ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И УСЛОВИЯ ЗА ИЗПЪЛНЕНИЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

" ЗАКУПУВАНЕ НА ЛИЦЕНЗ ЗА АБОНАМЕНТНА ПОДДРЪЖКА НА СОФТУЕРЕН ПРОДУКТ (СП) CHECK POINT, ЗАКУПУВАНЕ НА НОВ СЪРВЪР ЗА ЗАЩИТНАТА СТЕНА И ЗАКУПУВАНЕ НА СП ЗА НАБЛЮДЕНИЕ И КОНТРОЛ НА ДОСТЪП ДО ОТДАЛЕЧЕНИ ИТ СИСТЕМИ."

1. ПРЕДМЕТ НА ПОРЪЧКАТА

Предметът на поръчката е „Закупуване на лиценз за абонаментна поддръжка на софтуерен продукт (СП) Check Point, закупуване на нов сървър за защитната стена и закупуване на СП за наблюдение и контрол на достъп до отдалечени ИТ системи."

Предметът на обществената поръчка включва изпълнението на следните дейности:

- Закупуване на допълнителна защитна стена, която да е съвместима с наличното оборудване и да позволява работа в клъстер;
- Закупуване на система за наблюдение, управление и контрол на достъп на отдалечени защитни стени Check Point;
- Закупуване на лиценз за абонамент за ползване на софтуерен продукт Check Point;
- Осигуряване на извънгаранционна поддръжка на съществуващо оборудване SunFire X4100.

2. ПРОГНОЗНА СТОЙНОСТ НА ПОРЪЧКАТА

Прогнозната стойност на поръчката е до 175 000 лв. (сто седемдесет и пет хиляди лева) без ДДС или до 210 000лв. (двеста и десет хиляди лева) с включен ДДС.

3. МЯСТО И СРОК ЗА ИЗПЪЛНЕНИЕ НА УСЛУГАТА

Място на изпълнение на поръчката – Министерство на здравеопазването, гр. София. пл. "Света Неделя" № 5.

- Срок на доставка на допълнителната защитна стена и на системата за наблюдение, управление и контрол на достъп на отдалечени защитни стени е до 3 месеца от

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И УСЛОВИЯ ЗА ИЗПЪЛНЕНИЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

" ЗАКУПУВАНЕ НА ЛИЦЕНЗ ЗА АБОНАМЕНТНА ПОДДРЪЖКА НА СОФТУЕРЕН ПРОДУКТ (СП) CHECK POINT, ЗАКУПУВАНЕ НА НОВ СЪРВЪР ЗА ЗАЩИТНАТА СТЕНА И ЗАКУПУВАНЕ НА СП ЗА НАБЛЮДЕНИЕ И КОНТРОЛ НА ДОСТЪП ДО ОТДАЛЕЧЕНИ ИТ СИСТЕМИ."

1. ПРЕДМЕТ НА ПОРЪЧКАТА

Предметът на поръчката е „Закупуване на лиценз за абонаментна поддръжка на софтуерен продукт (СП) Check Point, закупуване на нов сървър за защитната стена и закупуване на СП за наблюдение и контрол на достъп до отдалечени ИТ системи."

Предметът на обществената поръчка включва изпълнението на следните дейности:

- Закупуване на допълнителна защитна стена, която да е съвместима с наличното оборудване и да позволява работа в клъстер;
- Закупуване на система за наблюдение, управление и контрол на достъп на отдалечени защитни стени Check Point;
- Закупуване на лиценз за абонамент за ползване на софтуерен продукт Check Point;
- Осигуряване на извънгаранционна поддръжка на съществуващо оборудване SunFire X4100.

2. ПРОГНОЗНА СТОЙНОСТ НА ПОРЪЧКАТА

Прогнозната стойност на поръчката е до 175 000 лв. (сто седемдесет и пет хиляди лева) без ДДС или до 210 000лв. (двеста и десет хиляди лева) с включен ДДС.

3. МЯСТО И СРОК ЗА ИЗПЪЛНЕНИЕ НА УСЛУГАТА

Място на изпълнение на поръчката – Министерство на здравеопазването, гр. София, пл. "Света Неделя" № 5.

- Срок на доставка на допълнителната защитна стена и на системата за наблюдение, управление и контрол на достъп на отдалечени защитни стени е до 3 месеца от

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ И УСЛОВИЯ ЗА ИЗПЪЛНЕНИЕ НА ОБЩЕСТВЕНА ПОРЪЧКА С ПРЕДМЕТ:

" ЗАКУПУВАНЕ НА ЛИЦЕНЗ ЗА АБОНАМЕНТНА ПОДДРЪЖКА НА СОФТУЕРЕН ПРОДУКТ (СП) CHECK POINT, ЗАКУПУВАНЕ НА НОВ СЪРВЪР ЗА ЗАЩИТНАТА СТЕНА И ЗАКУПУВАНЕ НА СП ЗА НАБЛЮДЕНИЕ И КОНТРОЛ НА ДОСТЪП ДО ОТДАЛЕЧЕНИ ИТ СИСТЕМИ."

1. ПРЕДМЕТ НА ПОРЪЧКАТА

Предметът на поръчката е „Закупуване на лиценз за абонаментна поддръжка на софтуерен продукт (СП) Check Point, закупуване на нов сървър за защитната стена и закупуване на СП за наблюдение и контрол на достъп до отдалечени ИТ системи."

Предметът на обществената поръчка включва изпълнението на следните дейности:

- Закупуване на допълнителна защитна стена, която да е съвместима с наличното оборудване и да позволява работа в клъстер;
- Закупуване на система за наблюдение, управление и контрол на достъп на отдалечени защитни стени Check Point;
- Закупуване на лиценз за абонамент за ползване на софтуерен продукт Check Point;
- Осигуряване на извънгаранционна поддръжка на съществуващо оборудване SunFire X4100.

2. ПРОГНОЗНА СТОЙНОСТ НА ПОРЪЧКАТА

Прогнозната стойност на поръчката е до 175 000 лв. (сто седемдесет и пет хиляди лева) без ДДС или до 210 000лв. (двеста и десет хиляди лева) с включен ДДС.

3. МЯСТО И СРОК ЗА ИЗПЪЛНЕНИЕ НА УСЛУГАТА

Място на изпълнение на поръчката – Министерство на здравеопазването, гр. София, пл. "Света Неделя" № 5.

- Срок на доставка на допълнителната защитна стена и на системата за наблюдение, управление и контрол на достъп на отдалечени защитни стени е до 3 месеца от

подписването на договора;

- Срок за гаранционна поддръжка на допълнителната защитна стена и на системата за наблюдение, управление и контрол на достъп на отдалечени защитни стени - 3 години от въвеждане в експлоатация.
- Срокът за доставка и инсталиране на лиценз за абонамент за ползване на софтуерен продукт Check Point – до 5 (пет) дни от подписване на договора.
- Срок за извънгаранционна абонаментна поддръжка на сървър Sun Fire X4100 - 3 години от датата на сключване на договора.

4. ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ НА ДОГОВОРА. УСЛОВИЯ, РАЗМЕР И НАЧИН НА ПЛАЩАНЕ.

4.1. Гаранцията за изпълнение е в размер на 3% от стойността на договора за обществена поръчка, без включен ДДС.

Гаранцията се предоставя в една от следните форми:

1. парична сума;

2. банкова гаранция;

3. застраховка, която обезпечава изпълнението чрез покритие на отговорността на изпълнителя.

Гаранцията по т.1 и т.2 може да се предостави от името на изпълнителя за сметка на трето лице - гарант.

Участникът, определен за изпълнител, избира сам формата на гаранцията за изпълнение.

Когато участник в процедурата е обединение, което не е юридическо лице, всеки от участниците в обединението може да бъде наредител по банковата гаранция, съответно вносител на сумата по гаранцията.

Участникът, определен за изпълнител на обществената поръчка, представя банковата гаранция, застрахователната полица или платежния документ за внесената по банков път гаранция за изпълнение на договора при неговото сключване и се освобождава след неговото приключване.

Гаранцията за изпълнение под формата на парична сума трябва да бъде внесена по следната сметка на възложителя:

Банка: БНБ Централно управление,

Банков код (BIC): BNBG BGSD,

Банкова сметка (IBAN): BG21 BNBG 9661 3300 1293 01

Ако участникът, определен за изпълнител, избере да представи гаранцията за изпълнение под формата на «парична сума», платена по банков път, документът, удостоверяващ платената гаранция, следва да бъде заверен с подпис и печат от съответната банка. В случай че участникът е превел парите по електронен път (електронно банкиране), той следва да завери съответния документ с подпис и печат.

В случай, че участника избере да представи гаранция за изпълнението на договора, под формата на банкова гаранция или застраховка, която обезпечава изпълнението чрез покритие на отговорността на Изпълнителя, документът за нея се представя в оригинал. При представяне на документа за гаранцията, в нея изрично се посочва договора, за който се представя гаранцията.

В случай, че участника избере да представи гаранция за изпълнението на договора, под формата на банкова гаранция или застраховка, която обезпечава изпълнението чрез покритие на отговорността на Изпълнителя, трябва да бъде изрично записано, че тя е безусловна и неотменима, че е в полза на възложителя, със срок на валидност 60 дни след датата на изпълнение на договора и е изискуема при първо писмено поискване, в което Възложителят заяви, че изпълнителят не е изпълнил задължение по договора за възлагане на обществената поръчка.

Възложителят ще освободи гаранцията за изпълнение, без да дължи лихви за периода, през който средствата са престояли законно при него.

Условията за задържане и освобождаване на гаранцията за изпълнение се определят с договора за възлагане на обществената поръчка.

5. УСЛОВИЯ И НАЧИН НА ПЛАЩАНЕ

5.1. Плащането по настоящия договор се осъществява чрез банков превод от страна на **ВЪЗЛОЖИТЕЛЯ** по посочената банкова сметка на **ИЗПЪЛНИТЕЛЯ.**

5.1.1. За **„закупуване на допълнителна защитна стена, която да е съвместима с наличното оборудване и да позволява работа в клъстер“; „закупуване на система за наблюдение, управление и контрол на достъп на отдалечени защитни стени“** и **„закупуване на лиценз за абонамент за ползване на софтуерен продукт Check Point“** ,

плащането се извършва еднократно в български лева, по банков път в срок до 30/тридесет/ дни след представяне на оригинална фактура с включен ДДС и подписан от Възложителя приемателно-предавателен протокол за инсталирането им.

5.1.2. За **извънгаранционната абонаментна поддръжка на сървър SunFire x4100**, плащането се извършва на тримесечие в български лева по банков път до 30 /тридесет/ дни след изтичане на съответното тримесечие, след представяне на оригинална фактура/ за период от три месеца/ и подписан за всеки месец двустранен протокол за извършената дейност.

5.1.3. Заплащането на стоките по договора се извършва в български лева, по банкова сметка на изпълнителя.

6. СРОК НА ВАЛИДНОСТ НА ОФЕРТИТЕ

Срокът на валидност на офертите трябва да бъде съобразен с определения срок в обявлението за обществената поръчка – 4 (четири) месеца, считано от датата, посочена като краен срок за получаване на офертите, и представлява времето, през което участниците са обвързани с условията на представените от тях оферти.

7. КРИТЕРИЙ ЗА ОЦЕНКА НА ОФЕРТИТЕ

7.1. Назначената от Възложителя комисия за разглеждане, оценка и класиране на постъпилите оферти извършва оценка на икономически най-изгодната оферта въз основа на определения критерий – **„Най – ниска цена"**, съгласно чл. 70, ал. 2, т. 1 от ЗОП.

7.2. В случай, че предлаганите цени на две или повече оферти са равни, комисията провежда публично жребий за определяне на изпълнител между участниците, предложили равните цени, съгласно чл. 58, ал. 3 от ППЗОП.

Предложената цена в български лева, трябва да е фиксирана и да не подлежи на промяна за срока на действие на договора.

Комисията класира допуснатите до разглеждане оферти по възходящ ред, въз основа на предложената от тях единична цена, като предложената най-ниска цена се класира на първо място. Участникът, предложил най-ниска цена, се определя за изпълнител. След приключване на работата на комисията по разглеждане и оценка на офертите, Възложителят обявява с решение класирането на участниците и участниците, определени за изпълнители

на обществената поръчка. Участниците се уведомяват писмено за резултата от проведената процедура, като им се връчва (изпраща) копие от решението.

8. ВЪЗМОЖНОСТ ЗА ПРЕДСТАВЯНЕ НА ВАРИАНТИ В ОФЕРТИТЕ

Не се допуска представяне на варианти в офертите.

Представянето на оферта задължава участника да приеме напълно всички изисквания и условия, посочени в тази документация, при спазване изискванията на ЗОП. Поставянето от страна на участника на условия и изисквания, които не отговарят на обявените в документацията, води до отстраняване на този участник от участие в процедурата.

До изтичане на срока за подаване на офертите, всеки участник може да промени, допълни или оттегли офертата си.

Офертата се изготвя и представя на български език. Когато участникът в процедурата е чуждестранно физическо или юридическо лице, офертата се подава на български език.

Офертата се подписва от представляващия участника или от надлежно упълномощено/и лице/а, като в офертата се прилага пълномощното от представляващия участника (с изключение на изискуемите документи, които обективизират лично изявление на конкретно лице/а – представляващ/и участника, и не могат да се подпишат и представят от пълномощник).

9. КРИТЕРИИ ЗА ПОДБОР

9.1. Минимални изисквания за годността (правоспособността) за упражняване на професионална дейност съгласно ЗОП:

Възложителят няма изисквания за годността (правоспособността) за упражняване на професионална дейност.

9.2. Минимални изисквания за икономическо и финансово състояние на участниците съгласно ЗОП:

Възложителят няма изисквания за икономическо и финансово състояние на участниците.

9.3 Минимални изисквания за техническите и професионалните способности на участниците, съгласно ЗОП:

9.3.1. Участникът следва да има изпълнени минимум 3 /три/ дейности през последните три години, считано от датата на подаване на офертата с предмет и обем, идентични или сходни с предмета на поръчката.

Под „идентични дейности“ се има предвид: Осигуряване на извънгаранционна поддръжка на хардуер произведен от фирмите SUN/Oracle.

Под „сходен“ предмет се разбира: Доставка и поддръжка на продукти за защита на информационни системи.

Под „изпълнени дейности“ се разбират такива, чиито срок за изпълнение е приключил към датата на подаване на офертата, работата на участника е изпълнена и е приета от възложителя/получателя на услугата.

Съответствието на участника с посоченото изискване се удостоверява с представяне на списък с посочване на стойностите, датите и получателите.

В случаите на чл. 67, ал. 5 и ал. 6 от ЗОП, участниците доказват съответствието си с това изискване с представяне на списък на изпълнените дейности, които са идентични или сходни с предмета на обществената поръчка, с посочване на стойностите, датите и получателите заедно с доказателство за извършените дейности.

ЗА УДОСТОВЕРЯВАНЕ НА ВЪЗМОЖНОСТИТЕ ПО Т. 9.3.1. СЕ ПОПЪЛВА ЧАСТ IV, БУКВА „В“, Т. 1Б ОТ ЕЕДОП.

9.3.2. Участниците в процедурата трябва да притежават валидни системи за управление на качеството и за управление на сигурността на информацията по стандарти БДС EN ISO/ 9001 и БДС EN ISO/27001 или по - нови версии или еквивалентни системи с обхват, съгласно предмета на обществената поръчка.

Съответствието на участниците с посоченото изискване се удостоверява с посочване в ЕЕДОП на информация относно притежаваните от участника валидни сертификати, с посочване на информация за номера и валидността на сертификата, органа който го е издал, и обхват, съгласно предмета на обществената поръчка.

В случаите на чл. 67, ал. 5 и ал. 6 от ЗОП, участниците доказват съответствието си с това изискване с представяне на заверени копия на сертификати, издадени от независими лица, които са акредитирани по съответната серия европейски стандарти от ИА "БСА" 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 отговарят 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, както и други доказателства за еквивалентни мерки.

ЗА УДОСТОВЕРЯВАНЕ НА ВЪЗМОЖНОСТИТЕ ПО Т. 9.3.2. СЕ ПОПЪЛВА ЧАСТ IV, БУКВА „Г“ ОТ ЕЕДОП.

9.3.3. Участникът следва да разполага с екип от минимум 3 лица сертифицирани от производителя, които ще осигурят поддръжката на Чек Пойнт продуктите.

Съответствието на участника с посоченото изискване се удостоверява с посочване на екип, сертифициран от производителя Чек Пойнт Технолъджис на предлаганото оборудване и софтуер. Посочват се лицата, които ще участват в изпълнението на поръчката, трите им имена, данни за документа за придобита професионална компетентност (учебно заведение или обучаваща организация, № и дата на издаване, образователна степен, специалност или квалификация), както и данни за притежаваните сертификати (вид, дата на издаване, срок на валидност, обхват и др.)

В случаите на чл. 67, ал. 5 и ал. 6 от ЗОП, участниците доказват съответствието с това изискване с представяне на списък на персонала, сертифициран от производителя Чек Пойнт Технолъджис на предлаганото оборудване и софтуер.

ЗА УДОСТОВЕРЯВАНЕ НА ВЪЗМОЖНОСТИТЕ ПО Т. 9.3.3. СЕ ПОПЪЛВА ЧАСТ IV, БУКВА „В“, Т. 6 ОТ ЕЕДОП.

10. ОПИСАНИЕ И ИЗИСКВАНИЯ

Целта на обществената поръчка е повишаване на отказоустойчивостта на съществуващият Firewall използван в момента от МЗ, както и подновяване на абонаментът за софтуерните лицензи и осигуряване на необходимата поддръжка чрез:

10.1. Закупуване на допълнителна защитна стена, която да е съвместима с наличното оборудване и да позволява работа в клъстер;

10.2. Закупуване на система за наблюдение, управление и контрол на достъп на отдалечени защитни стени;

10.3. Закупуване на лиценз за абонамент за ползване на софтуерен продукт Check Point;

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ

1. Допълнително устройство за защитна стена – 1 брой.

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
1	Хардуерна защитна стена - устройство, за работа в клъстер. Да има възможност да работи със съществуващото в момента устройство за защитна стена - CPAP-SG5400-NGTP. Да има възможност да участва е изграждане на Високо Надеждна Система (High Availability HA) и баланс на трафика през изградения клъстер. **<u>Производителност</u>** - не по-малко от 10 Gbps FW Throughput (пропускателна способност на защитната стена); - не по-малко от 2.16 Gbps VPN Throughput AES-128 (пропускателна способност на виртуалната частна мрежа с алгоритъм за криптиране AES-128); - не по-малко от 1 Gbps IPS Throughput (пропускателна способност на	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	системата за предпазване от атаки); - Max concurrent connections: 3 200 000 (поддържани конкурентни сесии); - Max connections per second: 150 000 (сесии за секунда). **Базовата конфигурация да включва:** - Формфактор- да може да се монтира в 19“ комуникационен шкаф; - Комплект за монтаж в 19“ шкаф (Rack mount kit); - поне 10 x 10/100/1000Base-T RJ45 ports /мрежови интерфейса; - възможност за разширение на мрежовите интерфейси с допълнителен разширителен слот с медни или оптични портове с SFP; - 500GB хард диск или по – голям; - поне 8GB памет; - поне 1 захранване 220V / 50 Hz; - захранващи кабели тип Шуко съответстващи на броя на захранванията. **Разширяемост:** - до 18 x 10/100/1000Base-T RJ45 ports - до 4 x 1000Base-F SFP ports	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	Работни характеристики: - Работен температурен диапазон от 0 до 40 °C - Да поддържа променливотоково захранване в диапазон 90-264V	
	Функционални възможности: Моделът на предложеното устройство да притежава следните функционални характеристики: **Защитна стена** - Защитна стена от тип stateful inspection - Възможност за работа в режим Active- Active или Active- Passive - Системата да сканира в реално време SMTP, HTTP, HTTPS, FTP, POP3 и други протоколи; **Виртуални частни мрежи** - Възможност за изграждане на виртуални частни мрежи (VPN) тип site to site - Full Mesh, Star, Hub and Spoke; - Да поддържа 1024 VLAN; **Съвременни мрежови и клъстерни функционалности**	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	- Възможност за изграждане на отказоустойчиви клъстерни решения от два или повече нода с баланс на трафика между тях; - Да поддържа протоколи за динамично рутиране - OSPF, BGP, RIP v1&v2, PIM; - Да поддържа конфигуриране на интерфейсите в Layer 3 (Routing Mode) и Layer 2 (Transparent Mode); - Да поддържа L2TP VPNs, - Да поддържа IPv6; - Да поддържа "dynamic routing" и "multicast" протоколи; - Да поддържа "QoS" категоризация на трафика; - Да има гъвкаво балансиране на натоварването на сървърите; - Да има надеждна връзка с Интернет чрез превключване към резервен ISP; - Поддръжка на многоядрени процесори с цел разпределение на трафика между отделните ядра на една система с оглед постигане на по-голямо бързодействие; - Да поддържа "dynamic routing" и "multicast" протоколи; - Да поддържа "QoS" категоризация на трафика; - Да има гъвкаво балансиране на натоварването на сървърите; - Да има надеждна връзка с Интернет чрез превключване към резервен	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	ISP; - Поддръжка на многоядрени процесори с цел разпределение на трафика между отделните ядра на една система с оглед постигане на по-голямо бързодействие	
	Контрол на достъпа на потребители - възможност за контролиране на достъпа на потребители от мрежата до конкретни приложения без да се конкретизира IP адрес; - възможност за детайлен мониторинг и управление на групи потребители; - интеграция с използваното във вътрешната мрежа на МЗ Microsoft Active Directory.	
	Защитен достъп на отдалечени потребители - отдалечен защитен достъп чрез SSL VPN на поне 5 конкурентни отдалечени потребителя.	
	Програмни средства за проследяване и предотвратяване опитите за проникване - Да проверява целия трафик за уязвимости и потенциални пробиви на база на шаблони и на сложни емпирични алгоритми; - Да проверява, както входящите заявки към публичните услуги, така и изходящия трафик на участниците в мрежата;	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	- Да защитава сървърите, намиращи се в DMZ и предоставящи публични услуги; - Да защитава потребителите в мрежата от неволно сваляне на зловреден код; - Да блокира атаки на мрежово, транспортно и приложно ниво;	
	Контрол на приложенията - Да може да контролира и наблюдава достъпа на потребителите от мрежата до конкретни приложения без да се конкретизира IP адрес или сайт например: Facebook, TOR, TeamViewer, Gtalk и др. - Да могат да се задават в политиката специфични widget-и на приложенията. - Приложенията да бъдат групирани по категории и ниво на риска. ***URL филтриране*** - Да проверява изходящи URL заявки и да предупреждава потребителя, че достъпва уеб страница, която разпространява зловреден код. - Динамично да осигурява, блокира или ограничава достъпа до уеб страници в чист или криптиран (SSL) вид в реално време на базата на потребител, група или определена работна станция. - Да поддържа облачно-базирана база данни със зловредни уеб страници и динамични обновления на базата данни	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	<u>Анти-вирус защита</u> - Да предотвратява достъп до зловредни уеб страници. - Да проверява SSL криптиран трафик - Да има актуализация в реално време чрез облачно-базирана услуга - Да спира входящи зловредни файлове - Политиките за анти-вирус трябва да се управляват централизирано ***<u>Анти-бот защита</u>*** - Да разпознава инфектирани с ботове работни станции, забранява тяхното разпространение чрез блокиране на комуникацията им с контролни центрове - Поддръжка на облачно-базирана база данни с категоризирани ботове и динамични обновления на базата данни в реално време - Политиките за анти-бот трябва да се управляват централизирано ***<u>Анти-спам и защита на електронна поща</u>*** - Защита на корпоративната инфраструктура за електронна поща, осигуряваща прецизна филтрация на спам и съдържащи вируси зловредни електронни писма.	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	- Поддръжка на облачно-базирана база данни с категоризирани спам, вирус и малуер дефиниции и динамични обновления на базата данни.	
	Емулация и извличане на заплахи - Решението трябва да осигурява способност за защита срещу „zero-day" атаки чрез симулиране на прикачен в електронната поща зловреден код или свалени файлове във виртуални среди. - Извличане на полезната информация от заразен файл и копирането й в нов без това да забавя нормалната работа. ***DLP*** - Решението трябва да осигурява способност за защита в реално време на чувствителна информация от умишлена или неумишлена загуба или изтичане. Контролът на трафика (входящ и изходящ) да става на базата на потребител и/или приложение.	
	Управление на защитната стена - Всички средства за защита трябва да се управляват от централизирана конзола. - Решението трябва да има механизъм за проверка на политиката за сигурност преди нейното инсталиране. - Решението трябва да има механизъм за контрол на ревизиите на	

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
	политиката за сигурност. ***<u>Преглеждане на логове</u>*** - Решението да има способността за съхранение на различни филтри с цел по-късната им употреба - Трябва да има способност за индексирано търсене - Трябва да има способността да регистрира всички интегрирани средства за сигурност на гейтуеите - Решението трябва да поддържа експортиране на логове във формат за база данни Всички изброени по-горе функционални възможности да бъдат интегрирани в защитната стена. Да има възможност да се прибавят други функционалности към защитната стена само с добавяне на допълнителен лиценз.	
	Монтаж и инсталация на предлаганото оборудване и софтуер	
	Гаранция на защитната стена: 3 години	

2. Система за наблюдение, управление и контрол на достъп на отдалечени защитни стени – 1 брой.

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
1.	**<u>Фуннкционални възможности:</u>**	

	- Да има възможност да управлява до 5 защитни стени Checkpoint. - Да може да съхранява и поддържа версии на политиките за сигурност за всяко устройство. В политиката се включват правила за защитна стена, виртуална частна мрежа, контрол на приложенията. - Да поддържа автентикация с LDAP, RADIUS, TACACS, TACACS+, SecurID, local database. - Да може да се осигури наблюдение в реално време на трафика, натоварването и състоянието на системата. Възможност за временно блокиране на услуга или потребител, ако има съмнение за нерегламентиран трафик. Данните да могат да се показват в графичен, или табличен вид. - Да се предложи хардуерна система, на която да се инсталира софтуера за управление на защитни стени; - Хардуерната система да отговаря на следните параметри: * Формфактор- да може да се монтира в 19“ комуникационен шкаф; * Комплект за монтаж в 19“ шкаф (Rack mount kit); * поне 2 x 10/100/1000Base-T RJ45 мрежови интерфейса; * 300GB хард диск или по – голям; * 16 GB оперативна памет; * Процесор Intel Xeon E3-1220 v6 или по-добър;	

	Монтаж и инсталация на предлаганото оборудване и софтуер	
	Гаранция на системата за управление: 3 години	

3. Закупуване на лиценз за абонамент за ползване на софтуерен продукт (СП) Check Point.

№	Минимални изисквания	Предложение на участника / производител, наименование, модел/
1.	Check Point абонамент за право на ползване на използваните към момента софтуерни лицензи за: Потребителски акаунт ID: 0006243388 Клиент: Ministry of Health Начална дата: 01-01-2018 Период за подновяване на лицензите: 3 години	
2.	Участникът в процедурата да има предоставени лицензионни права от производителя или от негов упълномощен представител за продажба, разпространение и техническо обслужване на продукти Check Point Текнолъджис на територията на Република България. Това обстоятелство се доказва с предоставяне на оторизационно писмо от производителя Чек Пойнт Текнолъджис, че участникът е упълномощен да доставя и обслужва продукти Check Point на територията на Република България.	

4. Осигуряване на извънгаранционна абонаментна поддръжка на сървър SunFire X4100.

№	Минимални изисквания	Предложение на участника / участник/
1.	Осигуряване на хардуерна поддръжка 5x8xNBD на сървър SunFire X4100 в рамките на 3 години. Поддръжката трябва да включва минимум осигуряване на: - Консултации по телефона; - Инженер на място за отстраняване на проблема.	