

# NGFW:

## **Континент 4**

FW/UTM/IPS/RA/VPN/Antivirus



## Безопасность

- Контроль сетевых приложений (4000 приложений)
- Система предотвращения вторжений (IDS/IPS)
- Блокировка доступа к вредоносным сайтам
- Поведенческий анализ на основе машинного обучения
- Поточный антивирус
- URL-фильтрация/SSL-инспекция



## Управление

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



## Режимы работы

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

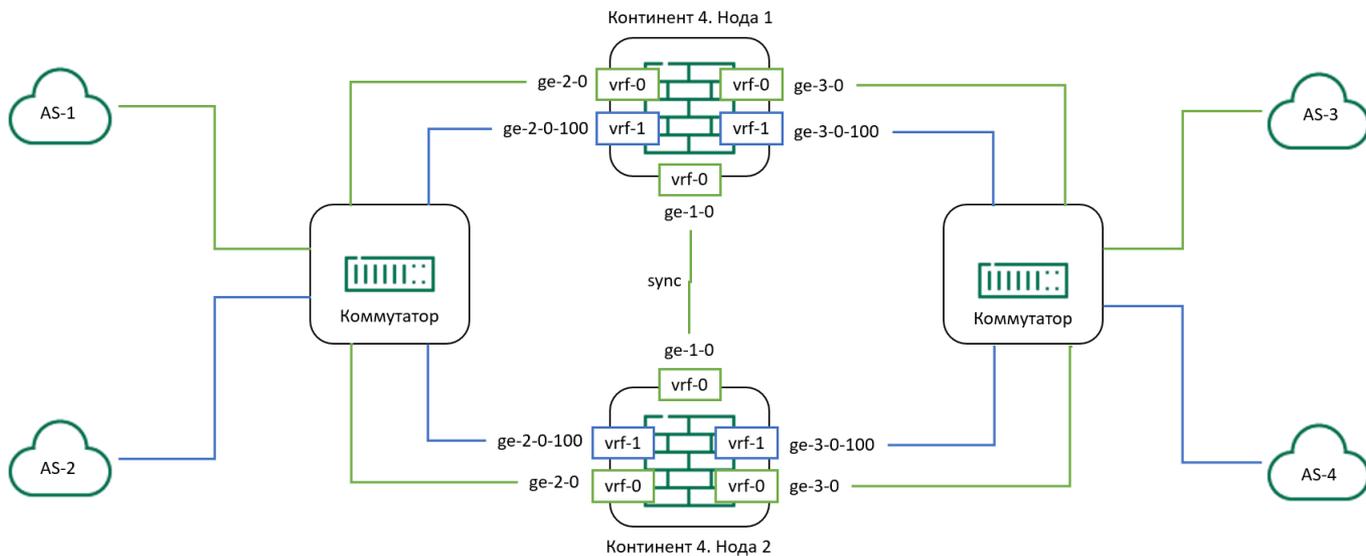


## Сетевые технологии

- Динамическая маршрутизация
- Поддержка NAT
- Multi-WAN
- QoS
- Кластеризация узлов безопасности

- ❖ Виртуальные маршрутизаторы (VRF)
- ❖ Явный прокси-сервер (Explicit Proxy)
- ❖ URL-фильтрация без вскрытия TLS/SSL-трафика (по SNI)
- ❖ Расширение источников Threat Intelligence
- ❖ Временные правила МСЭ
- ❖ Поддержка крупных доменов в SSO и Captive Portal
- ❖ Статические ARP-записи
- ❖ Инструменты автоматизации работы администратора
- ❖ Обновленная веб-система мониторинга

# Новое в 4.1.9 (VRF)



Механизм	VRF 0	VRF N
Трансляция адресов (NAT)	Да	Да
Фильтрация трафика (FW)	Да	Да
URL-фильтрация	Да	Нет
Контроль приложений	Да	Нет
Приоритизация трафика	Да	Нет
Поведенческий анализ	Да	Нет
Экспорт потоков по Netflow	Да	Нет
Антиспуфинг	Да	Нет
ЕСАР/ICAP	Да	Нет
Кластерные интерфейсы (VLAN)	Да	Да
Система мониторинга	Да	Нет
Идентификация пользователей	Да	Нет
Динамическая маршрутизация	Да	Да
Статическая маршрутизация	Да	Да
Мониторинг по SNMP	Да	Нет
DHCP сервер	Да	Нет

Механизм	VRF 0	VRF N
DHCP ретранслятор	Да	Нет
LLDP	Да	Нет
Аудит и мониторинг (доступ по веб)	Да	Нет
Подключение УБ к ЦУС	Да	Нет
Подключение МК к ЦУС	Да	Нет
Multi-WAN	Да	Нет
Загрузка обновлений	Да	Нет
DNS клиент/прокси	Да	Нет
Доступ к УБ по SSH	Да	Нет
Доступ к УБ по ICMP	Да	Нет
ARP	Да	Нет
L2 VPN	Да	Нет
L3 VPN	Да	Нет
Сервер доступа	Да	Нет
GeoProtection	Да	Нет
Обнаружение вторжений	Да	Нет

- Изоляция правил фильтрации (FW) и трансляции (NAT)
- Контроль динамической маршрутизации в VRF

Разделы (3), Правила фильтрации (13)												
Поиск...												
№	Название	Отправитель	Получатель	Сервис	Протокол/приложе...	Действие	Профиль	COB	Временной интерв...	Лог	VRF	Установить
▲ VRF-1 Rules												
1	VRF-1 Rule 1	Host-VRF-1	SNS	SNS-GC-LDS SNS-IPsec SNS-LDS SNS-PassChange-Kerberos-TCP SNS-PassChange-Kerberos-UDP	* Любое	Пропуст...	* Не задан	- Выкл	* Всегда	Лог	vrf-001	node-1015
2	VRF-1 Rule 2	VRF-1	Local Servers	DNS DNS FTP HTTP TLS ICMP	* Любое	Пропуст...	* Не задан	- Выкл	* Всегда	Лог	vrf-001	node-1015
3	VRF-1 Rule 3	VRF-1	Net-1-2	IPsec-NAT-T ISAKMP-TCP ISAKMP-UDP	* Любое	Пропуст...	* Не задан	- Выкл	* Всегда	Лог	vrf-001	node-1015
▲ VRF-2 Rules												
4	VRF-2 Rule 1	VRF-2 Net	SQL-host	PostgreSQL	* Любое	Пропуст...	* Не задан	- Выкл	* Всегда	- Нет	vrf-002	node-1015
5	VRF-2 Rule 2	VRF-2 Net	* Любой	TCP	* Любое	Отброси...	* Не задан	- Выкл	* Всегда	- Нет	vrf-002	node-1015
▲ Internet												
6	SC	LAN	securitycode.ru	* Любой	* Любое	Пропуст...	* Не задан	- Выкл	* Всегда	Лог	- Нет	node-1015
7	Block QUIC	* Любой	* Любой	QUIC	* Любое	Отброси...	* Не задан	- Выкл	* Всегда	- Нет	vrf-all	node-1015
8	Block Bad App	* Любой	* Любой	* Любой	anydesk bit bit telegram telegram tor	Отброси...	* Не задан	- Выкл	* Всегда	Лог	- Нет	node-1015

- Инструменты автоматизации работы администратора:

- ❖ Генерация правил МСЭ и NAT
- ❖ Генерация логических интерфейсов VLAN
- ❖ Экспорт конфигурации в сторонние системы
- ❖ Экспорт конфигурации в сторонние ЦУС
- ❖ Установка политики по расписанию
- ❖ Создание бэкапов по расписанию
- ❖ Импорт объектов IoC от вендора R-Vision <sup>new</sup>
- ❖ Импорт объектов IoC от вендора Security-Vision <sup>new</sup>
- ❖ Создание правил фильтрации и трансляции <sup>new</sup>

### Инструменты автоматизированной миграции:

- ❖ Миграция с Check Point
- ❖ Миграция с FortiGate
- ❖ Миграция с Cisco ASA
- ❖ Миграция в Palo Alto <sup>new</sup>
- ❖ Миграция с Континент 3
- ❖ Миграция данных с СД Континент 3 на СД Континент 4

Преимущество	Ценность
<ul style="list-style-type: none"><li>• API для работы с Континент 4</li><li>• Автоматизация процессов администрирования</li></ul>	Снижает нагрузку на команду администраторов

## Континент 4 - Инструменты

Важно! Последние изменения представлены в файле `patch_notes.txt`.

Репозиторий содержит инструменты для решения различных сервисных задач при использовании продукта Континент 4:

Инструмент	Назначение	Формат	Комментарий
<code>c4_lib</code>	Библиотека для работы с API Континент 4	Online	Нет
<code>c4_config_exporter</code>	Инструмент для экспорта конфигурации УБ для сторонних compliance-систем	Online	Только совместно с <code>c4_lib</code>
<code>c4_rules_maker</code>	Инструмент для генерации правил по заданным директивам	Online	Только совместно с <code>c4_lib</code>
<code>c4_vlan_maker</code>	Инструмент для генерации логических интерфейсов VLAN по заданному списку	Online	Только совместно с <code>c4_lib</code>
<code>c4_xls_rules_maker</code>	Инструмент для создания правил фильтрации (FW) и трансляции (NAT) по заданному шаблону	Online	Только совместно с <code>c4_lib</code> , в том числе для миграции данных из Palo Alto Networks
<code>c4_backup_tool</code>	Инструмент для создания и выгрузки резервной копии БД ЦУС	Online	Только совместно с <code>c4_lib</code>
<code>c4_config_transfer</code>	Инструмент для переноса в ограниченном объеме политики между разными ЦУС	Online	Только совместно с <code>c4_lib</code>
<code>c4_policy_install</code>	Инструмент для подачи ЦУС команды на установку политики	Online	Только совместно с <code>c4_lib</code>
<code>c4_ioc_importer_rv</code>	Инструмент для импорта объектов IoC (Indicator of Compromise) от вендора R-Vision	Online	Только совместно с <code>c4_lib</code> , Континент 4.1.9 и выше

**Подробнее о возможности:**

**[https://github.com/itseccode/c4\\_tools](https://github.com/itseccode/c4_tools)**



- ❖ IPSec AES и IPSec ГОСТ на одном устройстве
- ❖ Сертификация по требованиям ФСБ (КС1, КС2, КС3, МЭ4)
- ❖ Менеджер конфигураций по Linux
- ❖ Установка БРП без применения политики
- ❖ RADIUS

UTM



**Межсетевой экран**



Межсетевой экран с набором функционала

NF2



**Высокопроизводительный межсетевой экран**



Межсетевой экран с использованием технологии префиксных деревьев

L2 IPS/IDS



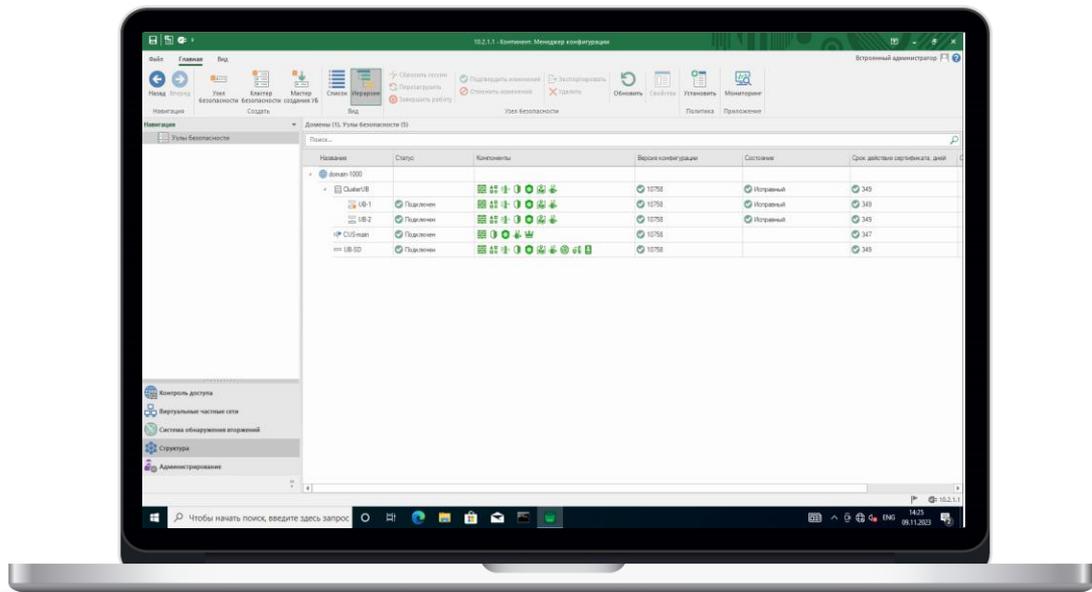
**Детектор атак**



Система обнаружения вторжений на канальном уровне (L2)

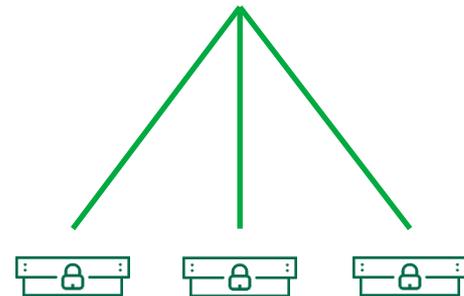
FW

Контроль приложений  
SSL инспекция/WEB-фильтрация  
Сервер доступа RA  
L2 VPN  
Антивирус  
COB на уровне L3



Менеджер конфигурации  
Web-мониторинг

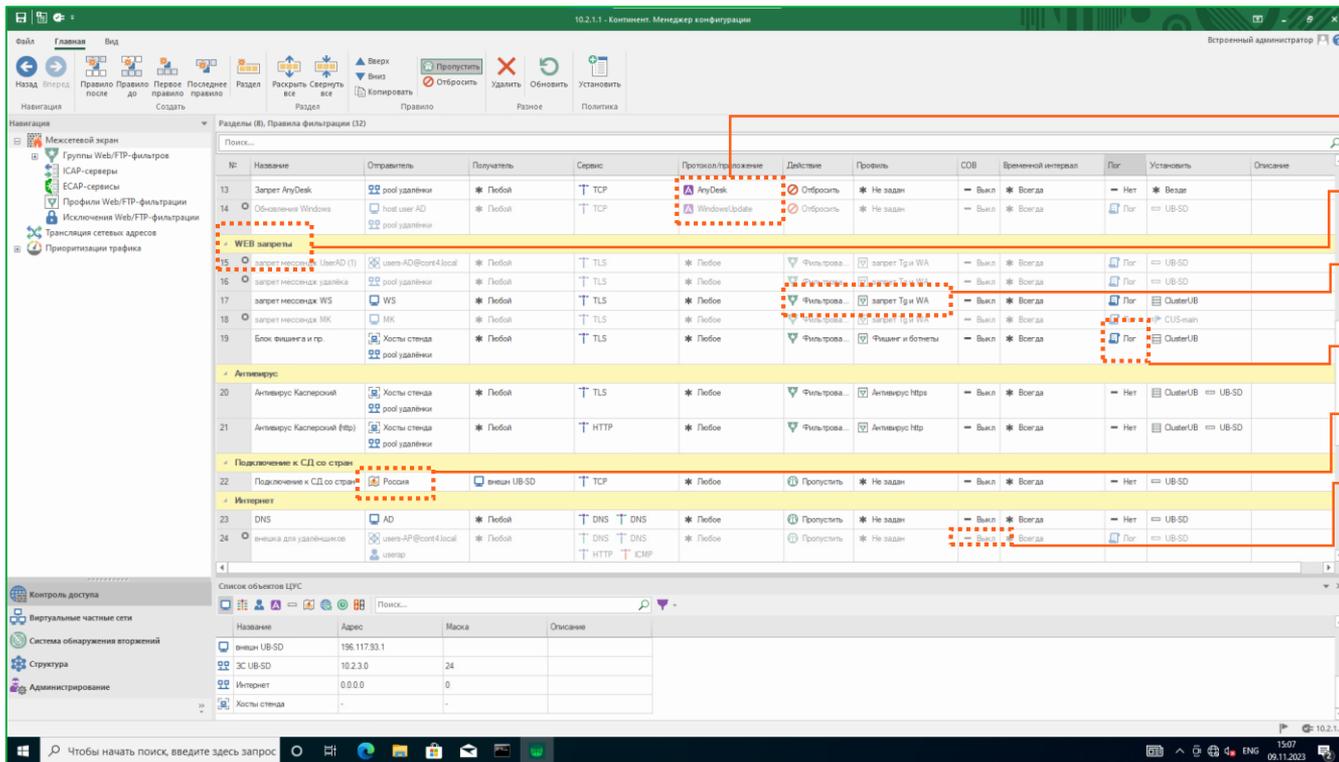
Центр управления сетью  
Континент 4



Узел  
безопасности  
UTM

Узел  
безопасности  
NF2

Узел  
безопасности  
IPS/IDS



Менеджер конфигурации 10.2.1.1 - Конфигурация

Разделы (8), Правила фильтрации (32)

№	Название	Отправитель	Получатель	Сервис	Протокол/приложение	Действие	Профиль	СОВ	Временной интервал	Лог	Установка	Описание
13	Запрет AnyDesk	root удаленки	* Любая	TCP	AnyDesk	Отбросить	* Не задан	Выкл	Всегда	Нет	Везде	
14	Обновления Windows	root user AD	* Любая	TCP	WindowsUpdate	Отбросить	* Не задан	Выкл	Всегда	Лог	UB-SD	
<b>WEB запреты</b>												
15	запрет сообщений LiveAD (1)	livead-AD@cont4.local	* Любая	TLS	Любое	Фильтрация	запрет Tr и WA	Выкл	Всегда	Лог	UB-SD	
16	запрет сообщений удаленки	root удаленки	* Любая	TLS	Любое	Фильтрация	запрет Tr и WA	Выкл	Всегда	Лог	UB-SD	
17	запрет сообщений WS	WS	* Любая	TLS	Любое	Фильтрация	запрет Tr и WA	Выкл	Всегда	Лог	ClusterUB	
18	запрет сообщений МК	МК	* Любая	TLS	Любое	Фильтрация	Фishing и ботнеты	Выкл	Всегда	Лог	ClusterUB	
19	Блок мошеннича и гр	Хосты стэнда	* Любая	TLS	Любое	Фильтрация	Фishing и ботнеты	Выкл	Всегда	Лог	ClusterUB	
<b>Антивирус</b>												
20	Антивирус Касперский	Хосты стэнда	* Любая	TLS	Любое	Фильтрация	Антивирус https	Выкл	Всегда	Нет	ClusterUB	UB-SD
21	Антивирус Касперский (ftp)	Хосты стэнда	* Любая	HTTP	Любое	Фильтрация	Антивирус http	Выкл	Всегда	Нет	ClusterUB	UB-SD
<b>Подключение к СД со стран</b>												
22	Подключение к СД со стран	Россия	вещи UB-SD	TCP	Любое	Пропустить	* Не задан	Выкл	Всегда	Нет	UB-SD	
<b>Интернет</b>												
23	DNS	AD	* Любая	DNS	DNS	Любое	Пропустить	* Не задан	Выкл	Всегда	Нет	UB-SD
24	вещи для удаленки	user-AP@cont4.local	* Любая	DNS	DNS	Любое	Пропустить	* Не задан	Выкл	Всегда	Лог	UB-SD
		winapp		HTTP	ICMP							

Список объектов ЦУС

Название	Адрес	Маска	Описание
вещи UB-SD	196.117.93.1		
3С UB-SD	10.2.3.0	24	
Интернет	0.0.0.0	0	
Хосты стэнда	-	-	

Контроль приложений

Пользовательские разделы

URL-фильтрация

Логирование

GeoIP. Фильтрация по странам

IPS/IDS L3

СОСТОЯНИЕ    ДЕТАЛЬНАЯ ИНФОРМАЦИЯ    ШАБЛОН    НАСТРОЙКИ    ДОСТУП    СОСЕДСТВО

Все события    Генерация отчета

Узел: UB-1

Активные события

Важность	Продолжительность
предупреждение	03 04 53

ЦП и память

50% ОЗУ	0% swp	35% ЦП	0°C температура
---------	--------	--------	-----------------

Подсистемы

Активный Можетевой ...	6% журнал	Активный syslog	Активный Кластер	2 VPN
------------------------	-----------	-----------------	------------------	-------

Жесткие диски

0 sda
-------

Разделы жестких дисков

39% Boot	6% Data	19% System	0% Температу
----------	---------	------------	--------------

Сетевые интерфейсы

Интерфейс	IP-адрес	MAC-адрес	Состояние	Получено
ge-0-0	216.117.94.1/24	00:50:56:96:35:a7	активный	22.70 MB

Журналы

https://monitor.con.tcc/journals/security

СИСТЕМА: 2546    261773    СЕТЕВАЯ БЕЗОПАСНОСТЬ: 801    8    8200    УПРАВЛЕНИЕ: 2645

Система    Сетевая безопасность    Управление

Автообновление    Записей: 2785

Дата	Действие	Узел безопасности	Адрес отправителя	Страна отправителя	Адрес получателя
03 11 2023 18:37:02.073	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:36:35.425	заблокировано	UB-SD	192.2.3.200	Частные адреса	152.199.15
03 11 2023 18:36:31.993	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:36:14.041	разрешить	UB-SD	192.2.3.200	Частные адреса	13.69.118
03 11 2023 18:36:01.881	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:35:31.801	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:35:19.129	заблокировано	UB-SD	192.2.3.200	Частные адреса	152.199.15
03 11 2023 18:35:01.689	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:34:31.609	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:34:01.529	разрешить	UB-SD	192.2.3.200	Частные адреса	13.69.118
03 11 2023 18:34:01.529	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:33:59.833	заблокировано	UB-SD	192.2.3.200	Частные адреса	152.199.15
03 11 2023 18:33:47.417	разрешить	UB-SD	192.2.3.200	Частные адреса	13.69.118
03 11 2023 18:33:46.041	разрешить	UB-SD	192.2.3.200	Частные адреса	13.69.118
03 11 2023 18:33:44.409	разрешить	UB-SD	192.2.3.200	Частные адреса	83.164.22
03 11 2023 18:33:30.937	разрешить	UB-SD	192.2.3.200	Частные адреса	194.51.205
03 11 2023 18:33:30.937	разрешить	UB-SD	192.2.3.200	Частные адреса	13.69.118

Детальная информация о событии

Компонент: Механизм эрлан  
 Действие: заблокировано  
 Важность: Оповещение

Информация о трафике

Адрес отправителя: 192.2.3.200  
 Страна отправителя: Частные адреса  
 Адрес получателя: 152.199.19.161  
 Страна получателя: Соединенные Штаты  
 Имя отправителя: user@CONT4.LOCAL  
 Домен получателя: Протокол: TCP  
 Порт получателя: 80  
 Порт отправителя: 50086

Дополнительная информация

Идентификатор подписи: 11  
 Подпись: windows-store  
 Тип подписи: Интерфейс: Количество срабатываний: 1  
 Платформенная информация: SNAT: 10.2.3.200 ↔ 172.17.148.50

Закрыть

Чтобы начать поиск, введите здесь запрос

## Динамическая маршрутизация

OSPF  
BGP

## Поддержка NAT

Входящий и исходящий

## Multi-WAN

Failover  
Балансировка трафика

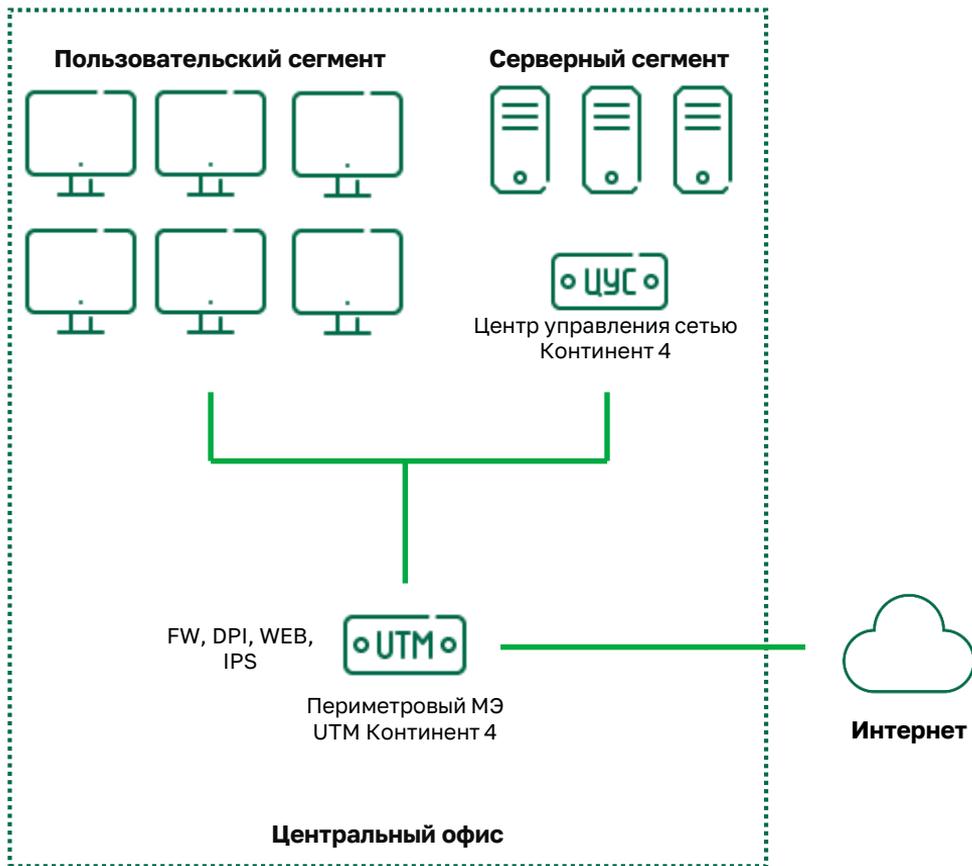
QoS

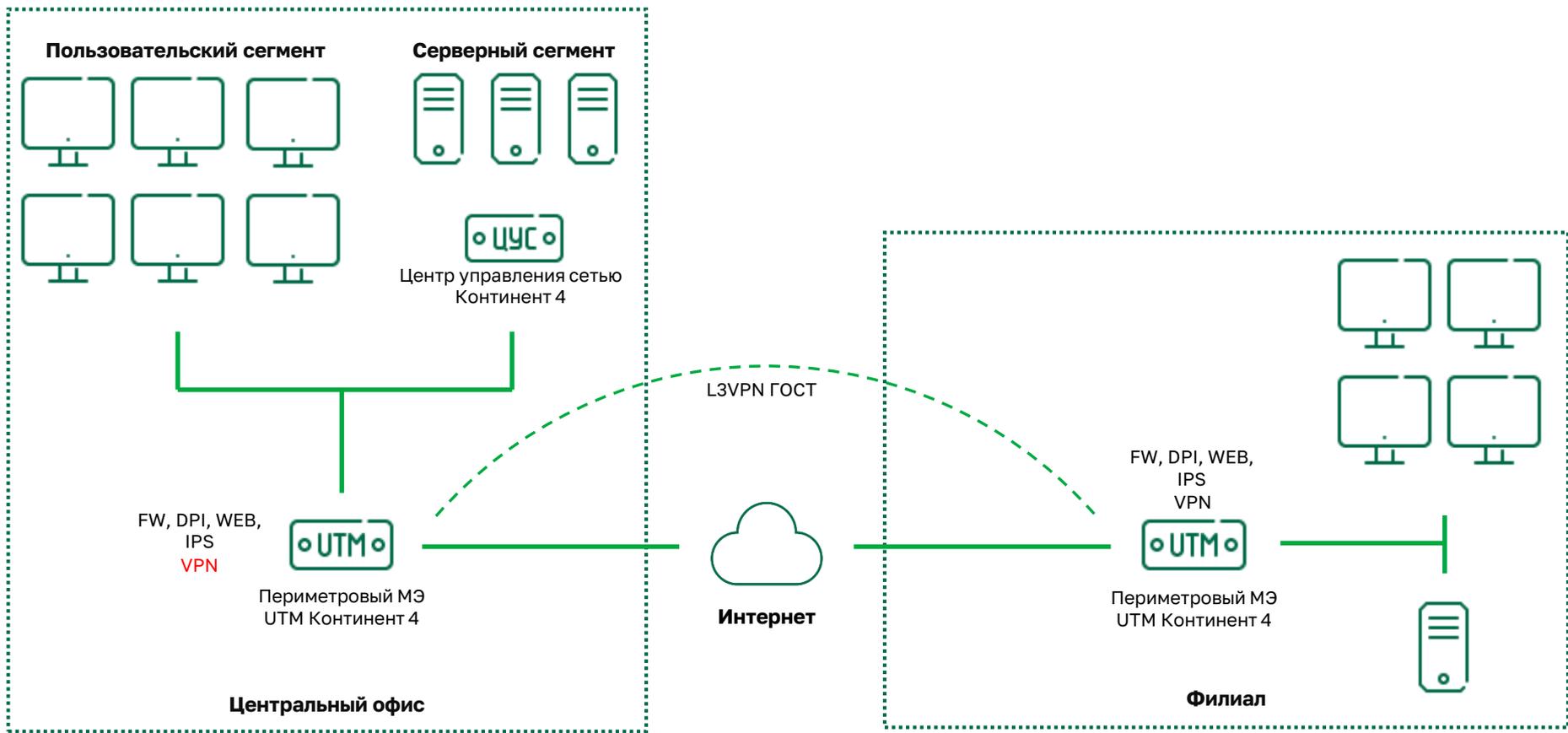
## Кластеризация узлов безопасности

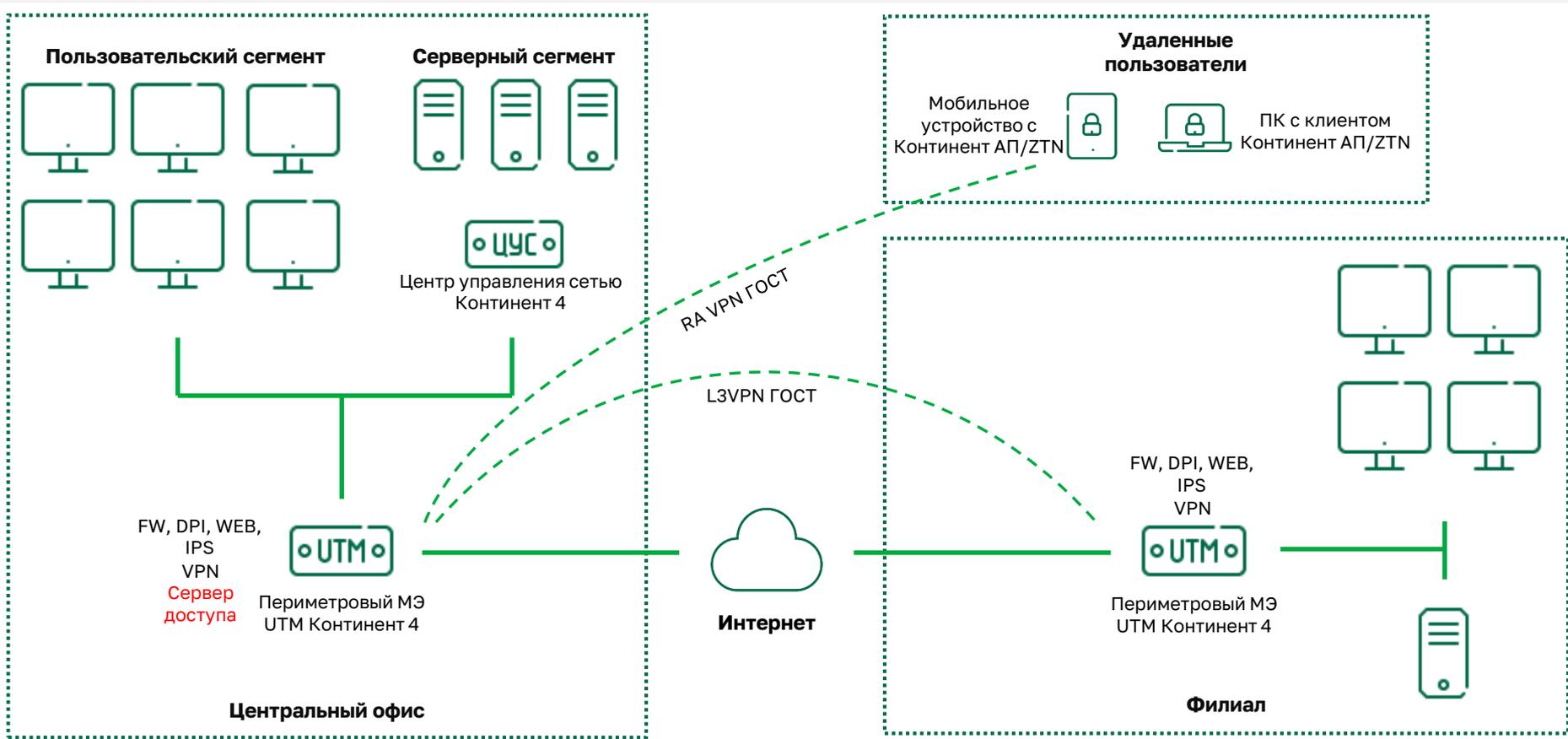
Active-Passive  
без разрыва сессий

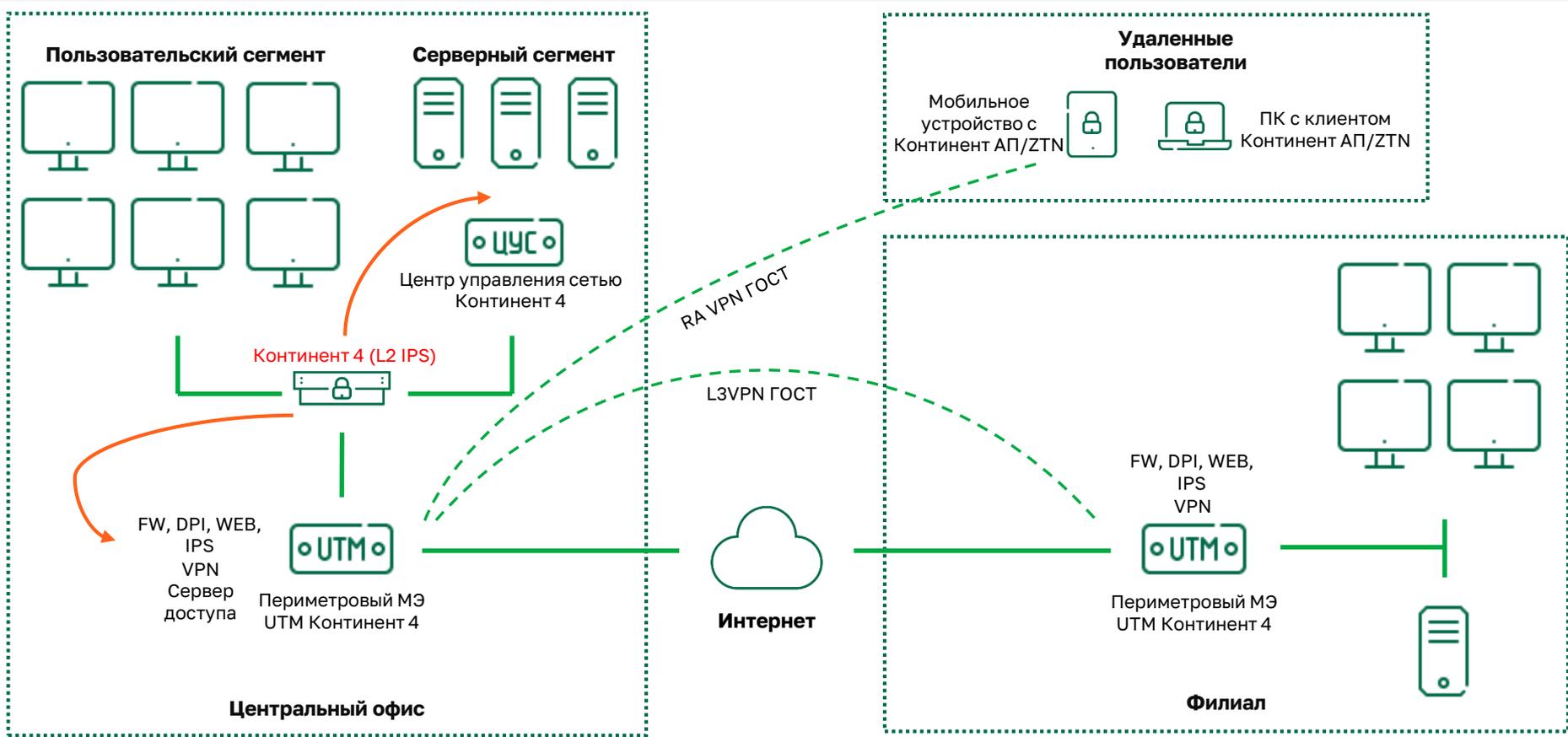
## Поддержка VLAN

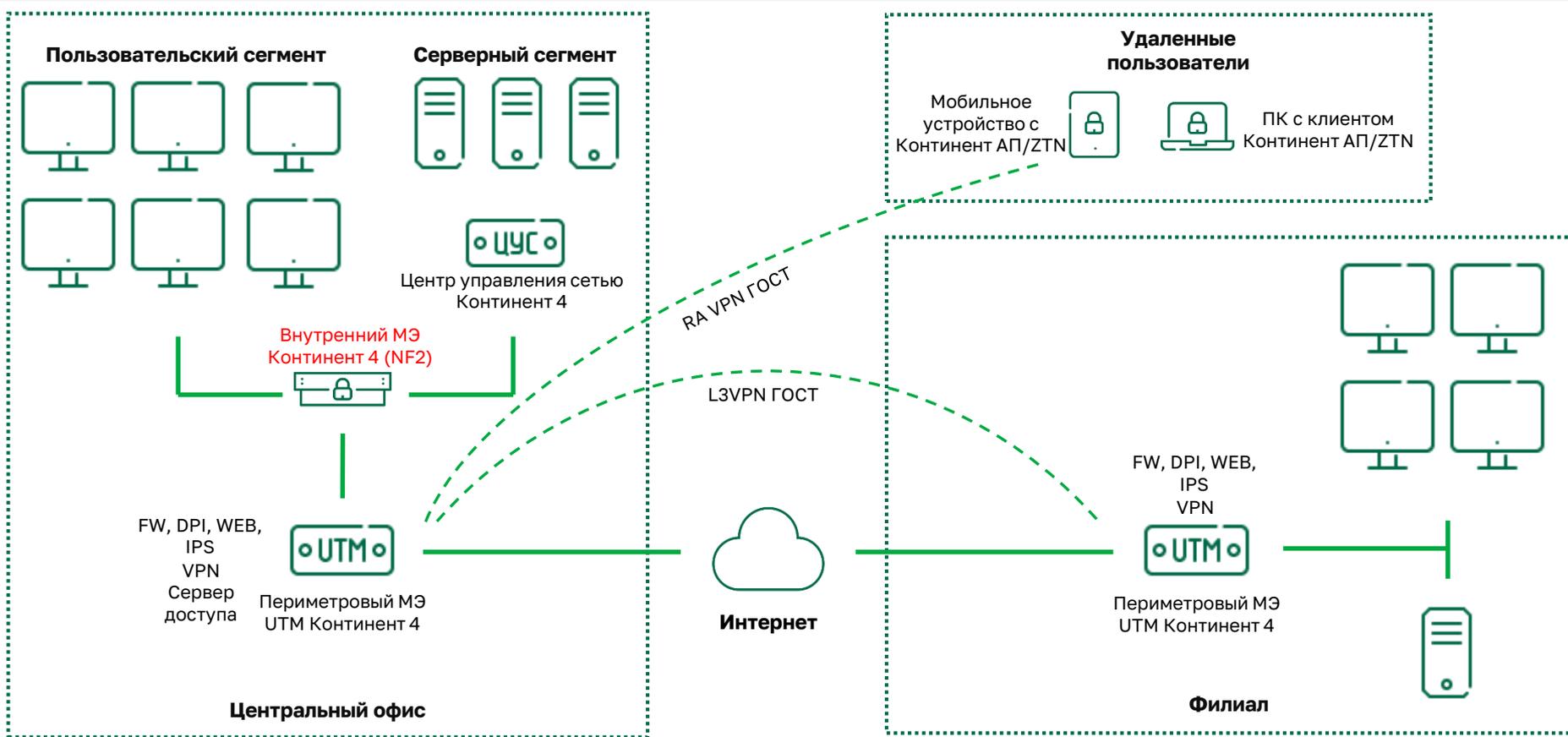
DHCP-сервер  
DHCP-ретранслятор

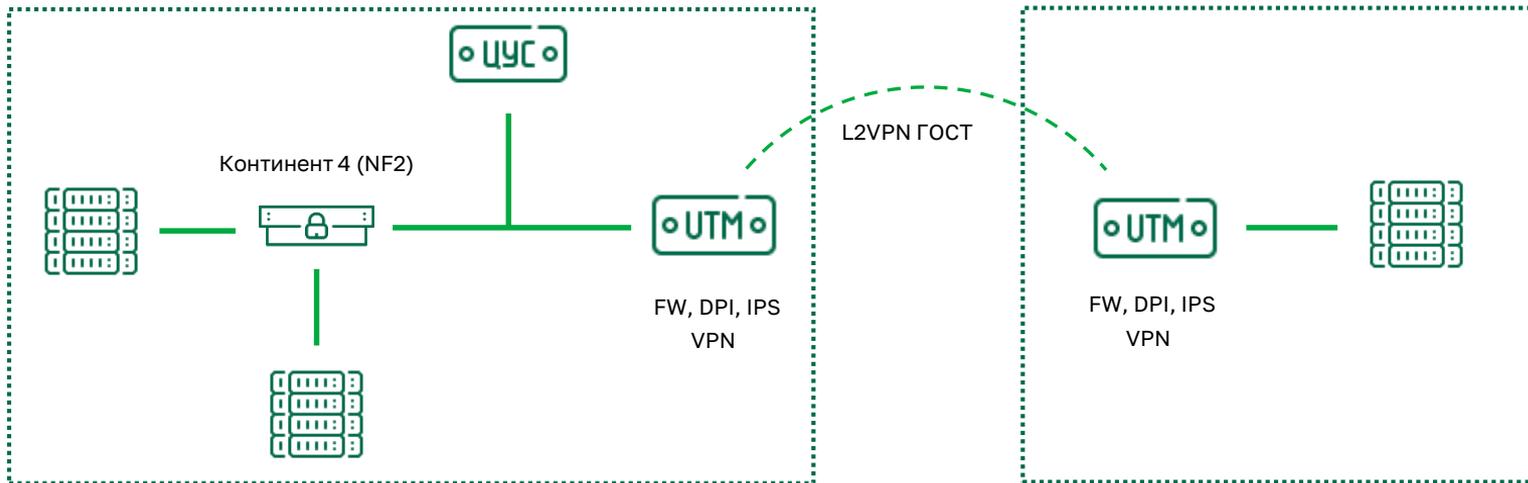






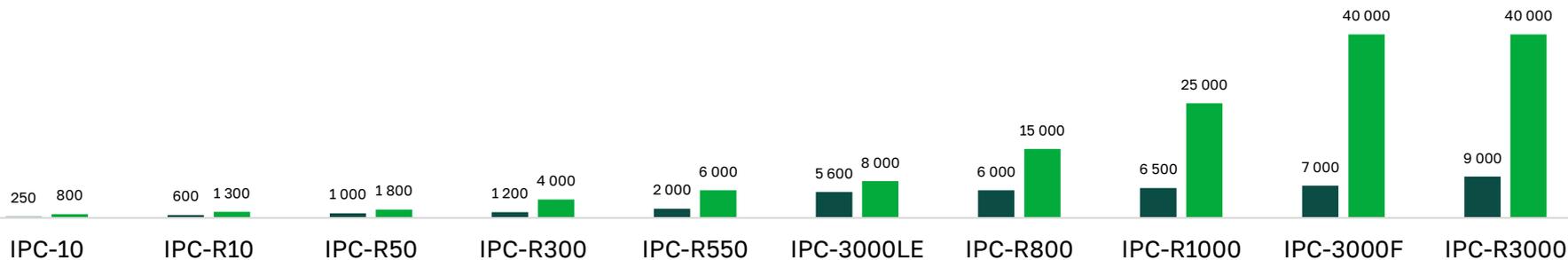






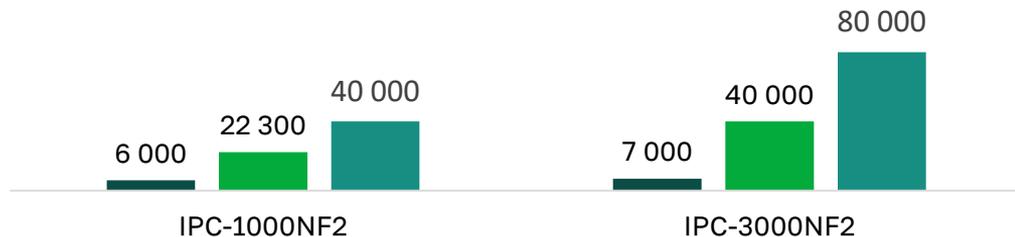
■ NGFW ■ MCЭ

## Производительность аппаратных платформ, Мбит/с



■ NGFW ■ MCЭ ■ NF2

## Производительность платформ NF2, Мбит/с



## 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
<b>SOHO</b>	2	2 000	7 00	1 000
<b>SMB</b>	4	11 000	2 500	2 000
<b>ENT</b>	8	15 000	4 000	5 500



**Прямой импорт политик CheckPoint, FortiGate**

**Импорт политик с Cisco ASA, Palo Alto через промежуточный импорт в Check Point**

**Миграция с Континент 3**

**Большой  
онлайн по  
Континент 4**



**Telegram канал  
Код на проводе**



**Импортозамещение  
NGFW**



**Telegram чат  
по Континенту**



# Спасибо за внимание!

KeyProjects@securitycode.ru по вопросам при пилоте  
info@securitycode.ru по общим вопросам

www.securitycode.ru сайт