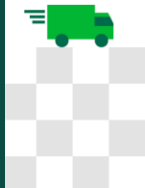


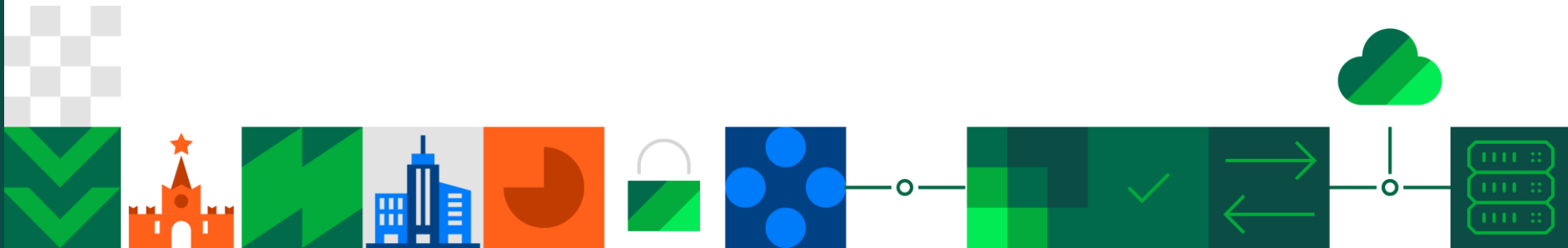


Континент 4





О продукте





Континент 4

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

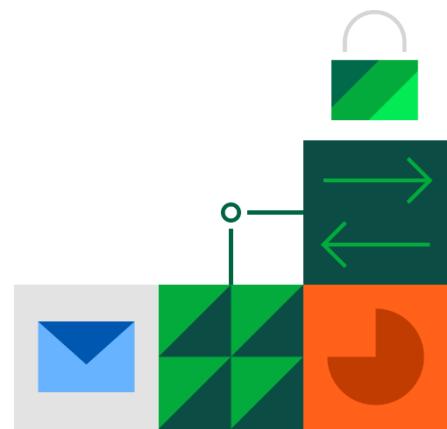
Предназначен для решения следующих задач:

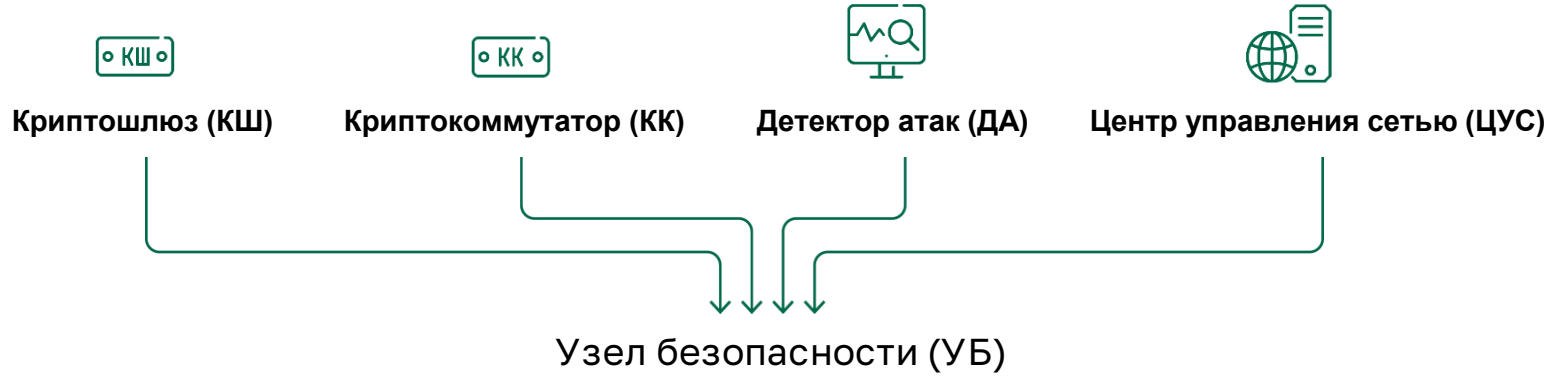
- ✓ Централизованная защита периметра корпоративной сети
- ✓ Контроль доступа пользователей в Интернет
- ✓ Предотвращение сетевых вторжений
- ✓ Организация защищенного удаленного доступа



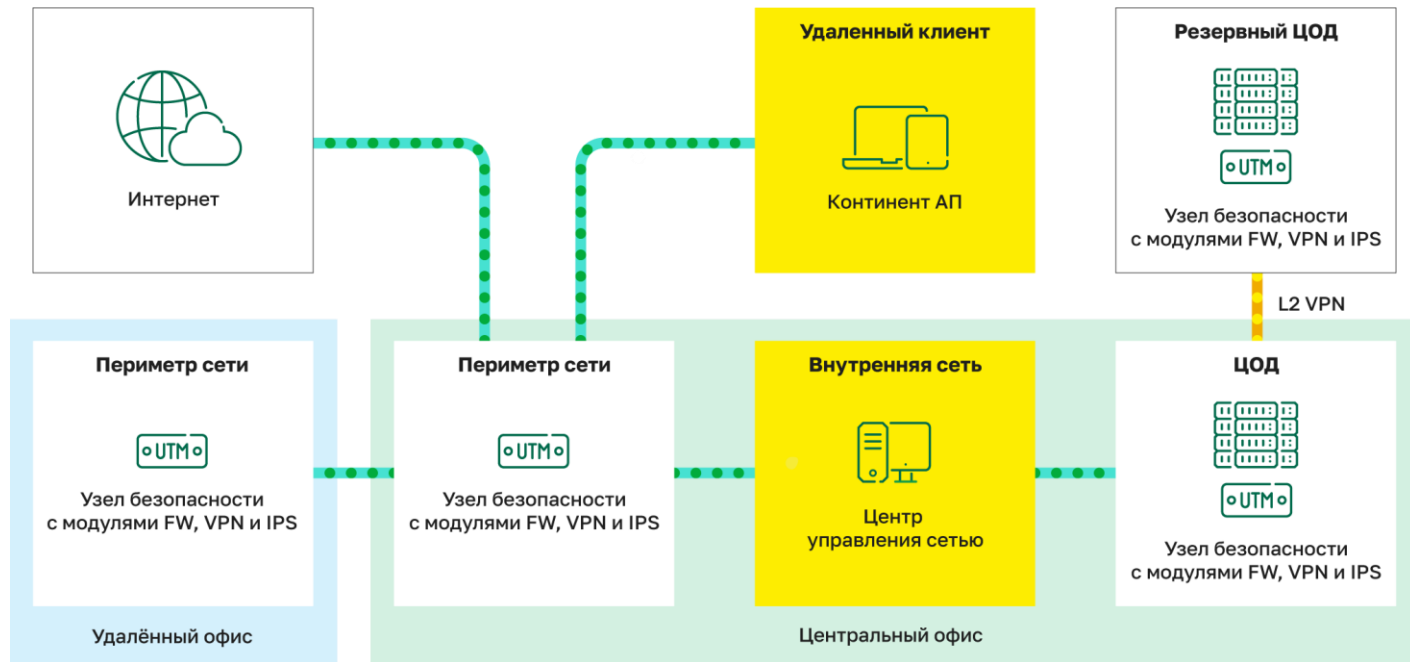
Сертифицирован ФСТЭК России:

- 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



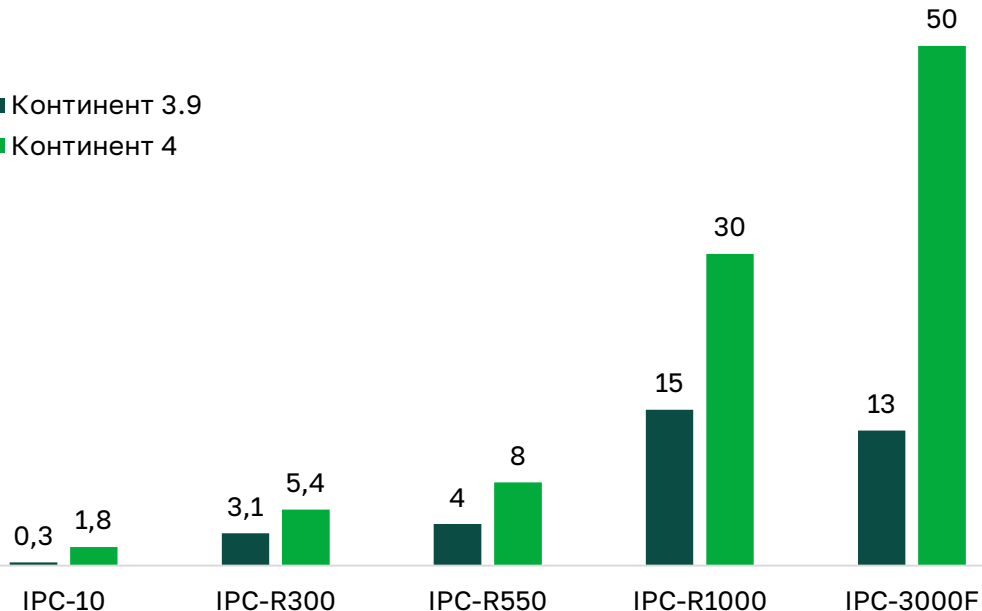


- FW
- IPS
- App control
- L2 VPN
- L3 VPN
- MGMT
- Threat Intelligence
- Log
- URL Filtering
- User Identity
- Antivirus
- GeoIP



Производительность межсетевого экрана, Гбит/с

■ Континент 3.9
■ Континент 4



НОВЫЙ ФУНКЦИОНАЛ

Одно устройство для всех механизмов безопасности

Управление компонентами из единой консоли

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



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.



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
- 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

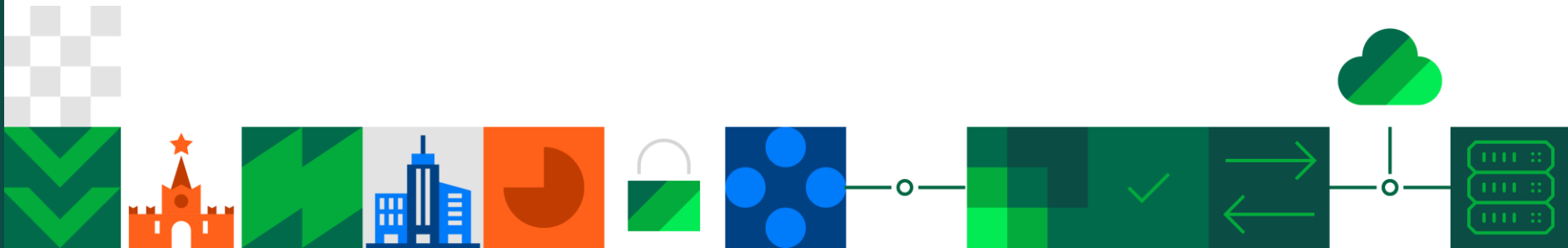


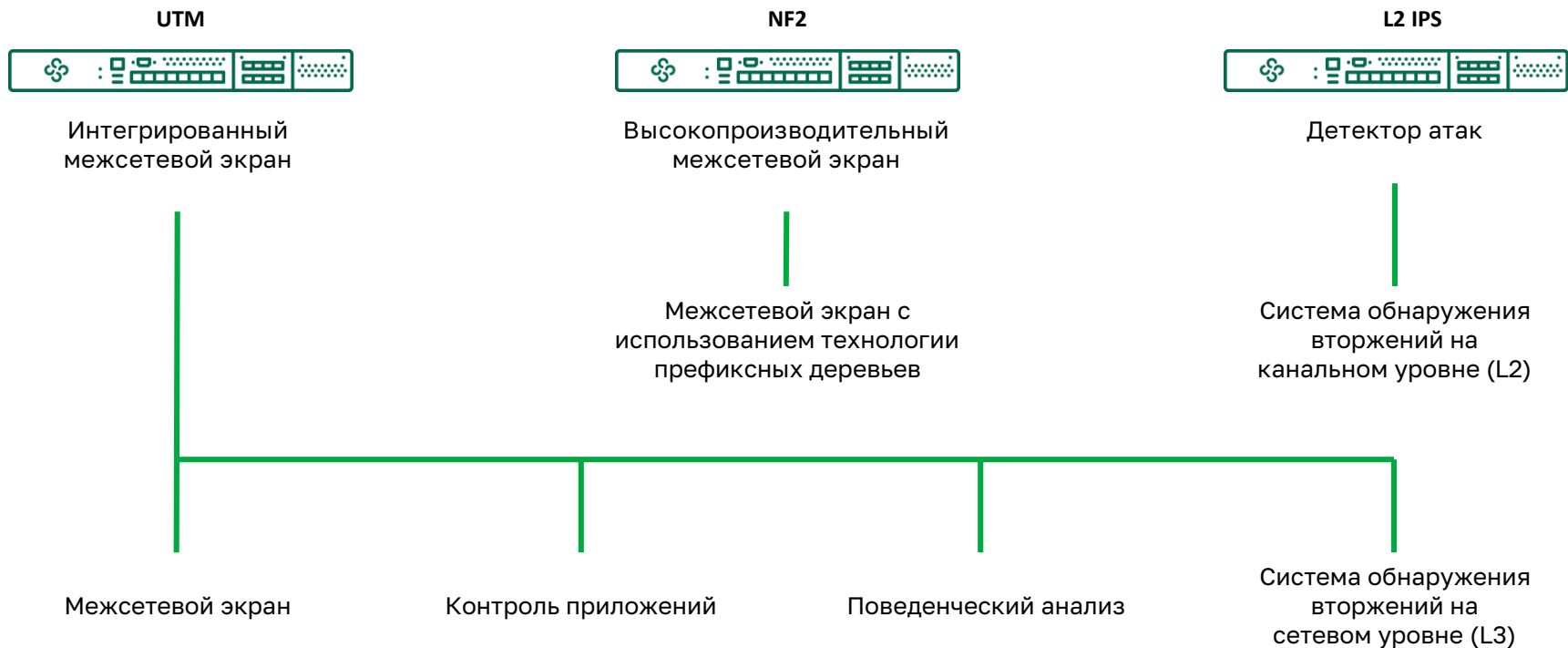
Сетевые технологии

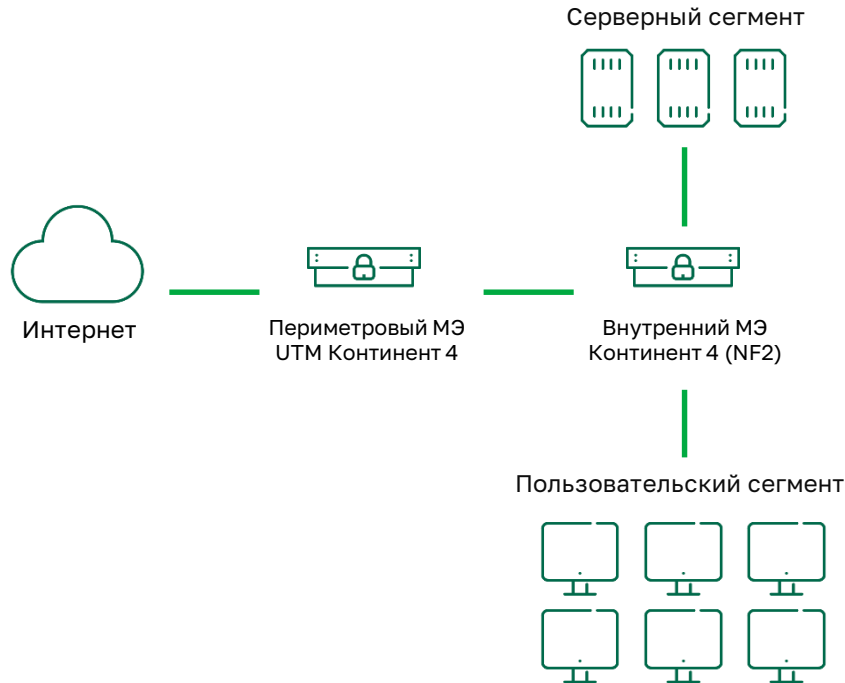
- Динамическая маршрутизация
- Поддержка NAT
- Multi-WAN
- QoS
- Кластеризация узлов безопасности (переключение менее 1 секунды)



Варианты применения



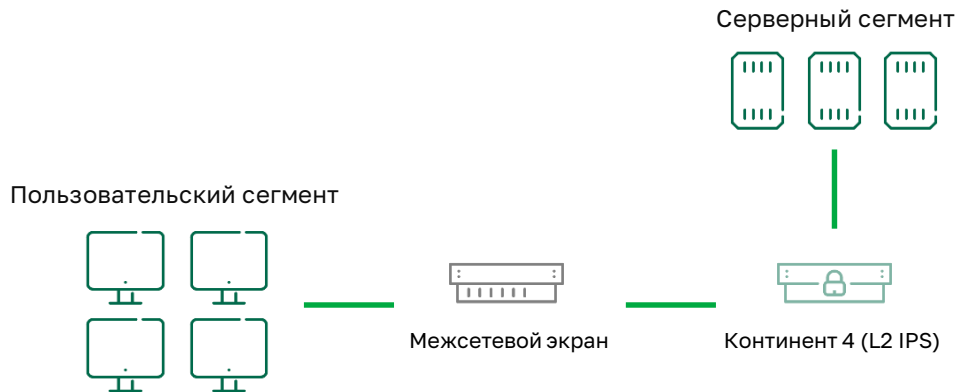




Задачи

- 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

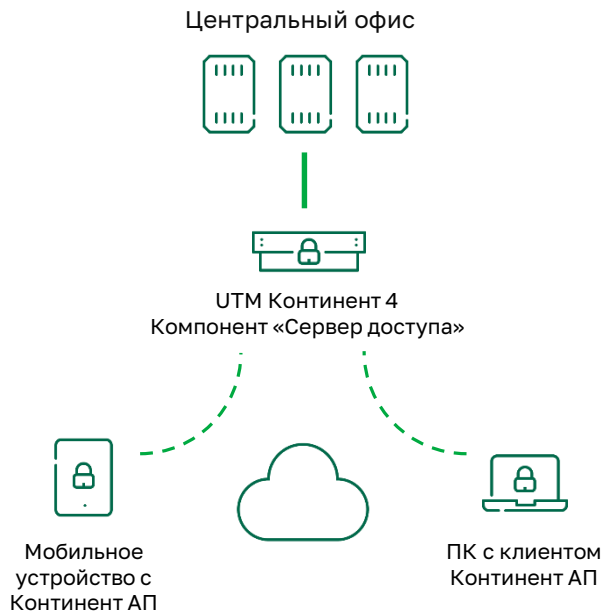




Задачи

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





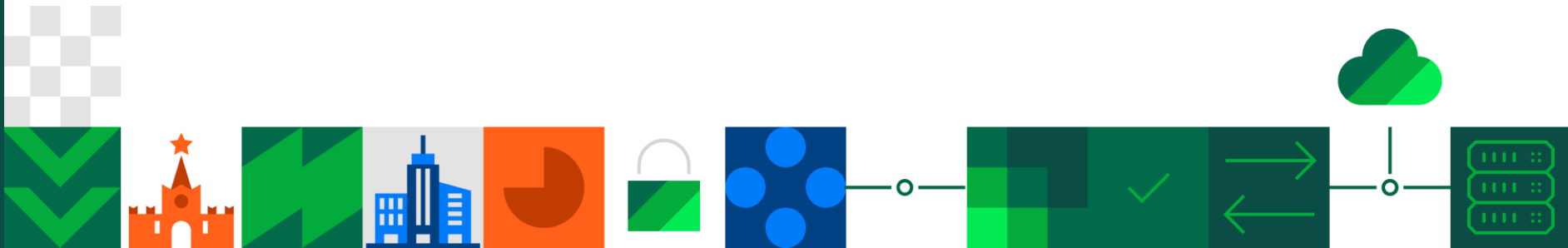
Задачи

- 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

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

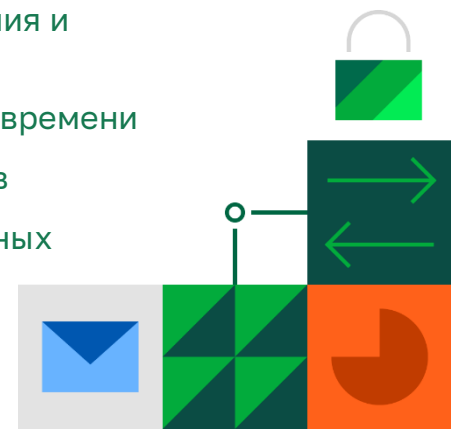
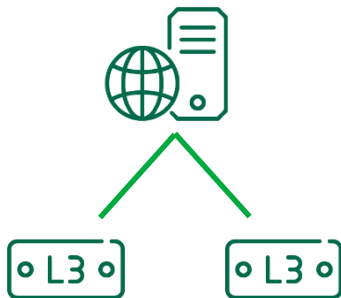
Высокопроизводительная система хранения и обработки событий безопасности

Мониторинг событий в режиме реального времени

Ролевая модель доступа администраторов

Многофакторная аутентификация удаленных пользователей:

- Сертификаты на USB-токенах
- Сервис Multifactor.ru



Файл Главная Вид Встроенный администратор

Назад Вперед Правило после Правило до Первое правило Последнее правило Создать Раздел Раскрыть все Свернуть все Вверх Вниз Копировать 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

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, RDP, SSH, TLS	* Любое	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												

Список объектов ЦСУ

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	

1 192.168.144.254

The screenshot displays the management interface for security nodes. A table lists the nodes, with the first row highlighted. A callout box labeled "Наименование узла безопасности" (Name of the security node) points to the "NGFW" entry in the "Название" (Name) column. Another callout box labeled "Компоненты" (Components) points to the "Компоненты" (Components) column header. A third callout box labeled "Версия политики" (Policy version) points to the "10146" entry in the "Версия конфигурации" (Configuration version) column. 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 "Компоненты" section in the modal is highlighted with a dashed green box, corresponding to the "Компоненты" callout. The configuration panel shows fields for "Идентификатор" (ID), "Название" (Name), "Описание" (Description), "Режим" (Mode) set to "UTM", and "Платформа" (Platform) set to "Custom platform".

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

Узел безопасности - NGFW

- Узел безопасности
 - Сертификаты
 - 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
 - Обновления
 - Мониторинг
 - Доступ к LVC
 - ICMP-сообщения
 - Система обнаружения вторжений
 - Переменные COB

Идентификатор: 1111
Название: NGFW
Описание:
Устройство:
Режим: UTM **Платформа:** Custom platform

Компоненты

- Центр управления сетью
- Межсетевой экран
- Расширенный контроль протоколов и приложений
- Защита от вредоносных веб-сайтов
- URL-фильтрация по категориям
- Антивирус
- Модуль GeoProtection
- Приоритизация трафика
- L2VPN
- L3VPN
- Система обнаружения вторжений
- Сервер доступа
- Идентификация пользователей
- Модуль поведенческого анализа

OK Отмена Применить

The screenshot shows a web-based management interface for VPNs. It is divided into several sections:

- Навигация (Navigation):** A sidebar menu on the left with options: L3VPN, L2VPN, and Удаленный доступ (Remote Access). A dashed green box highlights these options, with a callout box stating: "Управление всеми схемами VPN" (Management of all VPN schemes).
- Виртуальные частные сети (1) (Virtual Private Networks (1)):** A main content area with a search bar and a table. A dashed green box highlights the "Топология" (Topology) column, with a callout box stating: "Выбор топологии и типа VPN" (Selection of topology and type of VPN). Another dashed green box highlights the "Состав" (Composition) column, which lists "NGFW" and "NGFW-2", with a callout box stating: "УБ, между которыми строятся VPN туннели" (Firewalls between which VPN tunnels are built). A third dashed green box highlights the "Защищаемые ресурсы" (Protected resources) column, which lists IP ranges like "192.168.1.0/24-SMS-net...", with a callout box stating: "Защищаемые ресурсы" (Protected resources).
- Список объектов ЦУС (List of objects of the CUC):** A table at the bottom listing various network objects with columns for Name, Address, Mask, and Description.

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-100.12...	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

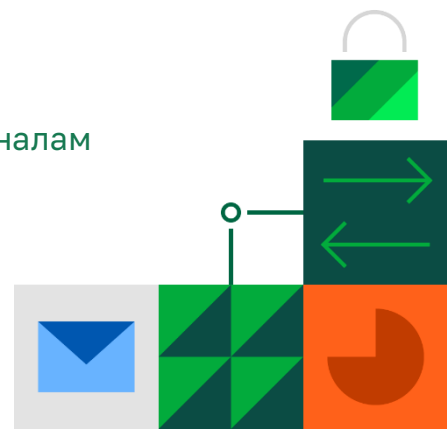
Поддержка приоритизации трафика (QoS)

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 – 700 приложений
- Продвинутый движок – 4000 приложений

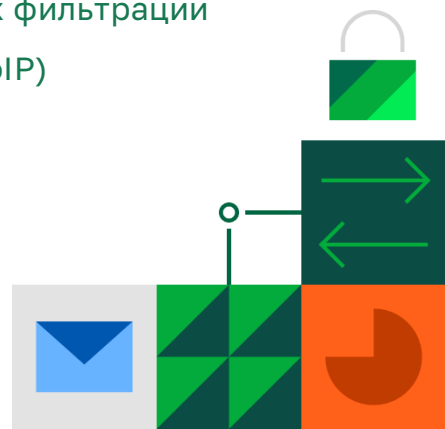
URL-фильтрация

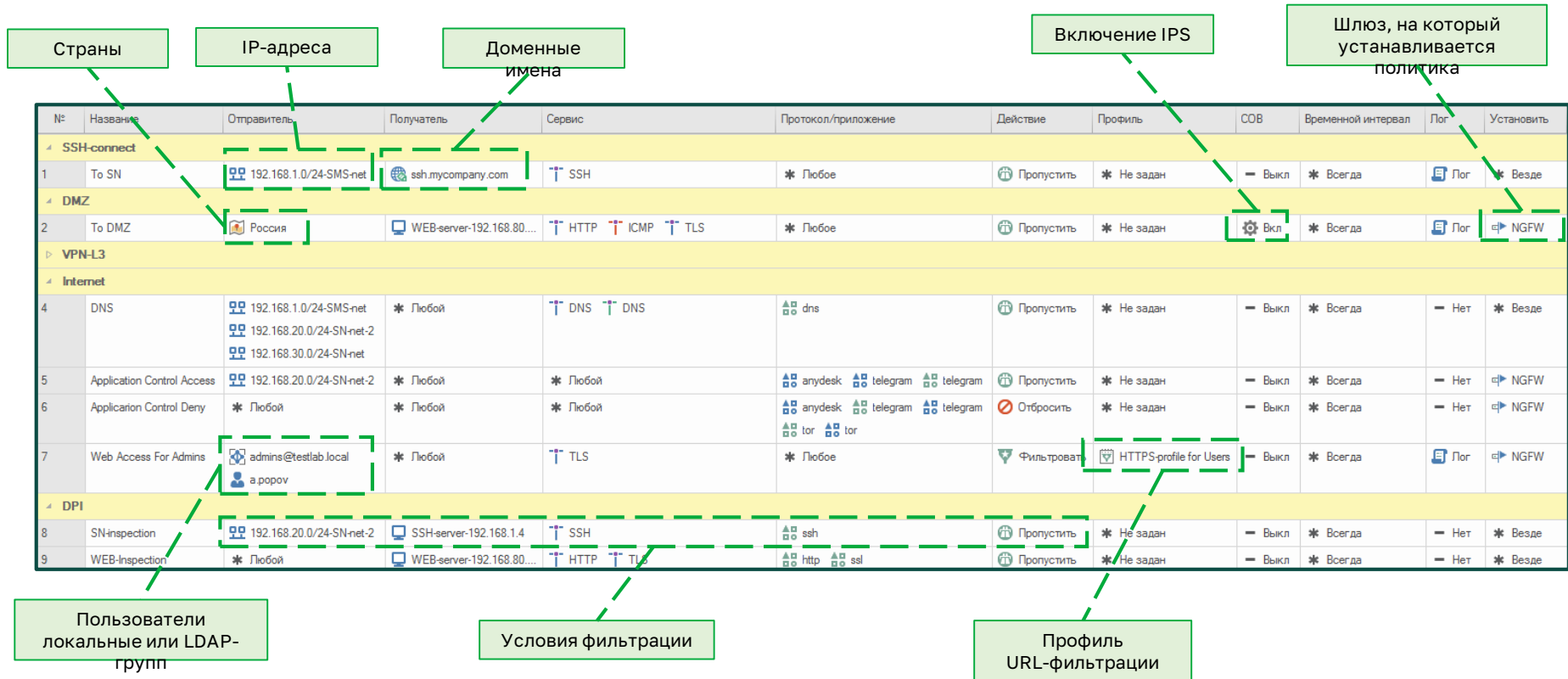
- На базе собственных черных и белых списков
- На базе predetermined categories of sites

Инспектирование SSL-трафика

Использование доменных имен в правилах фильтрации

Фильтрация трафика на основе стран (GeoIP)





The screenshot shows a table of firewall rules with the following columns: №, Название, Отправитель, Получатель, Сервис, Протокол/приложение, Действие, Профиль, COB, Временной интервал, Лог, and Установить. The rules are grouped into sections: SSH-connect, DMZ, VPN-L3, Internet, and DPI.

Callouts point to specific fields in the rules:

- Страны**: Points to the 'Отправитель' field of rule 2 (Russia).
- IP-адреса**: Points to the 'Отправитель' field of rule 1 (192.168.1.0/24-SMS-net).
- Доменные имена**: Points to the 'Получатель' field of rule 1 (ssh.mycompany.com).
- Включение IPS**: Points to the 'COB' field of rule 2 (Вкл).
- Шлюз, на который устанавливается политика**: Points to the 'Установить' field of rule 2 (NGFW).
- Пользователи локальные или LDAP-групп**: Points to the 'Отправитель' field of rule 7 (admins@testlab.local).
- Условия фильтрации**: Points to the 'Получатель' field of rule 8 (SSH-server-192.168.1.4).
- Профиль URL-фильтрации**: Points to the 'Действие' field of rule 7 (HTTPS-profile for Users).

№	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

Разделы (6), Правила фильтрации (14)

Поиск...

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие
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	T DNS T DNS	dns	Пропустить
5	Application Control Access	192.168.20.0/24-SN-net-2	* Любой	* Любой	anydesk telegram telegram Social	Пропустить
6	Application Control Deny	* Любой	* Любой	* Любой	anydesk telegram telegram tor tor	Отбросить
7	Web Access For Admins	admins@testlab.local a.porov	* Любой	T TLS	* Любое	Фильтровать
DPI						
8	SN-inspection	192.168.20.0/24-SN-net-2	SSH-server-192.168.1.4	T SSH	ssh	Пропустить

Список объектов ЦУС

Название	Категория	Тип	Комплект	Родитель	Описание
Tunnel	-	-	-	-	-
actmobile-services	Tunnel	Приложение	Расширенный	-	Actmobile Services
actmobile-services	Tunnel	Протокол	Расширенный	-	Actmobile Services
act-vpn	Tunnel	Приложение	Расширенный	-	Act VPN
act-vpn	Tunnel	Протокол	Расширенный	-	Act VPN
amaze-vpn	Tunnel	Приложение	Расширенный	-	Amaze VPN
anchorfree-services	Tunnel	Приложение	Расширенный	-	AnchorFree Services

Группы, прикладные протоколы, категории, приложения

Поиск

Список приложений



Предотвращение сетевых вторжений

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

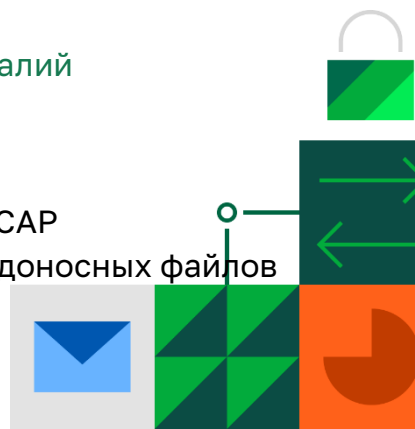
Блокировка доступа к вредоносным сайтам

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

Анализ сетевого трафика на наличие аномалий

Антивирусная проверка трафика

- Поточковый антивирус
- Взаимодействие с песочницами по ICAP
- Добавление собственных хэшей вредоносных файлов ^{new}



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	

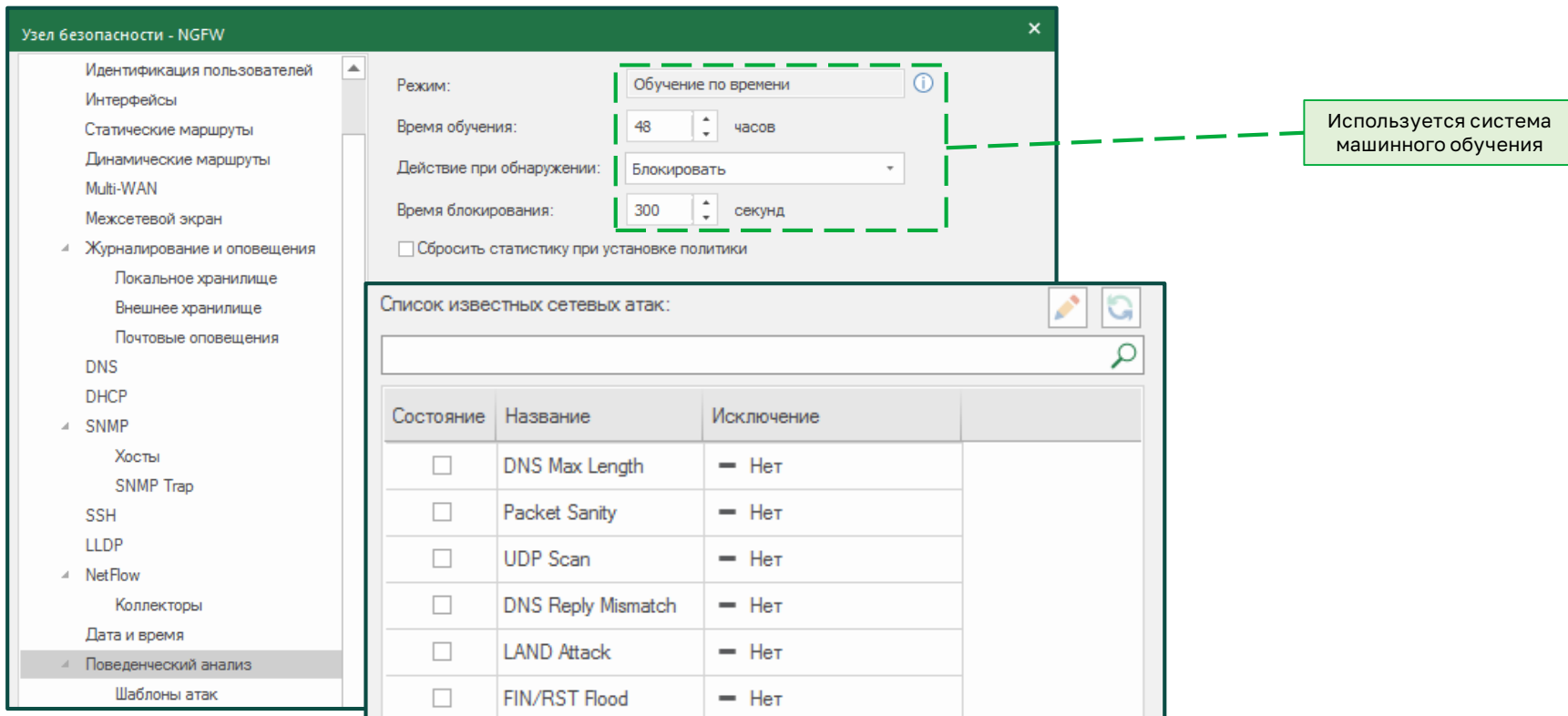
- Контроль доступа
- Виртуальные частные сети
- Система обнаружения вторжений
- Структура
- Администрирование

The image displays two screenshots of a security management interface. The top screenshot shows the 'Правила политики COV (1)' (COV Policy Rules) section. A table lists a rule named 'Новое правило' (New rule) associated with the 'IPS-profile' profile. The 'Установить' (Install) button for this rule is highlighted with a green dashed box. A callout box points to this button, stating: 'Узлы, на которые устанавливаются профили IPS' (Nodes to which IPS profiles are installed).

The bottom screenshot shows the 'Профили COV (4)' (COV Profiles) section. A table lists four profiles:

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 наиб...
IPS-profile	Пользовательский	

A callout box points to the 'IPS-profile' entry, stating: 'Специализированные профили под определенные типы угроз, в том числе 3 предустановленных профиля' (Specialized profiles for specific types of threats, including 3 pre-installed profiles).



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)

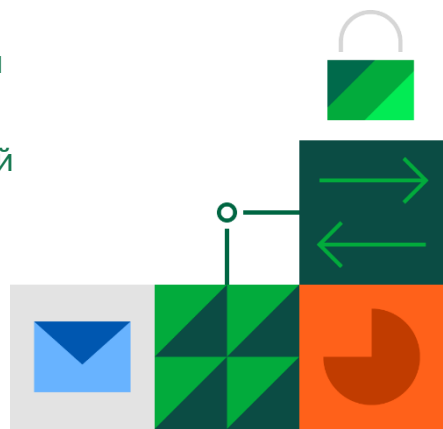
Поддержка различных ключевых носителей

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 ^{new}



Континент ZTN Клиент: новое поколение клиентов удаленного доступа

Единый криптографический клиент под все платформы
Контроль установленных приложений перед подключением



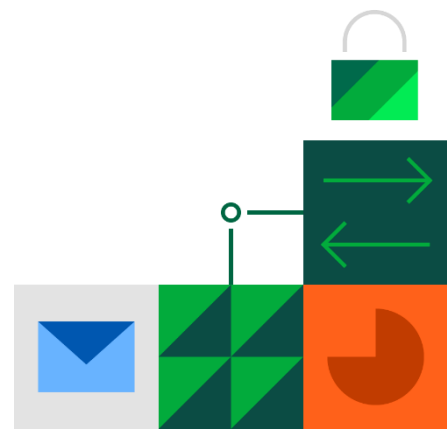
Подключение к ряду решений:

- 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)



Малые



- IPC-R10
- IPC-R50

Средние



- IPC-R300
- IPC-R550

Старшие



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

Название	Число ядер	МЭ, Мбит/с	УТМ, 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 (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.		