

Внедрение АС с поддержкой криптографических алгоритмов и протоколов ГОСТ

на базе КриптоПро NGate



Цели доклада



Описание проектирования и внедрения АС на базе КриптоПро NGate в инфраструктуре заказчика



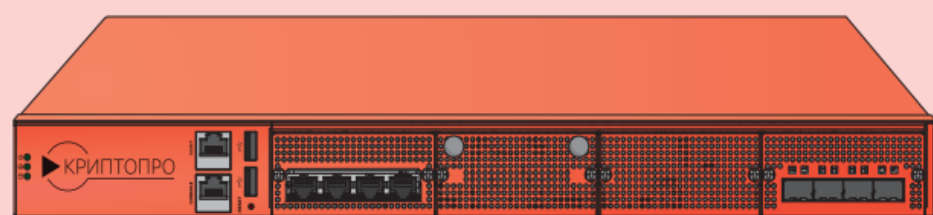
Указание функциональных возможностей КриптоПро NGate, которые были использованы в АС

Перечень функциональных требований к системе

- ▶ построения защищенных TLS-соединений с использованием алгоритмов группы ГОСТ.
- ▶ обратный прокси-сервер (reverse-proxy)
- ▶ прямой прокси-сервер (forward-proxy)
- ▶ аутентификации сервера и клиента по сертификату с передачей IP-адреса клиента в HTTP-заголовке.
- ▶ унификация решений по построению TLS-соединений
- ▶ отказо- и катастрофоустойчивость системы

Реализация системы

NGate-3000



■ Описание

КриптоПро NGate – это высокопроизводительный VPN-шлюз на базе протокола TLS, который позволяет безопасно и быстро организовать защищённый доступ удалённых пользователей к корпоративным ресурсам через незащищённые сети.

Аппаратная платформа **NGate-3000** предназначена для работы в качестве Узла шлюза NGate, создаваемого при помощи КриптоПро NGate.

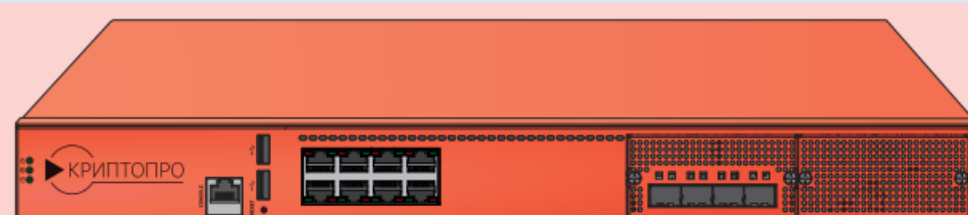
■ Основные технические характеристики

Класс криптографической защиты	КС1, КС2, КС3	
Основное назначение	Узел NGate	
	TLS VPN	TLS Proxy
Максимальное число соединений	12000 подкл.	45000 подкл.
Максимальная скорость передачи данных	8 Гбит/с	20 Гбит/с

■ Эксплуатационные характеристики

Охлаждение		Размеры при эксплуатации	
Процессор	CPU радиатор	(ДхШхВ) / Вес	438 × 630 × 44,45 (1U) мм / 19 кг
Система	4 вентилятора охлаждения	Размеры в упаковке	
Параметры окружающей среды		(ДхШхВ) / Вес	850 × 600 × 220 мм / 25 кг
Температура	0 - +40 °С рабочая температура	Параметры питания	
	-20 - +70 °С хранение		
Влажность (RH)	5 - 90 % рабочая влажность	Тип / мощность	650 Вт ATX резервный PSU
	5 - 95 % хранение	Характеристики	АС 100 - 240 В @ 47 - 63 Гц

NGate-ЦУС-200



■ Описание

КриптоПро NGate – это высокопроизводительный VPN-шлюз на базе протокола TLS, который позволяет безопасно и быстро организовать защищённый доступ удалённых пользователей к корпоративным ресурсам через незащищённые сети.

Аппаратная платформа **NGate-ЦУС-200** предназначена для работы в качестве Системы управления шлюза NGate, создаваемого при помощи КриптоПро NGate.

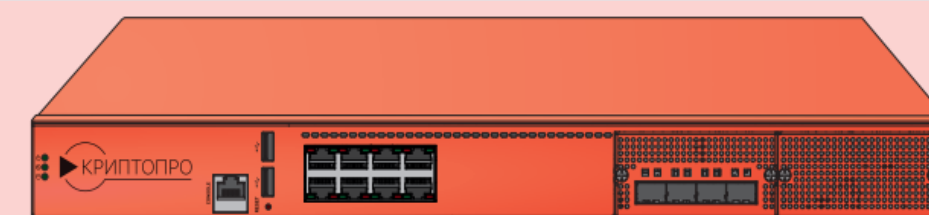
■ Основные технические характеристики

Класс криптографической защиты	КС1, КС2, КС3
Основное назначение	Система управления NGate
Максимальное число управляемых узлов	800
Максимальное число управляемых кластеров	Не ограничено

■ Эксплуатационные характеристики

Охлаждение		Размеры при эксплуатации	
Процессор	CPU радиатор	(ДхШхВ) / Вес	438 × 525 × 44,45 (1U) мм / 15 кг
Система	4 вентилятора охлаждения	Размеры в упаковке	
Параметры окружающей среды		(ДхШхВ) / Вес	790 × 600 × 220 мм / 16 кг
Температура	0 - +40 °С рабочая температура	Параметры питания	
	-20 - +70 °С хранение		
Влажность (RH)	5 - 90 % рабочая влажность	Тип / мощность	300 Вт + ATX резервный PSU
	5 - 95 % хранение	Характеристики	АС 90 - 264 В @ 47 - 63 Гц

NGate-1500



■ Описание

КриптоПро NGate – это высокопроизводительный VPN-шлюз на базе протокола TLS, который позволяет безопасно и быстро организовать защищённый доступ удалённых пользователей к корпоративным ресурсам через незащищённые сети.

Аппаратная платформа **NGate-1500** предназначена для работы в качестве Узла шлюза NGate, создаваемого при помощи КриптоПро NGate.

■ Основные технические характеристики

Класс криптографической защиты	КС1, КС2, КС3	
Основное назначение	Узел NGate	
	TLS VPN	TLS Proxy
Максимальное число соединений	4000 подкл.	8000 подкл.
Максимальная скорость передачи данных	2 Гбит/с	4 Гбит/с

■ Эксплуатационные характеристики

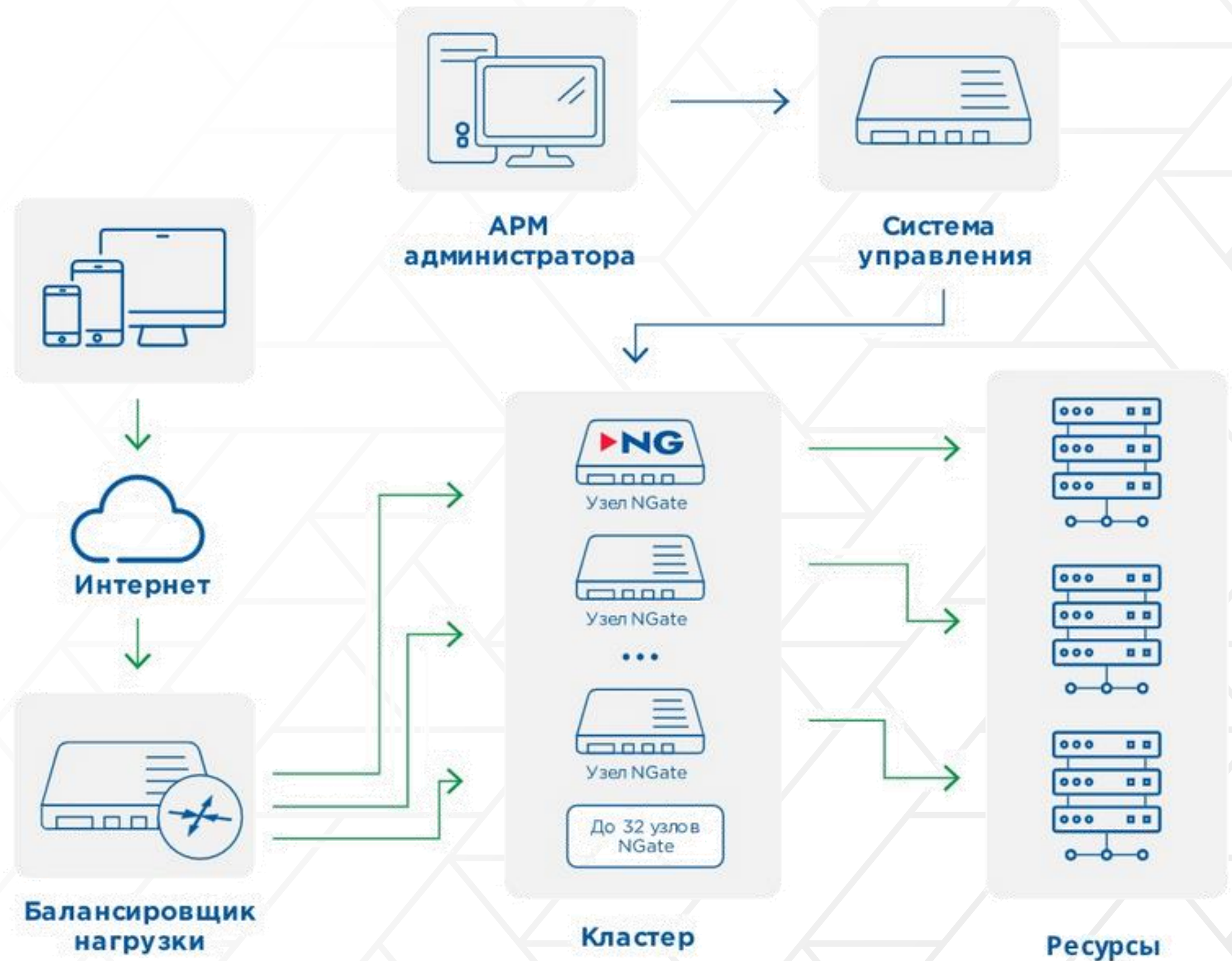
Охлаждение		Размеры при эксплуатации	
Процессор	CPU радиатор	(ДхШхВ) / Вес	438 × 525 × 44,45 (1U) мм / 15 кг
Система	4 вентилятора охлаждения	Размеры в упаковке	
Параметры окружающей среды		(ДхШхВ) / Вес	790 × 600 × 220 мм / 16 кг
Температура	0 - +40 °С рабочая температура	Параметры питания	
	-20 - +70 °С хранение		
Влажность (RH)	5 - 90 % рабочая влажность	Тип / мощность	300 Вт + ATX резервный PSU
	5 - 95 % хранение	Характеристики	АС 90 - 264 В @ 47 - 63 Гц

Отказо- и катастрофоустойчивость системы

Отказоустойчивая конфигурация включает в себя Балансировщик нагрузки, распределяющий поступающую от периферийных устройств нагрузку между Узлами NGate.

Соответственно, балансировка нагрузки возможна только при условии наличия в кластере не менее двух Узлов NGate.

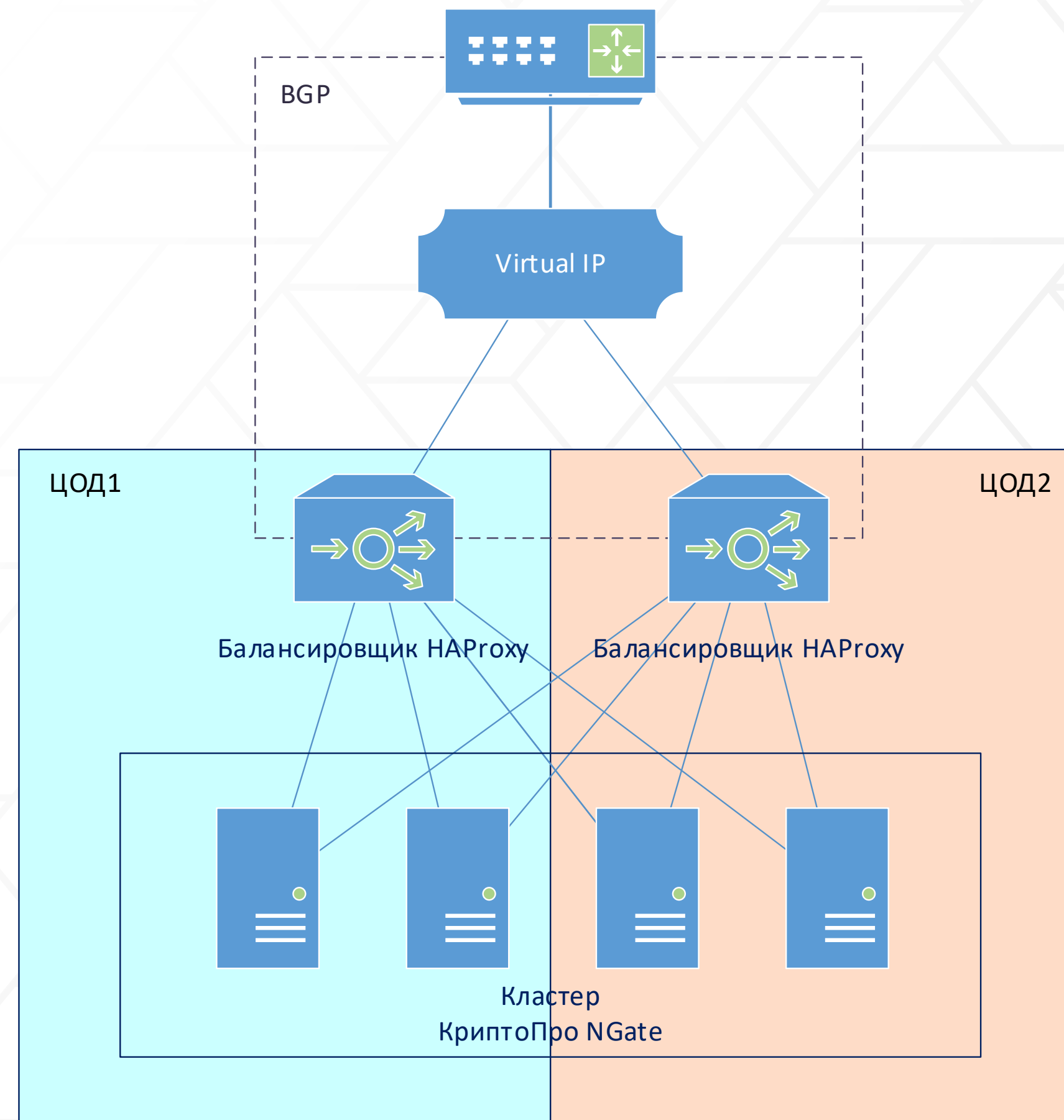
Узлы NGate в кластере управляются при помощи Системы управления системой NGate.



Отказо- и катастрофоустойчивость системы

Для реализации отказо- и катастрофоустойчивости системы в двух, географически разнесенных ЦОД заказчика, был размещен кластер из четырех узлов NGate и двух балансировщика HAProxy.

На каждый из ЦОД приходилось по два узла и одному балансировщику.



Сервер portalного доступа

NGate обеспечивает возможность подключаться к внутренним ресурсам организации в том числе с использованием веб-браузеров, поддерживающих протокол TLS с ГОСТ.

Это может быть особенно полезно в том случае, когда пользователям необходимо предоставить доступ к строго ограниченным ресурсам.



VPN-сервер

С использованием динамического VPN-туннеля шлюза NGate обеспечивается динамическое туннелирование – доступ клиентской машины к удаленной сети по любым протоколам и портам внутри туннеля без ограничения количества одновременно подключаемых приложений.

Таким образом, режим VPN-сервера используется для предоставления пользователям доступа к произвольным ресурсам корпоративной сети с помощью VPN-клиента, поддерживающего все популярные платформы. При этом разграничение доступа возможно на уровне подсетей, в том числе виртуальных (VLAN). При реализации VPN-доступа, также, как и в других режимах, возможно использование любых поддерживаемых методов аутентификации.



Внешние службы

Список доступных внешних служб можно увидеть (и настроить) как в особом разделе веб-интерфейса, так и на вкладке выбранной конфигурации кластера. Но во втором случае будут отображены только те системы и серверы, которые настроены для конкретного кластера.

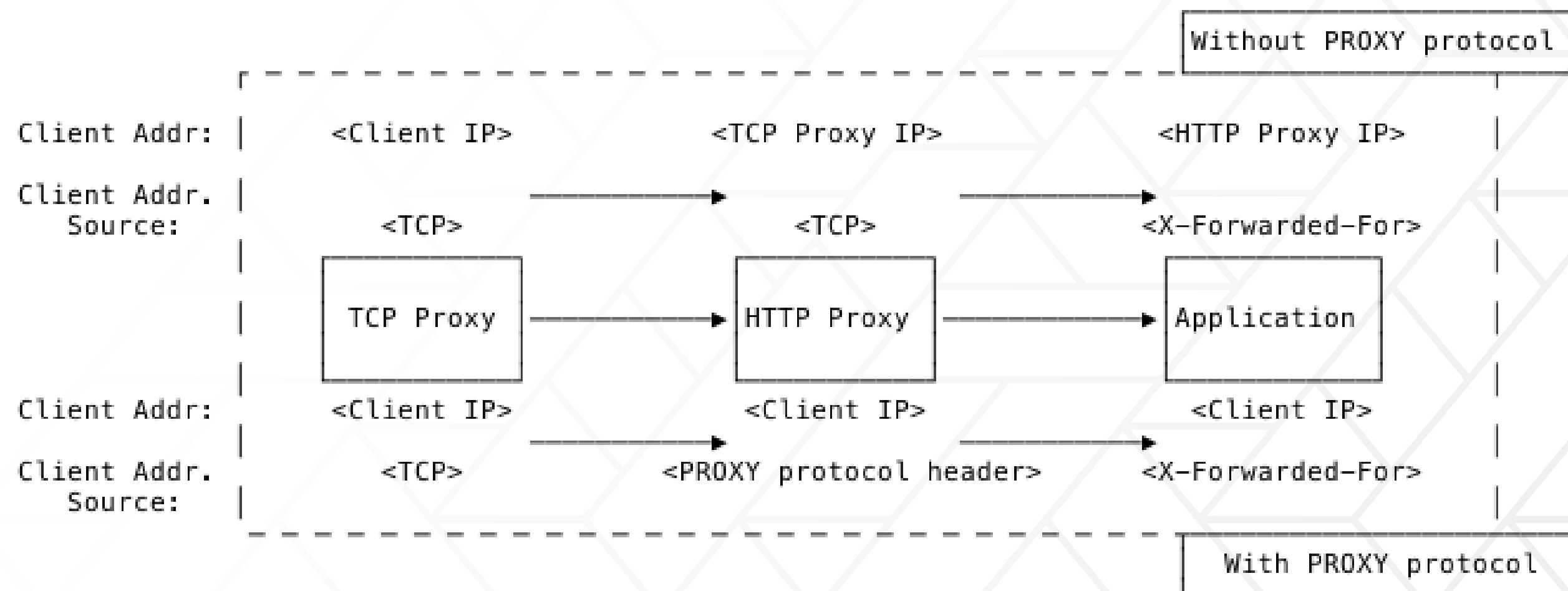
The screenshot shows the nGate Control Panel interface. The top navigation bar includes the nGate logo, a menu icon, a language dropdown set to 'English (en)', a 'Change Language' button, and a user profile 'ng-admin'. The main content area is titled 'Cluster' and shows the 'External Services' tab selected. Below the tabs, there is a table of services with their respective descriptions and 'Assign' buttons.

Service Name	Service Type	Action	Description
LDAP Server	LDAP	Assign	LDAP Server assigned to the configuration; used for user authentication
RADIUS Server	Radius	Assign	RADIUS Server assigned to the configuration; used for user authentication
NTP Servers	nGate_NTP	Assign	NTP Servers assigned to the configuration
DNS Settings	nGate_DNS	Assign	DNS Settings assigned to the configuration
Syslog Servers	Greylog	Assign	Syslog Servers assigned to the configuration for log forwarding

Поддержка Proxy протокола

Цель протокола PROXY состоит в том, чтобы позволить TCP-прокси, работающим на транспортном уровне (уровень 4 модели OSI), вводить данные об исходных адресах источника и назначения на свои вышестоящие серверы без знания базового протокола.

Протокол PROXY предназначен для поддержки любого протокола прикладного уровня, такого как FTP, SMTP, IMAP, протокол MySQL и других протоколов, построенных поверх TCP или UDP. Он позволяет прокси-серверу реализовать добавление заголовка протокола PROXY к запросу для предоставления данных исходному клиенту, ничего не зная о проксируемом протоколе.



Проверка ключевых контейнеров

Также в рамках данного проекта со стороны КриптоПро в ПО nGate был добавлен механизм проверки целостности ключевых контейнеров от сертификатов. При повреждении контейнера в веб-интерфейсе администратора появляется предупреждение об ошибке.

The screenshot displays the nGate Control Panel interface. At the top, there is a navigation bar with the title 'nGate Control Panel', a language dropdown set to 'English (en)', a 'Change Language' button, and a user profile 'ng-admin'. A left sidebar contains a menu with categories like 'Dashboard', 'System Info', 'Sessions', 'Management Center Settings', 'IP statistics', 'Access Control', 'Clusters', 'External Services', and 'HeaderSets'. The main content area is titled 'Dashboard' and features a prominent red error banner: 'ERROR: Some containers were damaged! Please, check ng-info for details!'. Below the banner, the 'Management Center' section provides system statistics: Uptime (4 day(s)), Disk R/W (186.35 MB/132.23 MB), Net I/O (6.60 MB/6.91 MB), and CSP License (March 16, 2023). Three donut charts are shown: 'RAM' (Used/Free), 'CPU Usage' (System/Used/Free), and 'Disk Usage' (with sub-categories /data, /var, /tmp). The bottom section is divided into four panels: 'Cluster' (Configuration, CSP License, NGATE Licenses, Creation date, Comment), 'Nodes' (listing three enabled gate nodes), 'Portals' (listing to_MB_portal, disabled from_MB_portal, api_test_resource, and GOST), and 'Resources' (listing web / (/)).

Сертификация

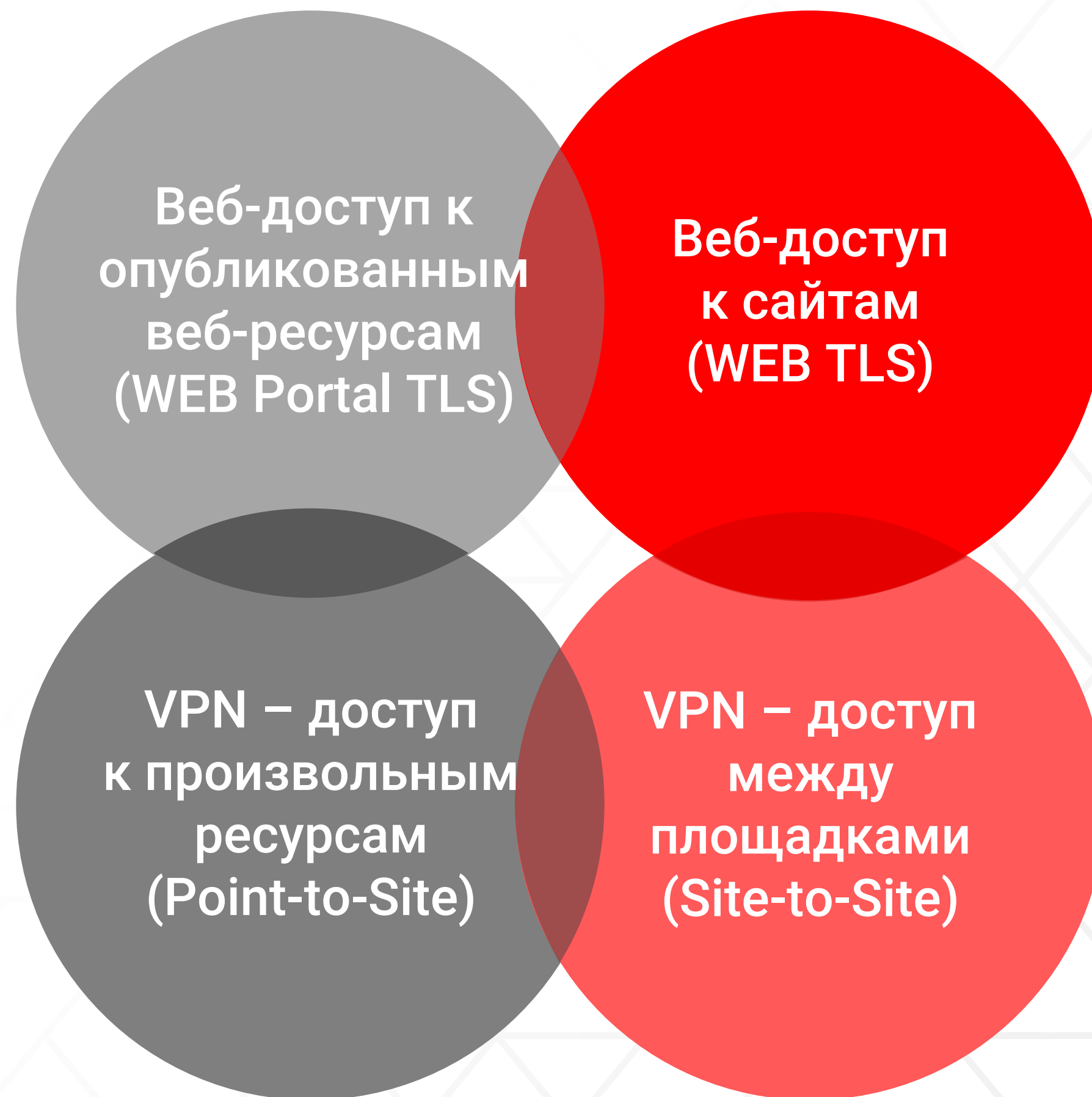
Соответствие требованиям регуляторов и ГОСТ.

Компоненты решения сертифицированы ФСБ России по классам КС1, КС2, КС3 и используют в своем составе сертифицированное ФСБ России СКЗИ КриптоПро CSP с российскими криптографическими алгоритмами ГОСТ 28147-89, ГОСТ Р 34.11-94/ГОСТ Р 34.11-2012, ГОСТ Р 34.10-2001/ГОСТ Р 34.10-2012.

При этом для классов КС2 и КС3 не требуется выполнение отдельных настроек, приобретение и конфигурирование электронных замков и прочих дополнительных мер защиты, все необходимое уже включено в аппаратные платформы решения.



Четыре типа доступа NGate



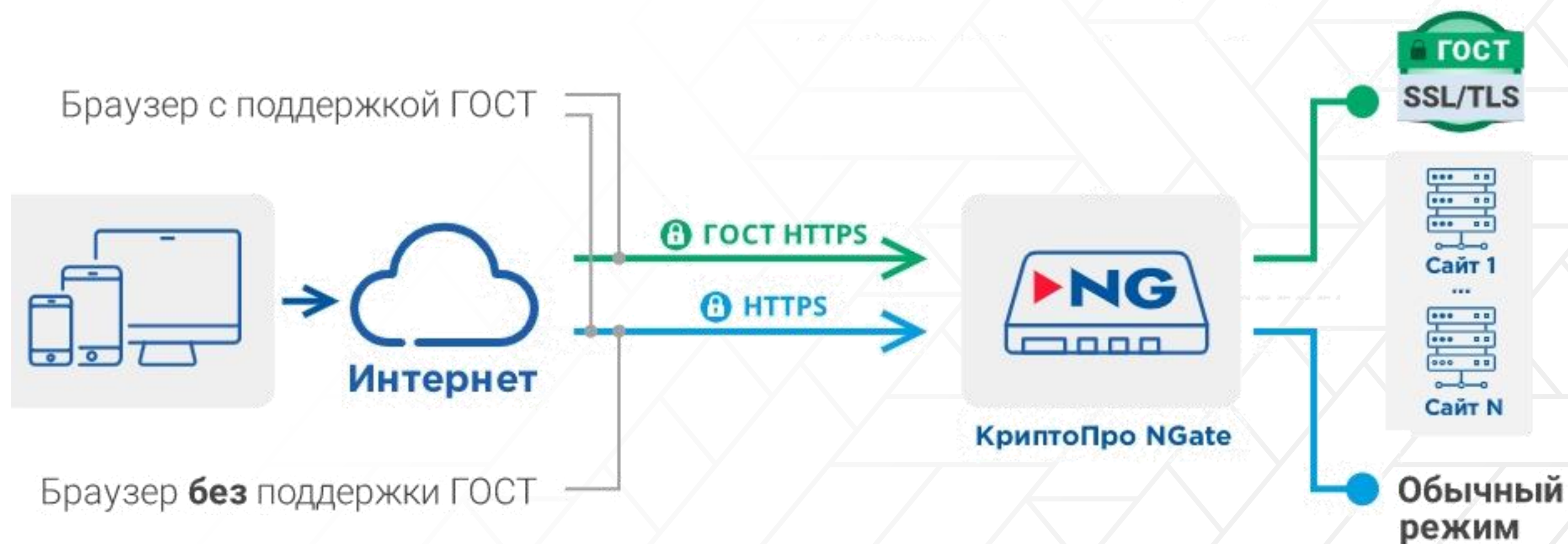
Замена Cisco AnyConnect



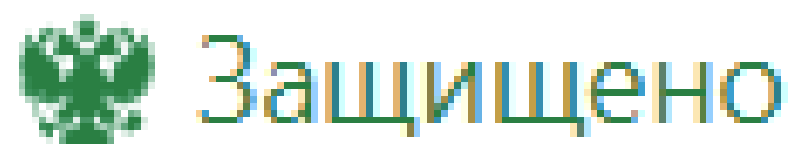
Постепенный переход на ГОСТ TLS

2022 – Отозваны сертификаты ВТБ, ЦБ, ПСБ, Минобороны

2022 – Прекращена выдача сертификатов для Рунета со стороны УЦ Sectigo (бывш. Comodo), DigiCert, Thawte, Rapid, GeoTrust



Поддержка ГОСТ TLS на веб-сайтах



<https://gosuslugi.ru> – ЕПГУ

<https://www.mos.ru> – госуслуги Москвы

<https://lkul.nalog.ru> – личный кабинет налогоплательщика (юрлица)

<https://eruz.zakupki.gov.ru/auth/> – единая ИС в сфере закупок

<https://agregatoreat.ru> – единый агрегатор торговли (по 44-ФЗ)

<https://cryptopro.ru> – сайт КриптоПро

NGate Site-to-Site VPN



VPN-доступ по стандартному протоколу IPSec



Совместимость с IPSec VPN-продуктами других вендоров



Возможность интеграции с отечественными FW



Контакты:

🏠 0ЭЗ «Иннополис», 422616, Республика Татарстан, Лаишевский район, с. Усады, ул. Дорожная, д. 42, к. 2

☎ +7 800 333 98 70

🌐 icl-services.com

✉ pr@icl-services.com

