КОД безопасности

NGFW:

Континент 4

FW/UTM/IPS/RA/VPN/Antivirus

КОД безопасности

Функциональность Континент 4

Безопасность

- Контроль сетевых приложений (4000 приложений)
- Система предотвращения вторжений (IDS/IPS)
- Блокировка доступа к вредоносным сайтам
- Поведенческий анализ на основе машинного обучения
- Потоковый 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

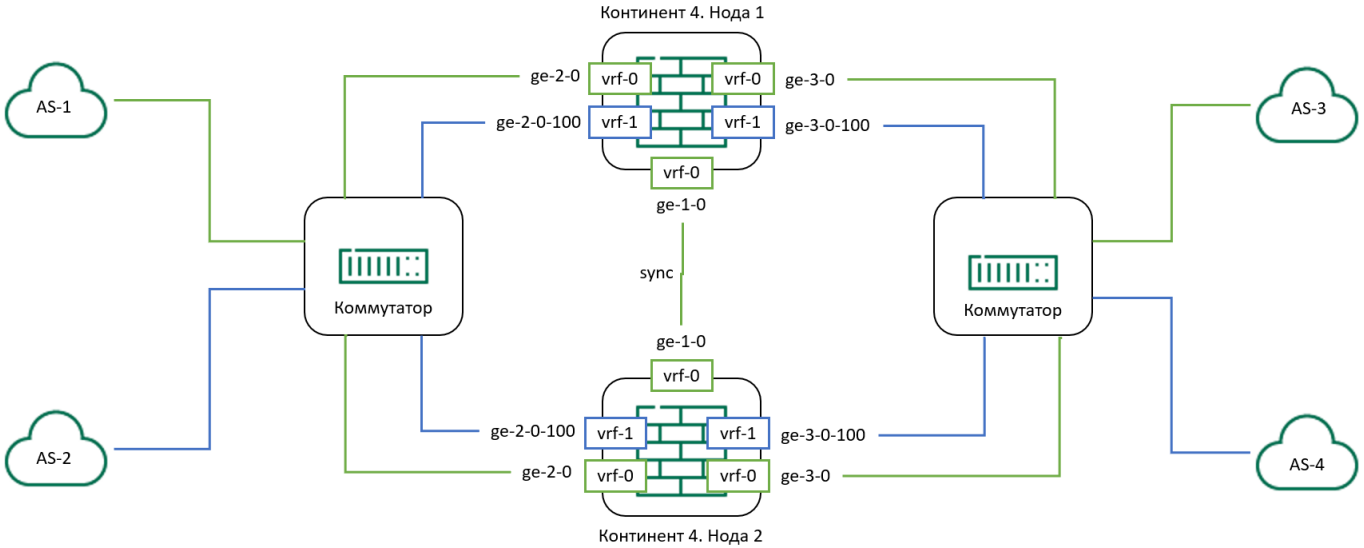
КОД безопасности

Новое в 4.1.9 (март 24)

- 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

КОД безопасности

Новое в 4.1.9 (VRF)



КОД безопасности

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
ECAP/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

КОД безопасности

Новое в 4.1.9 (VRF)

- 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	СОВ	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

КОД безопасности

Новое в 4.1.9 (автоматизация)

- 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 new
  - Импорт объектов IoC от вендора Security-Vision new
  - Создание правил фильтрации и трансляции new

Инструменты автоматизированной миграции:

- Миграция с Check Point
- Миграция с FortiGate
- Миграция с Cisco ASA
- Миграция в Palo Alto new
- Миграция с Континент 3
- Миграция данных с СД Континент 3 на СД Континент 4

Преимущество	Ценность
• API для работы с Континент 4 • Автоматизация процессов администрирования	Снижает нагрузку на команду администраторов

КОД безопасности

Новое в 4.1.9 (автоматизация)

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

Подробнее о возможности:

https://github.com/itseccode/c4_tools

КОД безопасности

Новое в 4.2 (3Q)

- 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

КОД безопасности

Режимы работы

UTM

Межсетевой экран

Межсетевой экран с набором функционала

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

NF2

Высокопроизводительный межсетевой экран

Межсетевой экран с использованием технологии префиксных деревьев

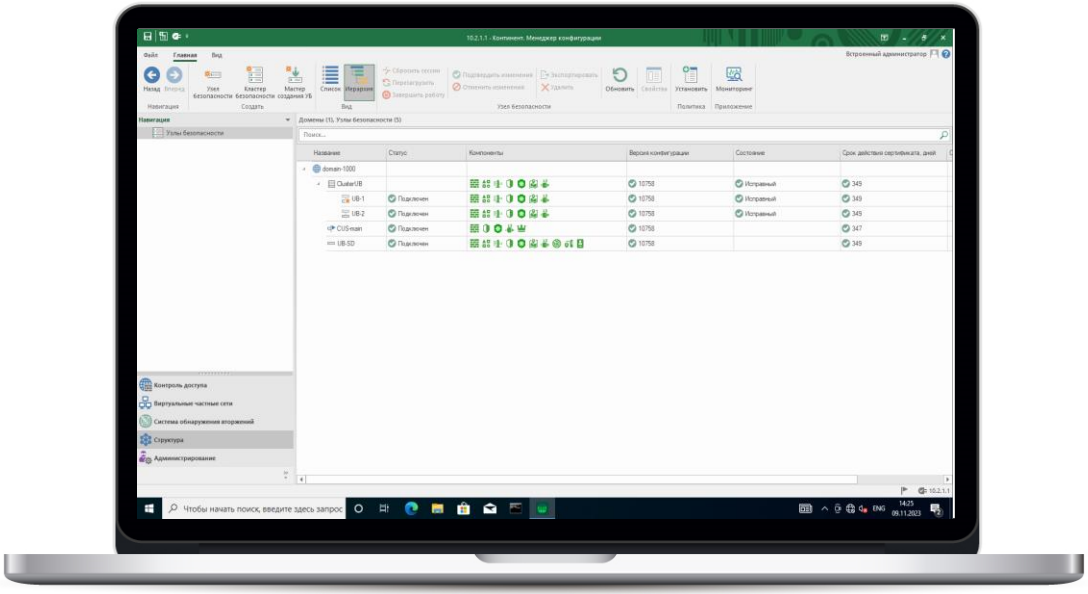
L2 IPS/IDS

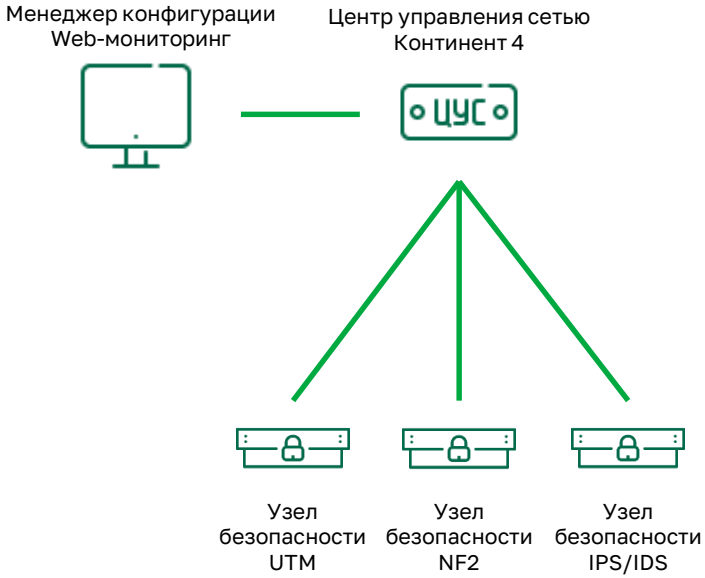
Детектор атак

Система обнаружения вторжений на канальном уровне (L2)

КОД безопасности

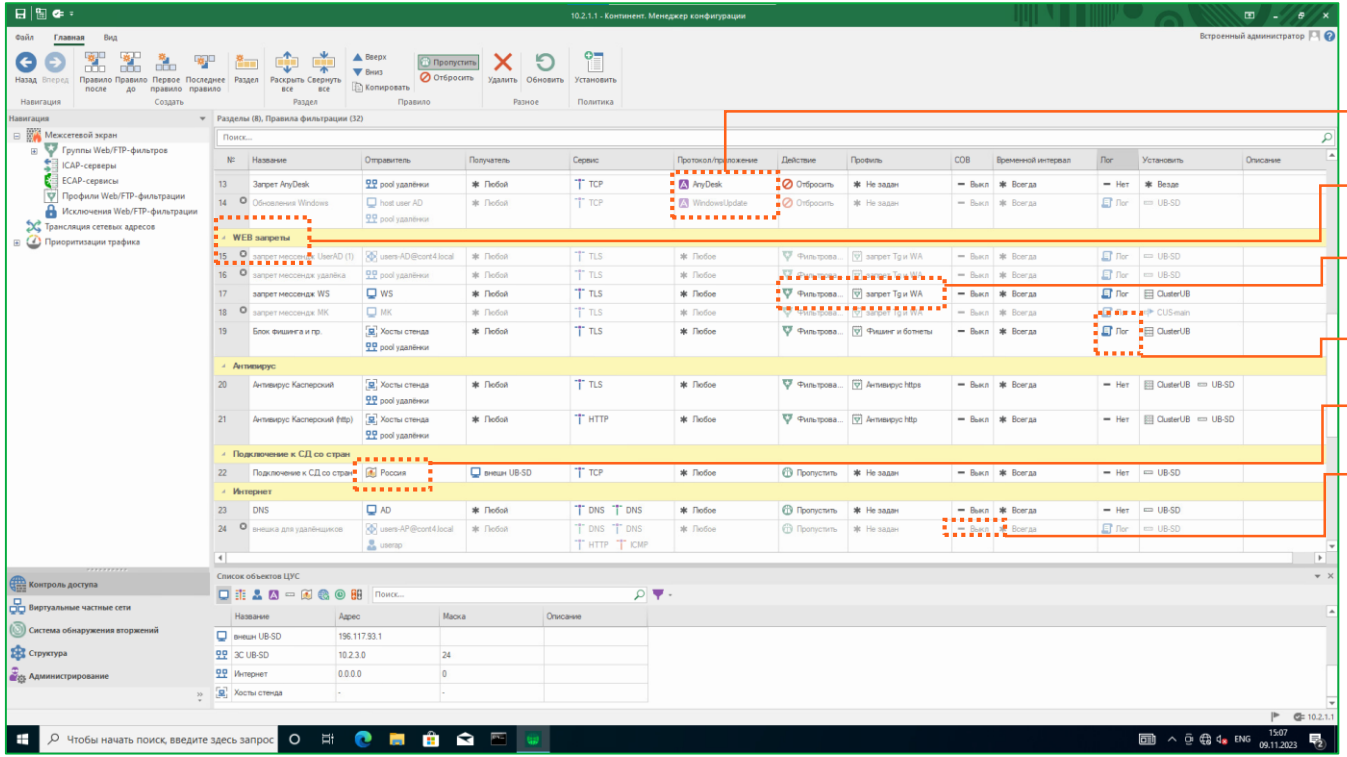
Архитектура устройства сети





КОД безопасности

Интерфейс правил фильтрации



Контроль приложений

Пользовательские разделы

URL-фильтрация

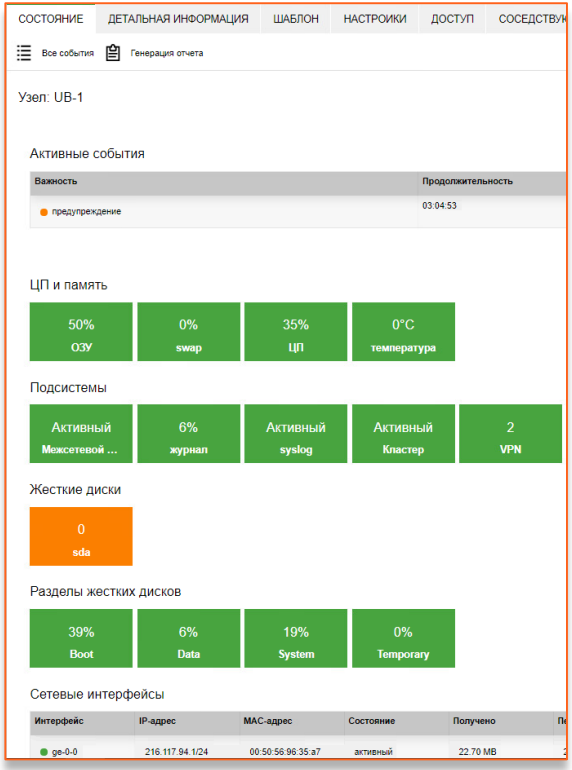
Логирование

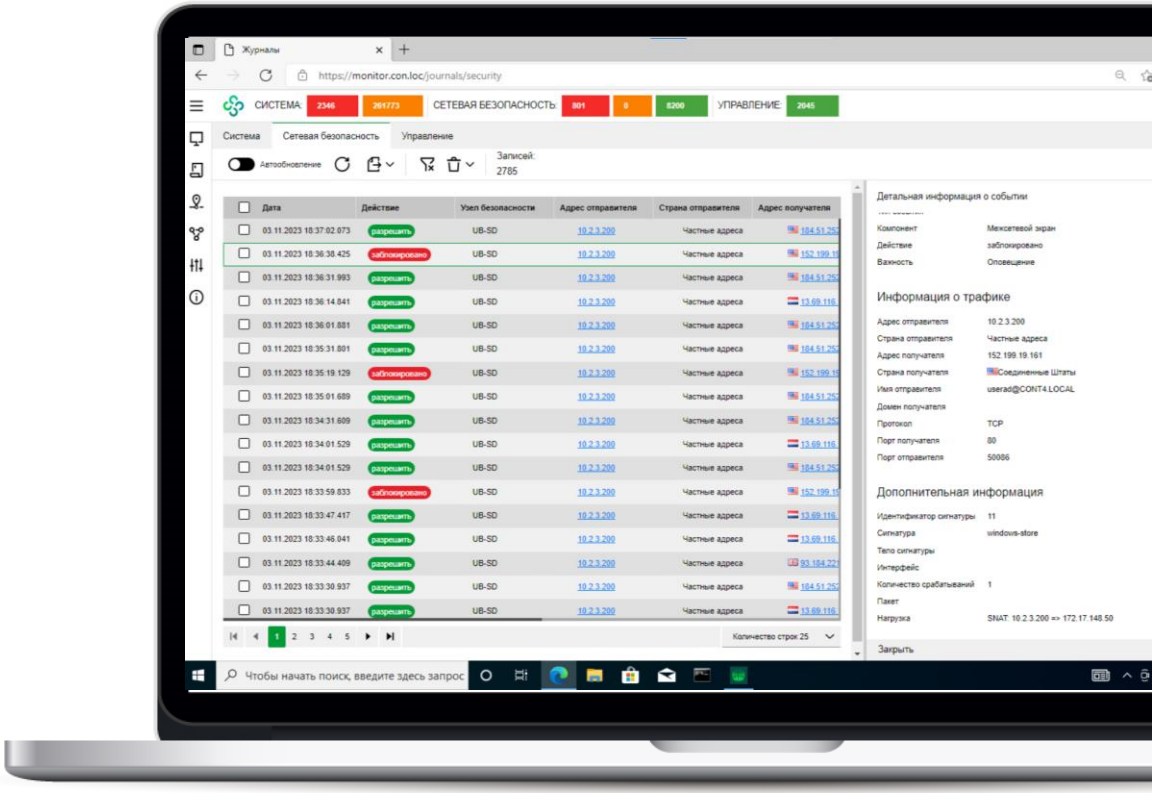
GeoIP. Фильтрация по странам

IPS/IDS L3

КОД безопасности

Мониторинг





КОД безопасности

Сетевые технологии

Динамическая маршрутизация
OSPF
BGP

Поддержка NAT
Входящий и исходящий

Multi-WAN
Failover
Балансировка трафика

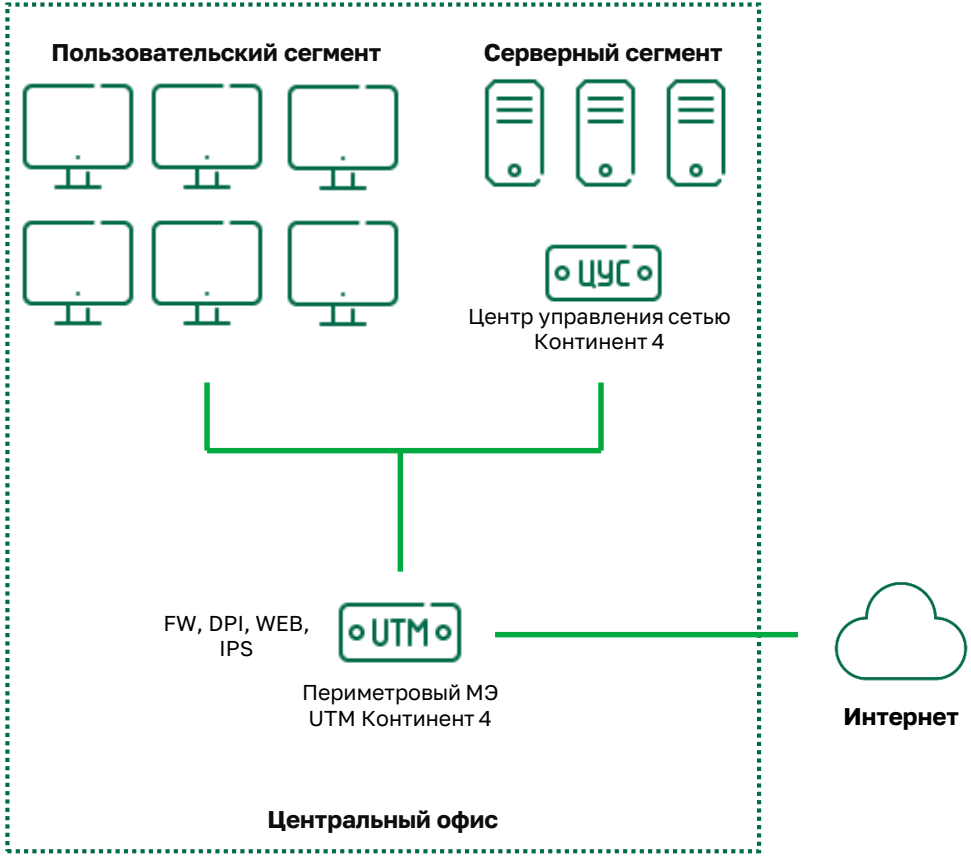
QoS

Кластеризация узлов безопасности
Active-Passive
без разрыва сессий

Поддержка VLAN

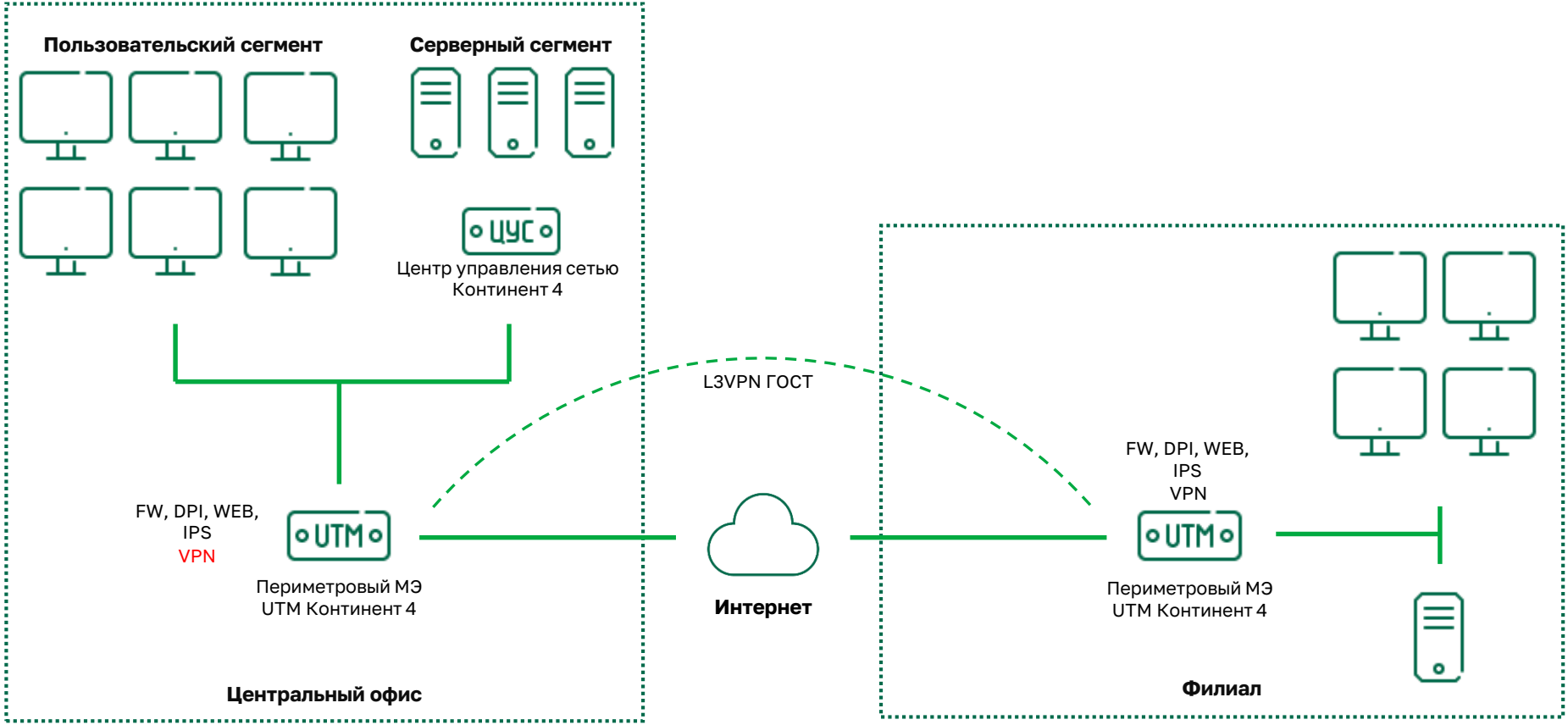
DHCP-сервер
DHCP-ретранслятор

Сценарии использования. Один офис

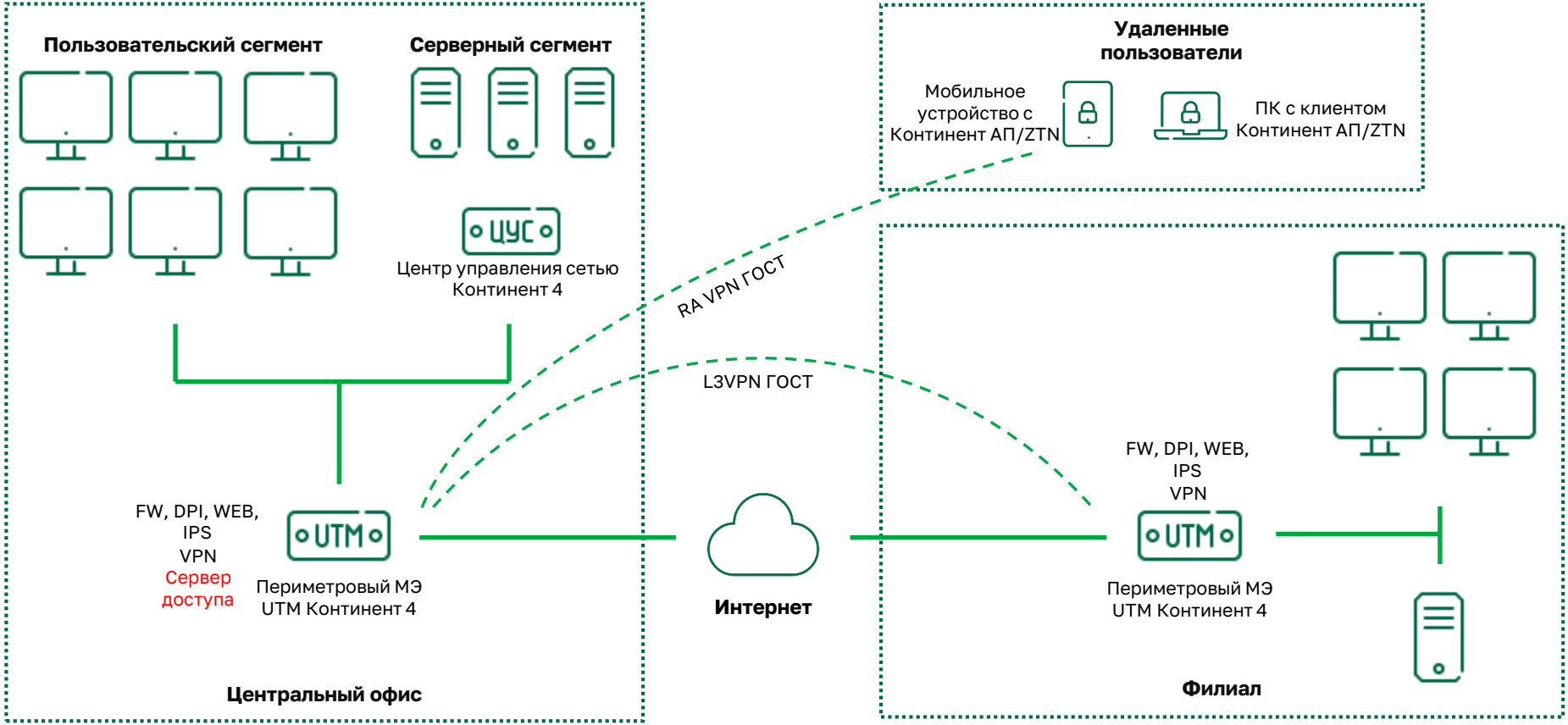


КОД безопасности

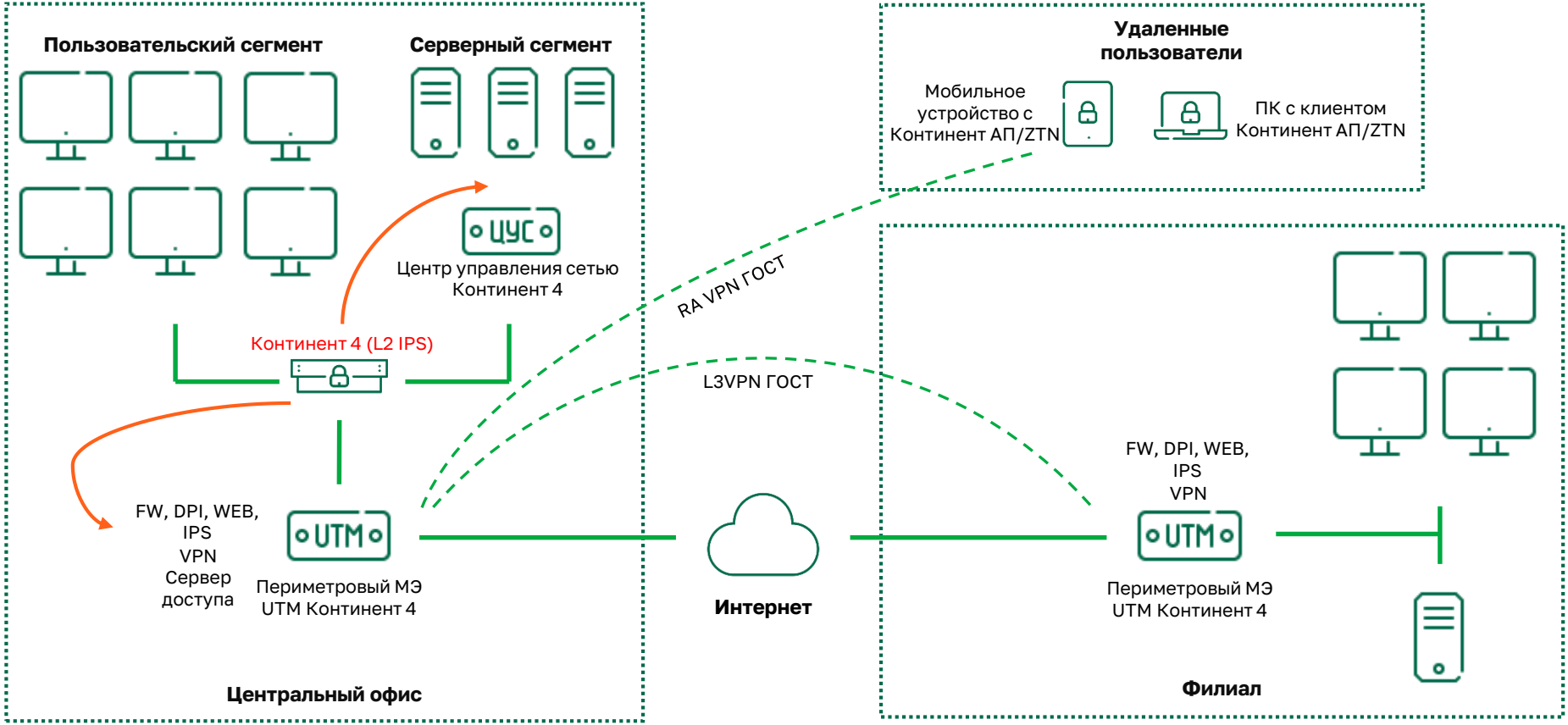
Сценарии использования. Филиалы



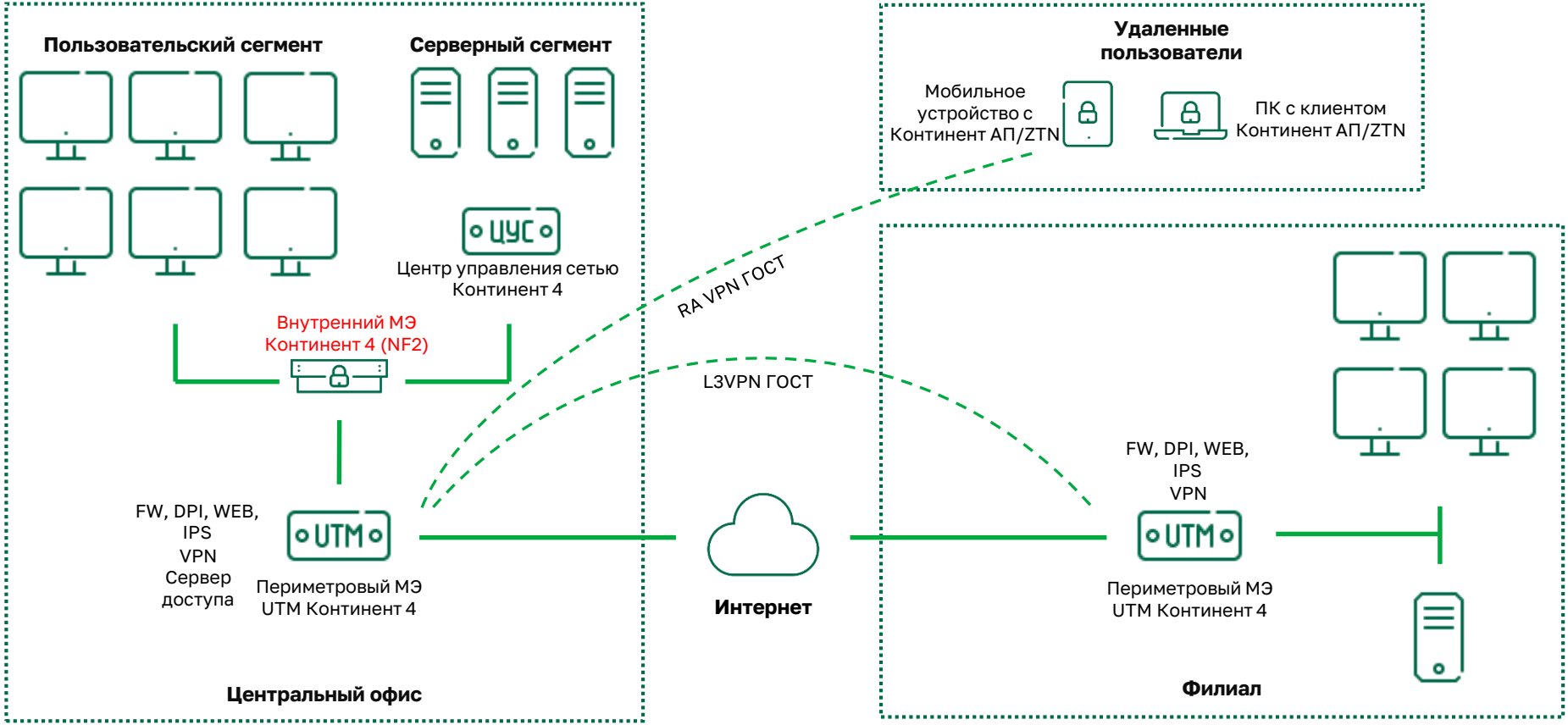
Сценарии использования. Удалёнка



Сценарии использования. СОВ уровня L2

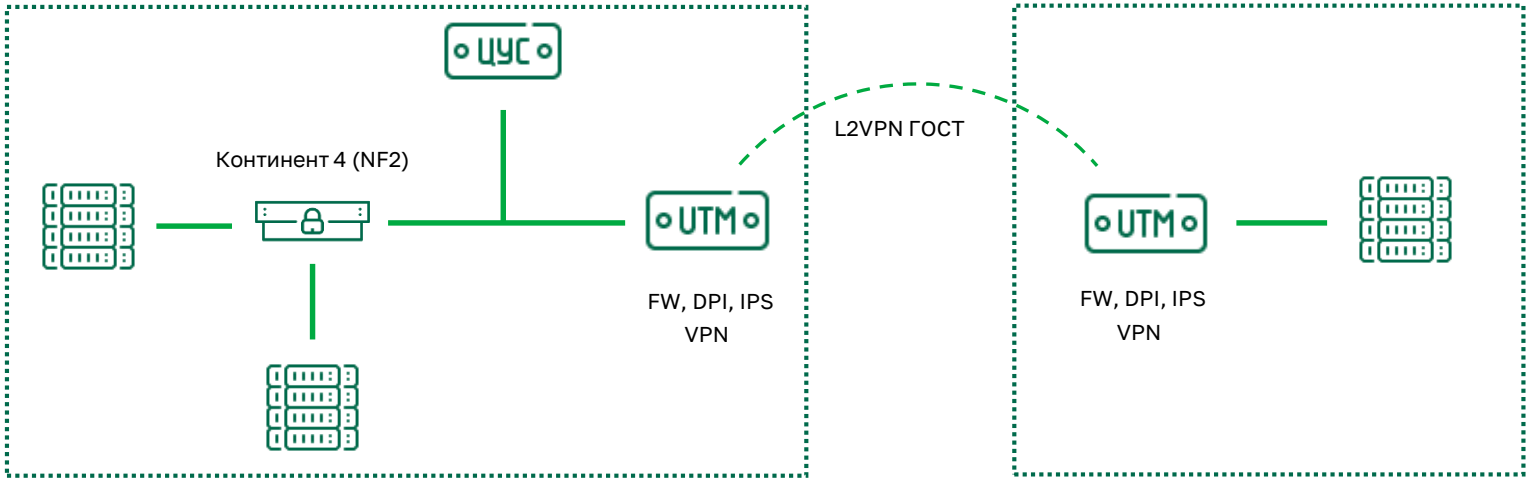


Сценарии использования. NF2



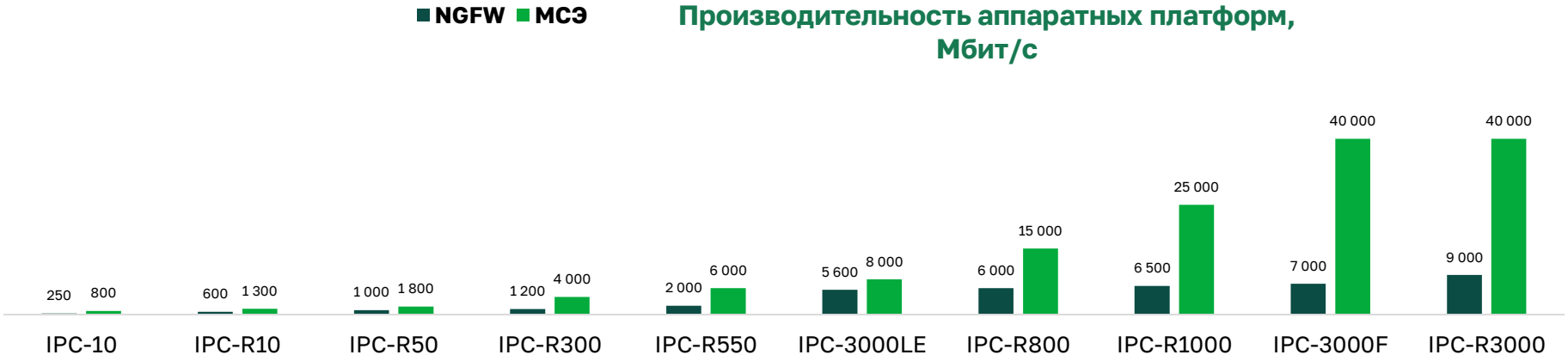
КОД безопасности

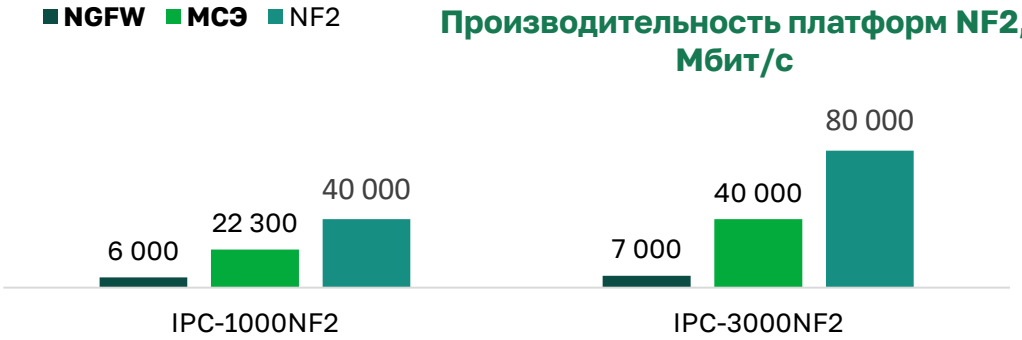
Сценарии использования. Защита ЦОД



КОД безопасности

Производительность





КОД безопасности

Российские платформы. Реестр ТОРП

Малые

IPC-R10
IPC-R50

Средние

IPC-R300
IPC-R550
IPC-R800

Старшие

IPC-R1000
IPC-R3000

КОД безопасности

Виртуальные платформы

Название	Число ядер	МЭ, Мбит/с	UTM, Мбит/с	L2 IPS, Мбит/с
SOHO	2	2 000	7 00	1 000
SMB	4	11 000	2 500	2 000
ENT	8	15 000	4 000	5 500

КОД безопасности

Варианты миграции

Прямой импорт политик CheckPoint, FortiGate

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

Миграция с Континент 3

КОД безопасности

Полезные ссылки

Большой онлайн по Континент 4

Импортозамещение NGFW

Телеграм канал Код на проводе

Телеграм чат по Континенту

КОД безопасности

Спасибо за внимание!

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