

Сергей Плотко

Коммерческий директор АО «НПП «Цифровые решения»

Балансировка от L4 до L7

Отделяем необходимое от достаточного



Зачем нужен балансировщик в современной инфраструктуре?



Горизонтальное
масштабирование
вычислительных ресурсов



Поддержание
производительности
средств ИБ при нагрузке



Обеспечение
отказоустойчивости

Балансировщик нагрузки — *ключевой элемент* системы масштабирования и обеспечения бесперебойной работы сервисов

Рынок балансировщиков в России



Решения на основе Open Source ПО



Необходимость в высококлассных ИТ-специалистах



Производительность



Зависимость от сообщества разработчиков



Несоответствие требованиям регуляторов

Рынок балансировщиков в России



ПАК зарубежных вендоров



net>scaler



Ограниченный доступ к новому оборудованию и обновлениям



Продление лицензий



Отсутствие официальной поддержки



Несоответствие требованиям регуляторов

ПАК зарубежных вендоров



Балансировщик? Нет, многофункциональный комбайн!



net>scaler



kemp

- L4 балансировка
- L7 балансировка
- Content switching
- Контроль состояния кластера до L7
- SSL offloading
- WAF
- Anti-DDoS
- TCP Optimization/Compression
- Caching
- SSO/MFA

Всё включено — *не значит* всё нужно



-  Сложность настройки L7-балансировки — требуется постоянная синхронизация с изменениями в логике приложений
-  Ограниченная применимость в российских реалиях — например, WAF не учитывает региональную специфику
-  Падение производительности — активация функций снижает эффективность работы балансировщика
-  Переплата за неиспользуемый функционал — многие возможности приобретаются «на всякий случай», но так и остаются невостребованными
-  Избыточность SSL-офлоадинга — его значимость снижается с появлением аппаратных ускорителей, таких как Intel QAT

Простота – залог надежности



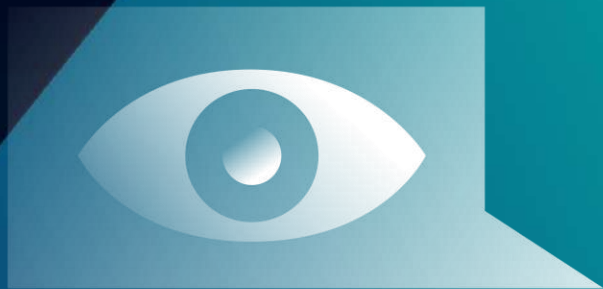
Дублирование функций — усложнение жизни: даже похожие модули могут конфликтовать или «жить своей жизнью»



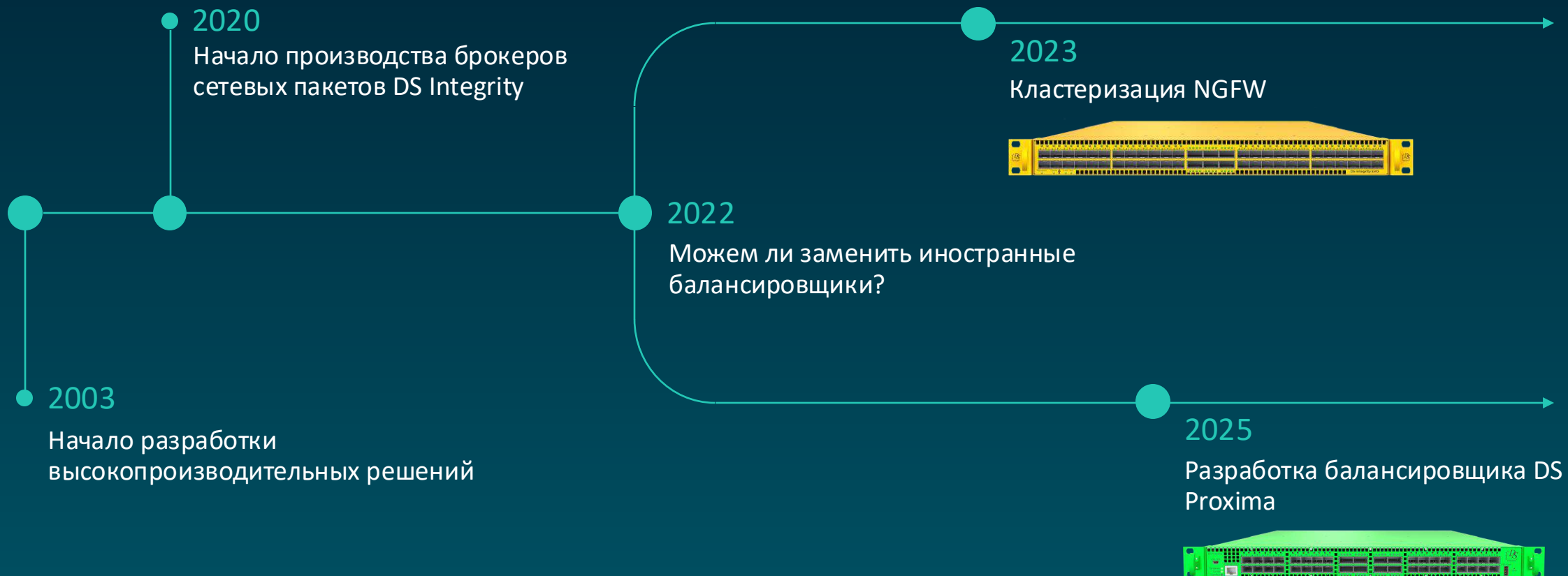
Не плоди сущности без надобности: больше настроек - больше точек отказа и сложнее искать причину проблем

Проектируйте архитектуру с запасом *надежности*, а не с избытком функций

Аппаратный балансировщик нагрузки DS Proxima

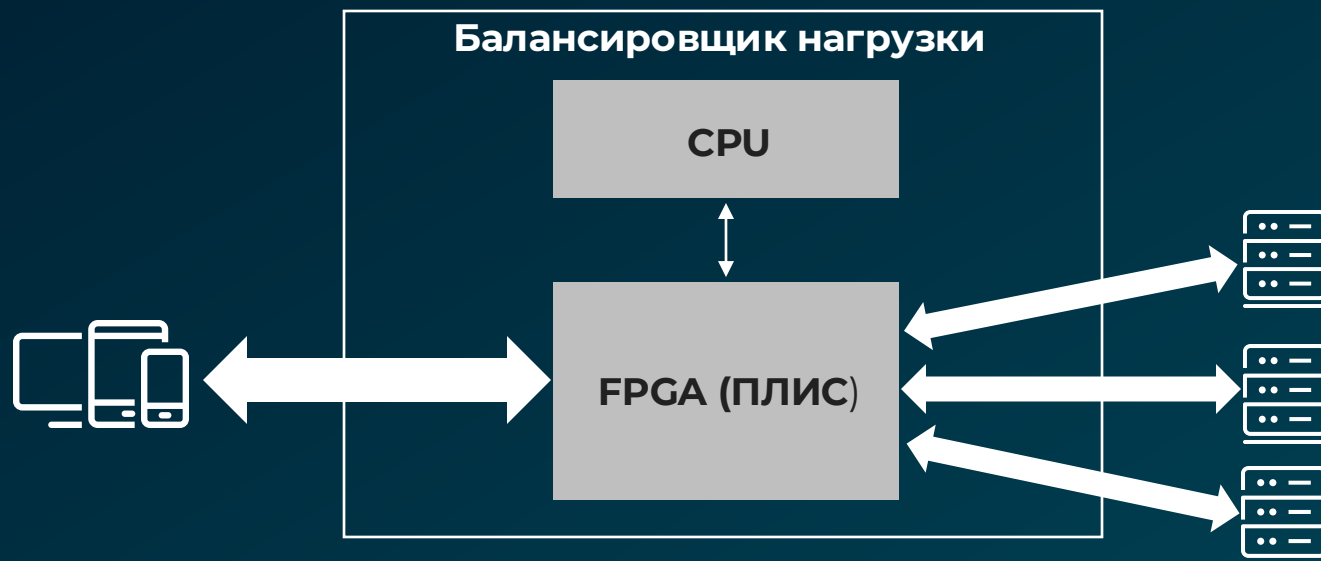


Эволюция наших решений по балансировке



Аппаратная обработка трафика

Максимальная надежность. Производительность – по умолчанию



CPU
Управление
Health checks до L7

FPGA (ПЛИС)
Обработка трафика на скорости канала
Балансировка до L4

Reliability by design

Изоляция от ОС: нет зависимости от ядра, драйверов и фоновых процессов

Минимум кода – минимум уязвимостей: простая логика, без библиотек, рантаймов и зависимостей

Предсказуемое поведение: стабильная задержка, без прерывания и “джиттера”

Функциональные возможности балансировки DS Proxima



Особенности реализации балансировки	• Симметричная балансировка трафика в обоих направлениях • Балансировка с подменой или сохранением Src/Dst IP • Согласованное хэширование для сохранения сессий при изменении состава кластера
Базовые алгоритмы балансировки	• Hash based per-session (симметричный L2/L3/L4 Hash: 5-tuple, 2-tuple, Src IP/Dst IP only) • Weighted per-session
Балансировка с отслеживанием сессий	• Least connections, Weighted least connections, Least response time • Плавный ввод/вывод устройств из кластера без прерывания сервиса
Контроль состояния кластера	• Настраиваемый Keepalive на уровнях L3/L4/L7 • Heartbeat пакеты для E2E контроля соединений • BFD для контроля сетевых соединений BGP и OSPF
Интеграция в инфраструктуру	• Стандартные протоколы L2 (MC-LAG) и L3 (OSPF, BGP) • GRE туннелирование/детуннелирование • Балансировка и фильтрация трафика по вложенным заголовкам в GRE туннелях
Отказоустойчивость	• Стандартные протоколы L2 (LAG LACP, MC-LAG) и L3 (VRRP)

Наш подход к импортозамещению



Аппаратный балансировщик нагрузки



NGFW



TLS-шлюзы



Proxy-серверы



NAC

WAF

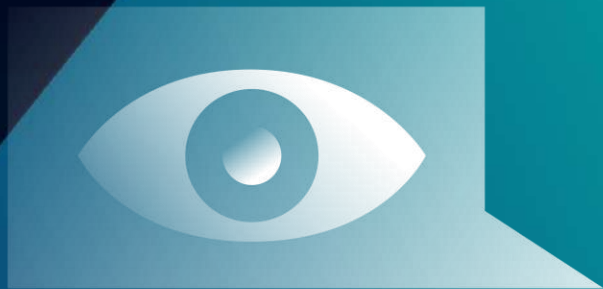


ВКС

Sandbox

Почта

Особенности балансировки WAF



Почему WAF и балансировщик должны работать в связке?



Один трафик — две задачи

Инфраструктурный уровень



Обеспечение масштабируемости
и отказоустойчивости

Прикладной уровень



Масштабирование и защита одних и тех же
сервисов

Связка L4-балансировщика и WAF



Рациональное распределение L7-функций между компонентами

L4-балансировщик

- L4 балансировка
- Контроль состояния кластера до L7

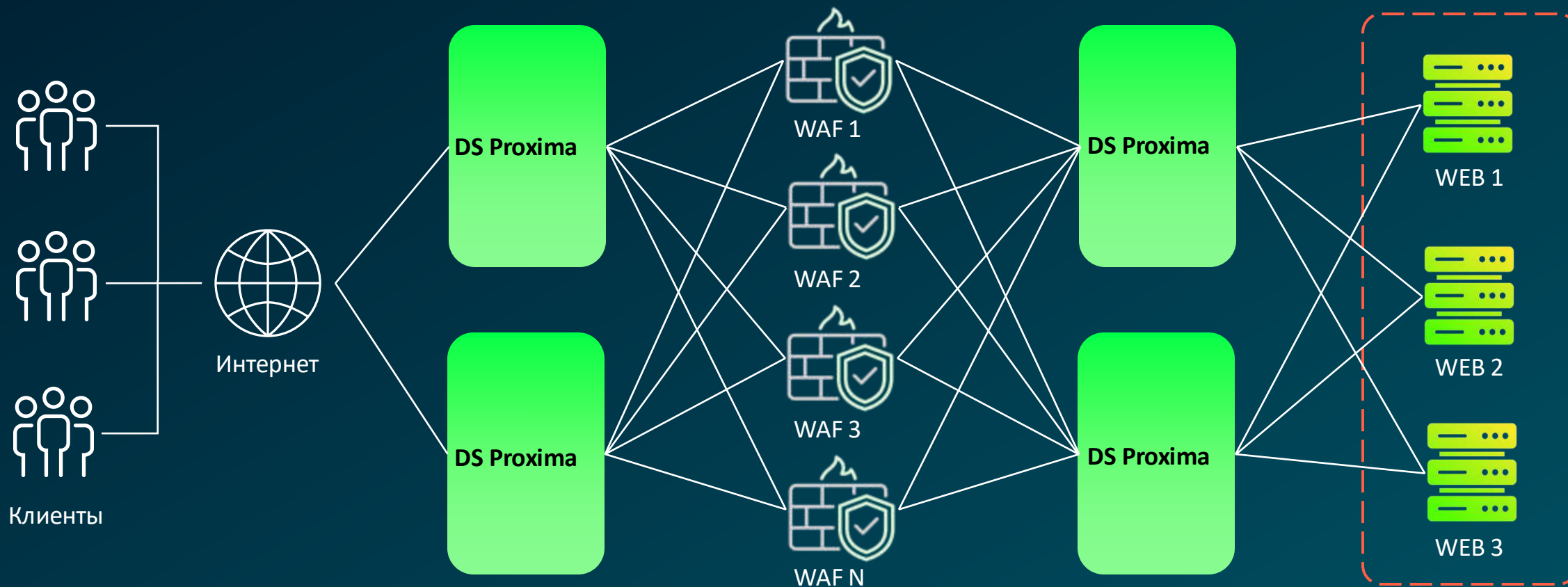
WAF

- WAF
- L7 балансировка
- Content switching
- SSL offloading

Не балансировка

- Anti-DDoS
- TCP Optimization/Compression
- Caching
- SSO/MFA

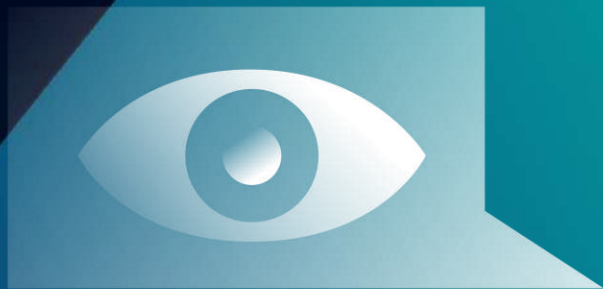
Балансировка кластера WAF



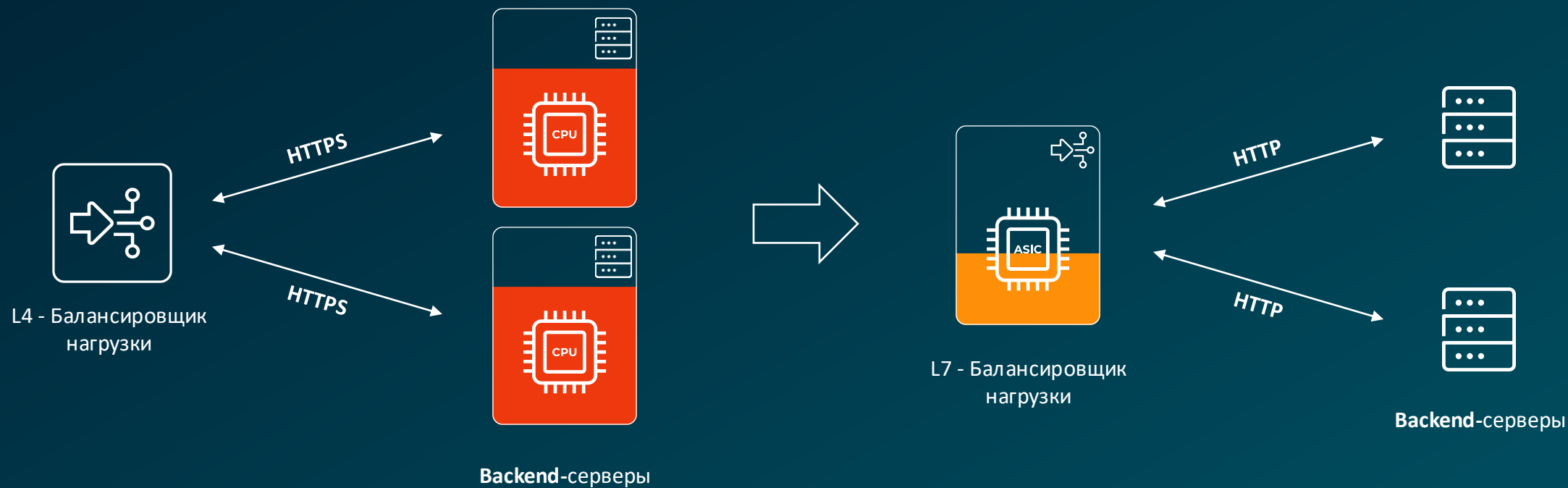
Оба контура балансировки могут реализовываться на одной паре DS Proxima

Защищаемые
WEB-ресурсы

Нужен ли SSL-
оффлоадинг при
наличии Intel QAT?



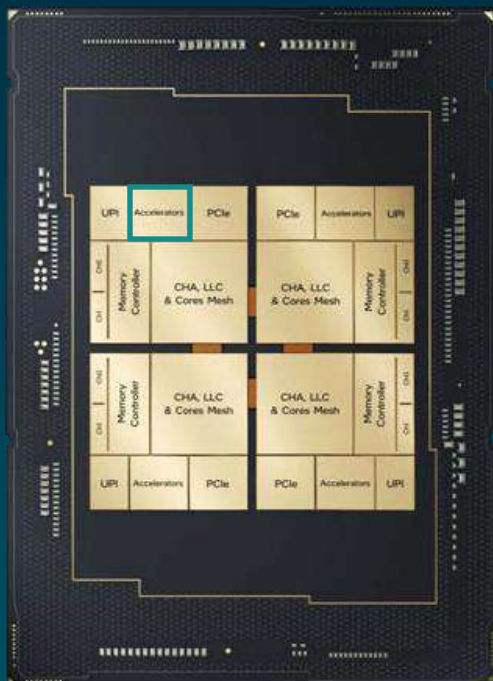
Рост HTTPS-трафика как драйвер перехода на SSL-офлоадинг



Аппаратное ускорение SSL прямо в CPU *делает внешние SSL-офлоадеры избыточными*



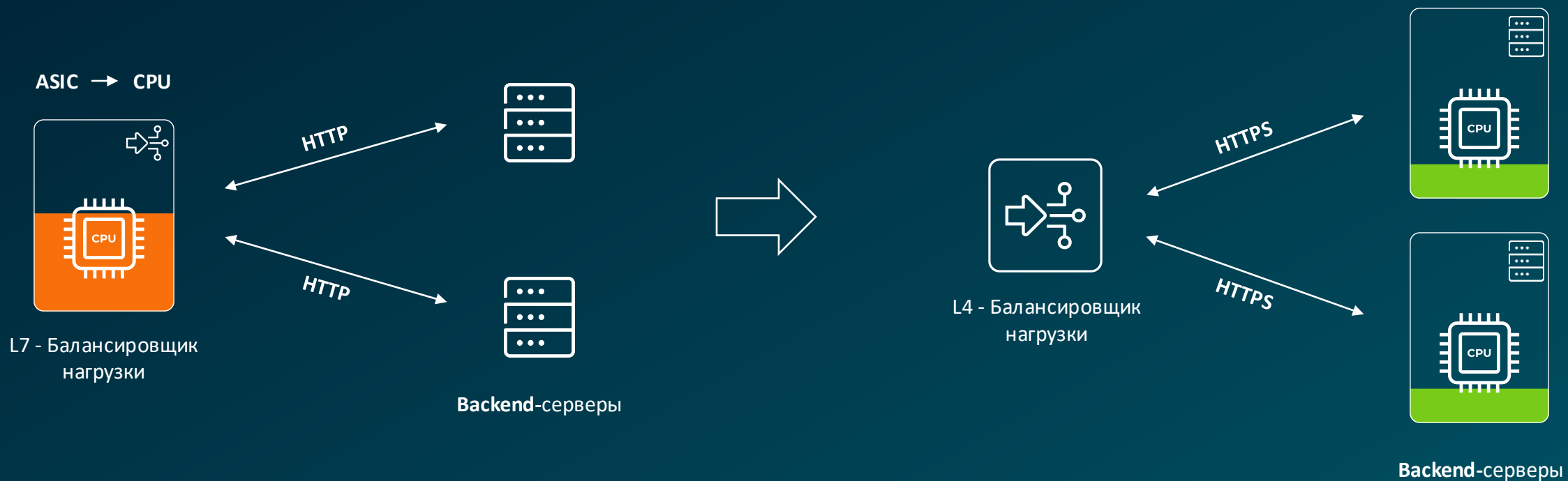
QuickAssist Technology (QAT) в процессорах Intel Xeon обеспечивает ускорение криптографических операций **в 5-6 раз**



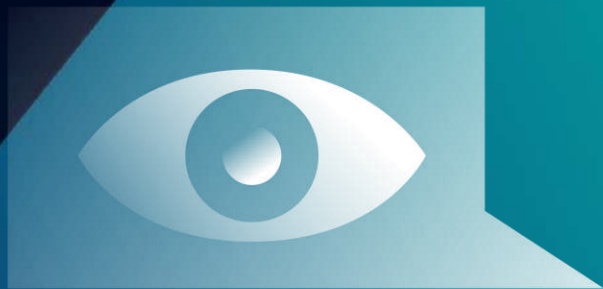
	Загрузка процессора
Без QAT	92%
С QAT	15%

Intel Xeon Platinum 8470N
40K TLS Handshakes (Connections per second)
TLS 1.3 ECDHE-X25519-RSA2K

С Intel QAT распределенная SSL-обработка снова эффективна



Особенности балансировки NGFW



Актуальная задача кластеризации NGFW



NGFW — критический элемент ИБ-инфраструктуры

- Разворачивается не только на периметре, но и внутри сети
- Часто является единственным защитным рубежом в сегментах

Кластеризация NGFW на CPU

- Зарубежные NGFW используют ASIC/NPU или кластеризацию при обработке трафика на CPU
- Российские NGFW работают на CPU, поэтому оптимальное решение это горизонтальное масштабирование через объединение в кластеры

Симметрия — технический императив

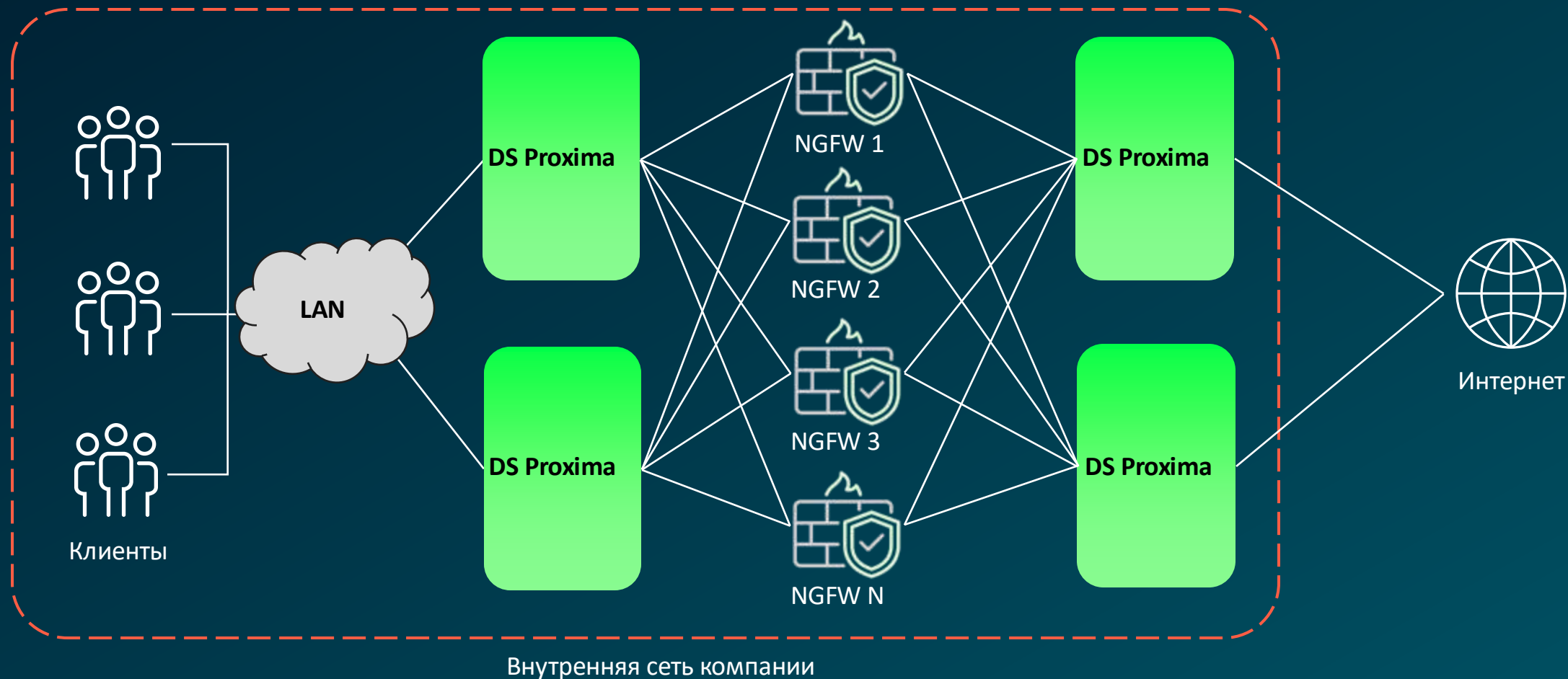
- Stateful-фильтрация требует, чтобы прямой и обратный трафик шёл через один и тот же узел
- При асимметрии возможен дроп соединения из-за отсутствия состояния

Сравнение кластеризации NGFW

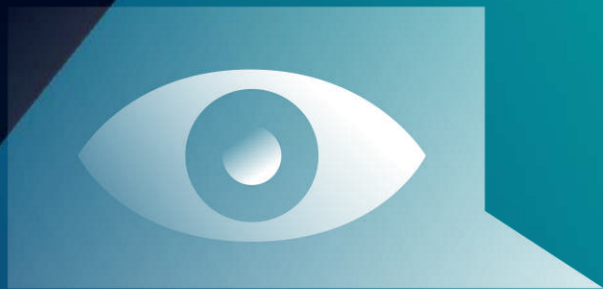


	Брокер пакетов	Балансировщик
Интеграция в инфраструктуру L3	Интеграция каждого NGFW с настройкой ACL	Интеграция всего кластера через стандартные протоколы L3 (OSPF, BGP)
Интеграция в инфраструктуру L2	Настройка ACL	Стандартные протоколы L2 (MC-LAG)
Алгоритмы балансировки	Статические hash-алгоритмы	Механизм отслеживания сессий
Health checks	Link monitor, E2E heartbeats, Ping, TCP port, HTTP get	Link monitor, E2E heartbeats, Ping, TCP port, HTTP get, дальнейшее расширение
Отказоустойчивость L3	Проприетарный механизм	Стандартные протоколы L3 (VRRP)
Отказоустойчивость L2	Проприетарный механизмы	Стандартные протоколы L2 (MC-LAG)
API	Отсутствует	Netconf

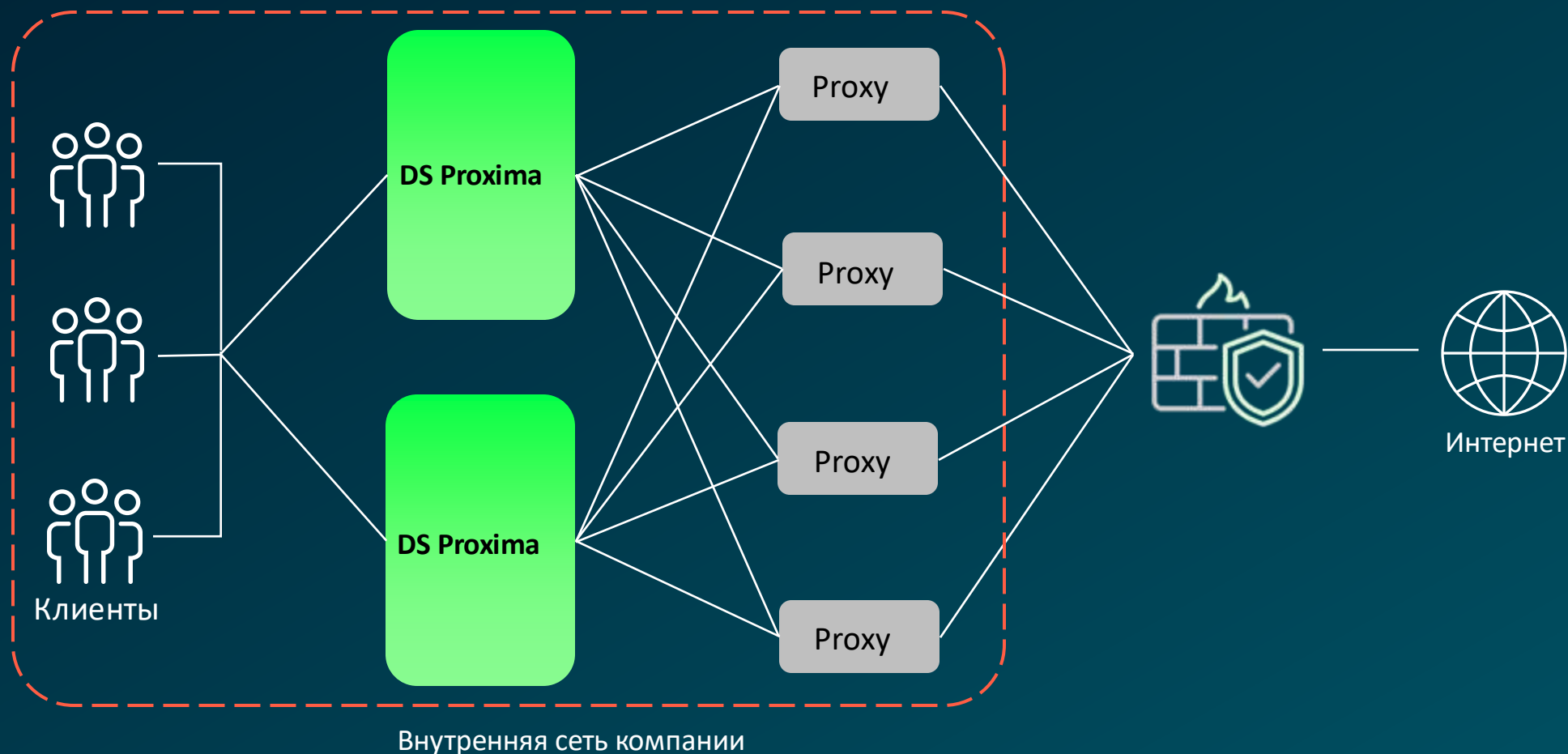
Балансировка кластера NGFW



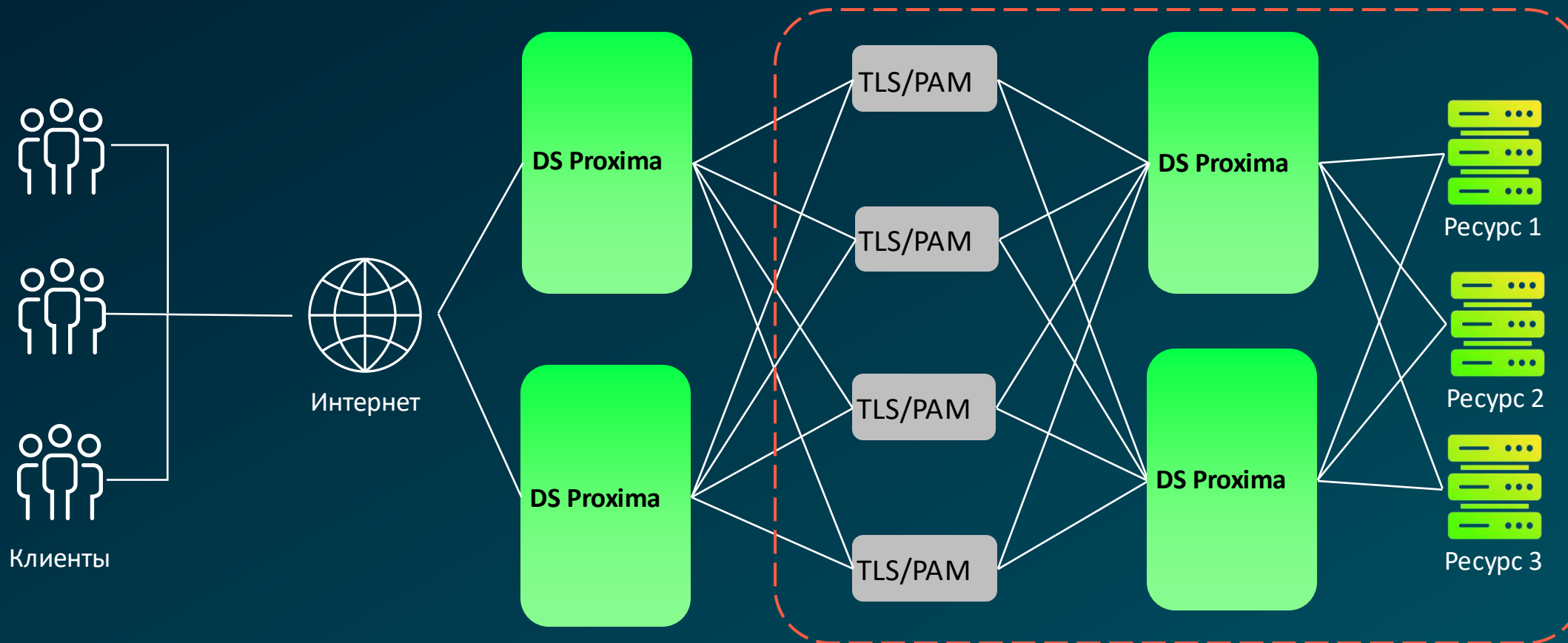
Где еще работает
балансировка



Балансировка кластера Proxy-серверов

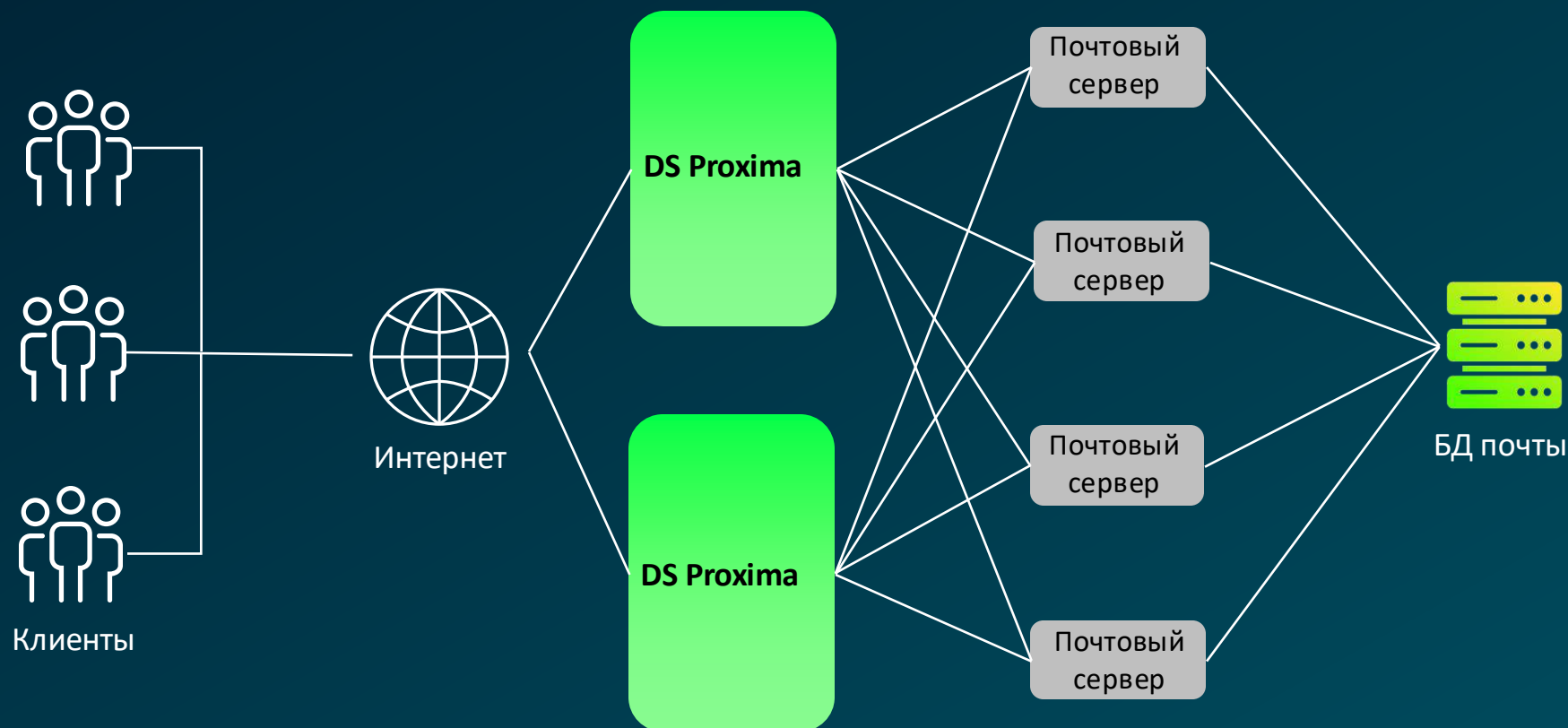


Балансировка кластера TLS-шлюзов/PAM

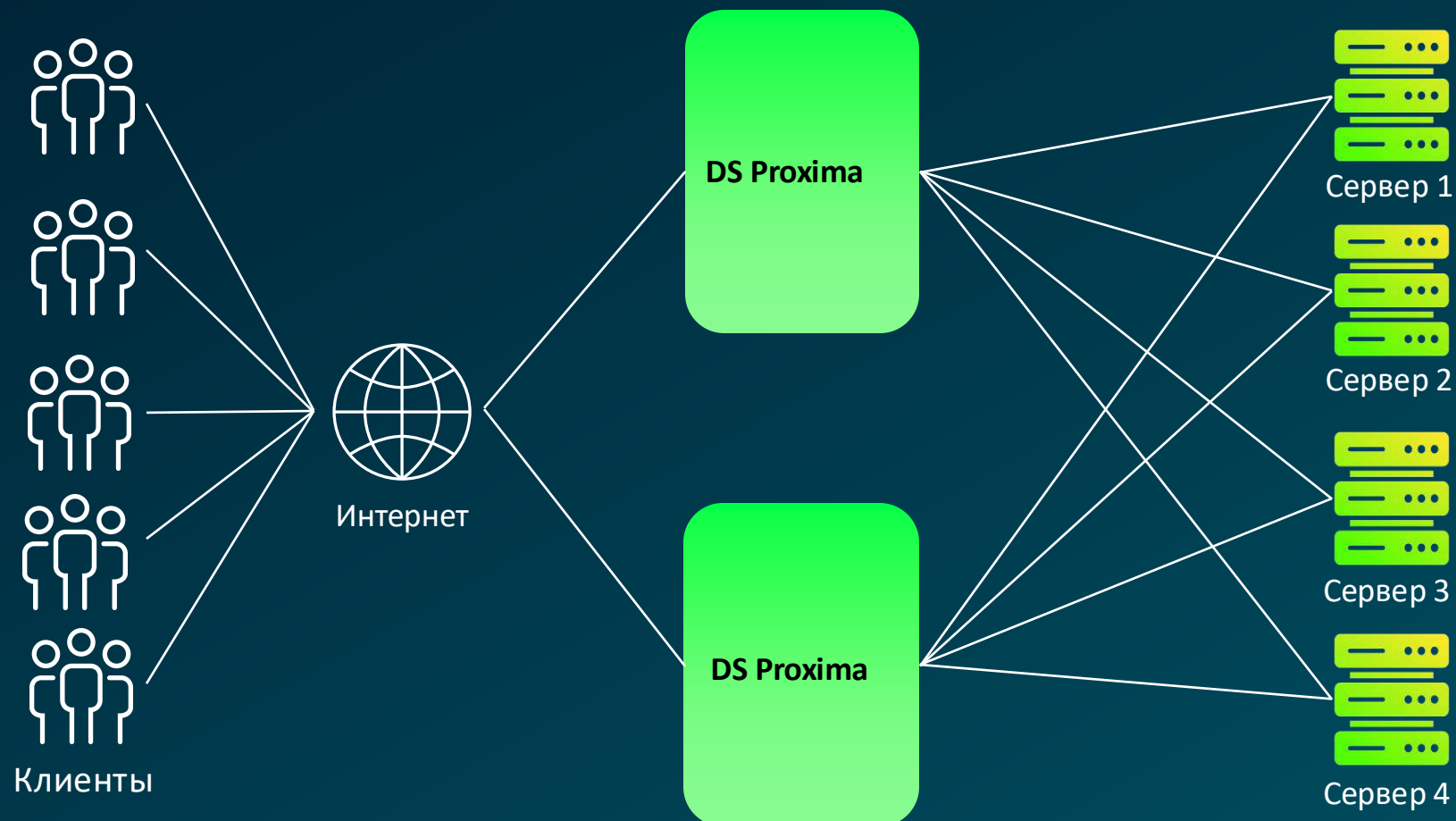


Оба контура балансировки могут реализовываться на одной паре Proxima

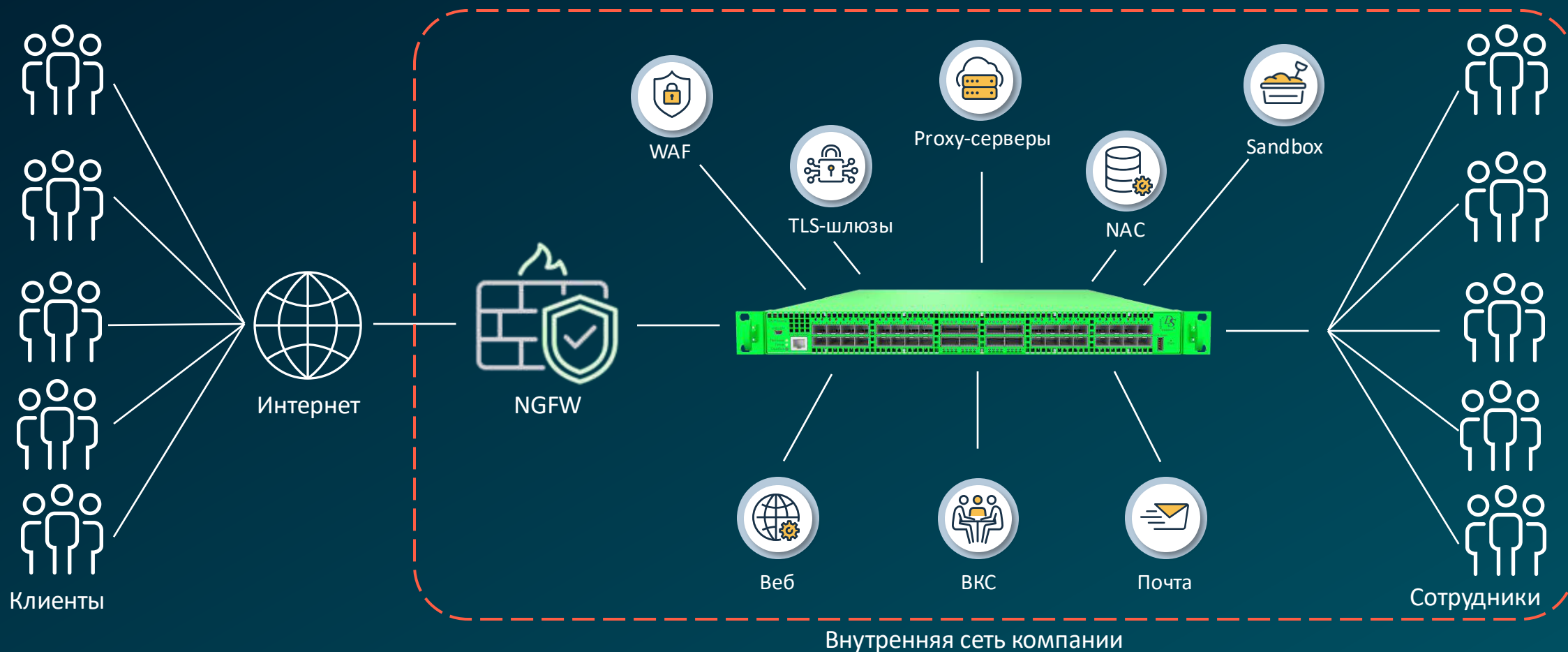
Балансировка кластера почтовых серверов



Балансировка ВКС и серверов приложений



Кластер управления вашими сервисами



Ключевые рекомендации



Спасибо за внимание!



Чат по DS Proxima



Оцените выступление



Сергей Плотко
Коммерческий директор