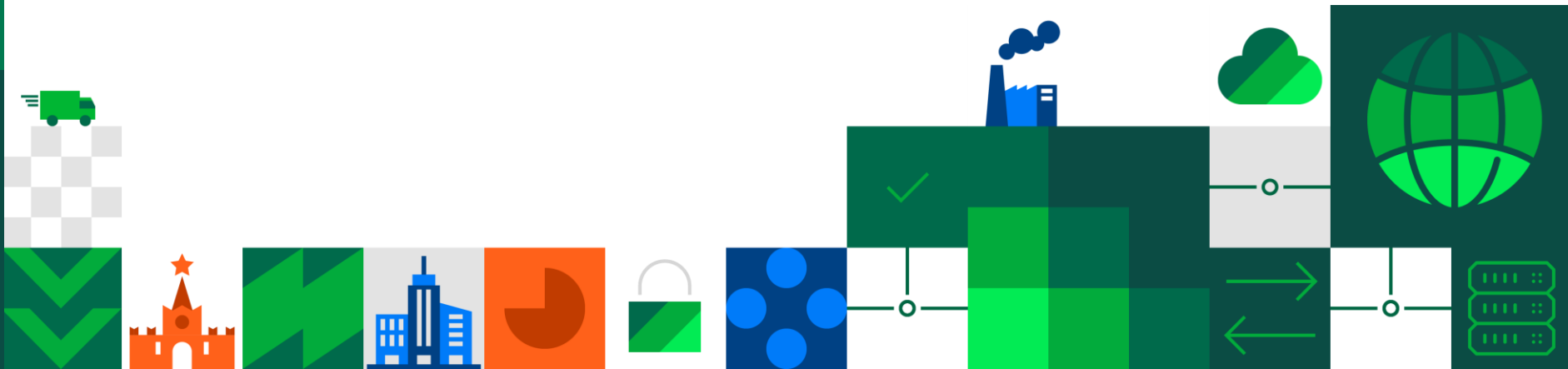


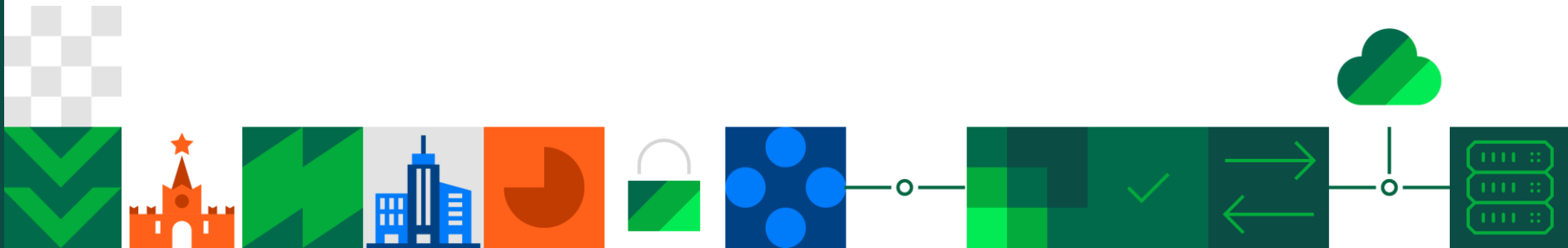


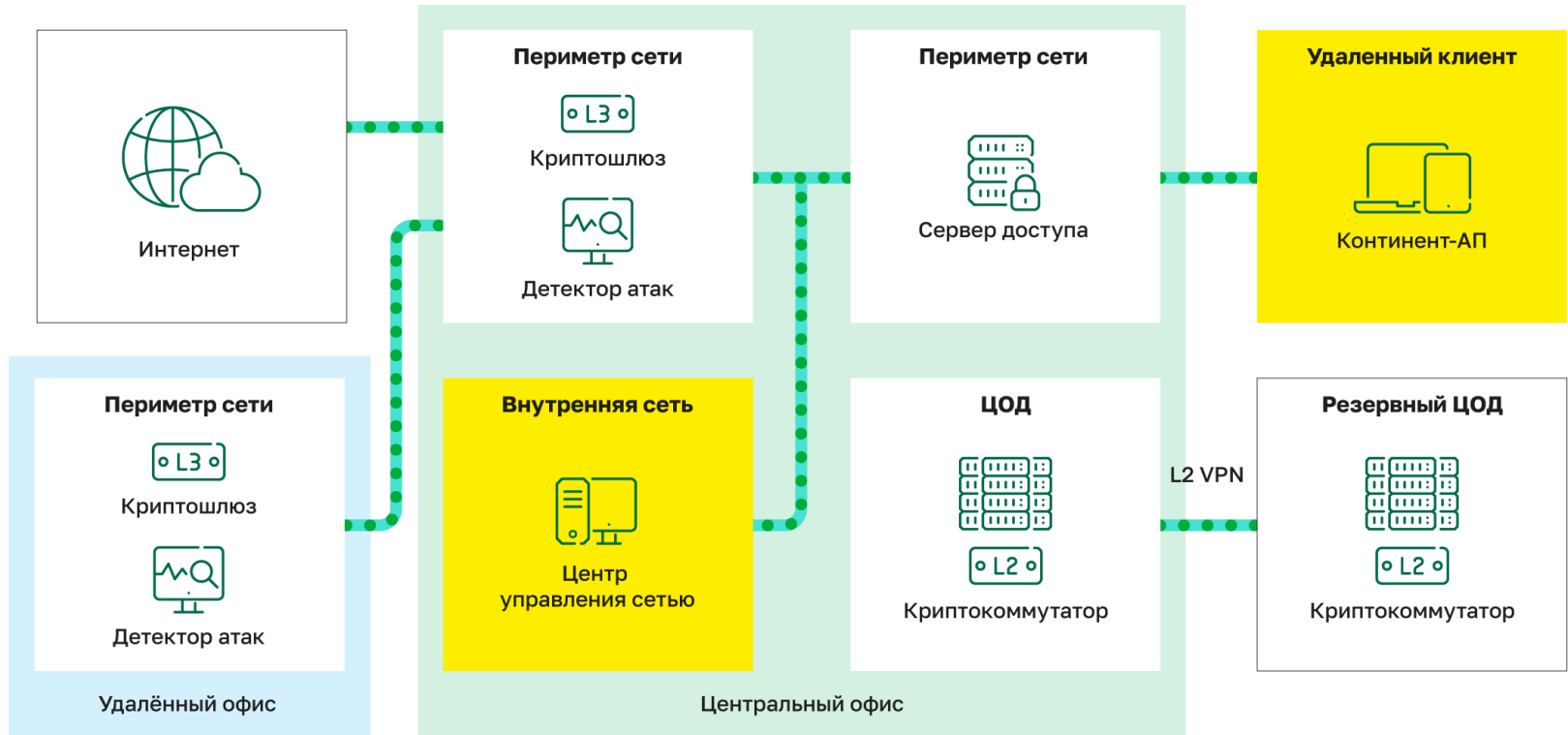
Континент 4 NGFW: Развитие продукта





АПКШ «Континент 3». Немного предыстории





1 Сущность = 1 Платформа



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

Планируется сертификация ФСТЭК России:

- 4-й класс защиты МЭ типа «Д»

Планируется сертификация ФСБ России:

- КС1/КС2/КС3 (версия 4.2)



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



АПКШ «Континент 3»



Континент 4 NGFW

РАЗНЫЕ

ОС

Логика работы

Команды разработки

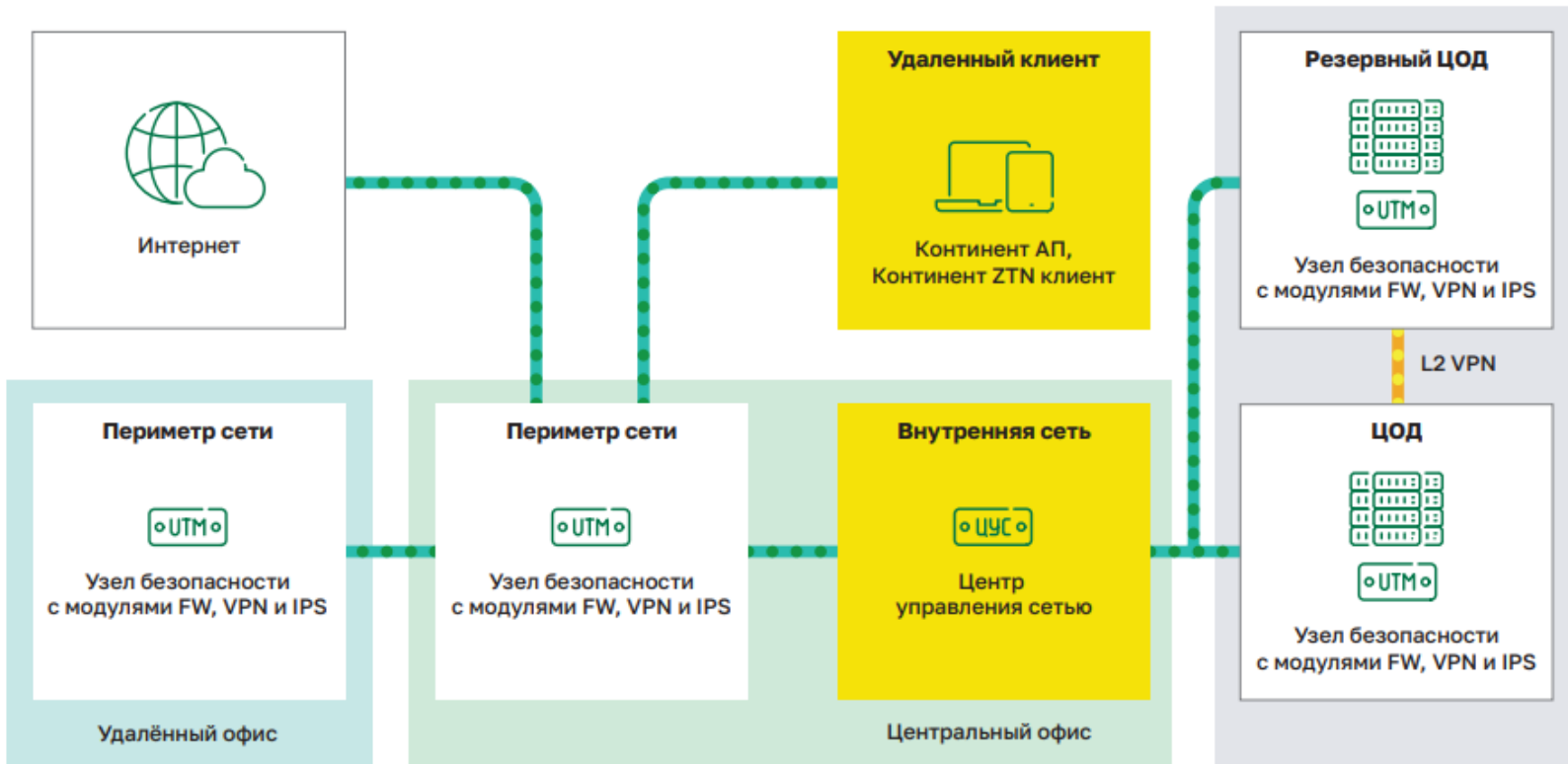
Концепции применения

ОБЩИЕ

Название

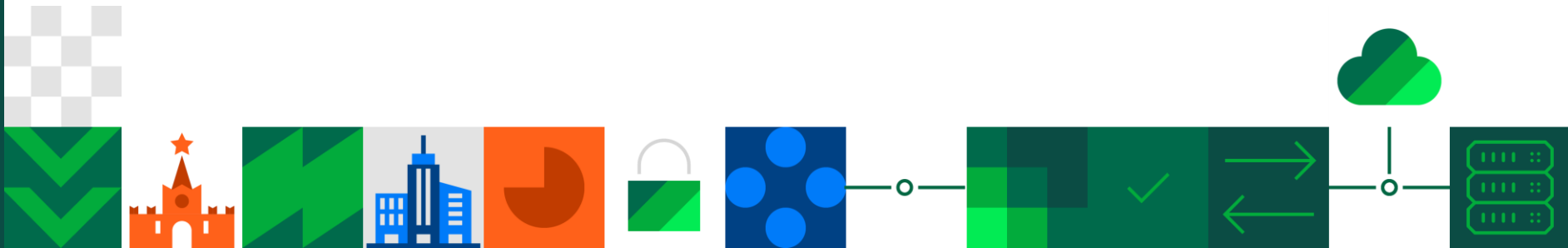
Платформы

Континент 4 NGFW. Новая архитектура

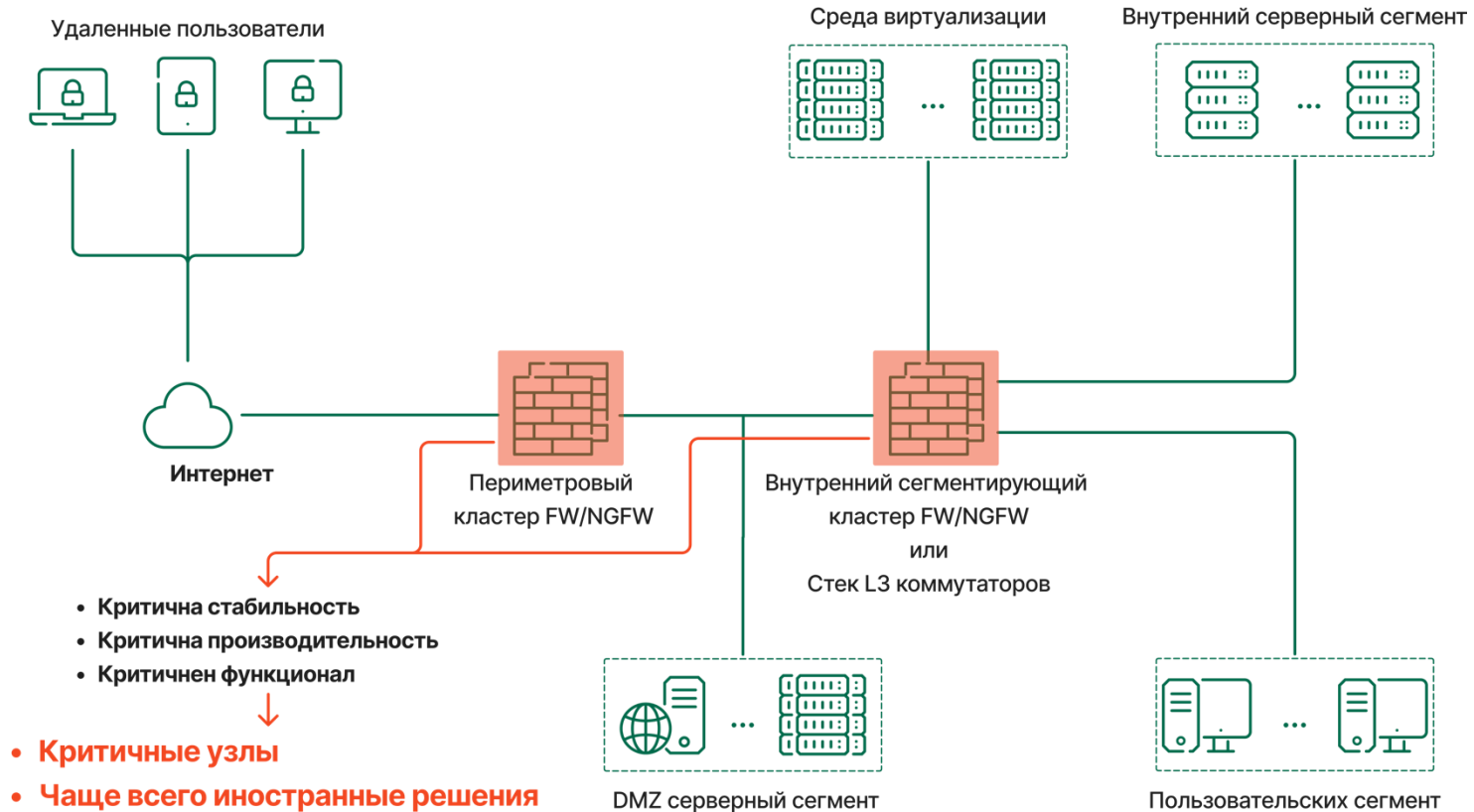




Защита физической сети

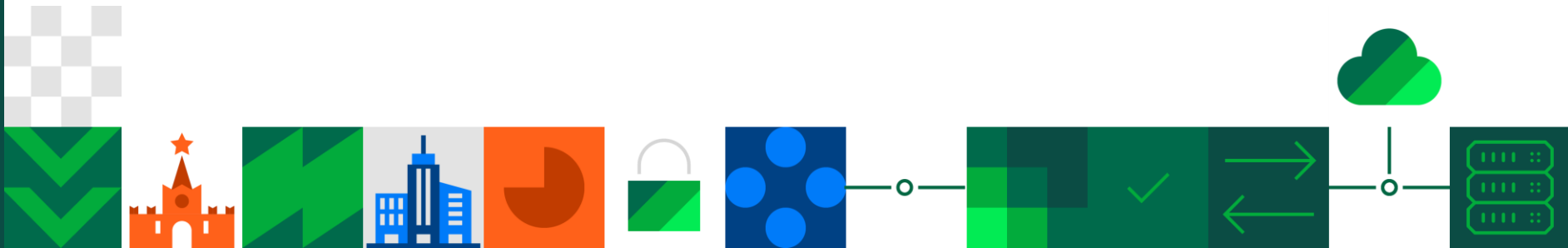


Как выглядит корпоративная сеть





Производительность



Базовые



IPC-R10
IPC-R50

Средние




IPC-R300
IPC-R550

Старшие



IPC-R800
IPC-R1000
IPC-R1000NF2
IPC-R3000

	SOHO	SMB	ENTERPRISE	UNLIMITED
Ядра:	2	4	8	XX
МСЭ:	4 Гбит/с	12 Гбит/с	16 Гбит/с	XX Гбит/с
ГГFW:	0,7 Гбит/с	2,5 Гбит/с	6 Гбит/с	XX Гбит/с
VPN:	1 Гбит/с	2 Гбит	5,5 Гбит/с	XX Гбит/с





МЭ: 100 Гбит/сек
Режим IPS: 15 Гбит/сек
Режим NGFW: 15 Гбит/сек

Континент 4.2

4 NGFW Континент 4

1 коммутатор-
балансировщик



Real-world mix
МЭ: 200 Гбит/сек
Режим IPS: 40 Гбит/сек
Режим NGFW: 25 Гбит/сек

Континент 4.3

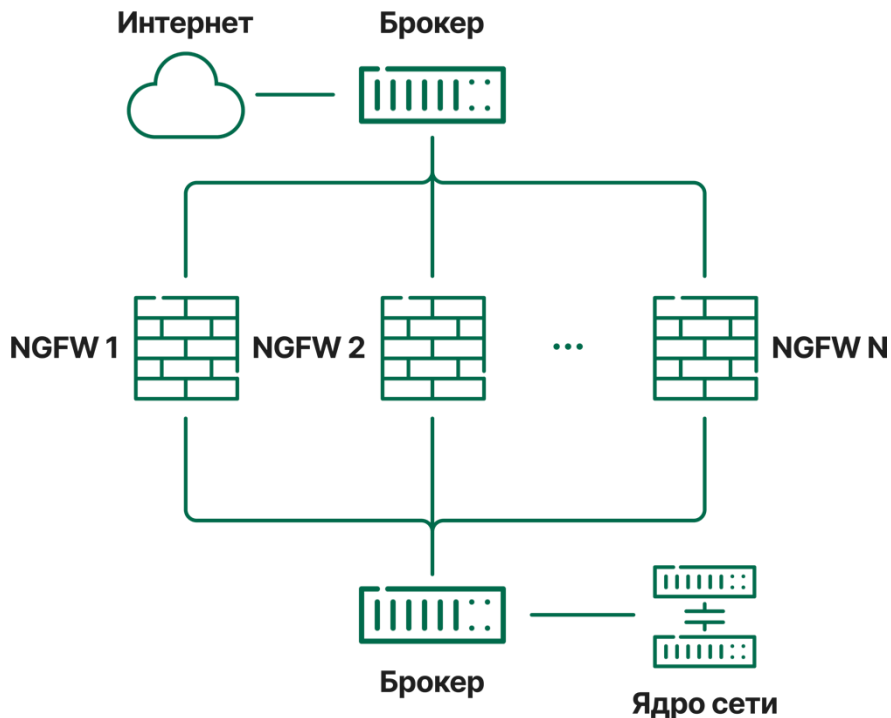
12 NGFW Континент 4

2 коммутатор-
балансировщика



Real-world mix
МЭ: 600 Гбит/сек
Режим IPS: 200 Гбит/сек
Режим NGFW: 100 Гбит/сек

Континент 4.3



Преимущества:

- Стабильность функционирования
- Линейное увеличение производительности
- Возможность использования менее производительных устройств
- Полное владение трафиков

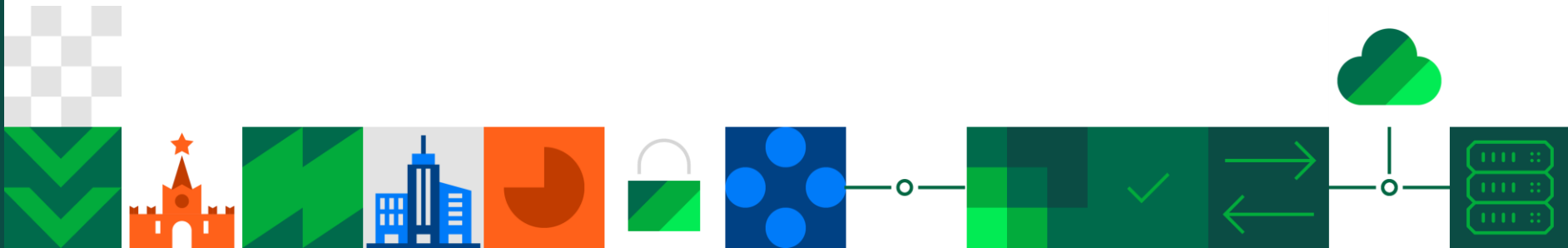
Тестирование:

- Достигли 400 Гбит/сек
- Подтвердили это в независимом тестировании VI.ZONE





Функционал



2018-2022

Q2 2022

4.0.3.6997
4.1.0.2825
4.1.0.3070
4.1.0.3175
4.1.5.2475

Первый

RN (26 пунктов):

RN (18 пунктов):

RN (10 пунктов):

RN (30 пунктов):

Релиз

- 24 нововведения

- 5 нововведений
- 13 оптимизаций

- 2 нововведения
- 4 оптимизации
- 4 исправления

- 22 нововведения
- 4 оптимизации
- 4 исправления

Q1 2023

Q1 2024

Q2 2024

4.1.7.1325
4.1.7.1395
4.1.7.1446
4.1.7.1525
4.1.9.2585

RN (102 пункта):

RN (6 пунктов):

RN (4 пункта):

RN (16 пунктов):

RN (16 пунктов):

- 77 нововведений
- 20 оптимизации
- 5 исправлений

- 3 нововведения
- 3 исправления

- 1 оптимизация
- 3 исправления

- 2 нововведения
- 3 оптимизации
- 11 исправлений

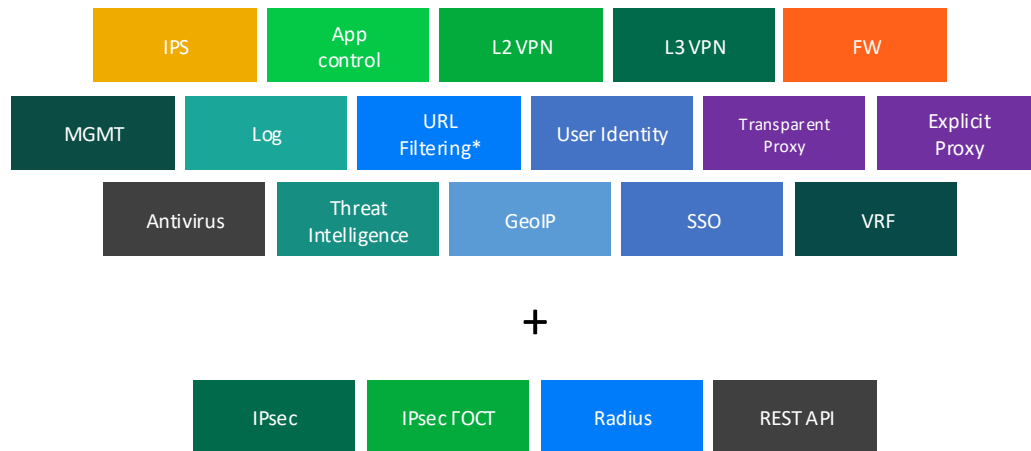
- 15 нововведений
- 1 оптимизация

Q4 2024

4.2.0.XXXX

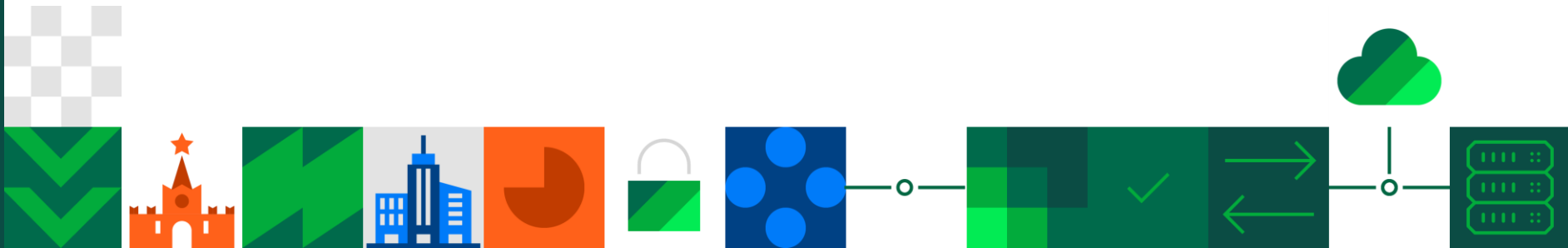
Планируемые функции:

- IPsec + IPsec ГОСТ
- Поддержка REST API
- Поддержка Radius
- Поддержка динамической маршрутизации внутри VPN
- Поддержка нескольких доменов
- МК под Linux





Стабильность



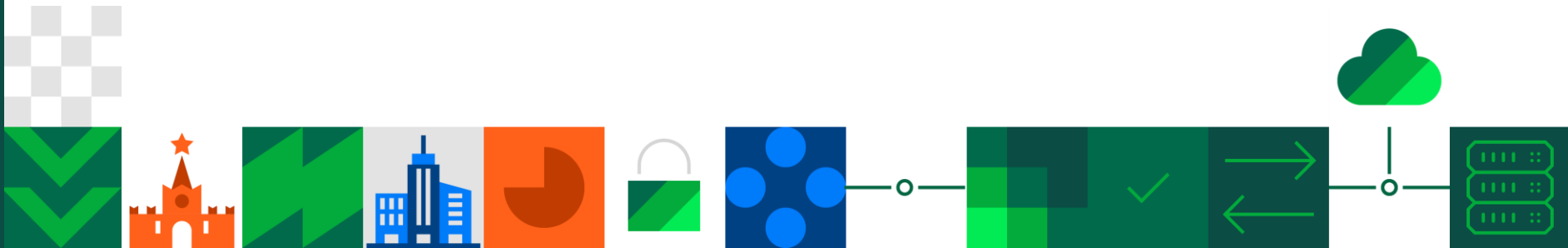
	Check Point R81.20 ↗	Ideco NGFW v16 ↗	ViPNet Coordinator HW5 5.3 ↗	Континент 4.1.7 ↗
EMIX, Гбит/с	9.50	5	1	4.90
Результаты теста вендора				
Результаты «Инфосистемы Джет»	8.50	0.75	1.22	2.50
Платформа	7000 Plus	EX	HW5000	IPC-R1000
Комментарий	<p>< значения других параметров при тестировании EMIX Throughput: PPS 1Mpps, CPS 8,47k, CC 4,98k</p>	<p>Значения других параметров при тестировании EMIX Throughput: PPS 0,09Mpps, CPS 0,85k, CC 0,55k Основное влияние на производительность оказывал модуль Контроль приложений. При отключении данного модуля были получены следующие результаты: EMIX Throughput 1,7Гбит/с, PPS 0,2Mpps, CPS 2k, CC 1,2k</p>	<p>Значения других параметров при тестировании EMIX Throughput: PPS 0,14Mpps, CPS 1,2k, CC 1,12k</p>	<p>Значения других параметров при тестировании EMIX Throughput: UDP PPS 0,35Mpps, HTTP CPS 2,5k, HTTP CC 1,64k</p>

Нагрузочное тестирование Заказчика





Дополнительные инструменты



itsecode / c4_tools Public

<> Code Issues Pull requests Actions Projects Security Insights

main 1 Branch 0 Tags

Go to file Code

File	Last commit	Commit date
itsecode Update patch_notes.md	16a077d	2 months ago
aserv_c4_importer	Update README.md	4 months ago
c4_backup_tool	Update README.md	4 months ago
c4_config_exporter	Update README.md	4 months ago
c4_config_transfer	Update README.md	4 months ago
c4_ioc_importer_k	Update README.md	4 months ago
c4_ioc_importer_rv	Update README.md	4 months ago
c4_ioc_importer_sv	Update README.md	4 months ago
c4_lib	Add files via upload	4 months ago
c4_policy_install	Update README.md	4 months ago
c4_rules_maker	Update README.md	4 months ago
c4_vlan_maker	Update README.md	4 months ago
c4_xls_rules_maker	Update README.md	4 months ago
convert_c3_to_c4	Update README.md	4 months ago
convert_cisco_to_c4	Update convert_cisco_to_c4.py	2 months ago
convert_cp_json_to_c4	Update README.md	4 months ago
convert_cp_to_c4	Update README.md	4 months ago
convert_forti_to_c4	Update README.md	4 months ago
convert_ug_to_c4	Update README.md	4 months ago
README.md	Update README.md	4 months ago
patch_notes.md	Update patch_notes.md	2 months ago

Экспорт конфигурации всех или выбранных Континент 4 под управлением отдельного ЦУС через API

Миграции со сторонних NGFW (UserGate, FortiGate, Check Point, Palo Alto, Cisco)

Импорт индикаторов компрометации (IoC) в Континент 4

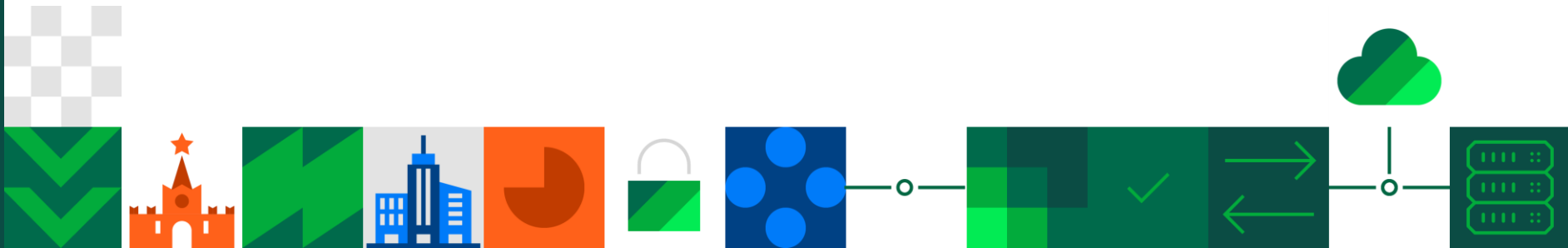
Создание политик безопасности

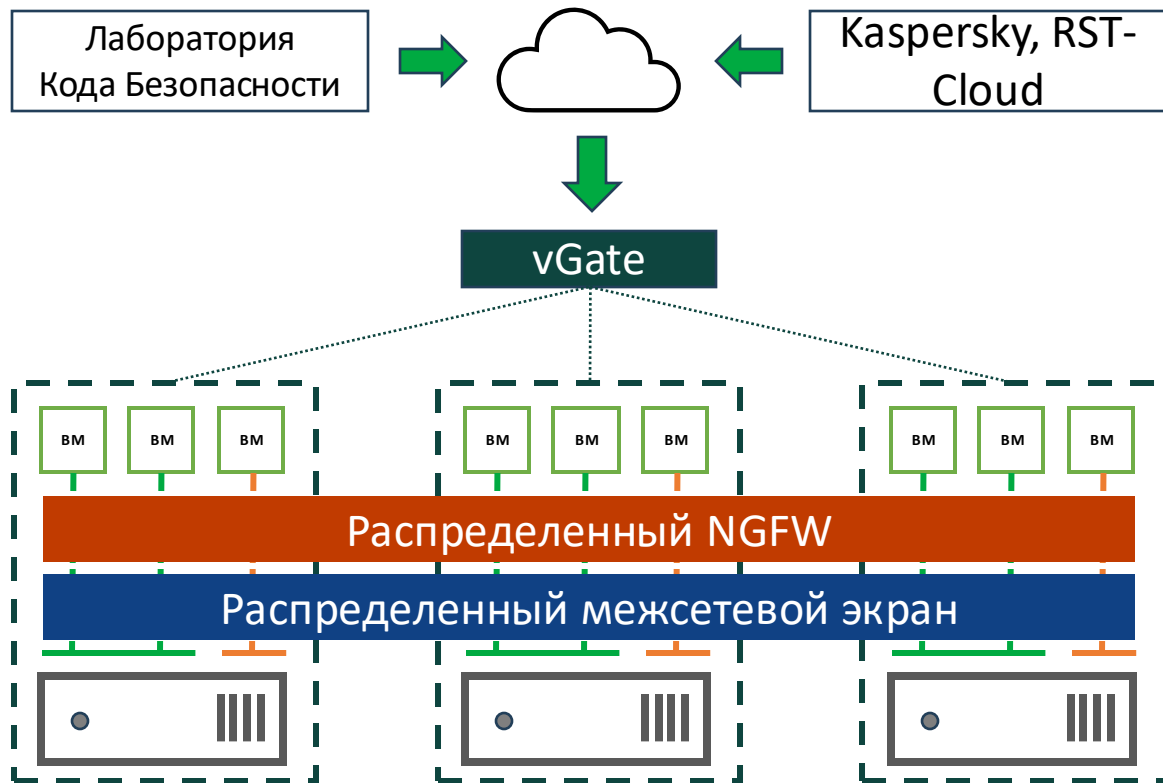






Защита сети виртуализации





Для каждой виртуальной машины:

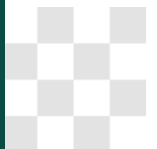
- Межсетевой экран
- Контроль приложений
- Анализ индикаторов компрометации
- Обнаружение сетевых вторжений

Политики на основе разных критериев

- Атрибуты VM
- Сетевые атрибуты



Заключение



«Код Безопасности» Инкома поставили NGFW «Континент 4» в авиакомпанию

03 сентября 2024

После ухода иностранных вендоров NGFW с российского рынка заказчики столкнулись с тремя проблемами.

[Читать полностью](#)

«Код Безопасности» и ГК Softline провели миграцию с Check Point на предприятии, которое является субъектом КИИ

08 июля 2024

Команда «Код Безопасности» и ГК Softline провела модернизацию сетевой инфраструктуры для предприятия из отрасли энергетической промышленности. Перед специалистами ГК Softline стояла задача импортозамещения межсетевого экрана (МСЭ) в следующих сценариях.

«Код Безопасности» и «Траст Технолоджиз» провели комплексную модернизацию системы сетевой безопасности в кредитно-финансовой организации

02 апреля 2024

Команда «Код Безопасности» и «Траст Технолоджиз» провели модернизацию сетевой инфраструктуры в ПАО УКБ «Новобанк».

[Читать полностью](#)

«Код Безопасности» и «ТС Солюшен» осуществили миграцию с Check Point на Континент 4 на предприятии в отрасли машиностроения

24 января 2024

Перед специалистами «ТС Солюшен» стояла задача импортозамещения межсетевого экрана (МСЭ) на периметре организации. Ранее Заказчик использовал МСЭ Check Point.

[Читать полностью](#)

Сколько NGFW сейчас на
рынке? А сколько
разрабатывают?

>30!!!

Как в таком многообразии
NGFW понять где правда, а где
только маркетинг?

Мы за независимые тестирования

Инфосистемы Джет



Функциональное
тестирование

ТС Солюшен



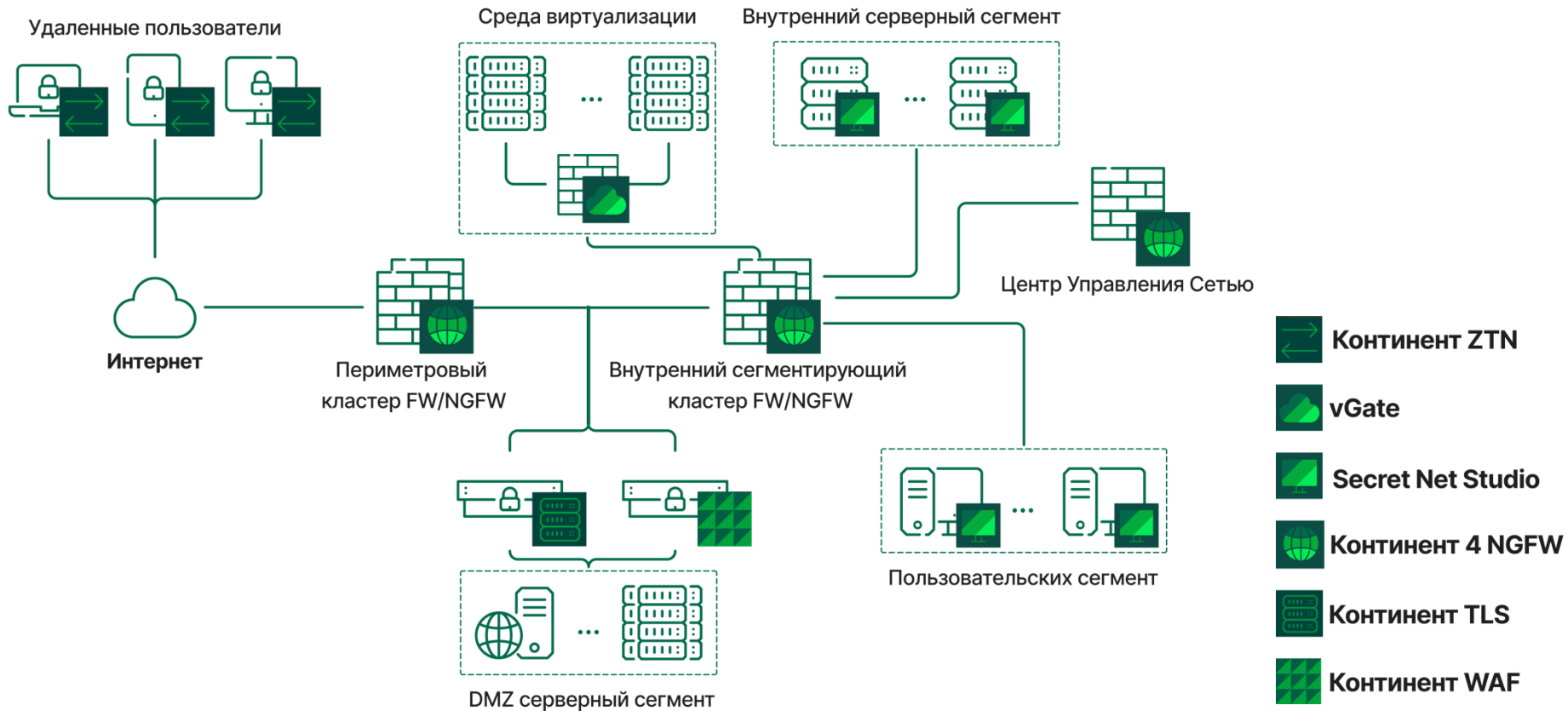
Тестирование механизмов
безопасности

VI.ZONE



Тестирование
производительности

Схема сети с продуктами Кода Безопасности





Спасибо за внимание!

info@securitycode.ru

www.securitycode.ru

