ТЕХНИЧЕСКО ПРЕДЛОЖЕНИЕ

по 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“.

Настоящето техническо предложение е подадено от:

АСТ СОФИЯ ООД

(наименование на участника)

и подписано от: Катя Маркова Танева

/три имена/

в качеството му на: Управител

/длъжност/

Съдържание:

1. Документ за упълномощаване, когато лицето, което подава офертата, не е законният представител на участника- неприложимо.
2. Предложение за изпълнение на поръчката в съответствие с техническите спецификации и изискванията на възложителя.
3. Декларация за съгласие с клаузите на приложения проект на договор.
4. Декларация за срока на валидност на офертата.

ДАТА: 20.02.2018 г. ПОДПИС и ПЕЧАТ:_____

АСТ София
АСТ Sofia
ООД

ПРЕДЛОЖЕНИЕ ЗА ИЗПЪЛНЕНИЕ НА ПОРЪЧКАТА

ДО: **МИНИСТЕРСТВО НА ЗДРАВЕОПАЗВАНЕТО**

Адрес : 1000 гр. София, пл. Света Неделя № 5

(наименование и адрес на възложителя)

От: **АСТ СОФИЯ ООД**

(наименование на участника)

с адрес: 1784 гр. София, бул. „Цариградско шосе" №133, БИЦ-ИЗОТ, ет.7

тел.: 02/ 971 8354, 02/971 8271, факс: 02/ 971 8343, e-mail: sales@actsofia.bg

Булстат / ЕИК: 121007294,

УВАЖАЕМИ ДАМИ И ГОСПОДА,

С настоящото, Ви представяме нашето предложение за изпълнение на обявената от Вас процедура за възлагане 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".***

Участникът е специализиран в извършването на дейности свързани с изграждането на решения за кибер сигурност, като в предмета му на дейност са включени:

-Проектиране, разработване, внедряване, гаранционно и следгаранционно поддържане на системи за защита на чувствителна информация, информационни ресурси и центрове за данни;

-Анализ, оценка и препоръки на съществуващи реализации- проучвайки получената информация от системите за информационна сигурност, се изготвят препоръки за предотвратяване на пробиви в съществуващата система за сигурност и подобряване на нейната структура.

1.1 Допълнително устройство за защитна стена- 1 брой.

Минимални изисквания на възложителя	Предложение от участника /производител, наименование, модел/
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. **Производителност** - 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 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 **Работни характеристики:** - Работен температурен диапазон от 0 до 40 ºC - Да поддържа променливотоково захранване в диапазон 90-264V	Производител: Check Point Software Technologies Ltd 5400 Next Generation Threat Prevention & SandBlast (NGTX) -HA Предлаганият от нас модел има възможност да работи със съществуващото в момента устройство за защитна стена.Също така притежава възможността да участва е изграждане на Високо Надеждна Система (High Availability HA) и да осигури баланс на трафика през изградения клъстер. **Производителност на модел 5400 Next Generation Threat Prevention & SandBlast (NGTX) -HA** - 10 Gbps FW Throughput (пропускателна способност на защитната стена); - 2.16 Gbps VPN Throughput AES-128 (пропускателна способност на виртуалната частна мрежа с ползване на алгоритъм за криптиране AES-128); - 1 Gbps IPS Throughput (пропускателна способност на 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 включва:** - Формфактор- позволява да се монтира в 19" комуникационен шкаф; - Има комплект за монтаж в 19" шкаф (Rack mount kit); - има 10 x 10/100/1000Base-T RJ45 ports /мрежови интерфейса; - има възможност за разширение на мрежовите интерфейси с допълнителен разширителен слот с медни или оптични портове с SFP; - 500GB хард диск; - 8GB памет; - един 2- core процесор - 1 захранване 220V / 50 Hz; - 1 захранващи кабели тип Шуко за включеното захранване. **Разширяемост, която позволява предлаганото устройство:** - до 18 x 10/100/1000Base-T RJ45 ports - до 4 x 1000Base-F SFP ports **Работни характеристики:** - Работен температурен диапазон от 0 до 40 ºC - 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** - 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 ISP; - Поддръжка на многоядрени процесори с цел разпределение на трафика между отделните ядра на една система с оглед постигане на по-голямо бързодействие	**Функционални възможности:** Предлаганият от нас модел устройство притежава следните следните функционални характеристики: **Защитна стена** - Защитна стена от тип stateful inspection - Има възможност за работа в режим Active- Active или Active- Passive - Системата може да сканира в реално време SMTP, HTTP, HTTPS, FTP, POP3 и други протоколи; **Виртуални частни мрежи** - Има възможност за изграждане на виртуални частни мрежи (VPN) тип site to site - Full Mesh, Star, Hub and Spoke; - Поддържа 1024 VLAN; **Съвременни мрежови и клъстерни функционалности** - 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; - Поддържа "dynamic routing" и "multicast" протоколи; - Поддържа "QoS" категоризация на трафика; -Има гъвкаво балансиране на натоварването на сървърите; - Има надеждна връзка с Интернет чрез превключване към резервен ISP; -Има 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 М3 Microsoft Active Directory.	**Контрол на достъпа на потребители** - Има възможност за контролиране на достъпа на потребители от мрежата до конкретни приложения без да се конкретизира IP адрес; - Има възможност за детайлен мониторинг и управление на групи потребители; - дава възможност за интеграция с използваното във вътрешната мрежа на М3 Microsoft Active Directory.

Защитен достъп на отдалечени потребители - отдалечен защитен достъп чрез SSL VPN на поне 5 конкурентни отдалечени потребителя.	**Защитен достъп на отдалечени потребители** - позволява да се осъществи 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; - 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;	***Програмни средства за проследяване и предотвратяване опитите за проникване*** - може да проверява целия трафик за уязвимости и потенциални пробиви на база на шаблони и на сложни емпирични алгоритми; - може да проверява, както входящите заявки към публичните услуги, така и изходящия трафик на участниците в мрежата; - защитава сървърите, намиращи се в DMZ и предоставящи публични услуги; - защитава потребителите в мрежата от неволно сваляне на зловреден код; - 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	***Контрол на приложенията*** - 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. - могат да се задават в политиката специфични widget-и на приложенията. - Приложенията могат да бъдат групирани по категории и ниво на риска. ***URL филтриране*** - дава възможност за проверкя на изходящи URL заявки и да предупреждава потребителя, че достъпва уеб страница, която разпространява зловреден код. - Има възможност 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. - Поддържа облачно-базирана база данни със зловредни уеб страници и динамични обновления на базата данни
Анти-вирус защита - 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 ***Анти-бот защита*** - Да разпознава инфектирани с ботове работни станции, забранява тяхното разпространение чрез	***Анти-вирус защита*** - Предотвратява достъп до зловредни уеб страници. - Проверява SSL криптиран трафик -Има актуализация в реално време чрез облачно-базирана услуга - Спира входящи зловредни файлове - Политиките за анти-вирус трябва да се управляват централизирано ***Анти-бот защита*** - разпознава инфектирани с ботове работни станции, забранява тяхното разпространение чрез блокиране на комуникацията им с контролни центрове

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 ***Анти-спам и защита на електронна поща*** - Защита на корпоративната инфраструктура за електронна поща, осигуряваща прецизна филтрация на спам и съдържащи вируси зловредни електронни писма. - Поддръжка на облачно-базирана база данни с категоризирани спам, вирус и малуер дефиниции и динамични обновления на базата данни.	- Поддръжа облачно-базирана база данни с категоризирани ботове и динамични обновления на базата данни в реално време - Има централизирано управление на политиките за анти-бот ***Анти-спам и защита на електронна поща*** - Предоставя защита на корпоративната инфраструктура за електронна поща, осигурява прецизна филтрация на спам и съдържащи вируси зловредни електронни писма. - Поддръжа 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.	***Емулация и извличане на заплахи*** - Решението осигурява способност за защита срещу „zero-day" атаки чрез симулиране на прикачен в електронната поща зловреден код или свалени файлове във виртуални среди. - Има механизъм за извличане на полезната информация от заразен файл и копирането й в нов без това да забавя нормалната работа. ***DLP*** - Решението, което предлагаме осигурява способност за защита в реално време на чувствителна информация от умишлена или неумишлена загуба или изтичане. Контролът на трафика (входящ и изходящ) 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 политиката за сигурност. ***Преглеждане на логове*** - 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.	***Управление на защитната стена*** - Всички средства за защита се управляват от централизирана конзола. - Решението има механизъм за проверка на политиката за сигурност преди нейното инсталиране. - Решението има механизъм за контрол на ревизиите на политиката за сигурност. ***Преглеждане на логове*** - Решението има способността за съхранение на различни филтри с цел по-късната им употреба - Решението има способност за индексирано търсене - Решението има способността да регистрира всички интегрирани средства за сигурност на гейтуеите - Решението поддържа експортиране на логове във формат за база данни Всички изброени по-горе функционални възможности са интегрирани в предлаганото решение за защитна стена. Има възможност да се прибавят други функционалности към защитната стена само с добавяне на допълнителен лиценз.

Монтаж и инсталация на предлаганото оборудване и софтуер	Предлагаме да извършим монтаж и инсталация на предлаганото оборудване и софтуер
Гаранция на защитната стена: 3 години	Предлаганото от нас решение е с гаранция на защитната стена: 3 години

1.2 Система за наблюдение, управление и контрол на достъп на отдалечени защитни стени -1 брой.

Минимални изисквания на възложителя	Предложение от участника /производител, наименование, модел/
Фуннкционални възможности: - Да има възможност да управлява до 5 защитни стени Check Point. - 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 за 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 ports /мрежови интерфейса; * 300GB хард диск или по – голям; * 16 GB оперативна памет; * Процесор Intel Xeon E3-1220 v6 или по-добър;	Производител: Check Point Software Technologies Ltd Next Generation Security Management Software for 5 gateways Предлаганото решение има следните възможности: **Фуннкционални възможности:** - Има възможност да управлява до 5 защитни стени Check Point. - 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. - Поддържа автентикация с LDAP, RADIUS, TACACS, TACACS+, SecurID, local database. - Може да се осигури наблюдение в реално време на трафика, натоварването и състоянието на системата. Има 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. - Предлагаме хардуерна система, на която да се инсталира софтуера за управление на защитни стени със следните параметри: Supermicro SNK-P0046P * Формфактор- може да бъде монтирано в 19“ комуникационен шкаф; * Включва комплект за монтаж в 19“ шкаф (Rack mount kit); * поне 2 x 10/100/1000Base-T RJ45 ports /мрежови интерфейса; * 300GB SAS3 10000 rpm, хард диск ; * 16 GB DDR4 оперативна памет; * Процесор Intel Xeon E3-1220v6, 4 cores, 3.00GHz, 8MB cache, 72W (Haswell)
Монтаж и инсталация на предлаганото оборудване и софтуер	Предлагаме да извършим монтаж и инсталация на предлаганото оборудване и софтуер
Гаранция на системата за управление: 3 години	Предлаганото от нас решение е с гаранция на системата за управление: 3 години

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

Минимални изисквания на възложителя	Предложение от участника /производител, наименование, модел/
Check Point абонамент за право на ползване на ползваните 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	Производител: Check Point Software Technologies Ltd Collaborative Enterprise Subscription Standard Check Point абонамент за право на ползване на ползваните към момента софтуерни лицензи за: Потребителски акаунт ID: 0006243388 Клиент: Ministry of Health Подновяване на лицензите е за период от 3 години с Крайна дата: 01-01-2021
Участникът в процедурата да има предоставени лицензионни права от производителя или негов упълномощен представител за продажба, разпространение и техническо обслужване на продукти Check Point Текнолъджис на територията на Република България. Това обстоятелство се доказва с предоставянето на оторизационно писмо от производителя Чек Пойнт Текнолъджис, че участникът е упълномощен да доставя и обслужва продукти на Check Point на територията на Република България.	Нашата фирма е единствената сред всички интегратори на производителя Check Point Software Technologies за Република България с акредитация „Партньор 3 звезди с Добавена стойност". Това високо ниво на сертификация дава право фирмата ни да доставя софтуерни и хардуерни продукти на CheckPoint. Нашите сертифицираните специалисти притежават квалификацията да извършват услуги по инсталиране, конфигуриране и обслужване на инфраструктурата на Check Point. Фирмата ни ще предостави оторизационно писмо от производителя Чек Пойнт Текнолъджис.

1.4 Осигуряване на извънгаранционна абонаментна поддръжка на сървър SinFire X4100

Минимални изисквания на възложителя	Предложение от участника /производител, наименование, модел/
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.	Ние предлагаме на осигурим хардуерна поддръжка 5x8xNBD на сървър SunFire X4100 в рамките на 3 години. Поддръжката, която предлгаме включва осигуряването на: - Консултации по телефона с наши специалисти; - Инженер на място за отстраняване на проблема, след получена заявка.

1. Приемаме общите и технически изисквания за изпълнение на предмета поръчката.

2. Изпълнението на поръчката ще бъде в съответствие с изискванията на техническата спецификация и проекта на договора.

3. Гарантираме, че сме в състояние да изпълним качествено поръчката в пълно съответствие с гореописаната оферта.

4. Заверено копие на оторизационно писмо от производителя Чек Пойнт Технолъджис, че участникът е упълномощен да доставя и обслужва продукти Check Point на територията на Република България.

ДАТА: 20.02.2018 г. ИМЕ, ПОДПИС и ПЕЧАТ:_____

/ Катя Танева, Управител/