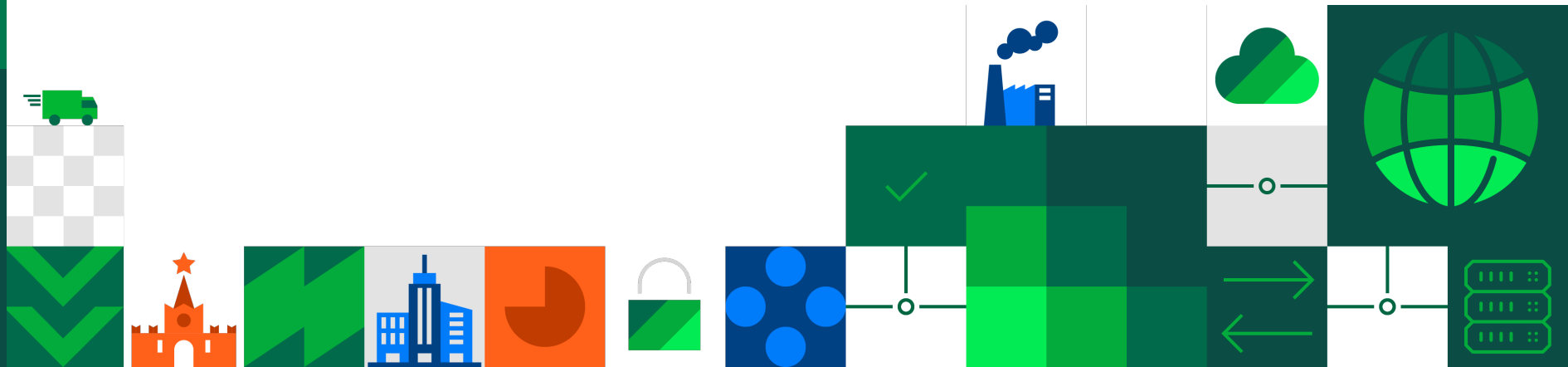
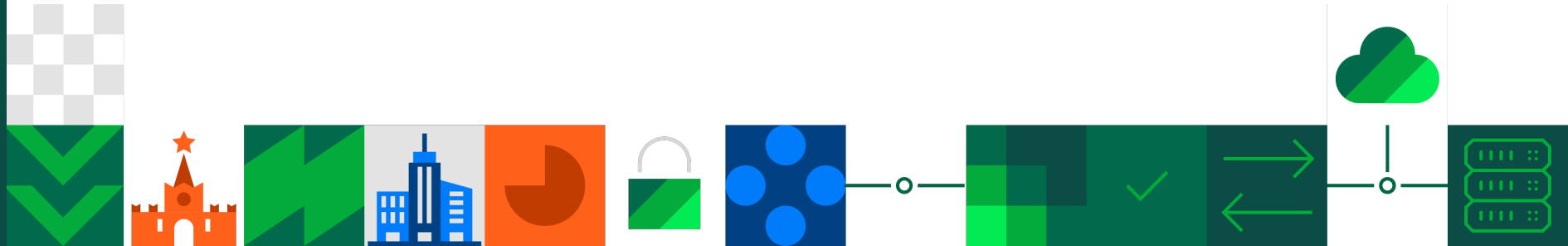
КОД безопасности

Практика миграции с иностранных NGFW



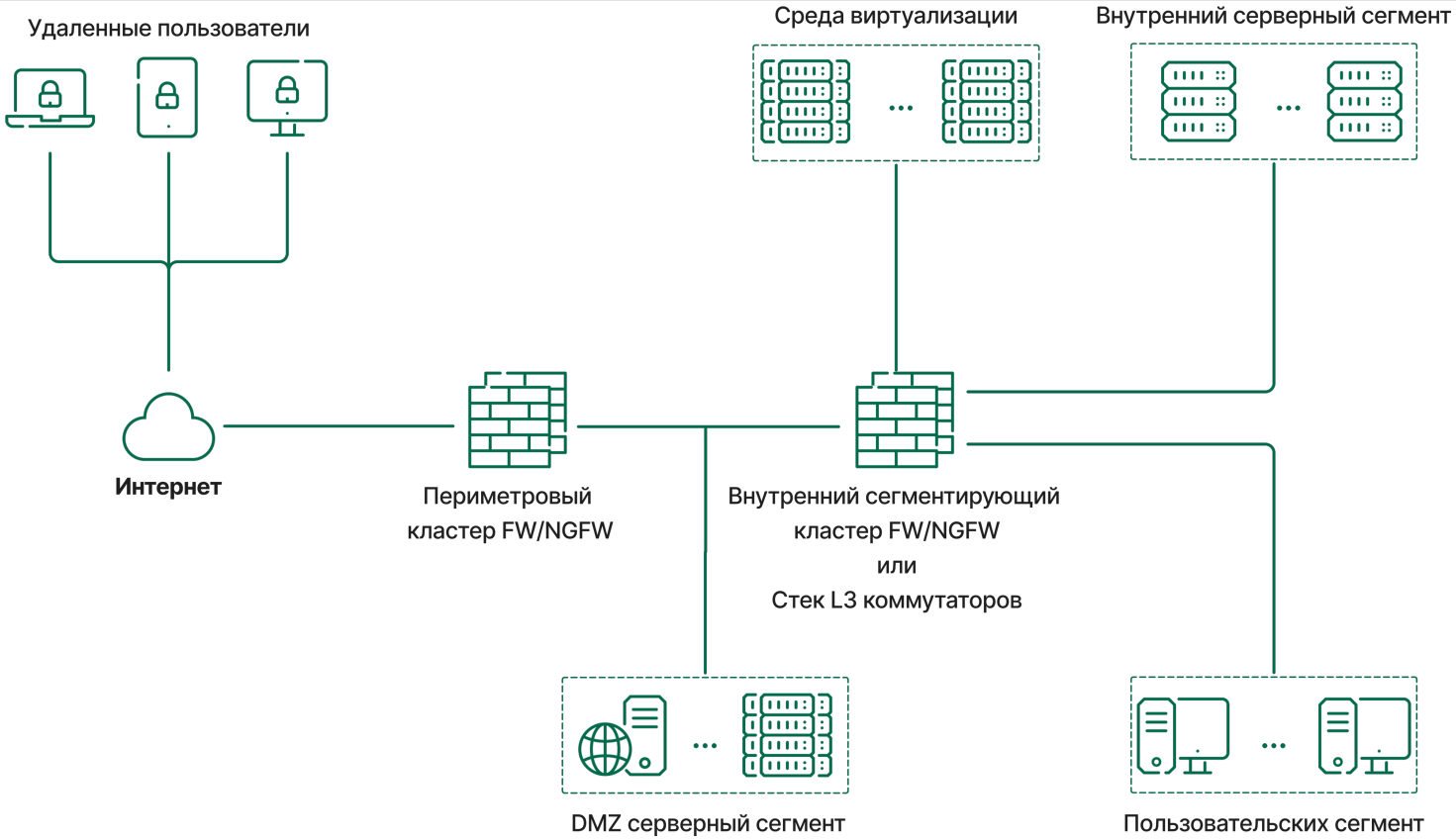
КОД безопасности

Защита физической сети



КОД безопасности

Как выглядит корпоративная сеть



КОД безопасности

Сценарии использования NGFW

Сценарии использования

- Защита периметра организации
-
- Защита георасределенной сети
-
- Защита технологических сетей

Что требуется:

- Механизмы безопасности (IDS/IPS, контроль приложений, антивирус и др.)
- VPN (Site-to-Site VPN, Remote Access VPN)
- Централизованное управление и мониторинг
- Поддержка фильтрации трафика по технологическим протоколам
- Сертификация ФСТЭК

В этих сегментах импортозамещение NGFW проходит хорошо

КОД безопасности

Сценарии использования NGFW

Сценарии использования

- Защита внутренней сети организации
- Защита ЦОД

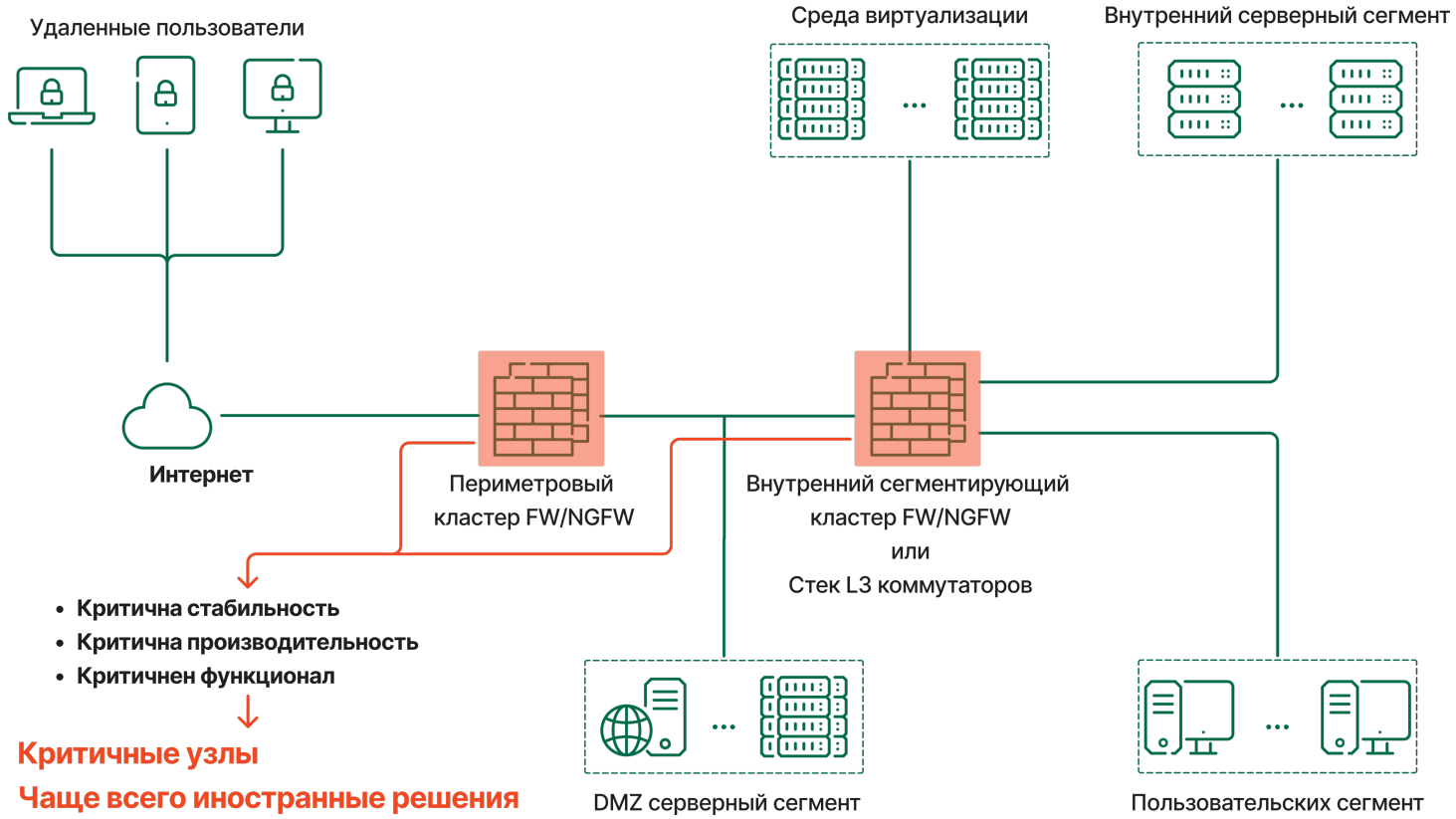
Общие сложности на рынке:

- Слабая производительность NGFW (иногда надо сегментировать десятки гигабит для внутренней сети и сотни гигабит для ЦОД)
- Слабая стабильность функционирования отечественных NGFW
- Недостаточный сетевой функционал
- Дорого ставить мощный NGFW в ядро, если трафика много

Заказчики боятся ставить отечественные NGFW в ядро сети, так как от NGFW будет зависеть вся работоспособность сети

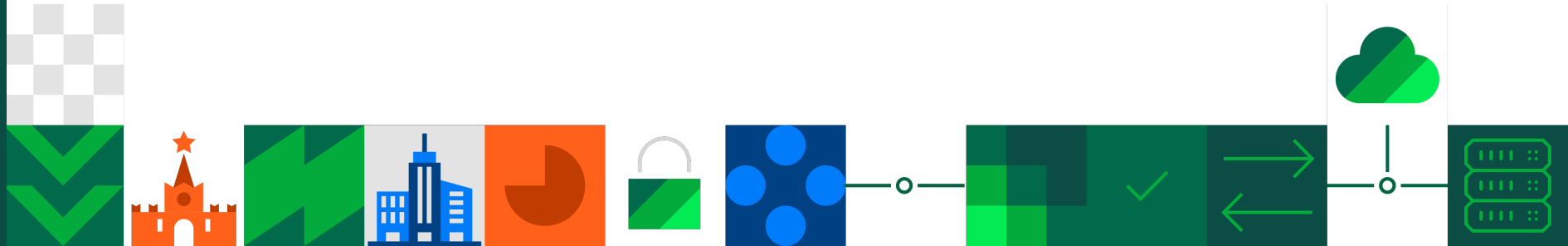
КОД безопасности

Как выглядит корпоративная сеть



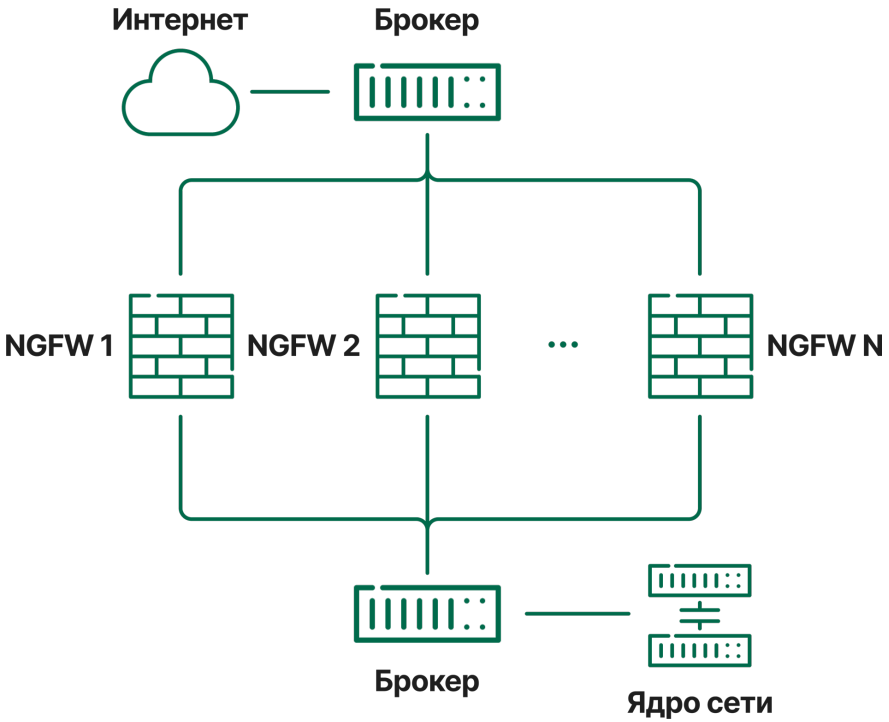
КОД безопасности

Производительность



КОД безопасности

Масштабируемость через брокер



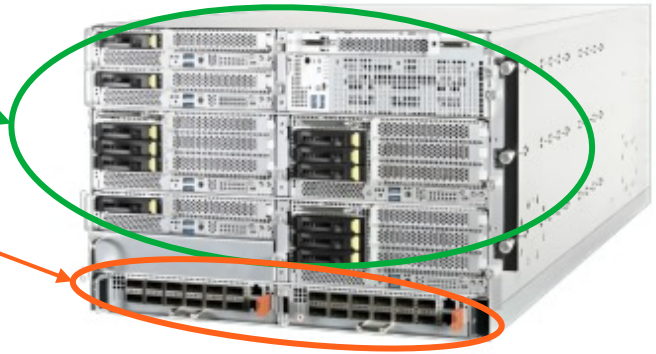
Преимущества:

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

Тестирование:

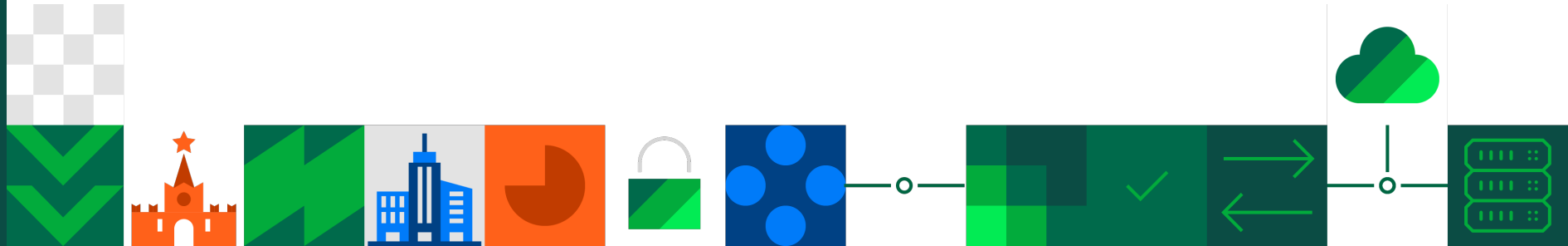
- Достигли 400 Гбит/сек
- Подтвердили это в независимом тестировании BI.ZONE

КОД безопасности

Платформа	Производительность	Версия
	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

КОД безопасности

Функционал



КОД безопасности

Развитие продукта

2018-2022

4.0.3.6997	4.1.0.2825	4.1.0.3070	4.1.0.3175	4.1.5.2475
Первый Релиз	RN (26 пунктов): • 24 нововведения	RN (18 пунктов): • 5 нововведений • 13 оптимизаций	RN (10 пунктов): • 2 нововведения • 4 оптимизации • 4 исправления	RN (30 пунктов): • 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): • 77 нововведений • 20 оптимизации • 5 исправлений	RN (6 пунктов): • 3 нововведения • 3 исправления	RN (4 пункта): • 1 оптимизация • 3 исправления	RN (16 пунктов): • 2 нововведения • 3 оптимизации • 11 исправлений	RN (16 пунктов): • 15 нововведений • 1 оптимизация

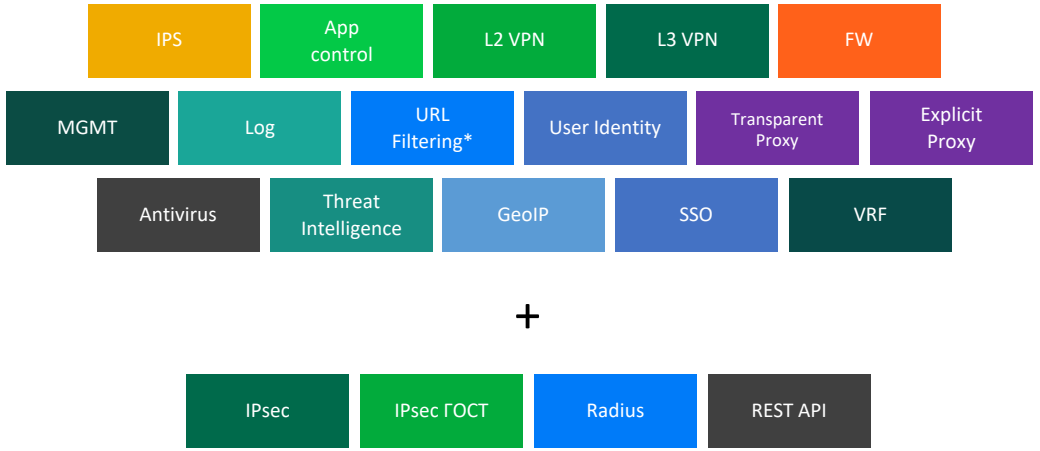
Развитие продукта. Ветка 4.2.X

Q4 2024

4.2.0.XXXX

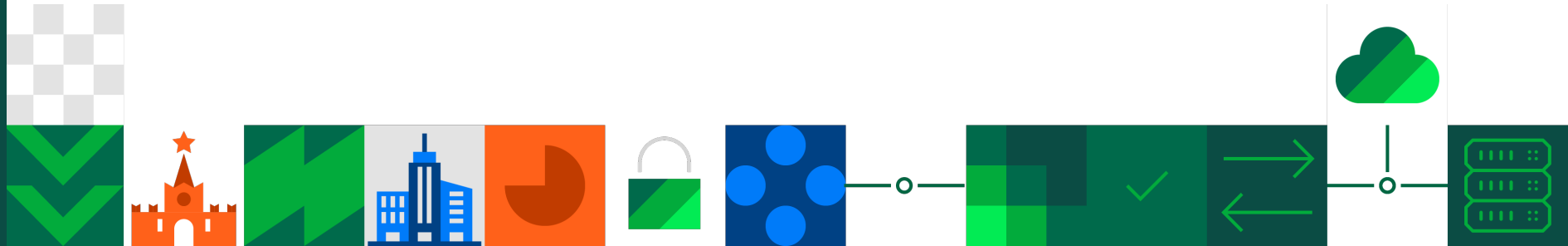
Планируемые функции:

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



КОД безопасности

Стабильность



КОД безопасности

Нагрузочное тестирование Партнера

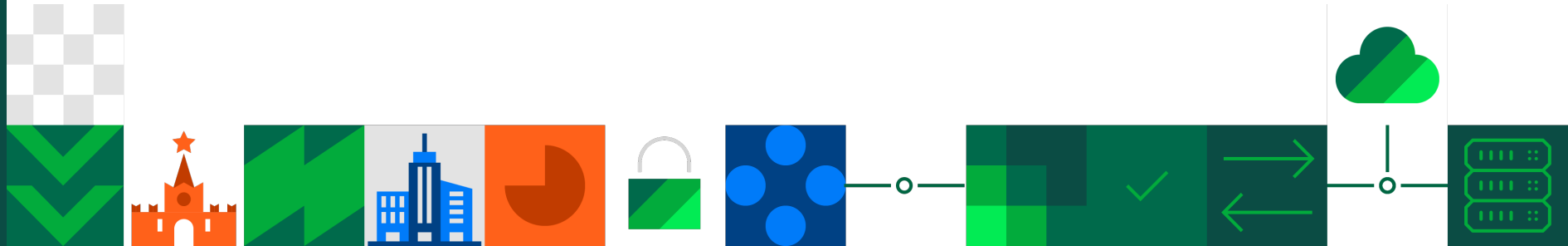
	Check Point R81.20 ↗	Ideco NGFW v16 ↗	ViPNet Coordinator HW5 5.3 ↗	Континент 4.1.7 ↗
EMIX, Гбит/с	9.50	5	1	4.90
Результаты теста вендора				
Результаты «Инфосистемы Джет»	8.50	0.75	1.22	2.50
Платформа	7000 Plus	EX	HW5000	IPC-R1000
Комментарий	...ения других параметров при тестировании EMIX Throughput: PPS 1Mpps, CPS 8,47k, CC 4,98k	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	Значения других параметров при тестировании EMIX Throughput: PPS 0,14Mpps, CPS 1,2k, CC 1,12k	Значения других параметров при тестировании EMIX Throughput: UDP PPS 0,35Mpps, HTTP CPS 2,5k, HTTP CC 1,64k

КОД безопасности

Нагрузочное тестирование Заказчика

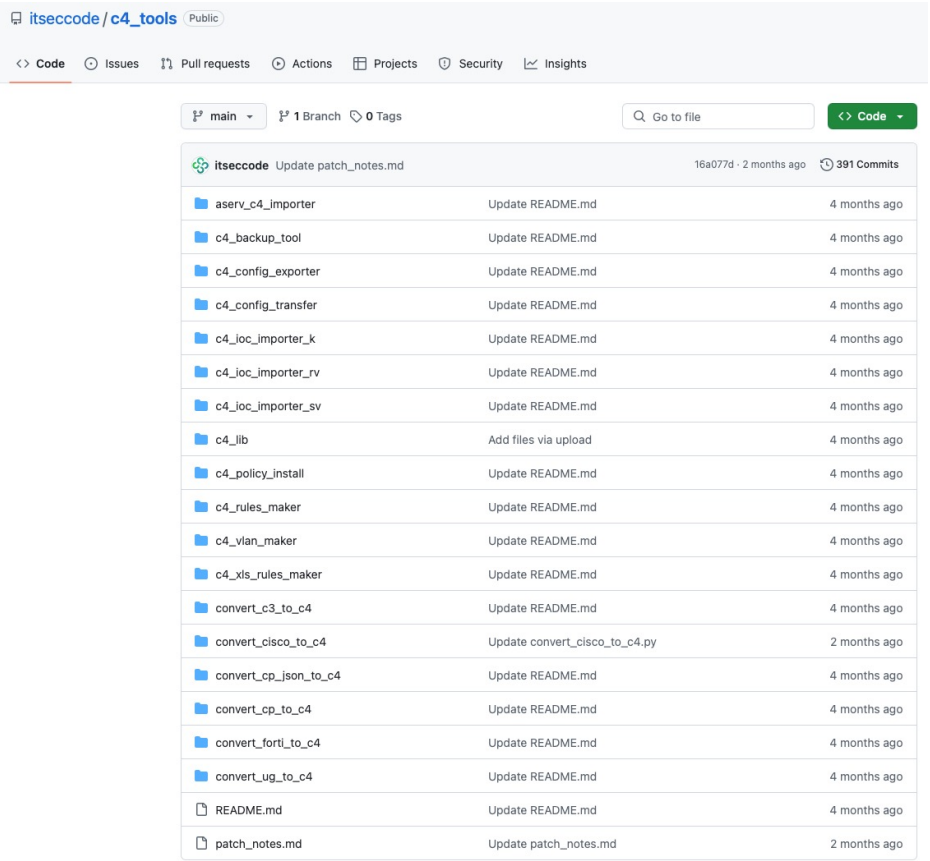
КОД безопасности

Инструменты миграции



КОД безопасности

Утилиты c4_tools на GitHub



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

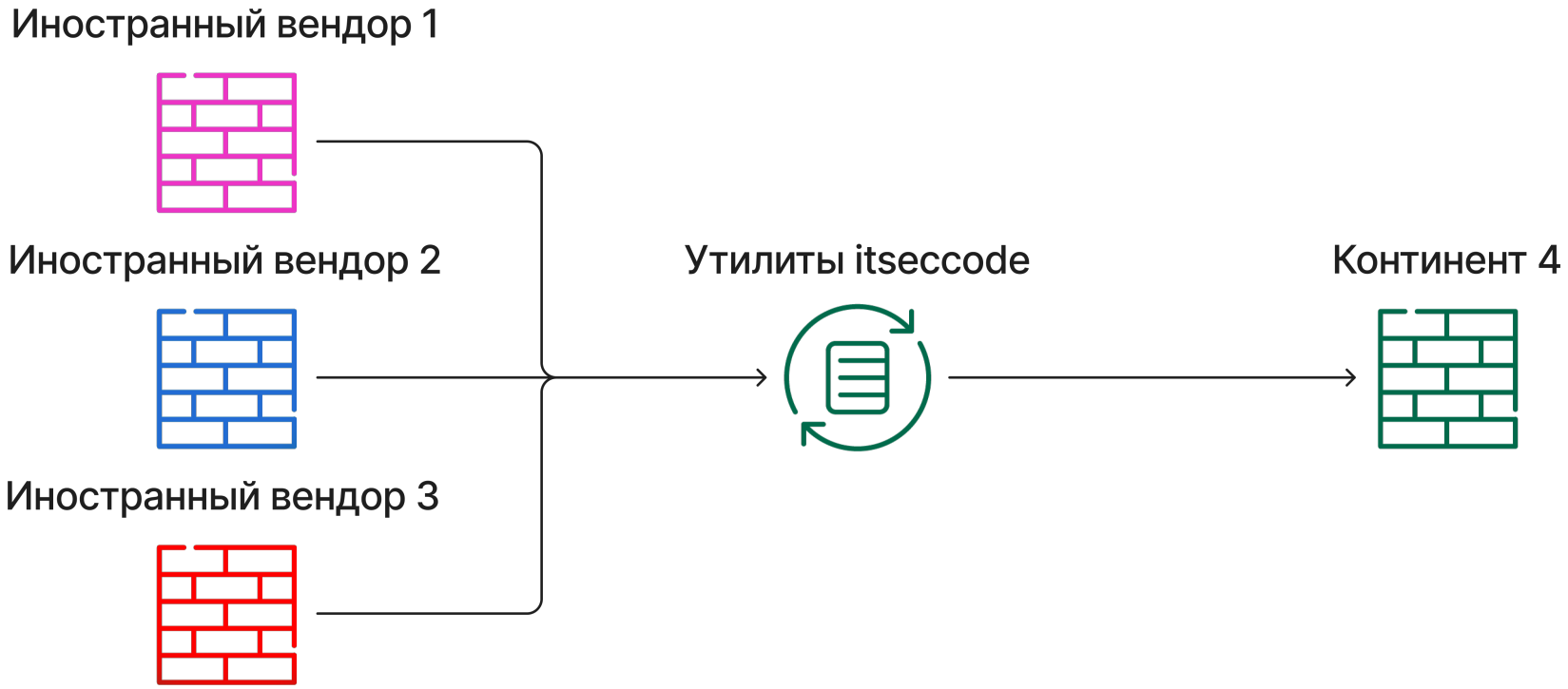
Миграции со сторонних NGFW (UserGate, FortiGate, Check Point, Palo Alto, Cisco)

Импорт индикаторов компрометации (IoC) в Континент 4

Создание политик безопасности

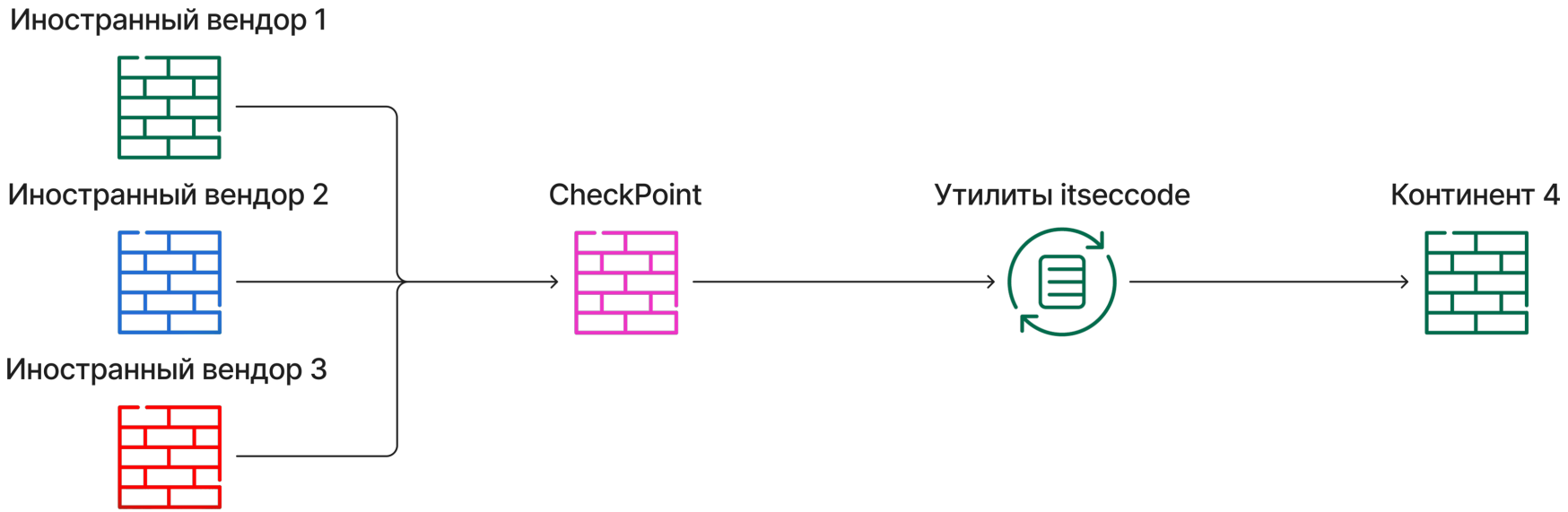
КОД безопасности

Миграция с иностранных решений. Вариант 1



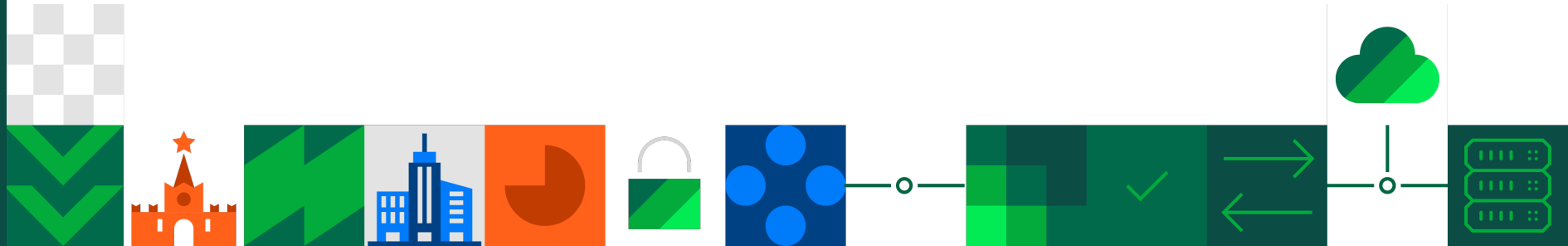
КОД безопасности

Миграция с иностранных решений. Вариант 2



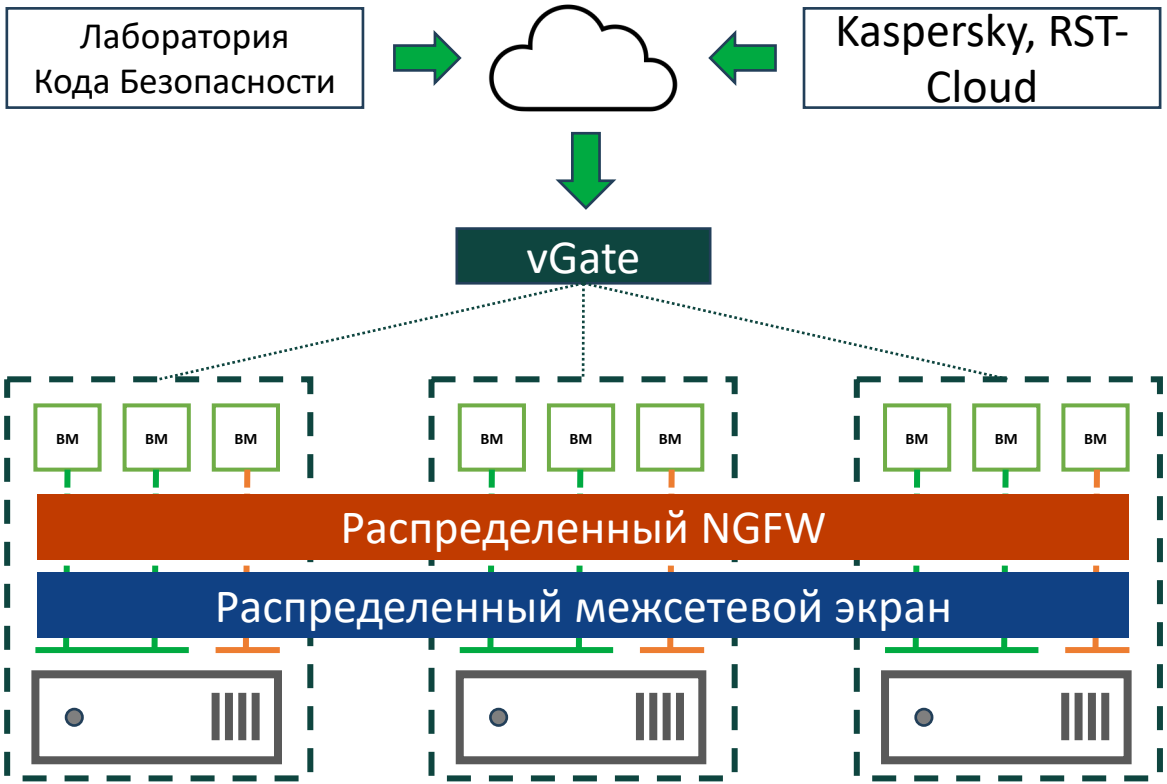
КОД безопасности

Защита сети виртуализации



КОД безопасности

Распределенный NGFW



Для каждой виртуальной машины:

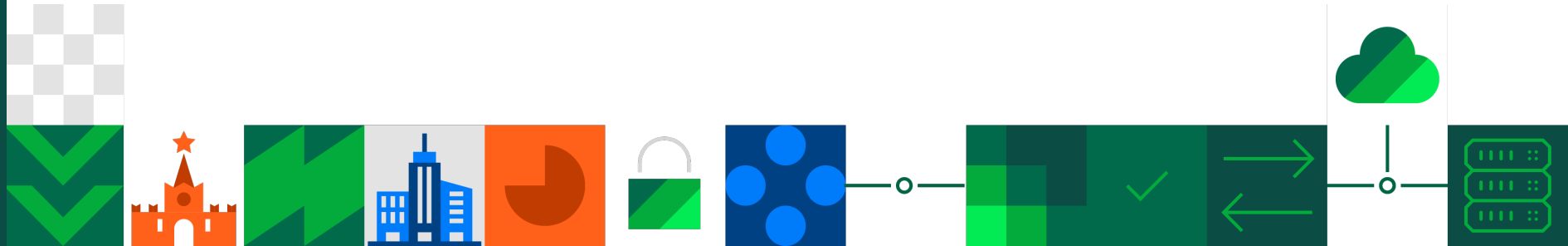
- Межсетевой экран
- Контроль приложений
- Анализ индикаторов компрометации
- Обнаружение сетевых вторжений

Политики на основе разных критериев

- Атрибуты ВМ
- Сетевые атрибуты

КОД безопасности

Заключение



КОД безопасности

Главная задача – подтвердить делом

«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

КОД безопасности

Много NGFW на рынке

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

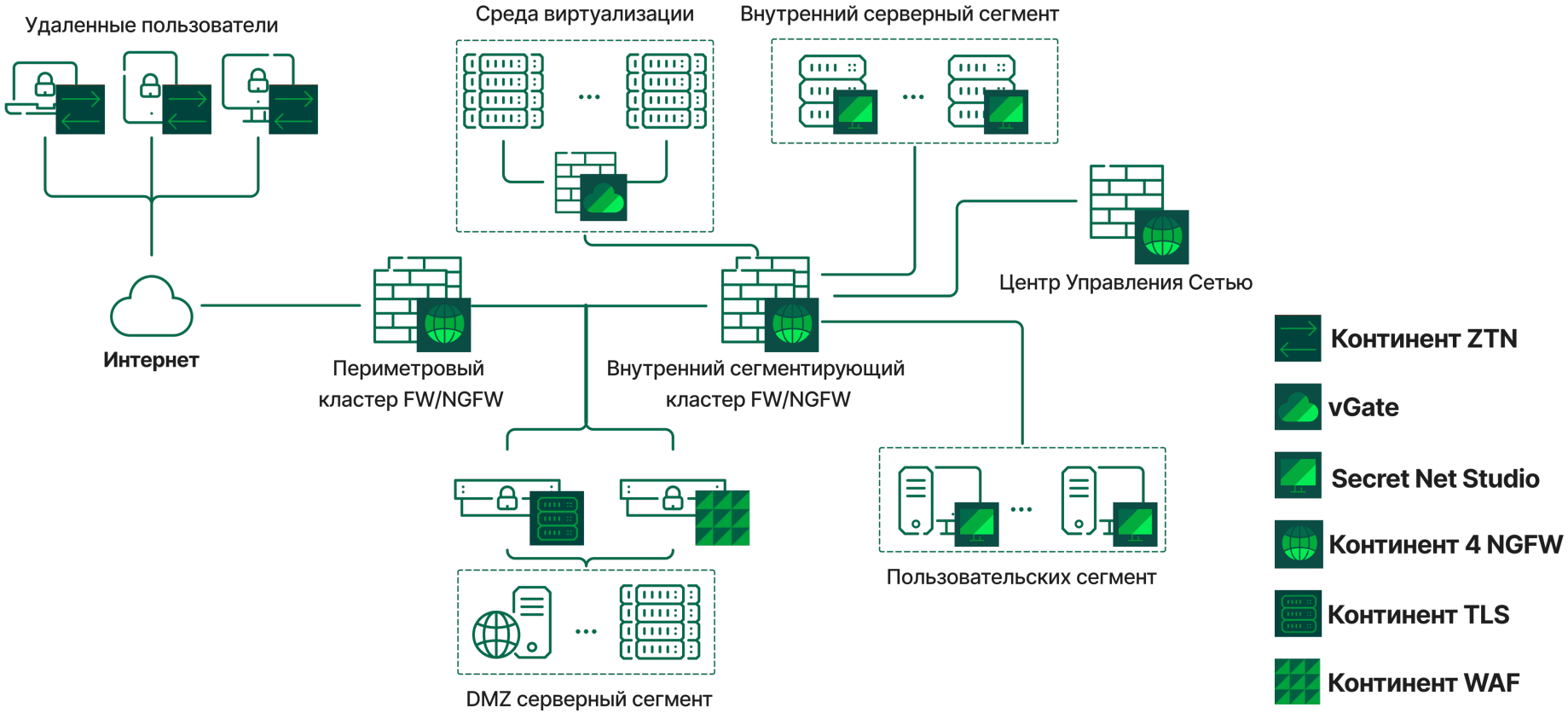
Тестирование механизмов безопасности

BI.ZONE

Тестирование производительности

КОД безопасности

Схема сети с продуктами Кода Безопасности



Приглашаем принять участие в Исследовательской группе Кода Безопасности

Давайте вместе развивать российский рынок информационной безопасности!

КОД безопасности

Социальные сети

КОД безопасности

Спасибо за внимание!

info@securitycode.ru

www.securitycode.ru