Приложение1

ТЕХНИЧЕСКА СПЕЦИФИКАЦИЯ ЗА ДОСТАВКА, ИНСТАЛАЦИЯ И ГАРАНЦИОННА ПОДДРЪЖКА НА „СИСТЕМА ИЗПОЛЗВАНА ЗА ВЪНШНА „ЗАЩИТА СТЕНА“ – СЪСТАВЕНА ОТ 2 БРОЯ УСТРОЙСТВА (АКТИВНО И РЕЗЕРВНО)“:

Минимални технически характеристики, функционалности и изисквания
Обособяване на зони с различна степен на доверие, като разделя мрежата на отделни сегменти според функционалните им характеристики;
Обособяване на зони за комуникация с външна мрежа и контролира достъпа до тях.
Контролира трафика между зоните с вътрешни потребители и Интернет.
На база на акредитация от Активната Директория контролира поведението на всеки един потребител при достъпа му до Интернет и вътрешните ресурси.
Предмет на настоящата поръчка е доставка на система от 2 броя устройства (активно и резервно) със следните характеристики и функционалности:
Системата трябва да извършва инспекция на трафика и идентификация на приложенията.
Системата трябва да осъществява ааащита от мрежови атаки чрез система за превенция на атаките (IPS).
Системата трябва да анализира съдържанието за наличие на зловреден код (AntiVirus и AntiSpyware). Да се прилагат различен анализ на база категория от URLs или група от приложения.
Системата следва да има възможност чрез добавяне на допълнителен лиценз да анализира Zero Day на зловреден код чрез стартиране на файла във защитената среда.
Системата трябва да осъществява филтриране на уеб сайтовете по категории с цел да се ограничи достъпа на потребителите на вътрешни за мрежа до ресурси до опасно съдържание в Интернет.
Системата трябва да притежава DLP (Data Loss Prevention) функционалност, като по този начин ще се осъществява идентификация на файлове по име и разширение, изпращани и/или получавани в мрежовия трафик, за да се минимизира възможността за изнасяне на конфиденциална информация и контрол на информационните канали.
Системата трябва да осъществява инспекция на HTTPS протокола - декриптиране и инспекция на входяща и изходящ SSL мрежова комуникация.
Системата трябва да осъществява инспекция на HTTP 2.0 протокола инспекция на входяща и изходящ комуникация
Системата трябва да притежава функционалности за декриптиране на SSL мрежова комуникация, която транспортира в себе си криптирани SMTP, IMAP, POP3, FTP и пр.
Декриптирането на SSL трафика, трябва да е прозрачно за всички функционални компоненти на системата: IPS, AntiVirus, AntiSpyware, инспекция на данни и файлове, и URL филтриране.
Политиката за декриптиране трябва да има възможност да се настройва на база на URL категория.
Политиката за декриптиране трябва да има възможност да блокира достъпа до даден Web Site в случай, че отсрещната страна не използва необходимо ниво на криптиране или валиден сертификат.
Системата трябва да бъде оборудвано с всички лицензи необходими за изграждане на отдалечен VPN достъп от крайно клиентски станции като персонални компютри и лаптоп.
Системата трябва да осъществява блокиране на всички приложения чрез прилагане на принципа за минималния достъп (The Principle of Least Privileges) – всички приложения, които не са изрично указани като разрешени за използване в конфигурираните в системата политики, да бъдат блокирани.

Системата трябва да осъществява идентификация на приложенията без оглед на използвания от тях комуникационен порт, протокол (включително P2P, IM, Skype, Webmail, Webex и пр.) и криптирана или не форма на комуникация с цел налагане на политики и спазване на правилата за информационна сигурност
Системата трябва да предоставя възможност за конфигурация на политиките за сигурност чрез дефиниране на източника на мрежовата комуникация, крайната цел на мрежовата комуникация (посока), приложението и/или приложенията, за които се отнася политиката, дефиниране на мрежовите услуги както и каква да бъде активната реакция ако критериите бъдат изпълнени.
Системата трябва да осъществява препращане на подозрителните DNS заявки към специално подбран произволен адрес с цел бърза идентификация и блокиране на комуникацията на заразени хостове от вътрешната мрежа.
Системата трябва да предоставя механизъм, интегриран в мениджмънт интерфейса, който да позволява корелация между аномалиите в мрежовия трафик и поведението на крайните потребители с цел идентификация на потенциално заразени крайни станции, които са част от ботнет мрежи.
Системата трябва да предоставя функционалност за дефиниране на VLAN-и за Layer 2 и Layer 3 интерфейсите с цел да се осигурят гъвкави механизми за инспекция на трафика, които да поддържат създадените за нуждите на организацията мрежови сегменти.
Системата трябва да предоставя функционалност за изграждане на site-to-site VPN тунели на база IPSec и IKE стандартите. Приложение на SSL стандарта за реализация на client-to-site топология за предоставяне на сигурен криптиран достъп до централизираните информационни ресурси
Системата трябва да предоставя функционалност за управление и приоритизиране на трафика (QoS) според типа приложение.
Системата трябва да предоставя прозрачна идентификация на потребителите без изискване да се предоставят потребителско име и парола.
Системата трябва да предоставя защита на корпоративните потребителски имена и пароли да бъдат използвани в системи на публично достъпни доставчици. (Dropbox, Google, Facebook, LinkedIn)
Системата трябва да предоставя функционалност за дефиниране на индивидуални маршрутизиращи таблици с цел осигуряване на маршрутизиращи функционалности за различните мрежови сегменти.
Системата трябва да предоставя функционалност за мониторинг, анализ на логовете и репортинг от самото устройство.
Системата трябва да притежава уеб базиран интерфейс за управление на устройството и индивидуално дефинируеми в системата полета за показване на различни статистики на база време, приложение, категории, потребители, заплахи и пр.
Логовете на системата трябва да са достъпни в уеб интерфейса с възможност за контекстуално филтриране или филтриране на база ключова дума. Информацията следва да е обогатена контекстуално с данни за потребител и група, получена от интеграция с бази за управление на потребителите (Active Directory, LDAP и др.).
Системата трябва да притежава функционалност за интегриране с централизирана мениджмънт система, с която да могат да се прилагат предварително конфигурирани политики за защитни стени и крайно клиентска защита.
Системата трябва да притежава функционалност за интеграция с крайно клиентски софтуер за защита от същия производител работещ на база на machine learning и анализ на поведение на приложенията.

Системата трябва да притежава функционалност за интеграция с централизирана облачна платформа от същия производител за анализ на логовете и предоставяне на анализ за текущи атаки в организацията чрез автоматична детекция базирана на поведение. (Unsupervised machine learning)	
Системата трябва да притежава функционалност за интеграция с облачна услуга на същия производител за анализ и отчет на текущите атаки/ заплахи както за организацията така и за сходни с нея. Показване на тенденции, анализи и методи за превенция в световен мащаб.	
Системата трябва да може да инспектира DNS трафик и да прави превенция на атаки базирани на DNS Tunneling .	
Системата трябва да може да следи и ограничава достъпа до автоматично генерирани домейни (Domain generation algorithms (DGA))	
Системата трябва да притежава възможност за миграция на работещата конфигурация (Backup) от основното устройство към резервното, включваща всички функционалности и лицензи	
Минимални технически характеристики на устройствата (активно и резервно):	
Минимална пропускателна способност	4.6 Gbps
Минимална пропускателна способност с активирана функция за идентификация на приложенията	4.5 Gbps
Минимална пропускателна способност с активирани функционалности за IPS/AntiVirus/ AntiMalware защита, URL филтриране и идентификация на файлове и чувствително съдържание в трафика	2.1 Gbps
Идентификация на приложенията	Функционалността следва да се осигурява от самата защитна стена
Минимален брой TCP сесии	900,000
Минимален брой нови сесии в секунда	52,000
Да поддържа интеграция с HSM	Да
Минимален брой на разпознати и поддържани приложения	2750
Минимален брой интерфейси	Да разполага 12x10/100/1000Base-T ports и 4x10G SFP+ Ports.
Режими на интерфейсите	L2, L3, Tap, Transparent mode (Virtual Wire)
Машрутизиращи функции	OSPFv2/v3, BGP with graceful restart, RIP, static routing Policy-based forwarding Point-to-Point Protocol over Ethernet (PPPoE) Multicast: PIM-SM, PIM-SSM, IGMP v1, v2, and v3 Bidirectional Forwarding Detection (BFD)
Минимални изисквания към IPSec имплементация	Key exchange: manual key, IKEv1 and IKEv2 (pre-shared key, certificate authentication) Encryption: 3DES, AES (128-bit, 192-bit, 256-bit) Authentication: MD5, SHA-1, SHA-256, SHA-384, SHA-512

Минимален брой конкурентни SSL VPN потребителя включени в системата	1000 SSL VPN потребителя
Минимален брой IPSec Site-to-Site VPN тунела/тунелни интерфейси	3000 тунела/тунелни интерфейси
Устройството да има възможност за виртуални контексти минимум	5 броя
Устройството да поддържа виртуални таблици за маршрутизация минимум	10 броя
Минимален брой поддържани VLAN	4,094 броя IEEE 802.1q VLAN маркера (tags), конфигурируеми за всеки интерфейс и общо за устройството
IPv6 поддръжка	Всички конфигурации за интерфейсните модули на защитната стена трябва да поддържат IPv6 както и всички контролни функции на системата трябва да се налични и за IPv6
Инспекция на SSL криптиран трафик, без оглед на прилежащия протокол, като предоставя декриптирания трафик на всички свои функционални компоненти, за инспекция и налагане на политики над съдържанието	Системата следва да декриптира и инспектира SSL
Споделяне на декриптирания SSL трафик	Системата следва да предоставя възможност декриптирания SSL трафик да може да бъде споделян през mirror port с други системи, които не разполагат с възможност за декриптиране на SSL трафик
Управление на канала	Управлението на канала (QoS) следва да е налично и приложимо за всяко идентифицирано приложение
Управление на устройството	Всяко от устройствата в системата да има възможност да се управлява посредством имплементация на REST based API за преглед на конфигурациите, изпълнение на команди и извличане на данни и репорти в XML формати. Всяко от устройствата в системата следва да поддържа всеки един от следните методи за управление: CLI, уеб конзола, централизирана система за управление
Минимален брой интерфейси за управление	1 x 10/100/1000 out-of-band management port 2 x 10/100/1000 интерфейси за отказоустойчивост 1 x RJ-45 конзолен порт
Монтаж и размери	Предназначена за вграждане в 19‘‘ шкаф с максимален размер 2U
Входно напрежение (Входяща	100-240VAC

честота)	(50-60Hz)
Софтуерна и хардуерна гаранционна поддръжка 365x24x7	Мин. 12 месеца. Изпълнителят следва да предостави всички необходими лицензи за гаранционна поддръжка от Производителя. Доказва се чрез посочване на партиден номер. Поддръжката се очаква да осигурява хардуерна подмяна на дефектирало устройство в рамките на следващия работен ден от регистрирането на проблем, време за реакция при проблеми: критични инциденти (отпадане на услуги) – 1 час, високо приоритетни (частично отпадане на услуги) – 2 часа, средно приоритетни (няма отпадане на услуги, проблем с отделни продукционни функционалности) – 4 часа, нисък приоритет – 8 часа.
Допълнителни изисквания:	
Предложените устройства следва да са нови, неупотребявани, нерециклирани и да бъдат налични в актуалната производствена листа на техния производител.	
Изпълнителят следва да има възможност да предложи оторизирано обучение от Производителя на български език за минимум 1 администратор на Възложителя с продължителност минимум (5 работни дни) и по програма одобрена от Производителя.	
Изпълнителят следва да предостави услуги по инсталация и конфигурация, като в техния обхват следва да бъдат изпълнени като минимум: монтаж на устройствата в шкаф на Възложителя, начална конфигурация и активация на лицензите, последваща конфигурация спрямо настоящо използваните политики за сигурност и модули за защита (Application & URL Filtering, IPS, Treat Prevention) текущо предоставяни от 2 броя устройства Check Point 4400 работещи в клъстер.	

Срок за доставка на 2 броя устройства (активно и резервно) съставляващи система използвана за външна „защита стена“: не по-голям от 30 (тридесет) работни дни.

Срок за инсталация и конфигурация: не по-голям от 30 (тридесет) работни дни.

Изисквания към техническите възможности на участниците:

Участникът следва да има внедрена система за управление на качеството по стандарт ISO 9001:20XX или еквивалентен с обхват включващ: доставка на ИТ оборудване и/или софтуерни продукти.