

ТЕХНИЧЕСКИ ИЗИСКВАНИЯ И СПЕЦИФИКАЦИИ

I. Цел на възлагането на обществената поръчка:

Основната цел на възлагането на поръчката е изграждане на виртуална частна мрежа (ВЧМ) между 28 Районни здравноосигурителни каси (РЗОК), 68 офиса и Централно Управление (ЦУ) на НЗОК и осигуряване на достъп до Интернет за нуждите на Националната здравноосигурителна каса (НЗОК) за срок от три години.

Изграждането на единна комуникационна среда и предоставяне на гарантиран достъп до Интернет следва да осигури:

- Информационна свързаност на всички структурни единици в НЗОК и възможност за добавяне на нови;
- Онлайн достъпни услуги за подразделенията/структурите и клиентите на НЗОК;
- Осигуряване на съвременна комуникационна инфраструктура;
- Възможност всички структурни единици на НЗОК да работят в единна мрежа;
- Възможност за подразделенията/структурите на НЗОК да имат достъп до общ сървърен ресурс и софтуерни приложения;
- Високо ниво на мрежова сигурност. Защита на мрежата, потребителите и приложенията от външни и вътрешни атаки;
- Възможност за лесна промяна на параметри на услугите. Скалируемост;
- Гъвкавост на структурата – възможност за бързо разширяване обхвата на мрежата чрез включване на нови подразделения/структури и преместване на съществуващи такива на НЗОК;
- Комуникация в реално време между офисите и подразделенията на НЗОК;
- Единна среда за пренос на данни за всички съществуващи и бъдещи подразделения/структури и услуги на НЗОК.

II. Общи изисквания към предоставяните услуги:

Да се изгради и поддържа за срока на договора единна комуникационна среда, базирана на национална MPLS и MAN мрежи в страната, което ще осигури информационна свързаност между всички подразделения/структури на НЗОК на територията на страната, независимо от тяхното разположение и ще предостави гарантиран достъп до Интернет в НЗОК.

Предоставяните услуги по достъп до интернет за нуждите на Националната здравноосигурителна каса и изграждането на виртуална частна мрежа между 28 РЗОК, 68 офиса и ЦУ на НЗОК, следва да отговарят на параметри, както следва:

1. Доставка на Интернет капацитет в ЦУ на НЗОК:
 - 1.1. Български Интернет трафик – 500 Mbps.
 - 1.2. Международен Интернет трафик – 100 Mbps.
2. Подсигуряване на резервна връзка между ЦУ на НЗОК и комуникационния център на доставчика в гр. София и осигуряване на механизъм за временно преключване към нея при отпадане на връзката по главното трасе.
3. Изграждане на Виртуална частна мрежа (ВЧМ) между:

3.1.26 (двадесет и шест) РЗОК и ЦУ на НЗОК с капацитет на каналите съгласно Приложение № 3 към документацията на поръчката;

3.2. РЗОК София-град, РЗОК София-област и ЦУ на НЗОК с капацитет на канала съгласно Приложение № 3 към документацията на поръчката.

4. Изграждане на Виртуална частна мрежа (ВЧМ) между:

4.1. 62 (шестдесет и два) офиса на РЗОК по приложен списък и ЦУ на НЗОК с терминиране в съответните РЗОК, на които йерархично се подчиняват и с капацитет на каналите от по 20 Mbps;

4.2. 5 (пет) офиса на РЗОК София- град в гр. София по приложен списък и ЦУ на НЗОК с терминиране в РЗОК София-град, на който йерархично се подчиняват и с капацитет на каналите от по 20 Mbps;

4.3.1 (един) офис на ЦУ на НЗОК по приложен списък и ЦУ на НЗОК с капацитет на каналите от по 20 Mbps.

5. Осигуряване на самостоятелни канали за трафик на данни с капацитети от по 20 Mbps всеки за нуждите на Интегрираната информационна система на НЗОК, като тези канали следва да бъдат включени във Виртуалната частна мрежа между 28 РЗОК и ЦУ на НЗОК и да бъдат част от капацитетите на каналите, посочени в т. 3 по-горе.

6. Поддържане и конфигуриране на комуникационно оборудване комуникационно оборудване в сградите на НЗОК и РЗОК, състоящо се от маршрутизатори до ниво LAN интерфейс към вътрешната мрежа на съответното подразделение в структурата на НЗОК съгласно т. V от настоящите Технически изисквания и спецификации.

7. Предоставяне на система за онлайн 24/7/365 наблюдение и поддръжка на мрежата на НЗОК.

III. Специфични технически изисквания по предоставяне на услугите.

1. Изисквания към Участниците:

1.1. Участниците следва да притежават сертификация по EN ISO 27001:2005 система за информационна сигурност или еквивалентна. За удостоверяване на това обстоятелство участниците следва да представят към Техническото си предложение заверено копие на валиден сертификат за система за информационна сигурност по стандарт EN ISO 27001-2005 или еквивалентен.

1.2. Участниците следва да притежават сертификация по EN ISO 20000-1:2011 система за управление на електронните услуги или еквивалентна. За удостоверяване на това обстоятелство участниците следва да представят към Техническото си предложение заверено копие на валиден сертификат за система за управление на електронните услуги по стандарт EN ISO 20000-1 :2011 или еквивалентен.

Забележка: Сертификатът за система за информационна сигурност по стандарт EN ISO 27001-2005 и сертификатът за система за управление на електронните услуги по стандарт EN ISO 20000-1 :2011 трябва да са валидни и да са издаден от независими лица, които са акредитирани по съответната серия европейски стандарти от Изпълнителна агенция "Българска служба за акредитация" или от друг национален орган по акредитация, който е страна по Многостранното споразумение за взаимно признаване на Европейската организация за акредитация, за съответната област или да отговаря на изискванията за признаване съгласно чл. 5а, ал. 2 от Закона за националната акредитация на органи за оценяване на съответствието. Възложителят приема еквивалентни сертификати, издадени от органи, установени в други държави членки.

Възложителят приема и други доказателства за еквивалентни мерки за осигуряване на качеството, когато участник не е имал достъп до такива сертификати или е нямал възможност да ги получи в съответните срокове по независещи от него причини. В тези случаи участникът трябва да е в състояние да докаже, че предлаганите мерки са еквивалентни на изискваните.

1.3. Участниците следва да разполагат с техническа поддръжка 7x24x365, helpdesk (дежурство за помощ), работеща trouble ticket (съобщение за проблеми) система и ясна схема за реакция и своевременно отстраняване на възникнали проблеми.

Във връзка с горното, в техническите предложения за изпълнение на поръчката участниците следва да посочат и опишат по какъв начин, по силата на каква процедура и за колко време в случай на необходимост екипът на helpdesk (дежурство за помощ) може да получи съдействие и да ескалира за решаване проблем към специалиста, отговорен за имплементацията на цялостното решение, предмет на настоящата поръчка.

1.4. Участниците следва да са регистрирани от RIPE NCC (<http://www.ripe.net>) като LIR (Local Internet Registry) със собствена/и автономна/и система/и опериращо адресно пространство от минимум 600 000 IPv4 адреса - посочва се линк и се прилага разпечатка от сайта на RIPE за номер на автономна/и система/и и адресни блокове - IPv4.

Във връзка с горното, в техническите предложения за изпълнение на поръчката участниците следва да посочат номер на автономна система и IP блокове.

1.5. Участниците следва да поддържат динамична маршрутизация (BGP4 протокол) по външните и вътрешните си канали.

1.6. Участниците следва да притежават поне два независими наземни двупосочни международни канала за достъп до Интернет, опериращи автономно, с общ сумарен симетричен капацитет минимум 70 Gbps.

Във връзка с горното, в техническите предложения за изпълнение на поръчката участниците следва да представят описание на връзките, скоростите и статистика на работоспособността им за последната година.

1.7. Участниците следва да предоставят възможност за наблюдение на горепосочените връзки през http – looking glass с възможност за ping, traceroute, BGP summary и др..

2. Специфични изисквания към предоставянето на услугите:

2.1. Доставка на Интернет капацитет в ЦУ на НЗОК

2.1.1. Доставката на Интернет трафик да става през 1Gbps оптична връзка от MAN мрежа на изпълнителя в гр. София до сградата на ЦУ на НЗОК.

2.1.2. Оптичната връзка се изгражда за сметка на изпълнителя.

2.1.3. Международният Интернет трафик до точката в MAN мрежата на изпълнителя в гр. София да се доставя по симетрична наземна оптична кабелна свързаност.

2.1.4. За времето на договора изпълнителят се задължава да поддържа домейн "nhif.bg".

2.1.5. Максимално закъснение при доставка на Интернет до първия POP Trier на изпълнителя - не повече от 50 ms.

2.1.6. Минимално ниво на достъпност на услугата - не по-малко от 99,8 % на годишна база.

2.1.7. Да се осигури възможност за предоставяне графична статистика на натоварването и използването на международен и български трафик.

2.1.8. Да се осигури възможност скоростите на трафика да се преразглеждат и при необходимост да бъдат увеличавани, но не повече от 3 % от договорената стойност,

при запазване размера на месечните плащания.

2.1.9. Да се предоставят 254 публични адреси от мрежа клас А с маска 255.255.255.0 от адресното пространство на изпълнителя.

2.2. Изграждане на резервна връзка между ЦУ на НЗОК и комуникационния център на доставчика в гр. София и изграждане на механизъм за временно превключване към нея при отпадане на връзката по главното трасе.

2.2.1. Резервната връзка да се изгради чрез оптична цифрова свързаност през MAN мрежата на второ алтернативно трасе, изцяло различно от първото, в гр. София и да покрива капацитета на основната линия от сградата на ЦУ на НЗОК до комуникационния център на изпълнителя.

2.2.2. Резервната връзка по т. 2.2.1. при необходимост се изгражда за сметка на изпълнителя, но от името на НЗОК

2.2.3. Резервната връзка физически да не минава по трасето на основните оптични връзки и да се терминира в различен POP на съответния оператор.

2.2.4. Превключване към резервната връзка при отпадане на основните оптични връзки да става автоматично. Механизмът за превключване между основна и резервна връзка е решение на изпълнителя.

2.3. Изграждане на Виртуална частна мрежа

2.3.1. Изграждане на Виртуална частна мрежа (ВЧМ) между 26 РЗОК и ЦУ на НЗОК.

2.3.1.1. ВЧМ да бъде MPLS базирана с топология full mesh, с капацитет на основните връзки съгласно Приложение № 3 към документацията на поръчката, с криптиран трафик за всяка VPN връзка между 26 РЗОК и ЦУ на НЗОК.

2.3.1.2. Капацитета на основните връзки между РЗОК София-град, РЗОК София-област и ЦУ на НЗОК да бъде 100 Mbps.

2.3.1.3. Капацитета на резервните връзки следва да бъде 80 Mbps за всяка от 26 РЗОК и 80 Mbps за РЗОК София-град и РЗОК София-област.

2.3.1.4. Връзката с ЦУ на НЗОК да става през 10 Gbps Ethernet наземна оптична кабелна свързаност от POP на доставчика в гр. София до сградата на ЦУ на НЗОК.

2.3.1.5. Оптичната връзка се изгражда при необходимост за сметка на изпълнителя, но от името на НЗОК.

2.3.1.6. Връзките до 26 РЗОК при необходимост се изграждат за сметка на изпълнителя и следва да бъдат по два броя – основна и резервна. Основните връзки следва да се изградят чрез наземни оптични кабелни свързаности. За резервните връзки няма такова изискване. Връзките до РЗОК София-град и РЗОК София-област се изграждат при необходимост за сметка на изпълнителя и следва да бъдат два броя – основна и резервна. Основната връзка следва да се изгради чрез оптична цифрова свързаност. За резервната по медия, осигуряваща гарантирана скорост.

2.3.1.7. При изграждането на основните и резервните връзки до РЗОК, изпълнителят да предвиди възможност за разширяване на капацитета им при условията на т.2.1.8. Превключване към резервната връзка при отпадане на основната връзка да става автоматично. Механизмът за превключване между основна и резервна връзка е решение на изпълнителя.

2.3.1.8. В изградената ВЧМ изпълнителят се задължава да спазва следните параметри:

2.3.1.8.1. Минимално ниво на достъпност на услугата - не по-малко от 99,8 % на годишна база.

2.3.1.8.2. Загуба на пакети (Packet loss) - не повече от 0,25 %

2.3.1.8.3. Максимално закъснение в едната посока между крайните устройства в

ЦУ на НЗОК, РЗОК София-град и РЗОК - не повече от 80 ms (Latency)

2.3.1.8.4. Неравномерност на отклонението във време-закъснението на IP пакетите (Jitter) - не повече от 40 ms.

2.3.1.9. Пропускателната способност в ЦУ на НЗОК през оптичната връзка да е не по-малка от сумата на пропускателните способности на връзките на всички РЗОК.

2.3.1.10. Технологията, използвана за изграждането на ВЧМ между 28 РЗОК и ЦУ на НЗОК трябва да осигурява разграничаването и задаването на приоритети на най-малко три различни типа IP трафик в мрежата на изпълнителя.

2.3.1.11. Осигуряване на самостоятелни канали за трафик на данни с капацитети от по 20 Mbps всеки за нуждите на единната интегрирана информационна система на НЗОК, като тези канали следва да бъдат включени във Виртуалната частна мрежа между 28 РЗОК и ЦУ на НЗОК и да бъдат част от капацитетите на каналите, които са с общ капацитет от 100 Mbps за РЗОК София-град и РЗОК София-област, а за останалите РЗОК съгласно Приложение № 3 към документацията на поръчката.

2.3.1.12. При изграждане на ВЧМ изпълнителят трябва да се съобрази задължително със схемата на вътрешната IP адресация на НЗОК, съгласно Приложение 2 към документацията на поръчката.

2.3.2. Изграждане на Виртуална частна мрежа (ВЧМ) между РЗОК София-град и 5 бр. офиси на РЗОК София-град в гр. София.

2.3.2.1. ВЧМ да бъде Layer2 базирана, с капацитет от по 100 Mbps за всяка VPN L2 ETHERNET.

2.3.2.2. Връзките с РЗОК София - град на НЗОК да стават през 100 Mbps Ethernet оптична свързаност от POP на доставчика в гр. София до сградата на РЗОК София - град.

2.3.2.3. Оптичната връзка по т. 2.3.2.2 се изгражда при необходимост за сметка на доставчика, но от името на НЗОК.

2.3.2.4. Връзките до 5 офиса на РЗОК София-град в гр. София се изграждат при необходимост за сметка на доставчика и следва да бъдат по един брой. Връзките следва да се изградят чрез оптични цифрови свързаности.

2.3.2.5. При изграждането на връзките до 5 офиса на РЗОК София-град в гр. София, доставчикът да предвиди възможност за разширяване на капацитета им съгласно т. 2.1.8.

2.3.2.6. В изградената Layer2 ВЧМ изпълнителят се задължава да спазва следните параметри:

2.3.2.6.1. Минимално ниво на достъпност на услугата - не по-малко от 99,8 % на годишна база.

2.3.2.6.2. Максимално закъснение в едната посока между крайните устройства в РЗОК София – град и 5 офиса на РЗОК София-град в гр. София - не повече от 80 ms (Latency).

2.3.2.7. Пропускателната способност в РЗОК София – град през оптичната връзка да е не по-малка от сумата на пропускателните способности на връзките на 5-те офиса на РЗОК София-град в гр. София.

2.4. Изграждане на Виртуална частна мрежа (ВЧМ) между 62 офиса на РЗОК по приложен списък и ЦУ на НЗОК с терминиране в съответната РЗОК.

2.4.1. ВЧМ да бъде IP VPN базирана с топология hub and spoke с hub-ове в съответните РЗОК, на които съответните офиси са йерархично подчинени spoke-ове, с капацитет на всяка spoke връзка съгласно Приложение № 3 към документацията на поръчката.

2.4.2. Връзката с ЦУ на НЗОК да става през 10 Gbps Ethernet оптична свързаност от POP на доставчика в гр. София до сградата на ЦУ на НЗОК.

2.4.3. Връзките до 62 офиса на РЗОК се изграждат при необходимост за сметка на изпълнителя.

2.4.4. При изграждането на връзките до 62 офиса на РЗОК, изпълнителят да предвиди възможност за разширяване на капацитета им при условията на т. 2.1.8.

2.4.5. В изградената ВЧМ изпълнителят се задължава да спазва следните параметри:

2.4.5.1. Минимално ниво на достъпност на услугата - не по-малко от 99,8 % на годишна база.

2.4.5.2. Загуба на пакети (Packet loss) - не повече от 0,25 %.

2.4.5.3. Максимално закъснение в едната посока между крайните устройства в ЦУ на НЗОК и офисите на НЗОК - не повече от 80 ms (Latency).

2.4.5.4. Неравномерност на отклонението във време- закъснението на IP пакетите (Jitter) - не повече от 40 ms.

2.4.6. Пропускателната способност в ЦУ на НЗОК да е не по-малка от сумата на пропускателните способности на връзките на 26-те РЗОК /без РЗОК София-град и РЗОК София-област/ и 62 офиса на РЗОК.

2.4.7. Технологиите, използвана за изграждането на ВЧМ трябва да осигурява разграничаването и задаването на приоритети на различни типове IP трафик в мрежата на доставчика.

2.4.8. С цел изграждане на ВЧМ, изпълнителят трябва да извърши конфигурация на всичките хардуерни устройства (маршрутизатори) в офисите на РЗОК. Типа и параметрите на устройствата са предоставени в т. V на настоящите технически изисквания и спецификации.

2.4.9. При изграждане на ВЧМ по т. 2.4. изпълнителят трябва да изготви схема на вътрешна IP адресация, като се съобрази със схемата на вътрешната IP адресация на НЗОК съгласно Приложение № 2 към документацията на поръчката за РЗОК и прилежащите им офиси.

2.4.10. Подновяване за срок от 3 години лицензите на съществуващите защитни стени тип Cisco ASA 5525-X в ЦУ на НЗОК.

2.5. Хардуерно криптиране на трафика в изградената ВЧМ.

- Минимална дължина на криптиращия ключ - 256 бита.

2.6. Статистика на мрежата и услугите

2.6.1. Да се предостави система за контрол на качествените параметри на основните типове трафик /необходимо е системата да известява при излизане на параметрите от дефинираните норми/.

2.6.2. Да се реализира централизирана система за събиране на статистика за предефинирани параметри, касаещи работоспособността на мрежата и услугите /SNTP collector, SNMP trap interpretation/.

2.6.3. Да се предостави система за събиране и анализ на трафика в реално време за предефиниран период.

2.6.4. Да се изгради система, визуализираща в общ план логическата топология на VPN мрежата и отчитаща статуса на всеки POP /свързаност, основна функционалност/.

2.6.5. Да се изгради система за съхранение на историята от промените по конфигурационните файлове на активното оборудване /дата и час на промяната и копие от променената конфигурация/.

3. Условия за поддръжка на системата

3.1. Участникът трябва да предложи Споразумение за ниво на техническо обслужване (Service Level Agreement - SLA) по отношение на предлаганата услуга,

което да включва:

3.1.1. Предлагащите от изпълнителя стойности по т.т. 2.1.5, 2.1.6, 2.3.1.8 и 2.4.5. и задължение за тяхното спазване.

3.1.2. Описание на trouble ticket (съобщение за проблеми) системата и схемата за реакция и отстраняване на възникнали проблеми.

3.1.3. Описание на нива на ескалация на проблеми и на начините, процедурите и времето, за което в случай на необходимост екипът на helpdesk (дежурство за помощ) може да получи съдействие и да ескалира за решаване проблем към специалиста, отговорен за имплементацията на цялостното решение, предмет на настоящата поръчка.

3.1.4. Ангажимент за незабавна реакция при заявен проблем.

3.1.5. Време за отстраняване на възникнал проблем – максимум до 4 /четири/ часа.

3.2. Поддръжката на комуникационното оборудване и предоставена свързаност е за срока на Договора. Срокът на поддръжката започва да тече от датата на успешното приключване на инсталацията, конфигурирането и тестването, които са удостоверени с окончателен приемо-предавателен протокол. Изпълнителят трябва да бъде напълно отговорен за всички гаранционни задължения за посочения период и да покрива обхвата на дейностите по сключения договор.

3.3. Поддържането следва да покрива:

- Конфигуриране и преконфигуриране на активното оборудване, обект на настоящите технически изисквания и спецификации и предоставената комуникационна свързаност и достъп до Интернет;

- Конфигуриране на възникнали функционални нужди, които са във възможностите на активното оборудване, собственост на НЗОК;

- Доставените 2 бр. опорни маршрутизатори с характеристики, отразени в т. IV настоящите технически изисквания и спецификации.

3.4. Всички сигнали за неизправности, дефекти и грешки да се предават на оторизирани служители на НЗОК и до екипа по поддръжка на изпълнителя по всяко време. Съобщенията се предават по телефон, факс, електронна поща или чрез автоматизираната система за on-line приемане и обработка на сервизни заявки на изпълнителя (ако изпълнителят разполага с такава система).

3.5. Типът на поддръжката за активното мрежово оборудване и осигуряване на преносна среда е 24 часа в денонощието, като в диапазона от 8 часа до 18 часа, в работните дни на седмицата, следва да има фиксирано време за отстраняване на неизправност до 4 часа.

3.6. В случай на невъзможност за отстраняване в рамките на 4 часа, изпълнителят трябва да осигури алтернатива, гарантирайки същата функционалност.

3.7. Изпълнителят осигурява непрекъснат мониторинг на всички устройства, изграждащи мрежата му, използвана за предоставяне на Единната комуникационна среда - наличие на национален център за управление и наблюдение на мрежата.

3.8. Доставка на резервни части, материали и консумативи, необходими за поддържането на комуникационното оборудване на НЗОК съгласно т. V. от настоящите технически изисквания и спецификации. Резервните части, материали и консумативи се заплащат отделно от Възложителя на доставни цени, след представяне на копие от фактурата доказваща цената им. Същите следва да бъдат нови и да отговарят на изискванията и приетите стандарти за качество в Република България .

Гаранционният срок по отношение на вложените резервни части - не по-малко от гаранцията на производителя.

При необходимост от влагане на резервни части при извършване на ремонтни дейности изпълнителят се задължава предварително да представи заявка за утвърждаване, съдържаща количествата, цените и доставчика или доставчиците (ако са няколко с различни цени и качество), и след утвърждаване се пристъпва към закупуването им.

3.8.1. Протоколиране на извършените ремонтни работи и вложените части, материали и консумативи:

Изготвя се двустранен констативен протокол за извършване на ремонт, който включва: вид за повредата, извършената работа, вложените резервни части, материали и консумативи, посочване на данните от фактурата за закупуването им, материали и консумативи, времетраене на извършените дейности.

4. Срокове за изпълнение и приемане в експлоатация на системата

4.1. Изпълнителят предоставя подробно описание на процедурите по стартиране на услугата във всеки град и предлага за съгласуване с НЗОК график за изпълнение в срок до 5 /пет/ работни дни след подписване на договора.

4.2. Изграждането и тестването на преносната среда трябва да се реализира в рамките на максимум до 30 /тридесет/ работни дни от датата на съгласувания с НЗОК график по т. 4.1, утвърден с двустранно подписан протокол.

4.3. Срок за пускане в експлоатация на услугите във всички обекти - не повече от 40 /четиридесет/ работни дни след подписване на договора.

4.4. При подписване на приемо-предавателен протокол за приемане в експлоатация от НЗОК на системата, изпълнителят предава на НЗОК:

- логическите схеми на изградената ВЧМ
- за устройствата, описани в раздел IV и раздел V: описание на извършените конфигурационни настройки, криптиращи ключове.

4.5. Изпълнителят ежесечно предоставя статистики по спазването на параметрите по т.т. 2.1.5, 2.1.6, 2.3.1.8 и 2.4.5.

5. Обучение

5.1. Изпълнителят следва да осигури за негова сметка обучение на 33 /тридесет и три/ служители на НЗОК, касаещо: управление, администриране и конфигуриране на маршрутизатори, както и запознаване с всички параметри, конфигурации и извършени настройки в изградената ВЧМ, както и със системата за мониторинг и поддръжка на мрежата на НЗОК.

5.2. Изпълнителят да представи програма за съдържанието и времетраенето на обучението, която да бъде съгласувана с Възложителя.

5.3. Обучението да приключи не по-късно от 90 работни дни след подписване на приемателно-предавателния протокол за приемане в експлоатация на услугите.

IV. Технически изисквания и спецификации за доставка и пускане в експлоатация на 2 броя опорни маршрутизатори.

С цел запазване на мрежовата топология, определена от административната структура на НЗОК и за покриване на завишените изисквания към скоростите на трасетата, е необходимо да бъдат подменени двата опорни комутатора CISCO 2951 в ЦУ на НЗОК, явяващи се вход и изход на Интернет и VPN услугите. За целта е необходимо в рамките на обществената поръчка, изпълнителят да достави две нови устройства с минимални технически изисквания и параметри описани в таблицата по-долу (устройствата може и да са с параметри по-високи от минимално изискваните).

Цената на устройствата се включва в общата цена на поръчката и се заплаща на 36

/тридесет и шест/ равни месечни вноски, като след изтичане срока на договора техниката остава собственост на НЗОК. Настройката и поддръжката на маршрутизаторите е за сметка на изпълнителя за срока на действие на договора

Освен доставката на 2-та опорни маршрутизатори е необходимо да се извърши ъпгрейд на съществуващите два броя защитни стени, съгласно спецификацията по т. 2 от таблицата по-долу.

1.	Минимални технически изисквания и параметри за доставка и пускане в експлоатация на 2 броя маршрутизатори за пренос на данни
1.1.	Системна платформа
1.1.1.	Да има минимум 6 1GE слота за интерфейсни модули
1.1.2.	Всеки маршрутизатор да бъде доставен с 6 броя 1G меден SFP модул
1.1.3.	Да има минимум 2 10GE слота за интерфейсни модули
1.1.4.	Всеки маршрутизатор да бъде доставен с един 10G модул с дължина на вълната от 850 nm за работа на близко разстояние и необходимия му лиценз.
1.1.5.	Всеки маршрутизатор да бъде доставен с един 10G модул с дължина на вълната от 1310 nm за работна дистанция до 10 км и необходимия му лиценз.
1.1.6.	Да има минимум един 10/100/1000BASE-T порт за управление
1.1.7.	Да поддържа поне един сериен порт за достъп до управляващата конзола
1.1.8.	Да има поне един USB интерфейс
1.1.9.	Да има минимум 8GB DRAM памет
1.1.10.	Да има възможност за надграждане до минимум 16GB DRAM
1.1.11.	Да има минимум 8GB flash памет
1.1.12.	Да има минимум 1 вграден специализиран процесор за обработка на мрежовия трафик
1.1.13.	Да има 64 битова операционна система
1.1.14.	Да има пропускателна способност от минимум 2,4 Gbps
1.1.15.	Всеки маршрутизатор да се достави с лиценз за допълнително увеличаване на пропускателната способност до поне 5 Gbps.
1.1.16.	Всеки маршрутизатор да бъде доставен с поддръжка на stateful packet inspection Firewall система с възможност за дефиниране на зони - Zone Based Firewall
1.1.17.	Всеки маршрутизатор да бъде доставен с поддръжка на IPSec криптиране.
1.1.18.	Да поддържа поне 5000 IPSec тунела от тип „сайт-сайт“
1.1.19.	Всеки маршрутизатор да поддържа минимум следните алгоритми за криптиране - 256 битов AES-CBC и AES-GCM , SHA-256, SHA-384, SHA-512, DH-2048, DH-3072, RSA-3072, DSA-3072, HMAC-SHA-1, HMAC-SHA-256, ECDH-384, ECDSA-384
1.1.20.	Да поддържа удостоверяване, оторизация и отчетност (AAA) чрез локална база и чрез външни RADIUS сървъри
1.1.21.	Да поддържа Generic routing encapsulation (GRE) тунели

1.1.22.	Да поддържа филтриране на трафика на базата на ACL (листи за контрол на достъпа), които използват произволни комбинации от L3 и L4 информация
1.1.23.	Да поддържа поне 5000 SSL тунела
1.1.24.	Да има възможност да поддържа минимум 2000 L2TP тунела
1.1.25.	Да поддържа поне 2000000 NAT и Firewall сесии
1.1.26.	Да поддържа NAT64 транслиране
1.1.27.	Да поддържа минимум 1000000 IPv4 и IPv6 маршрута
1.1.28.	Да има възможност за софтуерна резервираност на процесите
1.1.29.	Да поддържа MPLS и минимум следните RFC стандарти - 2547, 2702, 3031,3036, 3037, 3107, 3209, 3210,3478, 3815, 3813,4364.
1.1.30.	Да поддържа MPLS Layer 2 VPN
1.1.31.	Да поддържа MPLS Layer 3 VPN и минимум следните RFC стандарти - 3809, 4364, 4382, 4659
1.1.32.	Да поддържа MPLS Pseudo Wire
1.1.33.	Да поддържа BFD
1.1.34.	Да поддържа не по-малко от 8000 IPv4 VRF домейна
1.1.35.	Да поддържа VRF Lite
1.1.36.	Да поддържа филтриране на трафика на базата на ACL (листи за контрол на достъпа), които използват произволни комбинации от L3 и L4 информация.
1.1.37.	Да поддържа класифициране трафика на ниво 7 (приложения) с използване DPI механизми и обновяваща се база с приложения.
1.1.38.	Да поддържа филтриране на трафика на ниво приложения чрез използване на ACL
1.1.39.	Да поддържа минимум 3000 листа за контрол на достъпа (ACL) за цялата система
1.1.40.	Да поддържа минимум 4000 802.1Q VLAN мрежи на интерфейс
1.1.41.	Да поддържа следните протоколи да маршрутизация: IPv4, IPv6, static routes, Routing Information Protocol Versions 1 and 2 (RIP and RIPv2), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP),System-to-Intermediate System (IS-IS), Multicast Internet Group Management Protocol Version 3 (IGMPv3), Protocol Independent Multicast sparse mode (PIM SM), PIM Source Specific Multicast (SSM),
1.1.42.	Да поддържа маршрутизация на база Layer 7 информация
1.1.43.	Да поддържа автоматичен избор на маршрут, който предлага най-добрите параметри, за приложения или групи от приложения. <ul style="list-style-type: none"> - Да предлага автоматично следене на следните параметри за всеки маршрут/комуникационен канал: - Jitter - Загуба на пакети - Пропускателна способност на канала - Работеща IP свързаност до определен хост или хостове - MOS нивото на VoIP обаждания
1.1.44.	Да поддържа IPv4 и IPv6 QoS и HQoS с възможност за класифициране на

	<p>трафика в трафични класове на база минимум следните параметри:</p> <ul style="list-style-type: none"> - Класифициране на трафика на базата на ACL с произволна комбинация на 802.1p, DSCP/DiffServ, L3/L4 информация - Класифициране на трафичните потоци на база приложения - HQoS с поне 3 нива
1.1.45.	<p>Да поддържа минимум следните методи за управление на трафика:</p> <ul style="list-style-type: none"> - Маркиране и пре-маркиране на 802.1p и DSCP етикети на база политики - Traffic shaping на ниво интерфейс - Traffic shaping на ниво трафичен клас - Traffic policing на ниво интерфейс - Traffic policing на ниво трафичен клас - Йерархичен traffic policing - Конфигуриране на пропускателната способност в traffic policing и traffic shaping политиките като процент от интерфейлната пропускателна способност - Weghted Fair Queue и Class Based Queueing (CBQ) или подобни алгоритми за управление на опашките - Class Based Weighted Fair Queueing (CBWFQ) или подобен алгоритъм за управление на опашките с възможност за задаване на минимално гарантирана пропускателна способност за всяка опашка или минимално гарантиран процент от пропускателната способност на интерфейса - Управление на пакетната дълбочина на опашките - Предотвратяване на задръствания с използването на Weighted Random Early Detection или подобен алгоритъм - Възможност за дефиниране на приоритетна опашка (PQ), за трафик чувствителен към закъснение и jitter - Възможност за дефиниране множество PQ опашки с различен приоритет, за различни трафични класове, част от една политика - Прилагане на различни QoS политики върху IPSec VPN тунели
1.1.46.	<p>Да поддържа поне 16000 пакетни опашки</p>
1.1.47.	<p>Да поддържа минимум следните методи за управление и наблюдение:</p> <ul style="list-style-type: none"> - Управление чрез конзола, HTTP и HTTPS - RMON. - IPv4/v6 ping - DNS - TFTP - FTP - NTP - SSHv2 и SNMPv3 - Достъп до управлението и системните мрежови функции през отделен Ethernet интерфейс - Експортиране на трафична информация чрез IPFIX за поне 2000000 трафични потока - Конфигурация в отделен, конфигурационен, файл позволяваща бързото и лесно преместване на конфигурацията върху ново у-во - Задаване ниво на достъп до системата за управление за всеки потребител - Оторизация на потребителите за достъп до всяка команда

	<ul style="list-style-type: none"> - Работа с външна система за съхраняване на информация, за въведените от всеки потребител команди - Traffic policing за контролиране на мрежови трафик до контролната система на маршрутизатора
1.2.	Стандарти
1.2.1.	Да отговаря на GR-1089 стандарта
1.2.2.	<p>Да отговаря минимум на следните стандарти за електромагнитна съвместимост:</p> <ul style="list-style-type: none"> - EN55022/CISPR 22 Information Technology Equipment - EN55024/CISPR 24 Information Technology Equipmen - EN300 386 Telecommunications Network Equipment - EN50082-1/EN61000-6-1 Generic Immunity Standard
1.2.3.	<p>Да отговаря минимум на следните стандарти за безопасност:</p> <ul style="list-style-type: none"> - EN 60950-1 - UL60950-1 - No. 60950-1-03
1.3.	Други
1.3.1.	Да се монтира в стандартен 19“ комуникационен шкаф, като заема не повече от 1RU (Rack unit)
1.3.2.	Да има поне два АС токозахранващи модула работещи в режим на споделено натоварване
1.3.3.	Да поддържа входно напрежение в интервала от 100 до 240 V
1.3.4.	Да има максимална консумация при АС захранване, не по голяма от 260W на захранващ блок
1.3.5.	Да има минимален диапазон на работната температура от 0 до 40°C
1.3.6.	Устройствата да са окомплектовани със съответните лицензи и права за използване според условията на производителя
1.3.7.	Да се достави с всички необходими елементи за монтаж в 19 инчов шкаф (rack). Захранващ кабел – БДС стандарт или за захранване от UPS и всички необходими за монтаж болтове, гайки, аксесоари, пач корди и др.
1.3.8.	Да има инсталирана и лицензирана с постоянен лиценз операционна система която поддържа гореописаните модули и функции
1.3.9.	Да е съвместим с комуникаци-онната инфраструктура на Възложителя
1.4.	Гаранция и поддръжка
1.4.1.	Срок: минимум 3 години
1.4.2.	Режим: 8x5 (хардуерна подмяна на устройството при повреда)
1.4.3.	Възможност за получаване на нови версии на операционната система (updates and upgrades)
2.1	Ъпгрейд на съществуващите два броя защитни стени
2.1.1.	Да бъде доставен лиценз за FirePOWER с функционалности IPS и URL filtering
2.1.2.	Да бъде доставен и инсталиран софтуер за управление на FirePOWER
2.2.	Гаранция и поддръжка
2.2.1	Срок: минимум 3 години

2.2.2	Режим: 8x5 софтуерна поддръжка
2.2.3	Възможност за получаване на нови версии на софтуера (updates and upgrades)

V. Спецификация на съществуващо оборудване.

1.1.	Маршрутизатори в РЗОК – 26 бр. /CISCO 2901/	
1.1.1.	Архитектура	Модулна архитектура;
1.1.2.	Сигурност	IPSec 5DES/AES; GRE
1.1.3.	Криптиране	Вграден хардуерен Cripto Acceleration VPN модул, поддържащ криптоалгоритмите DES, 3DES, AES 128, AES 192 и AES 256
1.1.4.	Интерфейси	Вградени 2 (два) 10/100/1000 Ethernet порта, модул с 4 (четири) 10/100 Ethernet порта
1.1.5.	Слотове	3 (три) свободни слота за интерфейсни модули.
1.1.6.	Памет	512MB DRAM и 256MB Flash с възможност за бъдещо разширение до 2 GB DRAM и 8 GB Flash
1.1.7.	Производителност	Производителност – мин. 200 kpps
1.1.8.	VPN Производителност	VPN производителност – мин. 100 Mbps за IPsec 3DES/AES тунели
1.1.9.	Маршрутизиращи протоколи	Поддръжка на следните протоколи и услуги (или аналогични): AAA, ACL, BGP, OSPF, RIPv2, IPsec, IKE, DHCP, EEM, IP SLA, ZBFW, Modular QoS, IP Multicast, IGMP, IPv6, NAT, NBAR, NetFlow, SSH, SNMP, STP и др.
1.1.10.	Функции	Поддръжка на следните функции: TCP/IP; Bridging; PPP; Policy based routing; IP Filtering; RADIUS Autentication/Auditing;
1.1.11.	Протоколи за сигурност	Поддръжка на следните протоколи за автентикация: PAP; CHAP; RADIUS; TACACS+; локална база данни с имена и пароли;
1.1.12.	QoS	Поддръжка на Quality of Service (QoS): IP; Precedence; Generic Traffic Shaping (GTS) и Class-based Traffic Shaping; Weighted Random Early Detection (WRED); Class Based Class-based Fair Queuing (CBWFQ); Low Latency Queuing for PPP, HDLC,
1.1.13.	Други	Вграден DHCP сървър; Поддръжка на IEEE 802.1Q стандарт;
1.2.	Маршрутизатори в офисите на НЗОК – 65 бр. /CISCO 871/	
1.2.1.	Архитектура	Фиксирана архитектура;
1.2.2.	Сигурност	IPSec 3DES/AES, GRE
1.2.3.	Криптиране	Вграден хардуерен Crypto модул;
1.2.4.	Интерфейси	1 бр. 10/100 Ethernet WAN порт
1.2.5.	Интерфейси	Вградени 4 бр. 10/100 Ethernet LAN портове с VLAN поддръжка;
1.2.6.	Памет	128 MB RAM с възможност за увеличаване до 256 MB. 24 MB Flash с възможност за разширение до 50 MB
1.2.7.	Производителност	Производителност – мин. 25 kpps;
1.2.8.	VPN	VPN производителност – мин. 8 Mbps за криптиран IPSEC

	Производителност	3DES/AES тунелиран трафик (IMIX трафик);
1.2.9.	Маршрутизиращи протоколи	Поддръжка на следните функции: TCP/IP; Bridging; PPP; BGP, OSPF; RIP v1&2; Policy based routing; IP Filtering; RADIUS Authentication/Accounting; ACLs, GRE
1.2.10.	Функции	Поддръжка на следните VPN технологии и стандарти за криптиране на информация: IP Security (IPsec) VPNs (Triple Data Encryption Standard [3DES] or Advanced Encryption Standard [AES]) and Tunnel-less Group Encrypted Transport;
1.2.11.	Протоколи за сигурност	Поддръжка на следните протоколи за автентикация: PAP; CHAP; RADIUS; TACACS+; локална база данни с имена и пароли;
1.2.12.	QoS	Поддръжка на Quality of Service (QoS): IP; Precedence; Generic Traffic Shaping (GTS) и Class-based Traffic Shaping; Weighted Random Early Detection (WRED); Class Based Class-based Fair Queuing (CBWFQ); Low Latency Queuing for PPP, HDLC, Frame-Relay.
1.2.13.	Други	Поддръжка на NAT IEEE 802.1Q. Стандарт; Вграден DHCP сървър

Забележка:

* Всяко посочване в настоящите технически изисквания и спецификации или в документацията като цяло на стандарт, спецификация, техническа оценка, техническо одобрение или технически еталон следва да се чете и разбира „или еквивалентно/и“.

** Съдържащо се в настоящите технически изисквания и спецификации или в документацията като цяло на посочване на конкретен модел, източник или специфичен процес, който характеризира продуктите, предлагани от конкретен потенциален изпълнител, търговска марка, патент, тип или конкретен произход или производство, което облагодетелства или елиминира определени лица или някои продукти, следва да се чете и разбира „или еквивалентно/и“.

*** Когато участник с офертата си предлага еквивалентно на поставено в настоящите технически изисквания и спецификации за стандарт, спецификация, техническа оценка или техническо одобрение, международни стандарти или други стандартизационни документи, установени от европейски органи по стандартизация, участникът трябва да докаже в своята оферта с подходящи средства, включително чрез протокол от изпитване орган за оценяване на съответствието или сертификат, издаден от такъв орган, че предложеното от него решение удовлетворява по еквивалентен начин изискванията, определени в Техническата спецификация.

**** Когато участник с офертата си предлага еквивалентни на поставени в настоящите технически изисквания и спецификации работни характеристики или функционални изисквания, включително екологичните, които съответстват на български стандарт, въвеждащ европейски стандарт, европейска техническа оценка, обща техническа спецификация, международен стандарт или стандартизационен документ, установен от европейски орган по стандартизация, ако участникът докаже в своята оферта с подходящи средства, включително чрез протокол от изпитване орган за оценяване на съответствието или сертификат, издаден от такъв орган, че предложеното от него стандартизационни документи се отнасят до определените от възложителя изисквания за работни характеристики и функционални изисквания.