Аукциондық құжаттамаға 7-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	Түркістан облысының білім басқармасының "№16 колледж" мемлекеттік коммуналдық қазыналық кәсіпорны
Ұйымдастырушының атауы:	Түркістан облысының білім басқармасының "№16 колледж" мемлекеттік коммуналдық қазыналық кәсіпорны
Аукционның №:	№ 18007008-1
Аукционның атауы:	Техникалық сипаттамаларға сәйкес тауар сатып алу
Лоттың нөмірі:	№ 87945084-АУК1
Лоттың атауы	Арнайы экран
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	263021.900.000009
Тауардың атауы*:	Арнайы экран
Өлшем бірлігі*:	Дана
Саны (көлемі)*:	1
Қосылған құн салығын есептемегенде бірлік бағасы*:	3448275.86
Қосылған құн салығын есепке алмағанда, сатып алуға бөлінген жалпы сома*:	3448275.86
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*:	

Жеткізу шарттары (сәйкес ИНКОТЕРМС 2010)*	DDP термині келу орнын көрсете отырып қолданылады. Бұл сатып алушының елінде көрсетілген жерге тауар жеткізілгеннен кейін сатушының жауапкершілігі аяқталатынын білдіреді. Жүктерді жеткізу бойынша барлық тәуекелдер, барлық шығыстар (салықтар, баждар және т.б.), импорт кезінде төленетін баждар мен басқа да төлемдерді қоса алғанда, тауардың бүлінуі мен жоғалуы үшін жауапкершілік осы уақытқа дейін сатушыға жүктеледі, сатушы сонымен қатар кедендік тазартуға жауап береді
Жеткізу мерзімі*	Мемлекеттік сатып алу туралы шарт заңды күшіне енген күннен бастап күнтізбелік 15 (он бес) күн ішінде
Жеткізу орны*	616420100, Түркістан облысы, Шардара ауданы, Шардара қ. С. Аширова 16А
Аванстық төлем мөлшері*:	0
Ұлттық стандарттардың атауы, ал олар болмаған жағдайда сатып алынатын тауарларға арналған мемлекетаралық стандарттар. Ұлттық және мемлекетаралық стандарттар болмаған кезде мемлекеттік сатып алуды нормалауды ескере отырып, сатып алынатын тауарлардың талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары көрсетіледі.	СТ РК ISO/IEC 15408
Авиациялық техниканы сатып алуды қоспағанда, тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс	
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауарлардың қажетті функционалдық, техникалық, сапалық, өнімділігі мен басқа да сипаттамаларының сипатталуы	Келесі буын фаерволына қойылатын талаптар. Қауіпсіздік шлюзі желілік ағынды бақылау және басқару үшін байланыс пен қолданба күйін егжей-тегжейлі талдау негізінде қосылымдар күйін бақылауды пайдалануы тиіс. Шешім DHCP-ді, сервер және relay қолдауы тиіс. Шешім Transparent/Bridge режимінде жұмыс істеу мүмкіндігін қамтуы тиіс. Шешім OSI моделінің 2-деңгейінде (bridge режимі) жұмыс істеуді қолдауы тиіс. Шешім bridge режимінде Firewall, IPS, URL-сүзгілеу, Antibot, Antivirus, Қолданбаларды басқару, HTTPS инспекциясы, Identity Awareness және Sandboxing қолдауы тиіс. Шешім bridge режимінде Active/Standby кластерлеуді қолдауы тиіс. Шешім желілік қосылымдардың күйлерін синхрондай отырып, шлюздің жоғары қолжетімділігін қамтамасыз етуі тиіс. Шешім IPv6 қолдауын қамтамасыз етуі тиіс. Шешім QoS негізіндегі саясатты қолдауы тиіс. Шешім белгілі бір бастапқы IP, тағайындалған IP немесе сервис үшін өткізу қабілеттілігіне кепілдік беруге немесе оны шектеуге және кідірісті басқаруға мүмкіндік беруі тиіс. Шешімде VPN трафигі үшін QoS ережелерін еркін қолдану мүмкіндігі болуы тиіс. Шешім IPS (басып кіруді болдырмау жүйесі) функционалын қамтамасыз етуі тиіс. IPS жүйесі келесі анықтау механизмдеріне негізделуі тиіс: сигнатураларды пайдалану, хаттамалар ауытқуларын бақылау, қолданбаларды басқару және мінез-құлық негізінде анықтау. Шешім Пайдаланушыларды сәйкестендіру функционалын қамтамасыз етуі тиіс. Қауіпсіздік оқиғалары негізінде Microsoft Active Directory сұрауы арқылы пайдаланушы идентификаторларын жинауға қабілетті болуы тиіс. Доменге кірмейтін пайдаланушылар немесе компьютерлер үшін браузер негізінде пайдаланушы идентификаторын аутентификациялау әдісі болуы тиіс. Пайдаланушылардың компьютерлеріне саясат бойынша орнатылатын және идентификаторларды жинап, қауіпсіздік шлюзіне бере алатын арнайы агенті болуы тиіс. Шешім Қолданбаларды басқару және URL-сүзгілеу функционалын қамтамасыз етуі тиіс. Қолданбаларды басқару дерекқорында 10000-нан астам белгілі қолданба болуы тиіс. Шешім кемінде 255000 Web 2.0 виджеті үшін егжей-тегжейлі қауіпсіздік бақылауын қамтамасыз етуі тиіс. Шешім 200 миллионнан астам URL қамтитын URL санаттауды қамтамасыз етуі тиіс. Шешім Anti-Bot және Anti-Virus функционалын қамтамасыз етуі тиіс. Anti-bot қолданбасы күдікті қалыптан тыс желілік мінез-құлықты анықтап, тоқтатуға қабілетті болуы тиіс. Anti-Bot қолданбасы IP, URL және DNS мекенжайларының беделін және байланыс хаттамаларының үлгілері бойынша боттарды анықтауды қамтитын көп деңгейлі анықтау механизмін пайдалануы тиіс. Anti-virus қолданбасы зиянды веб-сайттарға кіруді болдырмауы және кіріс зиянды файлдарды тоқтатуы тиіс. Anti-virus қолданбасы шифрланған SSL трафигін тексере алуы тиіс. Шешім SSL инспекциясы (кіріс / шығыс трафигі) функционалын қамтамасыз етуі тиіс. Шешім лицензия болған кезде «құмсалғыш» - Sandboxing функционалын (инспекция – бұлтта немесе бөлінген жергілікті құрылғыда) қамтамасыз етуі тиіс. «Құмсалғыш» функционалы нөлдік күн шабуылдарынан (0-day attacks), сондай-ақ белгісіз

	зиянды БҚ-дан қорғауды қамтамасыз етуі тиіс – мұндай қатерлерден қорғайтын статикалық сигнатуралар пайда болғанға дейінгі кезеңде қорғауды қамтамасыз етеді. Құмсалғышты енгізу топологиясы: Желілік құмсалғыш режимін (network based) қолдау; Инлайн режимін (bridge mode) қолдау; Почта агенті режимін (mail transfer agent) қолдау; Айналық порт режимін (TAP/SPAN порт) қолдау; Шешім істен шығуға төзімділікті қамтамасыз ету үшін кластерлеуді қолдауы тиіс. Шешім орындалатын файлдарды, мұрағаттарды, құжаттарды, соның ішінде Java және flash эмуляциялауы тиіс. Эмуляция қозғалтқышы әртүрлі операциялық жүйелерді, мысалы, XP және Windows 7, 8.1, 10, соның ішінде арнайы бапталған бейнелерді (customized images) қолдауы тиіс. Эмуляция қозғалтқышы зиянды БҚ-дан қорғау инфрақұрылымына инспекциялауы, эмуляциялауы, болдырмауы және оқиғаларды беруі тиіс. Шешім шағын көлемді файлдардың да, 100Мбайт-қа дейінгі көлемдегі файлдардың да эмуляциясын қамтамасыз етуі тиіс. Шешім шабуылдарды эксплойттың орындалу (exploitation) сатысында – яғни шелл-код (shell code) іске қосылғанға дейін және зиянды БҚ кодының өзі жүктеліп/орындалғанға дейін анықтауы тиіс. Шешім орталық процессор нұсқаулары тізбегінің орындалуын мониторингілеу арқылы ROP (return oriented programming) және басқа да эксплойт техникаларын (соның ішінде артықшылықтарды эскалациялауды – privilege exploitation) анықтауы тиіс. Шешім нөлдік күн шабуылдарынан (0-day attacks), сондай-ақ белгісіз зиянды БҚ-дан қорғау үшін почта хабарламаларының ішіндегі сілтемелерді сканерлеуді қамтамасыз етуі тиіс. Шешімде құмсалғышта орындалуды анықтау әдістемелеріне қарсы күрес құралдары болуы тиіс. Шешім оны орталықтандырылған менеджменттен басқару мүмкіндігін қамтамасыз етуі тиіс. Шешім әрбір зақымдалған файлды талдау нәтижелері бойынша егжей-тегжейлі есеп жасауы тиіс. Шешім әлеуетті қауіпті құжаттың қауіпсіз көшірмесін лезде жеткізуді қолдауы тиіс. Шешім IPSEC VPN функционалын қамтамасыз етуі тиіс. Ішкі CA (Certificate Authority), сондай-ақ сыртқы үшінші тарап CA қолдауы болуы тиіс. Шешім IKE I және II IKEv2 фазалары үшін 3DES және AES-256 шифрлауын, сондай-ақ II фаза үшін "Suite-B-GCM-128" және "Suite-B-GCM-256" қолдауы тиіс. Шешім кемінде келесі Diffie-Hellman топтарын қолдауы тиіс: 1-топ (768 бит), 2-топ (1024 бит), 5-топ (1536 бит), 14-топ (2048 бит), 19-топ және 20-топ. Шешім md5, sha1 SHA-256, SHA-384 және AES-XCBC құралдарымен деректердің тұтастығын қамтамасыз етуді қолдауы тиіс. Шешім келесі топологиялардағы site-to-site типті VPN қолдауын қамтуы тиіс: Толық байланысқан желі (бәрі-бәрімен), Жұлдыз тәрізді желі (қашықтағы кеңселер орталық сайтқа) Желпуіш тәрізді желі (қашықтағы сайт орталық сайт арқылы басқа қашықтағы сайтқа) Қашықтағы мобильді қолжетімділік Шешім Қашықтағы мобильді қолжетімділік функционалын пайдаланушылардың кемінде 100 бір мезгілдегі қосылымы үшін қамтамасыз етуі тиіс. Шешім екі факторлы аутентификация шешімдерімен интеграцияны қолдауы тиіс. Шешім веб-қосымшаларда берілетін зиянды кодтан басып кіруді

	болдырмаудың біріктірілген жүйесі функционалын іске асыруы тиіс. Шешім құрттарды, буфердің толып кетуі, SQL және командалар инъекциялары, сайтаралық скрипттік орындау сияқты әртүрлі шабуылдарды бұғаттауға, HTTP құрттарын бұғаттаудың банталатын модулін, каталогты шарлаудан (directory traversal) қорғауды, тақырыптарды қабылдамаудан (header rejection) қорғауды, зиянды HTTP-кодтан қорғауды қамтамасыз етуге қабілетті болуы тиіс. Жалпы алғанда, шешім келесі функцияларды қамтамасыз етуі тиіс: Қауіпсіз VPN қолжетімділік Мобильді құрылғыларды соңғы пайдаланушылармен байланыстыру Шлюзге қойылатын аппараттық және жұмыс талаптары. Өнімді желілік интерфейстер (ең төменгі талаптар): SD card slot 6 x 1 Гбит/с LAN мыс порттары 1 x 1 Гбит/с DMZ опциялық оптикалық немесе мыс порты Консольдық порт USB Type-C 1 x 1 Гбит WAN опциялық оптикалық немесе мыс порты 1 x USB 3.0 порты 1 қуат көзі блогы Firewall өткізу қабілеттілігі: кемінде 2,25 Гбит/с. IPS өткізу қабілеттілігі: кемінде 1,72 Гбит/с. NGFW өткізу қабілеттілігі (Firewall, Application Control және IPS функционалы белсендірілген кезде): кемінде 1,2 Гбит/с. Threat Prevention өткізу қабілеттілігі (smart accel функционалымен): кемінде 750 Мбит/с. Firewall 1518 Byte UDP Packets: Кемінде 3 Гбит/с VPN AES-128 Throughput: кемінде 1,4 Гбит/с Бір мезгілдегі қосылымдар: кемінде 1 000 000. Жаңа қосылымдар: секундына кемінде 16 000. Шешім Қашықтағы мобильді қолжетімділік функционалын пайдаланушылардың кемінде 100 бір мезгілдегі қосылымы үшін қамтамасыз етуі тиіс. Шешім Мобильді VPN-Клиентті қамтамасыз етуі тиіс: IPsec туннель арқылы корпоративтік ресурстарға қауіпсіз қолжетімділікті қамтамасыз ететін VPN-қосымша. Қолдау және жазылым. Вендордан 1 жыл мерзімге қолдау, 24x7, жабдықты кепілдікті ауыстыру, қауіпсіздік сервистеріне барлық қажетті жазылымдар қосылуы тиіс. Жеткізушіге қойылатын талаптар. Әлеуетті жеткізуші құқық иеленушіден Қазақстан Республикасының аумағында өткізуге авторизациялық хат (электрондық көшірмесін қоса беру) ұсынуы тиіс. Авторизациялық хатта тиісті сатып алу лотының нөмірі болуы және ол өтінімге электрондық көшірме түрінде қоса берілуі тиіс. Жеткізуші Тапсырыс берушіге тауарды корпоративтік лицензиялау келісімі шеңберінде жеткізуді қамтамасыз етуі тиіс. Жеткізу Тапсырыс берушінің мекенжайына бір мезгілде және толық көлемде, түсіру жұмыстарын қоса алғанда жүзеге асырылуы тиіс. Жеткізу және ілеспе қызметтер көрсету – орнату және баптау мерзімі – шарт жасасылған және ҚР Қазынашылығында тіркелген сәттен бастап 30 күнтізбелік күн. Әлеуетті жеткізуші өзінің конкурстық өтінімінде Қазақстан Республикасының аумағында БҚ-ға корпоративтік лицензияларды жеткізу құқығын беретін құқық иеленуші өкілімен қолданыстағы серіктестік келісімнің бар екенін растауы (электрондық көшірмесін қоса беру) тиіс.

Ілеспе қызметтер (қажет болған жағдайда көрсетіледі) (тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	
Әлеуетті өнім беруші оны жеңімпаз деп айқындаған және онымен мемлекеттік сатып алу туралы шарт жасасқан жағдайда (қажет болған жағдайда көрсетіледі) (Әлеуетті өнім берушінің көрсетілген мәліметтерді көрсетпегені және ұсынбағаны үшін бас тартуына жол берілмейді)	

Ескертпе:
1. Функционалдық, техникалық, сапалық, пайдалану, өзге де сипаттамалар, ілеспе қызметтер және орындаушыға қосымша шарттар бойынша әрбір талап жеке жолда көрсетіледі.
2. Осы техникалық ерекшелікте әлеуетті өнім берушіге қойылатын біліктілік талаптарын белгілеуге жол берілмейді.
3. Өзге құжаттарда техникалық ерекшелік талаптарын белгілеуге жол берілмейді.
4. Әлеуетті өнім беруші аукцион жеңімпазы деп танылған және онымен шарт жасалған жағдайда, мұндай шарттың техникалық ерекшелігі аукцион жеңімпазының техникалық ерекшелігінің негізінде қалыптастырылады.
*мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

Приложение 7
к Аукционной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Государственное коммунальное казенное предприятие "Колледж №16" управления образования Туркестанской области
Наименование организатора	Государственное коммунальное казенное предприятие "Колледж №16" управления образования Туркестанской области
№ аукциона:	№ 18007008-1
Наименование аукциона:	Приобретение товаров согласно технической спецификации
Номер лота:	№ 87945084-АУК1
Наименование лота:	Экран специальный
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	263021.900.000009
Наименование товара*:	Экран специальный
Единица измерения*:	Штука
Количество (объем)*:	1
Цена за единицу, без учета налога на добавленную стоимость*:	3448275.86
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	3448275.86
Условия поставки (в соответствии с ИНКОТЕРМС 2010)*:	DDP термин употребляется с указанием места прибытия. Он означает, что ответственность продавца заканчивается после того, как товар доставлен в указанное место в стране покупателя. Все риски, все расходы по доставке груза (налоги, пошлины и т. д.), ответственность за порчу и потерю товара, включая пошлины и прочие выплаты, выплачиваемые при импорте, до этого момента несёт продавец, также он несёт ответственность за таможенную очистку.
Срок поставки*:	В течение 15 (пятнадцать) календарных дней со дня вступления договора о государственных закупках в законную силу

Место поставки товара*:	616420100, Туркестанская область, Шардаринский район, г.Шардара С. Аширова 16А
Размер авансового платежа* **:	0 %
Наименование национальных стандартов, а при их отсутствии межгосударственных стандартов на закупаемые товары. При отсутствии национальных и межгосударственных стандартов указываются требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров, с учетом нормирования государственных закупок.	СТ РК ISO/IEC 15408
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора, за исключением приобретения авиационной техники	
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	Требования к фаерволу следующего поколения. 1.1. Шлюз безопасности должен использовать контроль состояния соединений на основе детализированного анализа связи и состояния приложения для отслеживания и управления сетевым потоком. 1.2. Решение должно поддерживать DHCP, сервер и relay. 1.3. Решение должно включать в себя возможность работы в режиме Transparent/Bridge. 1.3.1. Решение должно поддерживать работу на 2 уровне модели OSI (режим bridge). 1.3.2. Решение должно поддерживать Firewall, IPS, URL-фильтрацию, Antibot, Antivirus, Управление приложениями, инспекцию HTTPS, Identity Awareness и Sandboxing в режиме bridge. 1.3.3. Решение должно поддерживать кластеризацию Active/Standby в режиме bridge. 1.4. Решение должно поддерживать высокую доступность шлюза с синхронизацией состояний сетевых соединений. 1.5. Решение должно обеспечивать поддержку IPv6. 1.6. Решение должно поддерживать политику, основанную на QoS. 1.6.1. Решение должно позволять гарантировать или ограничивать пропускную способность и управлять задержкой для определенного IP источника, IP пункта назначения или сервиса. 1.6.2. Решение должно иметь возможность произвольного применения правил QoS для VPN трафика. 1.7. Решение должно обеспечивать функционал IPS (системы предотвращения вторжений). 1.7.1. Система IPS должна основываться на следующих механизмах обнаружения: использование сигнатур, отслеживание аномалий протоколов, управление приложениями и обнаружение на основе поведения. 1.8. Решение должно обеспечивать функционал Идентификации пользователей. 1.8.1. Должно быть способно к сбору идентификаторов пользователей посредством запроса Microsoft Active Directory на основе событий безопасности. 1.8.2. Должно иметь метод аутентификации идентификатора пользователя на основе браузера для недоменных пользователей или компьютеров. 1.8.3. Должно иметь специального агента, который может быть установлен по политике на компьютерах пользователей, и который может собирать и передавать идентификаторы на шлюз безопасности. 1.9. Решение должно обеспечивать функционал Управления приложениями и URL-фильтрации. 1.9.1. База данных управления приложениями должна содержать свыше 10000 известных приложений. 1.9.2. Решение должно обеспечивать детальный контроль безопасности минимум для 255000 Web 2.0 виджетов. 1.9.3. Решение должно обеспечивать URL категоризацию, включающую более 200 миллионов URL. 1.10. Решение должно обеспечивать функционал Anti-Bot и Anti-Virus. 1.10.1. Приложение Anti-bot должно быть способно обнаружить и остановить подозрительное анормальное сетевое поведение. 1.10.2. Приложение Anti-Bot должно использовать многоуровневый механизм обнаружения, который включает репутацию IP, URL и DNS адресов и обнаружение ботов по шаблонам протоколов связи. 1.10.3. Приложение Anti-virus должно предотвращать доступ к вредоносным веб-сайтам и останавливать входящие вредоносные файлы. 1.10.4. Приложение Anti-virus должно быть способно проверять шифрованный SSL трафик. 1.11. Решение должно

	обеспечивать функционал инспекции SSL (входящего / исходящего трафика). 1.12. Решение должно обеспечивать функционал «песочницы» - Sandboxing (инспекция – в облаке или на выделенном локальном устройстве) при наличии лицензии. 1.12.1. Функционал «песочницы» должен обеспечивать защиту от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО – обеспечивая защиту в период до появления статических сигнатур, защищающих от таких угроз. 1.12.2. Топология внедрения песочницы: - Поддержка режима сетевой песочницы (network based); - Поддержка режима инлайн (bridge mode); - Поддержка режима почтового агента (mail transfer agent); - Поддержка режима зеркального порта (TAP/SPAN порт); 1.12.3. Решение должно поддерживать кластеризацию для обеспечения отказоустойчивости. 1.12.4. Решение должно эмулировать исполняемые файлы, архивы, документы, включая Java и flash. 1.12.5. Движок эмуляции должен поддерживать различные операционные системы, например, XP и Windows 7, 8.1, 10, в том числе специально настроенные образы (customized images). 1.12.6. Движок эмуляции должен инспектировать, эмулировать, предотвращать и передавать события в инфраструктуру защиты от зловредного ПО. 1.12.7. Решение должно обеспечивать эмуляцию файлов как небольшого размера, так и размером до 100Мбайт. 1.12.8. Решение должно детектировать атаки на стадии выполнения экслойта (exploitation) – т. е. до того, как запускается шелл-код (shell code) и осуществляется загрузка/исполнение самого кода зловредного ПО. 1.12.9. Решение должно детектировать ROP (return oriented programming) и другие техники эксплойтов (а том числе эскалацию привилегий – privilege exploitation) посредством мониторинга выполнения последовательности инструкций центрального процессора. 1.12.10. Решение должно обеспечивать сканирование ссылок внутри почтовых сообщений для защиты от атак нулевого дня (0-day attacks), а также от неизвестного зловредного ПО. 1.12.11. Решение должно содержать средства борьбы с методиками детектирования исполнения в песочнице. 1.12.12. Решение должно обеспечивать возможность управления им с централизованного менеджмента. 1.12.13. Решение должно генерировать детальный отчет по результатам анализа каждого зараженного файла. 1.12.14. Решение должно поддерживать мгновенную доставку безопасной копии потенциально опасного документа. 1.13. Решение должно обеспечивать функционал IPSEC VPN. 1.13.1. Должна быть поддержка внутреннего CA (Certificate Authority), а также внешних сторонних CA. 1.13.2. Решение должно поддерживать 3DES и AES-256 шифрование для IKE фазы I и II IKEv2, а также "Suite-B-GCM-128" и "Suite-B-GCM-256" для фазы II. 1.13.3. Решение должно поддерживать как минимум следующие группы Diffie-Hellman: Группа 1 (768 бит), Группа 2 (1024 бит), Группа 5 (1536 бит), Группа 14 (2048 бит), Группа 19 и Группа 20. 1.13.4. Решение должно поддерживать обеспечение целостности данных средствами md5, sha1 SHA-256, SHA-384 и AES-XCBC. 1.13.5. Решение должно включать в себя поддержку для

	VPN типа site-to-site в следующих топологиях: - Полносвязная сеть (все-со-всеми), - Звездообразная сеть (удаленные офисы к центральному сайту) - Веерная сеть (удаленный сайт через центральный сайт на другой удаленный сайт) 1.14. Удаленный мобильный доступ 1.14.1. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 100 одновременных соединений пользователей. 1.14.2. Решение должно поддерживать интеграцию с решениями двухфакторной аутентификации. 1.14.3. Решение должно реализовать функционал интегрированной системы предотвращение вторжений от вредоносного кода, передаваемого в веб-приложениях. Решение должно быть способно блокировать червей, различные атаки, такие как переполнение буфера, SQL и инъекции команд, межсайтовый скриптинг, настраиваемый модуль блокирования HTTP червей, защиту от обход каталога (directory traversal), защиту от отклонения заголовков (header rejection), защиту от вредоносного HTTP-кода. 1.14.4. В целом, решение должно обеспечивать следующие функции: - Безопасный VPN доступ - Ассоциирование мобильных устройств с конечными пользователями 1.15. Аппаратные и рабочие требования к шлюзу. 1.15.1. Продуктивные сетевые интерфейсы (минимальные требования): - SD card slot - 6 x 1 Гбит/с LAN медных портов - 1 x 1 Гбит/с DMZ опциональный оптический либо медный порт - Консольный порт USB Type-C - 1 x 1 Гбит WAN опциональный оптический либо медный порт - 1 x USB 3.0 порт - 1 блок питания 1.15.2. Пропускная способность Firewall: минимум 2,25 Гбит/с. 1.15.3. Пропускная способность IPS: минимум 1,72 Гбит/с. 1.15.4. Пропускная способность NGFW (с активированным функционалом Firewall, Application Control и IPS): минимум 1,2 Гбит/с. 1.15.5. Пропускная способность Threat Prevention (с функционалом smart accel): минимум 750 Мбит/с. 1.15.6. Firewall 1518 Byte UDP Packets: Минимум 3 Гбит/с 1.15.7. VPN AES-128 Throughput: минимум 1,4 Гбит/с 1.15.8. Одновременные соединения: минимум 1 000 000. 1.15.9. Новые соединения: минимум 16 000 в секунду. 1.15.10. Решение должно обеспечивать функционал Удаленного мобильного доступа минимум для 100 одновременных соединений пользователей. 1.15.11. Решение должно обеспечивать Мобильный VPN-Клиент: VPN-приложение, обеспечивающее безопасный доступ к корпоративным ресурсам через IPsec туннель. 1.16. Поддержка и подписка. 1.16.1. Поддержка сроком на 1 год от вендора, 24x7, гарантийная замена оборудования, должны быть включены все необходимые подписки на сервисы безопасности. 1.17. Требования к поставщику. Потенциальный поставщик должен предоставить авторизационное письмо (приложить электронную копию), от правообладателя, на реализацию на территории Республики Казахстан. Авторизационное письмо должно содержать номер соответствующего лота закупки и быть приложено к заявке в виде электронной копии. Поставщик должен обеспечить поставку Заказчику товара в рамках соглашения корпоративного лицензирования. Поставка должна быть осуществлена единовременно и в полном объеме в адрес Заказчика,

	включая разгрузочные работы. Срок поставки, и оказания сопутствующих услуг -установка и настройка – 30 календарных дней с момента заключения и регистрации договора в Казначействе РК. Потенциальный поставщик в своей конкурсной заявке должен подтвердить (приложить электронную копию) действующего партнерского соглашения с представителем правообладателя, дающее право на поставку корпоративных лицензий на ПО на территории Республики Казахстан.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	
Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках (указываются при необходимости) (Отклонение потенциального поставщика за не указание и непредставление указанных сведений не допускается)	

Примечание
1. Каждое требование по функциональным, техническим, качественным, эксплуатационным, иным характеристикам, сопутствующим услугам и дополнительным условиям к исполнителю указывается отдельной строкой.
2. Установление в настоящей технической спецификации квалификационных требований, предъявляемых к потенциальному поставщику, не допускается.
3. Установление требований технической спецификации в иных документах не допускается.
4. При признании потенциального поставщика победителем аукциона и заключения с ним договора, техническая спецификация такого договора формируется на основе технической спецификации победителя аукциона.
* сведения подтягиваются из плана государственных закупок (отображаются автоматически).