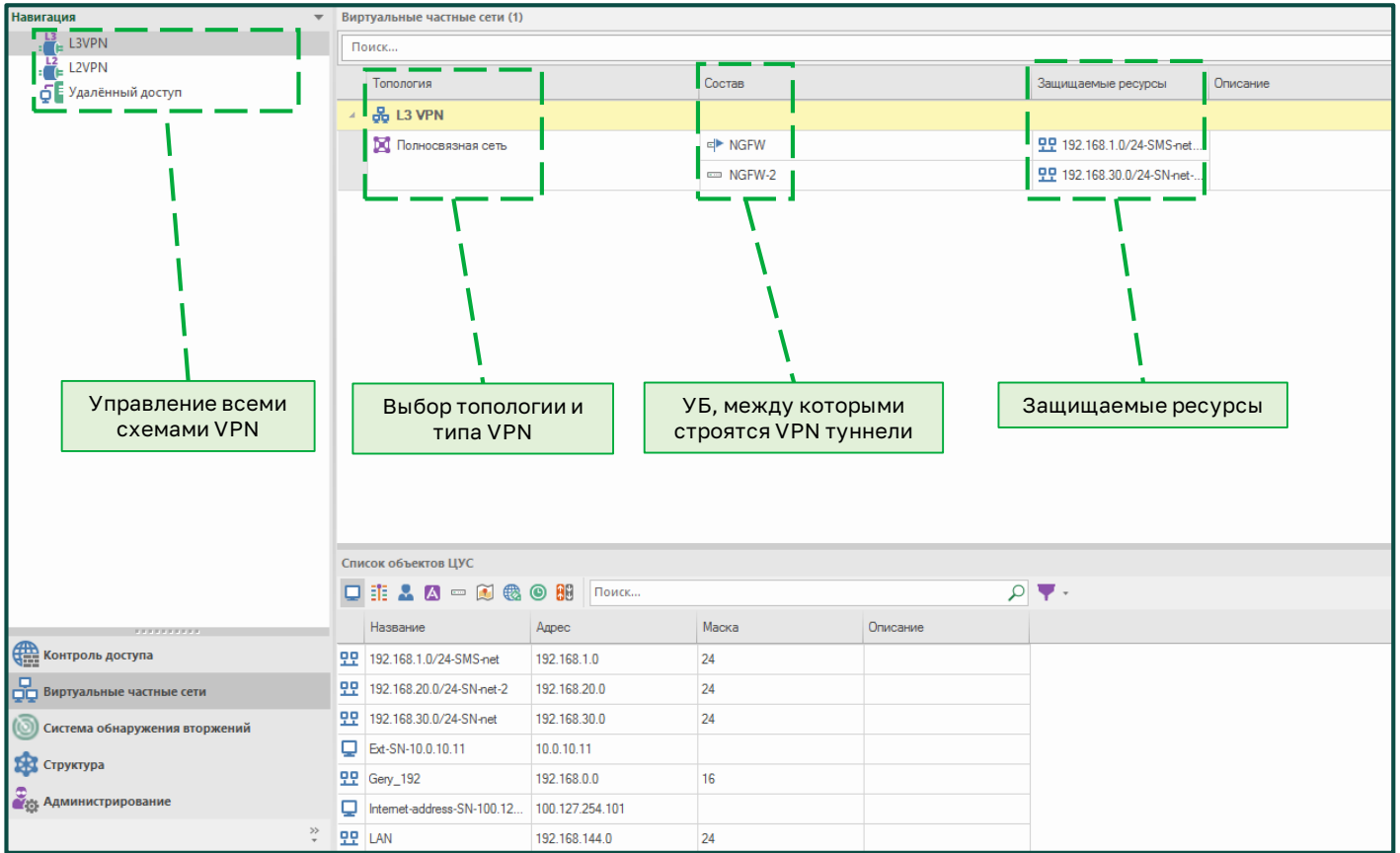
КОД безопасности

Управление узлами безопасности



КОД безопасности

Управление VPN



КОД безопасности

Межсетевое экранирование

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

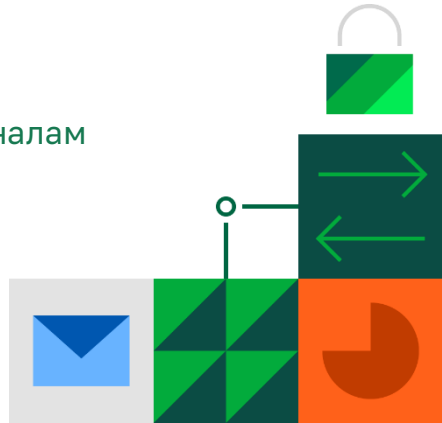
Поддержка приоритизации трафика (QoS)

Поддержка подключения к нескольким каналам провайдера (Multi-WAN)

Поддержка технологии VLAN (IEEE802.1Q)

Поддержка Jumbo-frame

Поддержка LLDP



КОД безопасности

Контроль приложений и URL-фильтрация

Определение приложений в сетевом трафике

- Базовый движок – 700 приложений
- Продвинутый движок – 4000 приложений

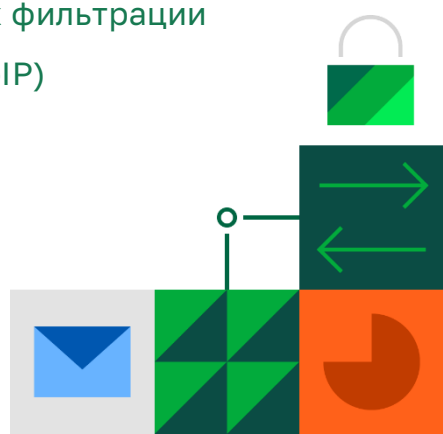
URL-фильтрация

- На базе собственных черных и белых списков
- На базе предопределенных категорий сайтов

Инспектирование SSL-трафика

Использование доменных имен в правилах фильтрации

Фильтрация трафика на основе стран (GeoIP)



КОД безопасности

Управление правилами фильтрации

Страны

IP-адреса

Доменные имена

Включение IPS

Шлюз, на который устанавливается политика

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	СОВ	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	Applicarion 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.popov	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

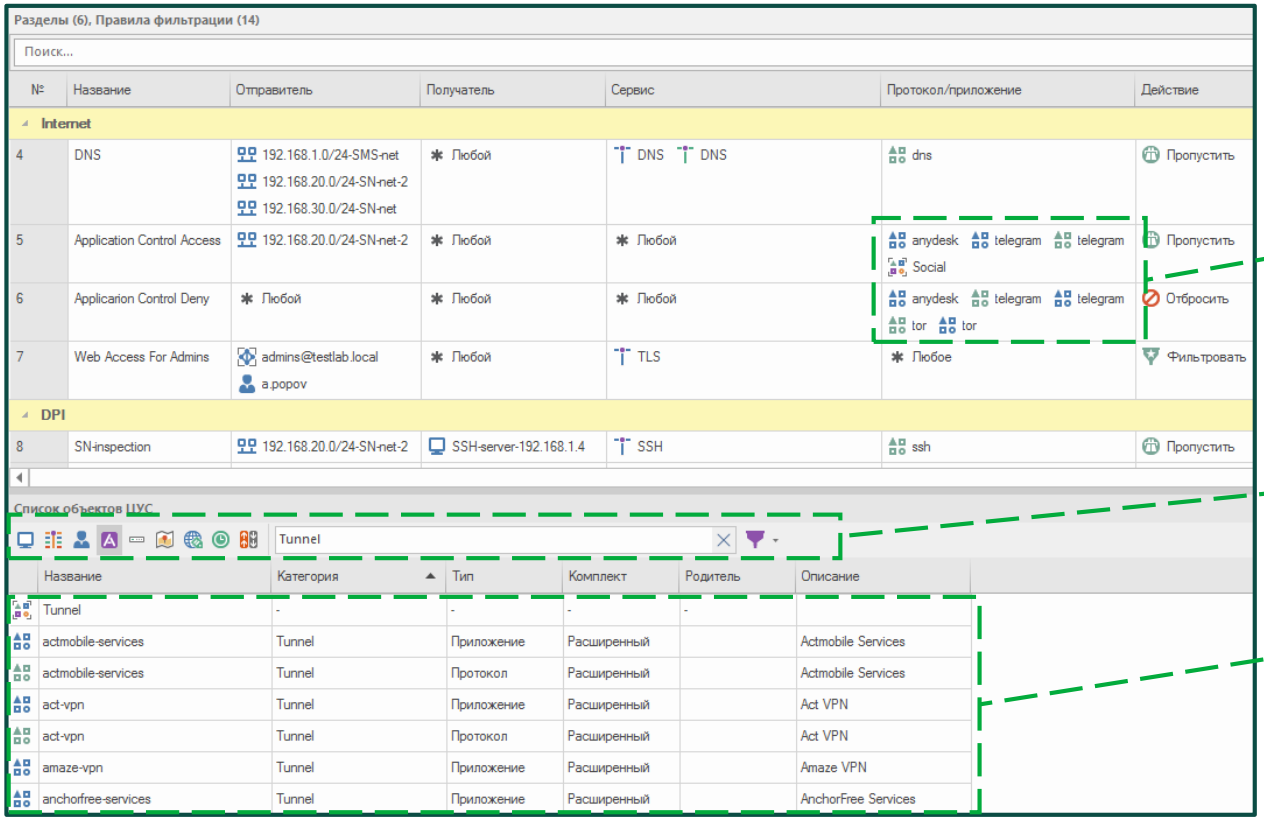
Пользователи локальные или LDAP-групп

Условия фильтрации

Профиль URL-фильтрации

КОД безопасности

Контроль приложений



Группы, прикладные протоколы, категории, приложения

Поиск

Список приложений

КОД безопасности

Обнаружение вторжений

Предотвращение сетевых вторжений

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

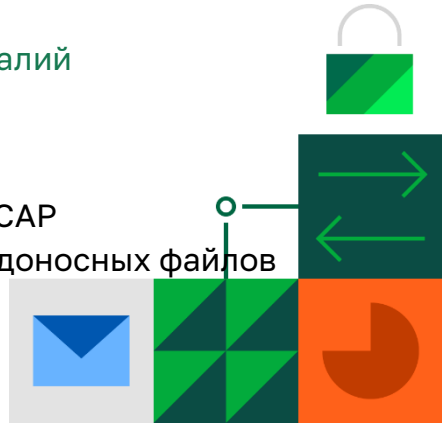
Блокировка доступа к вредоносным сайтам

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

Анализ сетевого трафика на наличие аномалий

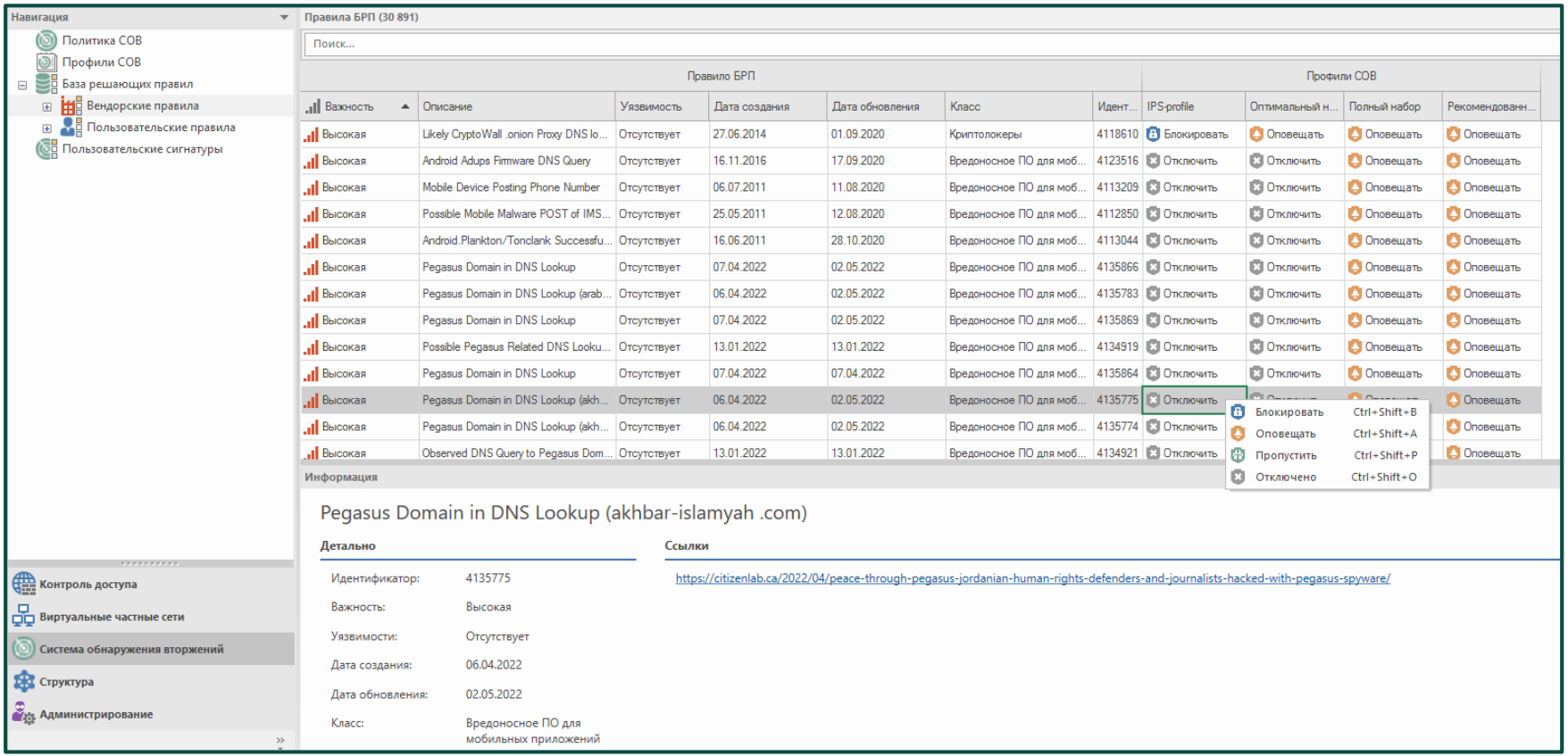
Антивирусная проверка трафика

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



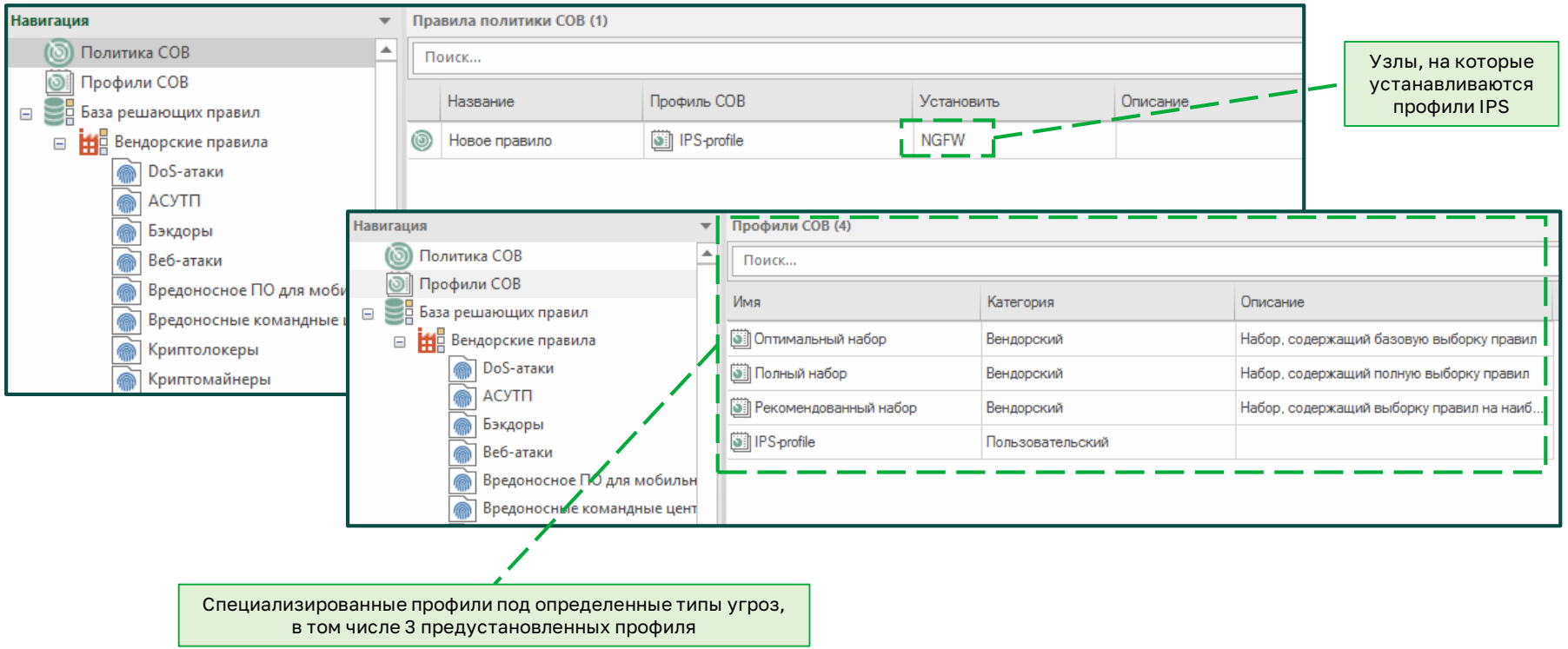
КОД безопасности

Управление сигнатурами (БРП)



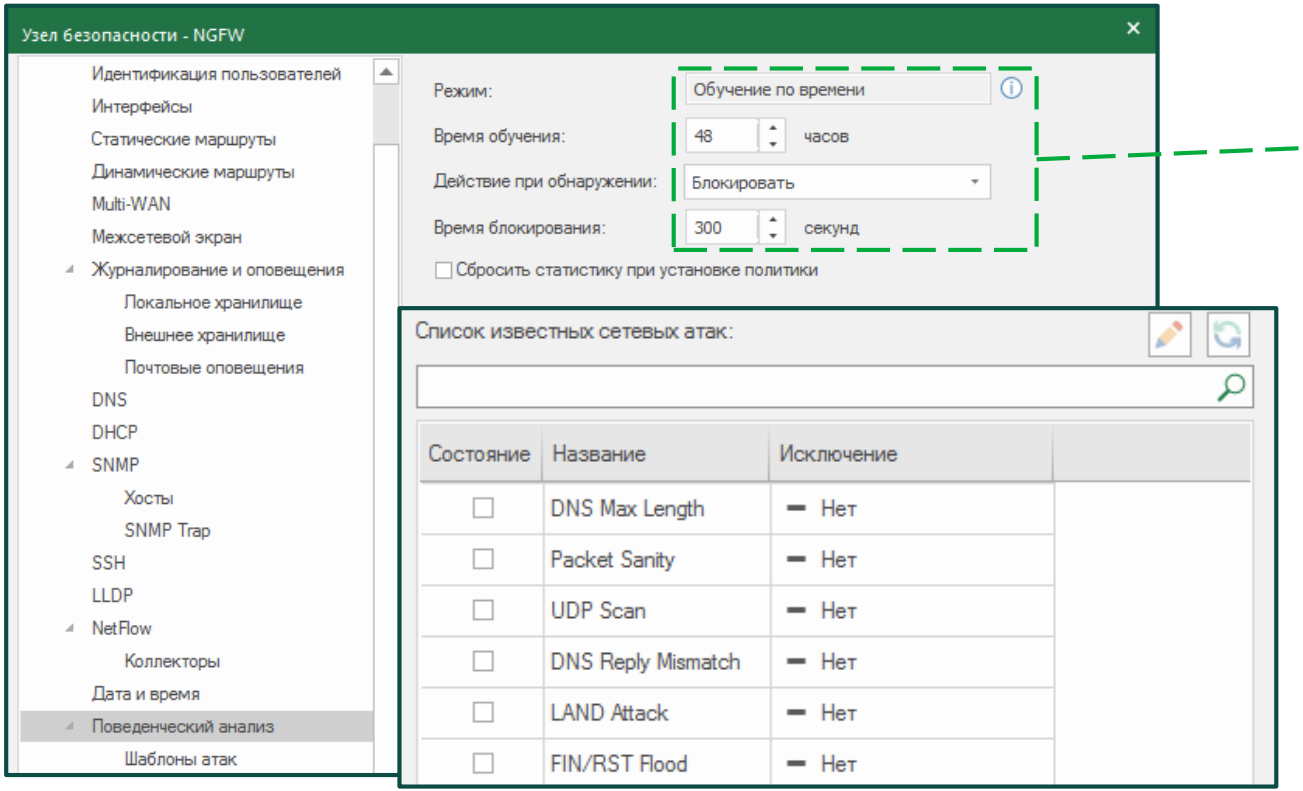
КОД безопасности

Управление IPS



КОД безопасности

Модуль поведенческого анализа



Используется система машинного обучения

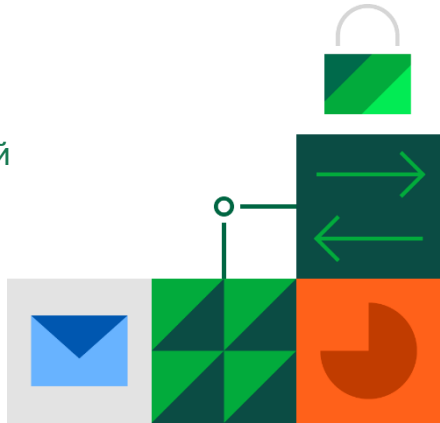
КОД безопасности

Удаленный доступ

Континент АП/ZTN

VPN-клиент для мобильных устройств и ПК

- Клиентские приложения для всех популярных платформ
- Поддержка Сервером доступа аутентификации по сертификатам ГОСТ 2012 (ТК26)
- 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 new



КОД безопасности

Континент ZTN Клиент: новое поколение клиентов удаленного доступа

Единый криптографический клиент под все платформы
Контроль установленных приложений перед подключением

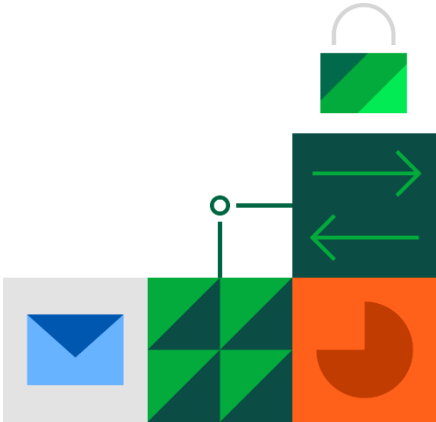
Подключение к ряду решений:

- 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)



Российские платформы

Малые

- IPC-R10
- IPC-R50

Средние

- IPC-R300
- IPC-R550

Старшие

- IPC-R800
- IPC-R1000
- IPC-R3000

КОД безопасности

Виртуальные платформы

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

vmware

KVM

КОД безопасности

Лицензирование

Модуль	Узел Безопасности (УБ)	UTM Базовый	UTM Расширенный
Центр управления сетью (ЦУС)	✓	✓	✓
Межсетевой экран (МЭ)	✓	✓	✓
Сервер Доступа (СД)	✓	✓	✓
Контроль приложений (700 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.		