**НАЦИОНАЛНА ЗДРАВНООСИГУРИТЕЛНА КАСА**

* ***София 1407, ул. “Кричим” No 1*** [***www.nhif.bg***](http://www.nhif.bg) ***тел: +359 2 9659121***

**Приложение № 1**

**ТЕХНИЧЕСКИ ИЗИСКВАНИЯ И УКАЗАНИЯ КЪМ**

**ИЗПЪЛНЕНИЕТО**

**„СИСТЕМА ЗА ЗАЩИТА, ОПТИМИЗАЦИЯ И УСКОРЯВАНЕ НА УЕБ ПРИЛОЖЕНИЯ“**

Дата: .....................

гр. ........................................ Подпис:....................................

**ТЕХНИЧЕСКИ ИЗИСКВАНИЯ И УКАЗАНИЯ КЪМ**

**ИЗПЪЛНЕНИЕТО**

**СИСТЕМА ЗА ЗАЩИТА, ОПТИМИЗАЦИЯ И УСКОРЯВАНЕ НА УЕБ ПРИЛОЖЕНИЯ**

## Цел на проекта

Целта на проекта за внедряване на система за защита, оптимизация и ускоряване на уеб приложения, предоставяни от НЗОК се диктува от изискванията на потребителите за бърз достъп до данни и ресурси и все по-голяма нужда от мерки срещу различни видове атаки, целящи компрометиране на уеб услуги. За да се изпълнят тези нужди и изисквания, трябва да се внедрят различни практики и решения, като подобряване сигурността на програмния код на приложенията, бързина и надеждност на предоставяните ресурси, както и достъпност от различни типове устройства (мобилни телефони, таблети, компютри). За да се реализира това в кратки времеви рамки и за да се ускори и опрости процеса на управление на измененията (change management) са нужни определен тип решения, предоставящи възможности, които не изменят логиката и данните на приложенията, но същевременно ги правят по-надеждни, лесно управляеми и предсказуеми по отношение на работоспособност. Това решение трябва да се постигне с устройства за управление на приложения (Application Delivery Controllers), които предоставят голям набор от функции, с чиято помощ биха могли да се реализират горните изисквания.

## Нужна функционалност

По-долу са изброени различните типове функционалност, които са нужни за да се изпълни целта на проекта:

## Балансиране на натоварването (Load Balancing)

Балансирането на натоварването трябва да разпределя заявките между няколко сървъра, поддържащи приложения. Достъпът до тези приложения трябва да може да става с различни протоколи, част от слоеве 4 до 7 на OSI модела. Поради различните специфики и изисквания на съвременните уеб и други приложения методите за избор на сървър (методи за балансиране на натоварването) трябва да включват различни параметри идващи, както от клиентите, така и от самите сървъри.

## Наблюдение на приложенията

За да се изпълнят все по-високите изисквания за надеждност на съвременните услуги, наблюдението на приложенията трябва да се извършва не само чрез тестване достъп до даден сървър, но и тестване на различни параметри на самото приложение и дори очакване на точно определен отговор при пускане на заявка. Съответно, при отпадане на един сървър или услуга трябва да може всички клиентски заявки да се пренасочат към все още работещ сървър, поддържащ даденото приложение.

## Балансиране на натоварването според желаното съдържание (Content Switching)

Приложенията в НЗОК са много динамични и потребителите трябва да получат възможност всички ресурси да се достъпват от едно място и чрез единен интерфейс. Различните ресурси се предоставят от различни ферми с приложения. За да се обединят различните приложения е нужна възможността за разпределяне на натоварването между отделни ферми от сървъри на база различни параметри идващи от страна на клиентите, като тип браузър, тип устройство, локация, нужен ресурс/приложение.

## Криптиране и сигурност на трафика

Поради чувствителността на данните в НЗОК трябва да се изключат напълно възможностите за компрометиране на данните идващи от и към приложенията. Данните трябва задължително да бъдат криптирани с подходящите алгоритми и стандарти. Същевременно, сървърите, обслужващи клиентите и предоставящи им нужните данни и ресурси трябва да са минимално натоварени, за да могат да обработят и предадат максимално бързо данните към потребителите. Това налага изнасяне на процеса на криптиране в устройството за балансиране на натоварването. Това трябва да води до намаляване на товара върху приложните сървъри и да ускорява предоставянето на данните.

## Манипулация на съдържанието

Дадено приложение чест се налага да бъде променено в програмната си част за да може да предостави определен тип съдържание на определен тип потребител и за определен период от време. Усложняването на този процес по управление на измененията и удължаването на срока за пускане в експлоатация на нужната функционалност трябва да се преодолява и ускорява с устройството за предоставяне на приложение, без да се променя логиката на приложението и произтичащите от този процес възможности за грешки и задължително време за тестване.

## Компресия на съдържанието

Съвременните браузъри предоставят възможност за разпознаване на компресирана информация и автоматичното ѝ декомпресиране в четим и прегледен вид. Съответно все повече сървъри за уеб приложения, позволяват компресиране на тази информация. Целта на проекта е да се избегнат ограниченията на мрежовата инфраструктура и данните да стигнат по-бързо до клиента. Поради факта, че това води до по-голямо натоварване на сървърите този процес трябва да се извършва от устройство балансиращо натоварването им.

## Сигурност и защита от атаки

От особена важност за сигурността на НЗОК е защита и изключване на възможността за най-популярния тип хакерска атака – Denial of Service (DoS). За да се предпазят сървърите от тази атака, тя би трябвало да се спре още преди злонамерените заявки да ги достигнат. Тъй като този тип атака има различни разновидности, методите за засичането ѝ и ефективното отблъскване трябва да са различни - от изпращане на SYN-cookies до използване на черни списъци с IP адреси.

## Възможност за добавяне на функционалност чрез закупуване на лицензи

За да се посрещат нарастващите бъдещи нужди на НЗОК и за оптимизиране на бюджетните й разходи предложената система трябва да има възможност за добавяне на функционалности. В допълнение тази възможност ще осигурява добавяне на функционалност, която липсва в текущо работещия пакет, при възникване на такава нужда в НЗОК.

**2. СПЕЦИФИКАЦИЯ НА ИЗИСКВАНИЯТА**

2.1 Предложеното решение трябва да отговаря на следните минимални и задължителни изисквания, специфицирани в *Табл. №1:*

*Табл. №1*

|  |  |
| --- | --- |
| **Общи Данни** | Изискване |
| Производител/Марка |  |
| Серия и модел |  |
| Лицензи |  |
| Количество | 1 |
| **Физически параметри** |  |
| Възможност за монтиране в стандартен 19-инчов сървърен шкаф (IEC 60297) | Задължително |
| Да е съвместим с Директива 2002/95/EC (RoHS) на ЕС | Задължително |
| Брой независими електрически захранвания | Минимум 2 |
| Ethernet портове (интерфейси) | Минимум 8 |
| Поддръжка на 1000BASE-X SFP | Задължително |
| **Производителност** |  |
| Обща мрежова пропускливост | Минимум 1Gbps |
| Обработка на минимален брой HTTP заявки в секунда | Минимум 100000 |
| Обработка на минимален брой SSL заявки в секунда (използвайки сертификат с 2048-битов ключ) | Минимум 3000 |
| Мрежова пропускливост при използване на SSL | Минимум 1 Gbps |
| Възможност за увеличаване производителността чрез закупуване на лиценз, без нужда от добавяне на ново устройство или замяна на текущото | Задължително |
| **Функционалност** |  |
| Възможност за работа на две устройства в режим активно/пасивно с цел резервираност | Задължително |
| Възможност за агрегиране на мрежови портове с цел резервираност и увеличаване на производителността (Link Aggregation) | Задължително |
| Поддръжка на VLANs | Задължително |
| Поддръжка на IPv4 и IPv6 | Задължително |
| Възможност за използване на устройството като маршрутизатор | Задължително |
| Възможност за управление както чрез уеб-базирана система, така и чрез Command Line Interface (CLI) | Задължително |
| Възможност за управление на контрола на достъпа чрез използване на LDAP протокол и сървър (LDAP based Authentication) | Задължително |
| Възможност за администрация, базирана на роли | Задължително |
| Поддръжка на 1024 и 2048 битово криптиране на трафика идващ от клиентите и към тях, с цел оптимизиране на ресурсите на сървърите, обслужващи даденото приложение (SSL Offload) | Задължително |
| Поддръжка на следните протоколи при дефиниране на услугите, които се предоставят: -DNS; -FTP; -HTTP; -RDP; -SIP-UDP; -SSL; -TCP; -UDP; | Задължително |
| Възможност за разпределяне на натоварването между отделни сървъри (ферми), предоставящи приложения (Layer 4-Layer 7 Load Balancing) | Задължително |
| Възможност за разпределяне на натоварването между отделни ферми от сървъри предоставящи приложения, на база различни параметри на клиентите (Layer 7 Content Switching) | Задължително |
| Да се поддържат следните механизми за балансиране на натоварването между отделните сървъри, поддържащи приложения:  -Най-малко сесии;  -Най-малко време за отговор;  -Дефинирана "тежест" на отделен сървър;  -Hash стойност на клиентски IP адрес, MAC адрес и други;  -Разлчини параметри на сървърите, следени чрез SNMP; | Задължително |
| Възможност за поддържане на постоянни сесии от даден клиент към определен сървър, поддържащ приложение (Persistence) | Задължително |
| Възможност за предоставяне на клиентския IP адрес и други негови атрибути към сървърите, обслужващи приложенията | Задължително |
| Възможност за наблюдение работоспособността на сървърите чрез използване на следните типове проби/монитори:  -TCP; -UDP; -ICMP(Ping) -TCP Port Based (проба за наличие на определн тип приложение на даден мрежови порт); -HTTP/S; -Проба за получаване на точно определен отговор при пускане на HTTP заявка; | Задължително |
| Възможност за пренасочване на трафика към друга услуга или сървър при отпадане на всички сървъри в дадена ферма | Задължително |
| Възможност за мултиплексиране на сесиите, идващи от клиентите към сървърите с цел оптимизиране на трафика и производителността (TCP Multiplexing) | Задължително |
| Възможност за буфериране на TCP заявките (TCP Buffering) | Задължително |
| Възможност за защита от Denial of Service (DoS) атаки чрез използване на SYN-Cookies (Layer 4 DoS protection) | Задължително |
| Възможност за филтриране (прекъсване, пренасочване, добавяне на хедър) достъпа до услуга или уеб страница на дадено приложение на база различни параметри (IP адрес на клиента, стойности на различни HTTP хедъри, мрежови интерфейс) | Задължително |
| Възможност за компресиране на отговора (Response) идващ от сървърите, поддържащи приложенията на база тип съдържание (txt, javascript, xml) чрез използване на различни методи (GZIP, DEFLATE) | Задължително |
| Поддръжка на AppFlow протокол | Задължително |
| Възможност за изпращане на логовете на устройството към SysLog сървър | Задължително |
| Възможност за промяна на отговора (Response) идващ от даден уеб сървър към клиент, на база различни параметри на клиента (URL адрес, IP адрес на клиента, стойности на различни HTTP хедъри) | Задължително |
| Възможност за промяна на заявката (Request) идваща от даден клиент към приложение, на база различни параметри на клиента (URL адрес, IP адрес на клиента, стойности на различни HTTP хедъри) | Задължително |
| Възможност за добавяне на функционалност чрез закупуване на допълнителен лиценз, без нужда от преинсталация на устройството или добавяне на ново такова | Задължително |

2.2. Инсталирането и гаранционната поддръжка да включва:

* Изпълнителят трябва да инсталира, конфигурира и извърши настройка на предложената система, според нуждите и изискванията на НЗОК.
* За срока на договора ИЗПЪЛНИТЕЛЯТ се задължава да оказва техническа помощ и сервизна поддръжка на инсталираната система и да осигурява изискваната функционалност. Това трябва да става по телефон или на място при ВЪЗЛОЖИТЕЛЯ.
* ИЗПЪЛНИТЕЛЯТ се задължава да осигурява висококвалифицирана специализирана помощ, включително и на място при констатирани от ВЪЗЛОЖИТЕЛЯ проблеми.
* В случай на възникнали и констатирани от ВЪЗЛОЖИТЕЛЯ технически проблеми ИЗПЪЛНИТЕЛЯТ се задължава да реагира до 4 (четири) часа след заявка в рамките на работното време на НЗОК, както и да отстрани проблема до 8 (осем) работни часа.

2.3 Място на изпълнение на поръчката – ЦУ на НЗОК.

2.4 Срок за изпълнение на поръчката:

2.4.1 За инсталира, конфигурира и настройка **-** 15 работни дни, считано от датата на подписване на договора.

2.4.2 За гаранционна поддръжка съгласно т.2.2. – една година считано от датата на подписване на договора