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

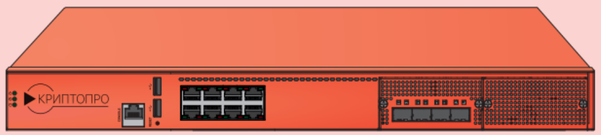
Класс криптографической защиты	КС1, КС2, КС3
Основное назначение	Узел NGate

	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 × 630x 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 ºС рабочая температура –20 – +70 ºС хранение	Параметры питания	
Влажность (RH)	5 – 90 % рабочая влажность 5 – 95 % хранение	Тип / мощность	650 Вт ATX резервный PSU
		Характеристики	AC 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 ºС рабочая температура –20 – +70 ºС хранение	Параметры питания	
Влажность (RH)	5 – 90 % рабочая влажность 5 – 95 % хранение	Тип / мощность	300 Вт + ATX резервный PSU
		Характеристики	AC 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

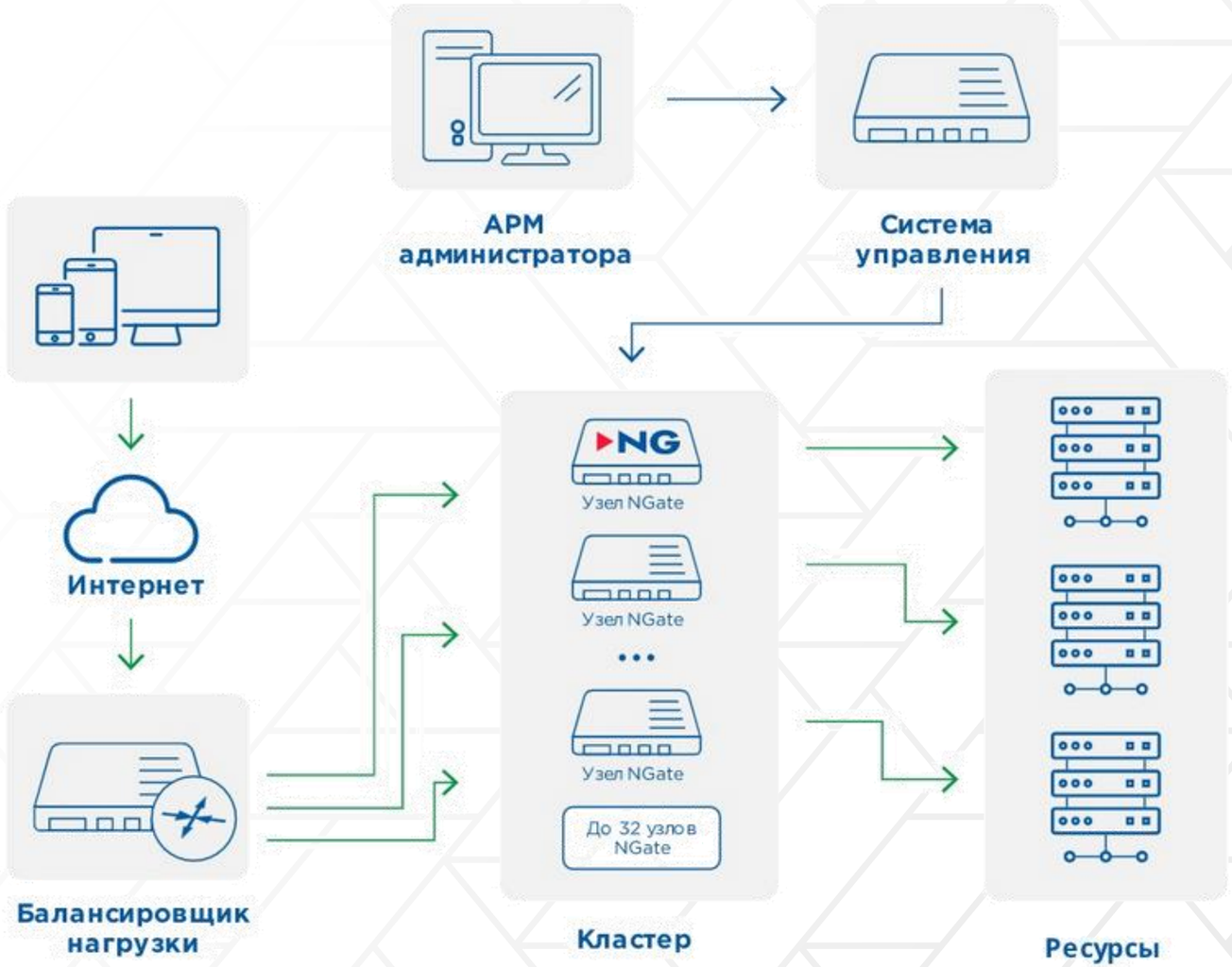
Охлаждение		Размеры при эксплуатации	
Процессор	CPU радиатор	(ДхШхВ) / Вес	438 × 525× 44,45 (1U) мм / 15 кг
Система	4 вентилятора охлаждения	Размеры в упаковке	
Параметры окружающей среды		(ДхШхВ) / Вес	790× 600 × 220 мм / 16 кг
Температура	0 – +40 ºС рабочая температура –20 – +70 ºС хранение	Параметры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

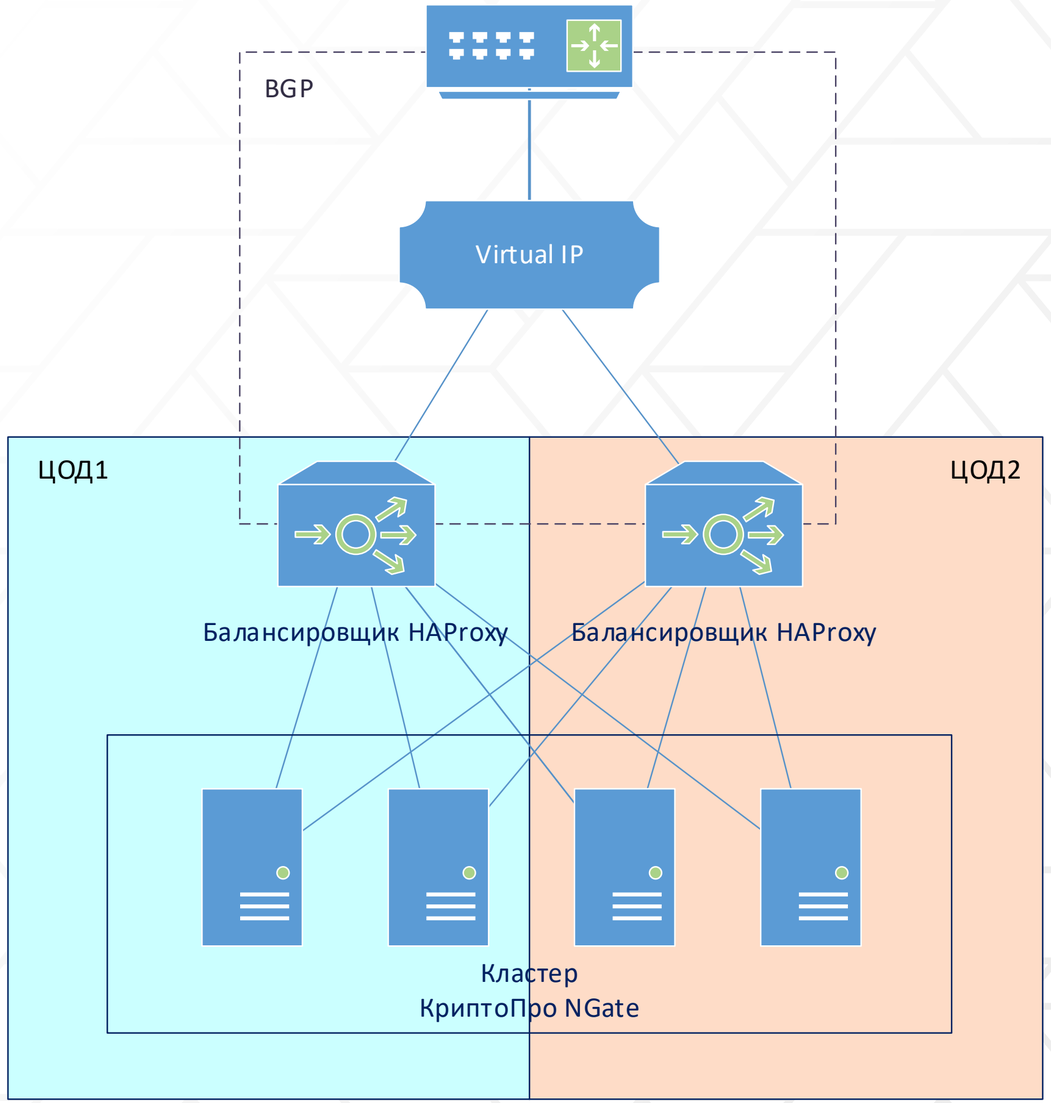
Узлы NGate в кластере управляются при помощи Системы управления системой NGate.



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 портального 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.

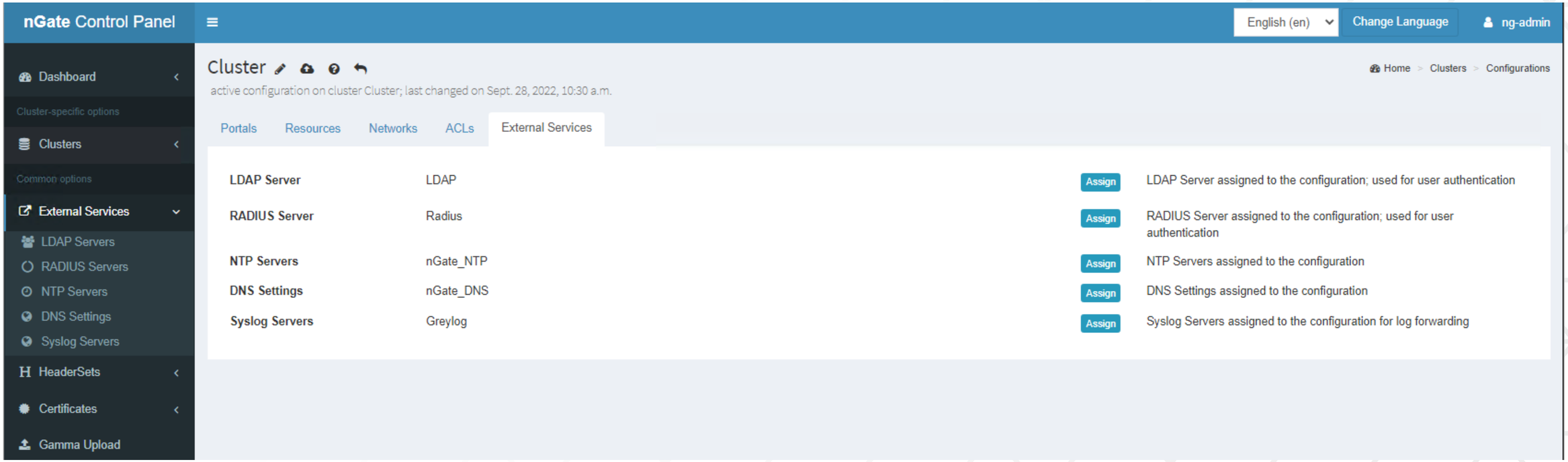
VPN-сервер

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

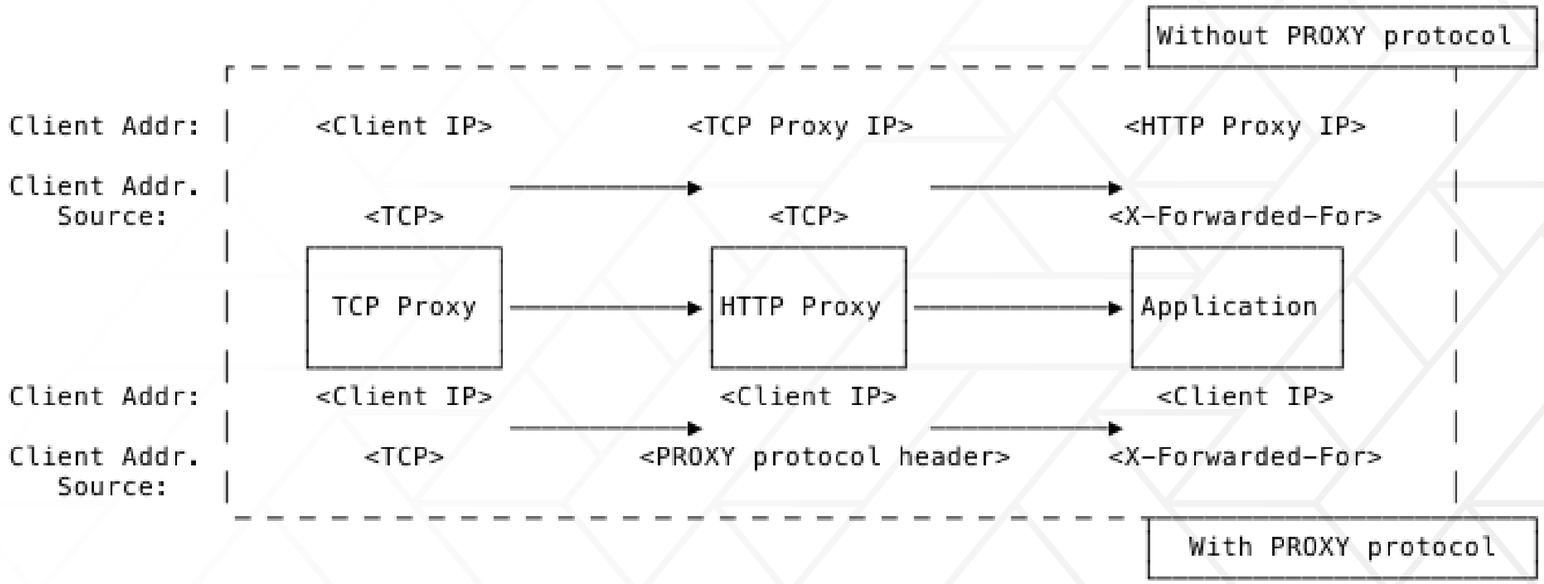
Список доступных внешних служб можно увидеть (и настроить) как в особом разделе веб-интерфейса, так и на вкладке выбранной конфигурации кластера. Но во втором случае будут отображены только те системы и серверы, которые настроены для конкретного кластера.



Поддержка Proxy протокола

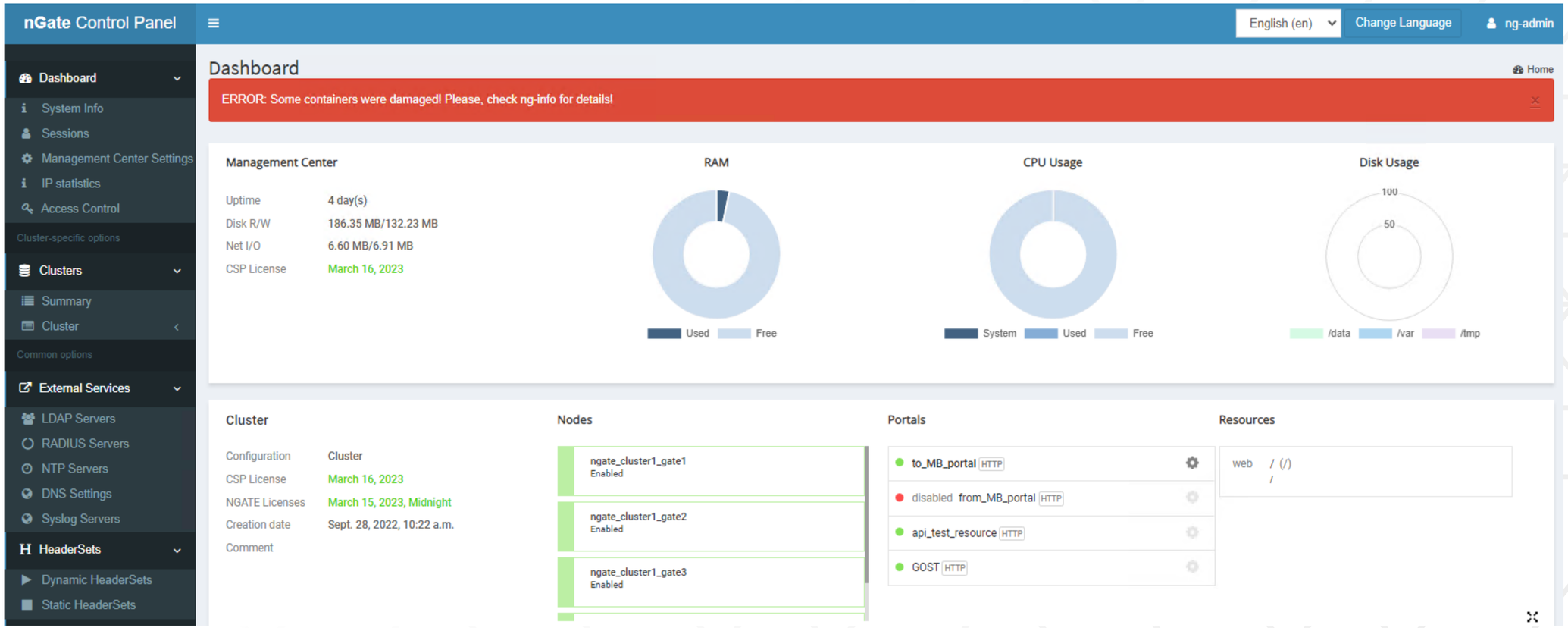
Цель протокола PROXY состоит в том, чтобы позволить TCP-прокси, работающим на транспортном уровне (уровень 4 модели OSI), вводить данные об исходных адресах источника и назначения на свои вышестоящие серверы без знания базового протокола.

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.



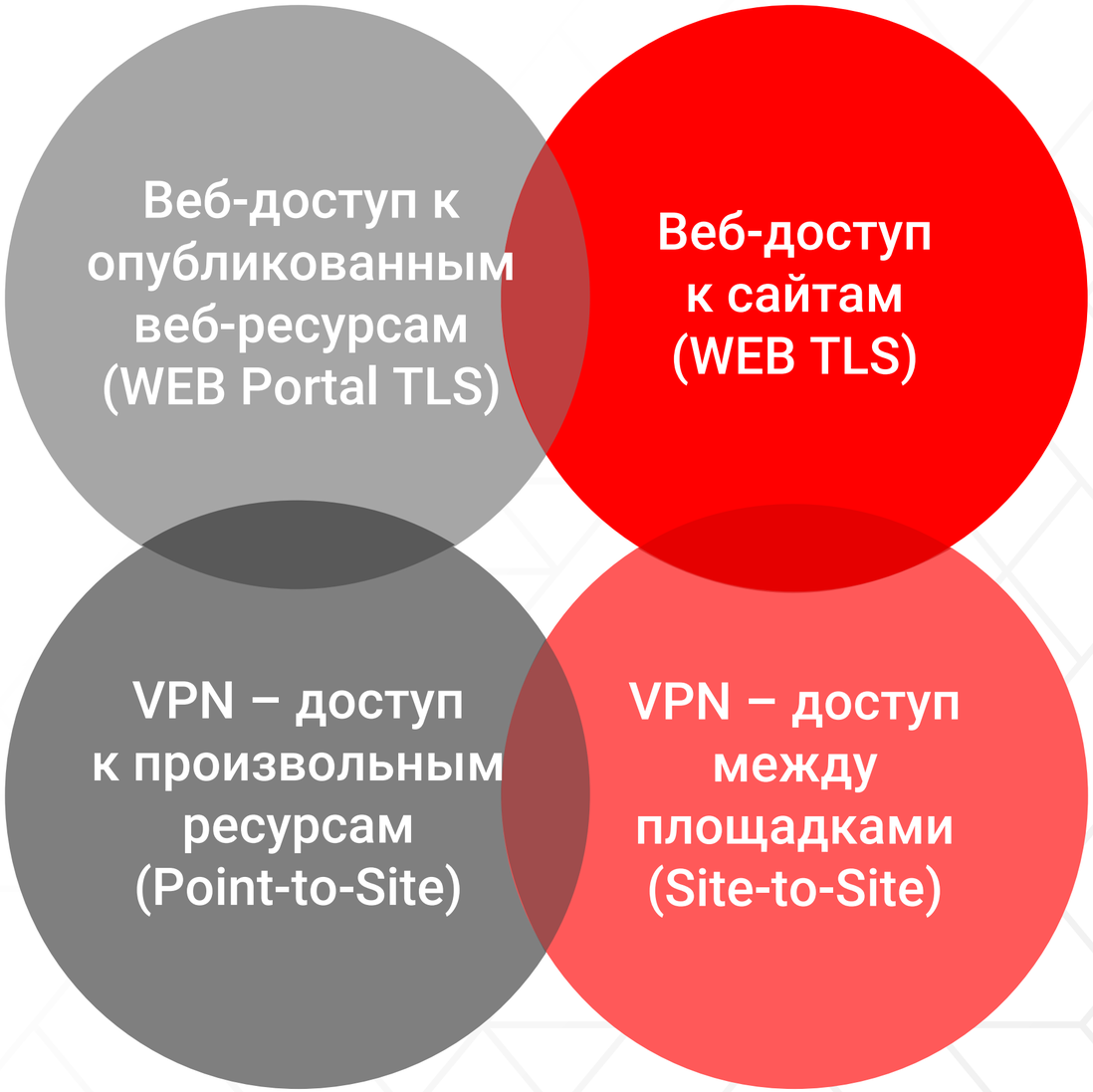
Сертификация

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

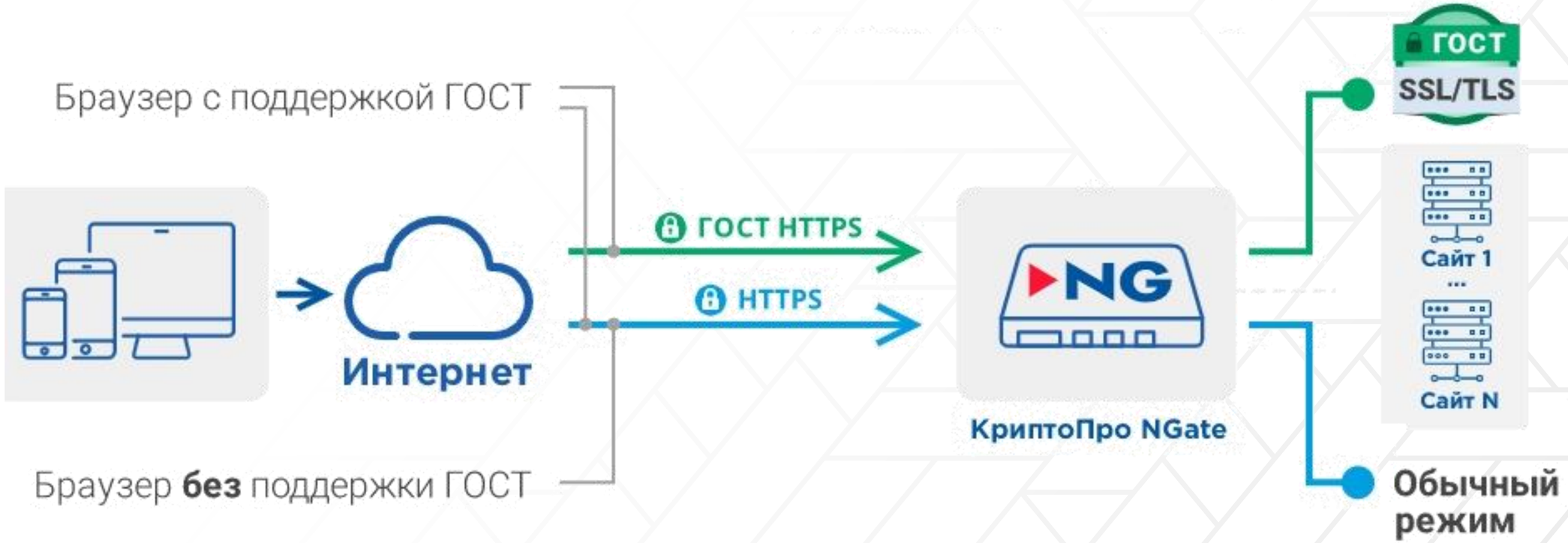


Замена Cisco AnyConnect

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

Защищено

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:

ОЭЗ «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