Конкурстық құжаттамаға
13-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі (тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасының Жоғары аудиторлық палатасы" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасының Жоғары аудиторлық палатасы" мемлекеттік мекемесі
Конкурстың №:	№ 14752475-1
Конкурстың атауы:	Желіаралық экран сатып алу
Лоттың нөмірі:	№ 74064910-ОК1
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)*:	2
Қосылған құн салығын есепке алмағандағы бірлік бағасы*:	10551763.39
Қосылған құн салығын есепке алмағанда, сатып алу үшін бөлінген жалпы сома*:	21103526.78
Жеткізу шарттары (ИНКОТЕРМС 2010 сәйкес)*	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*	техникалық ерекшелік талаптарына сәйкес
Жеткізу орны*	711210000, Астана қ., Есіл ауданы Мәңгілік Ел даңғ., 8-үй, "Министрліктер үйі" ғим., 10-кіреберіс
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.	
Тауар жаңа, пайдаланылмаған, шығарылған жылы шарт жасалған күнге дейін (үш жылға дейін) ерте болмауға тиіс*	
Кепілдік мерзімі (айлармен)	12

Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы	Желіаралық экрандарды саты алуға ТЕХНИКАЛЫҚ ӨЗІНДІК ЕРЕКШЕЛІК Осы техникалық өзіндік ерекшелік «Қазақстан Республикасының Жоғары аудиторлық палатасы» ММ-да желілік қауіпсіздікті қамтамасыз ету мақсатында әзірленді. 1. Жалпы талаптар: Жабдықтың барлық ұсынылған сипаттамалары осы техникалық өзіндік ерекшелікте көрсетілген ең төмен техникалық сипаттамаларға сәйкес келуі немесе асып түсуі тиіс. Жабдықтың құрамдас бөліктерін біріктіру үшін үйлесімділікті қамтамасыз ету және уақыт үнемдеу мақсатында жеткізілетін жабдық бір өндірушіден болуы тиіс. Жеткізілетін жабдық монтажды материалдарының барлық қажетті қорымен жинақталуы және орнатудан кейін тікелей пайдалануға толық дайын болуы тиіс. 1. Жеткізілетін жабдықтың көлемі: Желіаралық экран – кемінде 2 данадан. 2. Жеткізілетін жабдықтың техникалық сипаттамалары: Желіаралық экрандауға қойылатын техникалық талаптар: Firewall Throughput (1518/512/64 byte UDP): кемінде 26.5/26/10 Gbps; Бір мезгілдегі сессиялардың саны: кемінде 3 млн; Жаңа қосылыстарды орнату жылдамдығы: кемінде 275 000 сек; Application Control Throughput (HTTP 64K): кемінде 12 Gbps; IPsec VPN Throughput: кемінде 12 Gbps; SSL VPN Throughput: кемінде 2 Gbps; Базалық жиынтықтағы виртуалды қауіпсіздік контексінің саны: кемінде 10; Интерфейстердің саны: кемінде 4x10GE SFP +, 16x GE RJ45, 8x1GE SFP; USB порттарының саны: кемінде 1; RJ-45 консоль порты: кемінде 1; 100–240V AC, 50-60 Hz қуат көзі: кемінде 2 дана; Жергілікті SSD сақтау жүйесі: кемінде 470 GB; 3. Қауіпсіздік шлюзіне қойылатын талаптар: Желіаралық экрандауға қойылатын функционалдық талаптар: жүйені лицензиялау пайдаланушылардың шектеусіз санына жүзеге асырылуы тиіс; жүйе қауіпсіздік модульдерінің қолтаңбаларын және өндірушінің серверінен өзекті қауіптер тізімін үнемі алып отыруы тиіс; жүйе кластер түрлерін құру мүмкіндігімен кластерге кемінде 4 құрылғыны біріктіруді қолдауы тиіс: • суық резервпен (active/passive); • ыстық резервпен (active/active); • теңдестіру кластері; жүйеде желіаралық экран функционалдығы болуы тиіс, яғни IP мекенжайлар, порттар және қосымшалар негізінде желілік трафикті сүзу ережелерін жасау мүмкіндігін қамтамасыз етуі тиіс; жүйеде жүктемені теңдестіру функциясы болуы тиіс; жүйе SD-WAN (Software-Defined Wide Area Network, бағдарламалық қамтылым конфигурацияланатын желі) трафикті ақылды басқару технологиясын қолдауы тиіс; жүйеде трафиктің өткізу қабілеттілігін басқару функциясы болуы тиіс (traffic shaping); жүйе ICAP (Internet Content Adaptation Protocol) хаттамасы бойынша тексерілген трафикті талдау және сыртқы жүйелерге беру мүмкіндіктерімен трафиктің SSL инспекциясын қамтамасыз етуі тиіс; жүйе ZTNA (Zero Trust Network Access) шлюзін енгізу мүмкіндігін қамтамасыз етуі тиіс; жүйе трафиктің SSH талдауын (ssh inspection) қамтамасыз етуі тиіс; жүйе IPv4, IPv6 динамикалық бағыттауды қамтамасыз етуі тиіс; жүйе WCCP протоколы бойынша жұмыс істей алуы тиіс (сервер режимінде де, клиент режимінде де); жүйе WAN қосылуларын оңтайландыруды қамтамасыз етуі тиіс; жүйеде DLP деректерінің бұзылуынан қорғау функциясы болуы тиіс; жүйе аппараттық жеделдету арқылы вирусқа қарсы қорғауды қамтамасыз етуі тиіс; жүйе спамнан қорғауды қамтамасыз етуі тиіс (спамға қарсы); жүйеде аппараттық жеделдетілген IPS шабуылының алдын алу функционалдығы болуы тиіс; жүйеде аппараттық жеделдетумен IPS басып кіруін болдырмау функционалдығы болуы тиіс; жүйе белгілі бір сайттардың санаттарына қолжетімділікті шектеу мүмкіндігімен трафикті WEB сүзуді қамтамасыз етуі тиіс; трафикті кемінде 85 санат бойынша WEB сүзу қамтамасыз етілуі тиіс; танымал іздеу жүйелерінде қауіпсіз іздеу режимін мәжбүрлеп қосу; жүйеде қосымшаларды бақылау функционалдығы болуы тиіс; жүйеде WEB proxy функционалдығы болуы тиіс; жүйе әдепкі бойынша қол жетімді кемінде 10 виртуалды доменнің (бір құрылғының ішінде толық жұмыс істейтін виртуалды МӘС) болуын қамтамасыз етуі тиіс; жүйе HTTP, SMTP, POP3, IMAP, FTP және IM трафигіндегі вирустарды тексере алуы тиіс; жүйе кесте бойынша вирусқа қарсы базалардың жаңартуларын автоматты түрде ала алуы тиіс; жүйеде өлшеміне байланысты файлдарды беруді бұғаттау мүмкіндігі болуы тиіс; жүйеде типіне байланысты файлдарды беруді бұғаттау мүмкіндігі болуы тиіс; жүйе көптеген WAN желілерінің қосылуларын қолдауы тиіс; жүйе PPPoE және L2TP хаттамаларын қолдауы тиіс; жүйе «Клиент/Сервер» конфигурациясында DHCP хаттамасын қолдауы тиіс; жүйе саясаттар негізінде маршруттауды қолдауы тиіс; жүйе RIP v1 және v2, OSPF, BGP хаттамаларына негізделген динамикалық маршруттауды қолдауы тиіс; жүйе қауіпсіздік аймақтарын пайдалануды қолдауы тиіс; жүйе аймақтар арасындағы маршруттауды қолдауы тиіс; жүйе виртуалды желілер арасындағы маршруттауды қолдауы тиіс; жүйе рөлдерге негізделген әкімшілендіруді қолдауы тиіс; жүйе әкімшілер мен пайдаланушылардың бірнеше деңгейлерін қолдауы тиіс; жүйе TFTP хаттамасы және web-интерфейс арқылы орнатылған бағдарламалық қамтылымды жаңартуды қолдауы тиіс; жүйе кіріктірілген бағдарламалық қамтылымның алдыңғы жай-күйіне (нұсқасына) оралу мүмкіндігін қолдауы тиіс; жүйе ішкі дерекқор арқылы пайдаланушылардың аутентификациясын қолдауы тиіс; жүйе Kerberos пайдаланушының аутентификациясын қолдауы тиіс; жүйе Windows Active Directory арқылы пайдаланушылардың аутентификациясын қолдауы тиіс; бұл жағдайда доменге енгізілген Windows 7 және одан жоғары операциялық жүйелердің пайдаланушыларының аутентификациясы қосымша құпия сөзді сұрау рәсімінсіз автоматты түрде орындалуы тиіс; жүйе сыртқы RADIUS/LDAP дерекқоры арқылы пайдаланушылардың аутентификациясын қолдауы тиіс; жүйе IP/MAC мекенжайын байланыстыру арқылы пайдаланушылардың аутентификациясын қолдауы тиіс; жүйе пайдаланушы топтары негізінде аутентификацияны қолдауы тиіс; жүйе NAT, PAT, «мөлдір» (көпір) функцияларын қолдауы тиіс; жүйе саясатқа негізделген NAT функцияларын қолдауы тиіс; жүйе VLAN Tagging (802.1 Q) функцияларын қолдауы тиіс; жүйе SIP/H323 NAT Traversal функцияларын қолдауы тиіс; жүйе қауіпсіздік профильдерін орнатуды қолдауы тиіс; жүйе URL/кілт сөз/сөз тіркесі арқылы құлыпталуы тиіс; жүйе URL мекенжайларының «ақ» тізімдерін қолдауы тиіс; жүйе Java аплеттерін, Cookies, ActiveX басқару элементтерін бұғаттай алуы тиіс; жүйе желілік шабуылдардың кемінде 10000 типін болдырмауы тиіс; жүйенің шабуыл сигнатураларын тізімін баптау мүмкіндігі болуы тиіс; жүйе IPS шабуылдар мен сигнатуралар базасын автоматты түрде жаңартуды қолдауы тиіс; жүйе өндірушінің серверінен спамерлер мен ашық релеелердің IP мекенжайларының «қара» тізімін үнемі алып отыруы тиіс; жүйе MIME тақырыптарын тексеруді қолдауы тиіс; жүйе электрондық поштаны кілт сөздер мен сөз тіркестері бойынша сүзуді қолдауы тиіс; жүйе IP мекенжайларының «қара/ақ» тізімдері бойынша сүзуді қолдауы тиіс; жүйенің қашықтағы syslog серверіне логтарды жіберу мүмкіндігі болуы тиіс; жүйе бастапқы файл пішімін сақтай отырып, Microsoft Office және PDF форматындағы файлдардан орындалатын компонентті шығару қызметін қолдауы тиіс; жүйеде желілік трафиктің, жүйенің жай-күйінің және анықталған қатерлердің мониторингі үшін графикалық құралдар болуы тиіс; жүйенің вирустар мен желілік шабуылдар туралы электрондық пошта арқылы хабарламалар жіберу мүмкіндігі болуы тиіс; жүйе «0-day» класындағы белгісіз қауіп-қатерлерін табу үшін cloud sandbox-та талдау үшін файлдар мен URL-терді жіберуді қолдауы тиіс; жүйеде cloud sandbox-та талдау үшін жеткізу жиынтығында күніне (24 сағат) кемінде 10 000 объектіні (файлдар мен URL) лицензиялау болуы тиіс; жүйе VRRP хаттамасын қолдауы тиіс; жүйе SIEM интеграциялауды қолдауы тиіс; жүйенің кепілдік берілген, ең жоғары немесе басым өткізу қабілетін белгілеу мүмкіндігі болуы тиіс; жүйе жедел хабар алмасу қызметтерін анықтауды және пайдаланды бақылауды қолдауы тиіс; жүйе өткізу қабілеттілігін және Web ресурстарына қол жеткізу жылдамдығын оңтайландыру үшін Web мазмұнын Жергілікті сақтау мүмкіндігін қолдауы тиіс; жүйе WEB интерфейсі арқылы басқаруды қолдауы тиіс; жүйе орталықтандырылған басқару және есеп беру жүйелерімен интеграциялануы тиіс; жүйе NetFlow, sFlow хаттамаларын қолдауы тиіс; жүйе кері прокси-сервер (reverse proxy) режимін қамтамасыз етуі тиіс; жүйе мөлдір прокси-сервер (transparent proxy) режимін қамтамасыз етуі тиіс; жүйе командалық жолдан консольдық режимде қауіпсіздік саясатын басқару мүмкіндігін қамтамасыз етуі тиіс; жүйе пайдаланушылар, пайдаланылатын модель және операциялық жүйенің нұсқасы туралы ақпаратты, IP мекенжайын, MAC мекенжайын, анықталған осалдықтар туралы ақпаратты қамтитын телеметрия ақпаратын алу үшін сыртқы жүйелермен интеграцияны қолдауы тиіс; жүйе жұмыс станцияларының корпоративтік қауіпсіздік саясатына сәйкестігін бағалау үшін сыртқы жүйелермен интеграцияны қолдауы тиіс. Қауіпсіздік саясатына сәйкес келмеген жағдайда тексерілетін хост желілік қолжетімділікті шектеумен карантинге қойылуы тиіс; жүйе сымсыз қол жеткізу нүктелерін басқару мүмкіндігін қамтамасыз етуі тиіс; жүйе коммутаторларды басқару мүмкіндігін қамтамасыз етуі тиіс; Қауіпсіздік шлюздерінде кемінде 3 жыл ішінде қызметтерге жазылымдар болуы тиіс: Қосымшаларды бақылау IPS AV Web Filtering Antispam Sandbox Cloud Қызмет көрсетуге қойылатын талаптар және кепілдіктер: жүйе 24x7 режимінде кемінде 3 жыл өндірушінің кеңейтілген техникалық қолдауымен қамтамасыз етілуі тиіс; 4. Ілеспе қызметтер: Өнім беруші жабдықты орнату және баптау жұмыстарын орындауы тиіс. Жұмыстарды Өнім берушінің білікті мамандары орындауы тиіс. 5. Жеткізу орны: Қазақстан Республикасы, Астана қаласы, Мәңгілік ел даңғылы, 8, «Министрліктер үйі» әкімшілік ғимараты, 10-кіреберіс. 6. Жеткізу мерзімі: Шарт Қазынашылық органдарында тіркелген сәттен бастап 90 күнтізбелік күн ішінде. 7. Жеткізуге қойылатын талаптар: жеткізу түпнұсқа қаптамада жүзеге асырылуытиіс; бұрын қолданыста болған, қалпына келтірілген немесе қандай да бір түрде модификацияланған жабдықты жеткізуге жол берілмейді; қаптамада көрсетілген өндірістік код (Part number/Product number), модель, сериялық нөмір жабдықтың өзіндегі өндірістік кодпен, модельмен, сериялық нөмірмен сәйкес келуі тиіс; 8. Кепілдік қызмет көрсетуге қойылатын талаптар: Жабдыққа кепілдік мерзімі қабылдау-тапсыру актісіне қол қойылған күннен бастап 12 айды құрайды. Жабдықтың істен шыққан, ақаулы не зақымдалған құрамдауыш бөліктерін ауыстыру кепілдік бойынша өнім беруші ауыстыру қажеттігі туралы хабарламаны алған сәттен бастап 20 жұмыс күні ішінде жеткізу мекенжайынан өзі алып кету және әкелу арқылы жүргізіледі. Өнім беруші тауарды қабылдау-тапсыру актісіне қол қойған күннен бастап барлық жеткізілетін жабдықтарға 12 ай қызмет көрсетуге және жұмысқа жарамдылығын қамтамасыз етуге кепілдік талонын ұсынады және Тапсырыс берушінің пошта немесе e-mail арқылы жіберілген жазбаша өтінімі тіркелген сәттен бастап 30 жұмыс күні ішінде және кепілдік мерзімі ішінде кепілді жөндеуді не ауыстыруды көздейді. Өнім беруші жабдықты ауыстыруды, бағдарламалық қамтылымды және оның модульдерін жаңартуды қоса алғанда, жабдықтың жұмысқа жарамдылығында анықталған ақауларды Тапсырыс берушінің келісілген мерзімде анықталған ақаулар туралы хабарланған күннен бастап күнтізбелік 30 күн ішінде жояды. Жеткізілетін жабдыққа кепілді қызмет көрсету және техникалық қолдау Тапсырыс беруші тарапынан қосымша шығыстарсыз қамтамасыз етіледі. Кепілді қызмет көрсету және техникалық қолдау дегеніміз – кепілді кезеңде дұрыс пайдаланбаумен байланысты емес себептер бойынша оның істен шығуы кезінде жеке құрылғының (немесе бір бөлігінің, блогының, торабының) жұмысқа жарамдылығын қалпына келтіру. Кепілді қызмет көрсету және техникалық қолдау Тапсырыс берушінің орналасқан жері бойынша жүзеге асырылады. Жабдықты өндірушінің сервистік орталықтарына және кері жеткізу қажет болған жағдайда, бұл жеткізуді өнім беруші өз есебінен қамтамасыз етеді. 9. Әлеуетті Өнім берушіге қойылатын талаптар: Контрафактілік өнімді жеткізуді болдырмау үшін Әлеуетті өнім беруші Қазақстан Республикасы Қаржы министрінің 2024 жылғы 09 қазандағы № 687 бұйрығымен бекітілген Мемлекеттік сатып алуды жүзеге асыру қағидаларына № 4 қосымшаның 2-тармағының 7) тармақшасына сәйкес конкурстық өтінім құрамында Тапсырыс берушінің атына жіберілген жабдықты жеткізу құқығына арналған жабдық өндірушіден авторизациялық хаттың нөмірін көрсете отырып, (шет тіліндегі мәтін болған жағдайда - мемлекеттік немесе орыс тілдеріндегі мәтіннің нотариат растаған аудармасы қоса беріледі). Авторизациялық хаттың түпнұсқасы шарт қазынашылық органдарында тіркелген күннен бастап 10 жұмыс күні ішінде ұсынылады.
Ілеспе қызметтер (қажет болған жағдайда көрсетіледі тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	Өнім беруші жабдықты орнату және баптау жұмыстарын орындауы тиіс. Жұмыстарды Өнім берушінің білікті мамандары орындауы тиіс.

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.
*мәліметтер мемлекеттік сатып алу жоспарынан тартылады (автоматты түрде көрсетіледі).

Приложение 13
к конкурсной документации

Техническая спецификация закупаемых товаров (заполняется заказчиком)

Наименование заказчика	Государственное учреждение "Высшая аудиторская палата Республики Казахстан"
Наименование организатора	Государственное учреждение "Высшая аудиторская палата Республики Казахстан"
№ конкурса:	№ 14752475-1
Наименование конкурса:	Приобретение межсетевого экрана
Номер лота:	№ 74064910-ОК1
Наименование лота:	Экран специальный
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	263021.900.000009
Наименование товара*:	Экран специальный
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора за исключением приобретения здания, строения, сооружения, помещения, имеющих нежилое назначение:	
Единица измерения*:	Штука
Количество (объем)*:	2
Цена за единицу, без учета налога на добавленную стоимость*:	10551763.39
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	21103526.78
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*:	согласно требованиям технической спецификации
Место поставки товара*:	711210000, г.Астана, район Есиль пр. Мәңгілік Ел, д.8, зд. "Дом министерств", 10-подъезд
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.	
Товар должен быть новым, неиспользованным, год выпуска не ранее (до трех лет) до даты заключения договора за исключением приобретения здания, строения, сооружения, помещения, имеющих нежилое назначение	
Гарантийный срок (в месяцах)	12

Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара	ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ на приобретение межсетевых экранов Настоящая техническая спецификация разработана с целью обеспечения сетевой безопасности в ГУ «Высшая аудиторская палата Республики Казахстан». 1. Общие требования: Все предложенные характеристики оборудования должны соответствовать либо превосходить минимальные технические характеристики, указанные в данной технической спецификации. В целях обеспечения совместимости и сокращения затрат времени для интеграции компонентов оборудования, поставляемое оборудование должно быть одного производителя. Поставляемое оборудование должно быть укомплектовано всем необходимым запасом монтажных материалов и полностью готово к использованию непосредственно после инсталляции. 2. Объем поставляемого оборудования: Межсетевой экран – не менее 2 шт. 3. Технические характеристики поставляемого оборудования: Технические требования к межсетевому экранированию: Firewall Throughput (1518/512/64 byte UDP): не менее 26.5/26/10 Gbps; Одновременное количество сессий: не менее 3 млн; Скорость установки новых соединений: не менее 275 000 в сек; Application Control Throughput (HTTP 64K): не менее 12 Gbps; IPsec VPN Throughput: не менее 12 Gbps; SSL VPN Throughput: не менее 2 Gbps; Количество виртуальных контекстов безопасности в базовой комплектации: не менее 10; Количество интерфейсов: не менее 4x10GE SFP+, 16x GE RJ45, 8x1GE SFP. Количество USB портов: не менее 1; Консольный порт RJ-45: не менее 1; Блок питания 100–240V AC, 50–60 Hz: не менее 2 штук; Локальная система хранения SSD: не менее 470 GB; Требования к шлюзу безопасности: Функциональные требования к межсетевому экранированию: лицензирование системы должно осуществляться для неограниченного количества пользователей; система должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя; система должна поддерживать объединение в кластер не менее 4 устройств с возможностью создания типов кластеров: • с холодным резервом (active/passive); • с горячим резервом (active/active); • кластер балансировки; система должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений; система должна иметь функциональность балансировки нагрузки; система должна поддерживать технологию интеллектуального управления трафиком SD-WAN (Software-Defined Wide Area Network, программно-конфигурируемая сеть); система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); система должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol); система должна обеспечивать возможность реализации шлюза ZTNA (Zero Trust Network Access); система должна обеспечивать анализ SSH трафика (ssh inspection); система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; система должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента); система должна обеспечивать оптимизацию WAN соединений; система должна иметь функционал защиты от утечек данных DLP; система должна обеспечивать антивирусную защиту с аппаратным ускорением; система должна обеспечивать защиту от спама (антиспам); система должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением; система должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; должна обеспечиваться WEB фильтрация трафика по не менее 85 категориям; принудительное включение режима безопасного поиска в популярных поисковых системах; система должна иметь функциональность контроля приложений; система должна иметь функциональность WEB proxy; система должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию; система должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика; система должна иметь возможность автоматически по расписанию получать обновления антивирусных баз; система должна иметь возможность блокировки передачи файлов в зависимости от размера; система должна иметь возможность блокировки передачи файлов в зависимости от типа; система должна поддерживать соединения множества WAN сетей; система должна поддерживать протокол PPPoE и L2TP; система должна поддерживать DHCP протокол в конфигурации “Клиент/Сервер”; система должна поддерживать маршрутизацию на основе политик; система должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP; система должна поддерживать использование зон безопасности; система должна поддерживать маршрутизацию между зонами; система должна поддерживать маршрутизацию между виртуальными сетями; система должна поддерживать администрирование на основе ролей; система должна поддерживать несколько уровней администраторов и пользователей; система должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс; система должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО; система должна поддерживать аутентификацию пользователей посредством внутренней базы данных; система должна поддерживать Kerberos аутентификацию пользователей; система должна поддерживать аутентификацию пользователей посредством Windows Active Directory; при этом аутентификация пользователей операционных систем Windows 7 и выше, включенных в домен, должна выполняться автоматически без дополнительных процедур запроса паролей; система должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP; система должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу; система должна поддерживать аутентификацию на основе групп пользователей; система должна поддерживать функции NAT, PAT, «прозрачный» (мост); система должна поддерживать функции NAT на основе политик; система должна поддерживать функции VLAN Tagging (802.1Q); система должна поддерживать функции SIP/H.323 NAT Traversal; система должна поддерживать настройку профилей безопасности; система должна иметь возможность блокировки по URL/ключевому слову/фразе; система должна поддерживать «Белые» списки URL; система должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX; система должна уметь предотвращать не менее 10000 типов сетевых атак; система должна иметь возможность настройки списка сигнатур атак; система должна поддерживать автоматическое обновление базы атак и сигнатур IPS; система должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев; система должна поддерживать проверку заголовков MIME; система должна поддерживать фильтрацию электронной почты по ключевым словам и фразам; система должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов; система должна иметь возможность отсылки логов на удаленный syslog сервер; система должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла; система должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах; система должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках; система должна поддерживать отправку файлов и URL на анализ в cloud sandbox для обнаружения неизвестных угроз класса “0-day”; система должна иметь лицензирование в комплекте поставки для анализа в cloud sandbox не менее 10 000 объектов (файлов и URL) в день (24 часа); система должна поддерживать протокол VRRP; система должна поддерживать интеграцию с SIEM; система должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; система должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам; система должна поддерживать управление через Web интерфейс; система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; система должна поддерживать протоколы NetFlow, sFlow; система должна обеспечивать режим обратного прокси-сервера (reverse proxy); система должна обеспечивать режим прозрачного прокси-сервера (transparent proxy); система должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки; система должна поддерживать интеграцию с внешними системами для получения информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях; система должна поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности. В случае несоответствия политике безопасности проверяемый хост должен быть помещен в карантин с ограничением сетевого доступа; система должна обеспечивать возможность управления беспроводными точками доступа; система должна обеспечивать возможность управления коммутаторами; Шлюзы безопасности должны иметь подписки на сервисы в течение не менее 3 лет: Контроль приложений IPS AV Web Filtering Antispam Sandbox Cloud Требование к обслуживанию и гарантии: система должна обеспечиваться расширенной технической поддержкой производителя в режиме 24x7 не менее 3 лет; 4. Сопутствующие услуги: Поставщик должен выполнить работы по установке и настройке оборудования. Работы должны выполняться квалифицированными специалистами Поставщика. 5. Место поставки: Республика Казахстан, город Астана, проспект Мангилик ел, 8, административное здание «Дом Министерств», подъезд 10. 6. Сроки поставки: В течении 90 календарных дней с момента регистрации договора в органах Казначейства. 7. Требования к поставке: поставка должна быть осуществлена в оригинальной упаковке; недопустимо к поставке оборудование, бывшее в употреблении, восстановленное или каким-либо образом модифицированное; производственный код (Part number/Product number), модель, серийный номер, указанные на упаковке должны совпадать с производственным кодом, моделью, серийным номером на самом оборудовании. 8. Требование к гарантийному обслуживанию: Срок гарантии на оборудование составляет 12 месяцев с даты подписания акта-приема передачи. Замена вышедших из строя, бракованных либо поврежденных комплектующих частей оборудования, производится по гарантии путем самовывоза поставщиком и предоставления по адресу поставки в течение 20 рабочих дней, с момента получения уведомления поставщиком о необходимости замены. Поставщик предоставляет гарантийный талон на обслуживание и обеспечение работоспособности 12 месяцев на все поставляемые оборудование с даты подписания акта приема-передачи товара и предусматривает гарантийный ремонт либо замену в срок 30 рабочих дней с момента регистрации письменной заявки Заказчика отправленной по почте или по e-mail и в течение гарантийного срока. Поставщик устраняет выявленные неисправности в работоспособности оборудования, включая замену оборудования, обновления программного обеспечения и его модулей, в согласованные с Заказчиком сроки - 30 календарных дней со дня сообщения о выявленных неисправностях. Гарантийное обслуживание и техническая поддержка поставляемого оборудования обеспечивается без дополнительных расходов со стороны Заказчика. Под гарантийным обслуживанием и технической поддержкой подразумевается восстановление работоспособности отдельного устройства (или его части, блока, узла), при выходе его из строя по причинам, не связанным с некорректной эксплуатацией в гарантийный период. Гарантийное обслуживание и техническая поддержка осуществляются по месту нахождения Заказчика. В случае необходимости доставки оборудования в сервисные центры производителя оборудования и обратно, эту доставку обеспечивает поставщик за свой счет. 9. Требования к Потенциальному поставщику: Во избежание поставки контрафактной продукции, Потенциальный поставщик, в соответствии с подпунктом 7 пункта 2 приложения № 4 к Правилам осуществления государственных закупок, утвержденных приказом Министра финансов Республики Казахстан от 09 октября 2024 года № 687, в составе конкурсной заявки предоставляет копию авторизационного письма от производителя оборудования на право поставки оборудования, адресованную на имя Заказчика с указанием номера конкурса (в случае наличия текста на иностранном языке – прилагается нотариально заверенный перевод текста на государственном или русском языках). Оригинал авторизационного письма предоставляется в течении 10 рабочих дней со дня регистрации договора в органах казначейства.
Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	Поставщик должен выполнить работы по установке и настройке оборудования. Работы должны выполняться квалифицированными специалистами Поставщика.

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 исполнителюуказывается 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.
* сведения подтягиваются из плана государственных закупок (отображаются автоматически).