Конкурстық құжаттамаға
13-қосымша

Сатып алынатын тауарлардың техникалық ерекшелігі
(тапсырыс беруші толтырады)

Тапсырыс берушінің атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Атырау облысының Полиция департаменті" мемлекеттік мекемесі
Ұйымдастырушының атауы:	"Қазақстан Республикасы Ішкі істер министрлігі Атырау облысының Полиция департаменті" мемлекеттік мекемесі
Конкурстың №:	№ 14515895-2
Конкурстың атауы:	коммуникациялық жабдықты сатып алу/ техникалық сипаттамаға сәйкес
Лоттың нөмірі:	№ 74037017-ОК1
Лоттың атауы	Коммуникациялық модуль
Тауарлардың, жұмыстардың, көрсетілетін қызметтердің бірыңғай номенклатуралық анықтамалығы кодының атауы*:	265145.200.000009
Тауардың атауы*:	Коммуникациялық модуль
Өлшем бірлігі*:	Комплект
Саны (көлемі)*:	8
Қосылған құн салығын есепке алмағандағы бірлік бағасы*:	6660714.28
Қосылған құн салығын есепке алмағанда, сатып алу үшін бөлінген жалпы сома*:	53285714.24
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*	Келісім-шарт аумақтық Қазынашылық бөлімшесінен тіркеуден өткеннен кейін тауар 16 (он алты) күнтізбелік күннің ішінде жеткізілуі қажет.
Жеткізу орны*	231010000, Атырау облысы, Атырау қ. Атырау қаласы, пр.Абулхайыр хан даңғылы 55
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	Коммуникациялық жабдықты (коммутатор, Атырау ҚПБ және 7 АПБ үшін желіаралық экран) Жеткізу негізі: Атырау қаласының полиция бөлімі және Қазақстан Республикасы Ішкі істер министрлігі Атырау облысының полиция департаментінің аудандық бөлімшелері (Жылыой ауданының полиция бөлімі, Махамбет ауданының полиция бөлімі, Мақат ауданы, Құрманғазы ауданының полиция бөлімі, Қызылқоға ауданының полиция бөлімі, Исатай ауданының полиция бөлімі, Индер аудандық полиция бөлімі). Келісім-шарт аумақтық Қазынашылық бөлімшесінен тіркеуден өткеннен кейін тауар 90 (тоқсан) күнтізбелік күннің ішінде жеткізілуі қажет. Саны: 8 (сегіз) жиынтық. Мазмұнды орнату: Қол жеткізу коммутаторы – 1 (бір) дана; Қауіпсіздік шлюзі – 1 (бір) дана. Үйлесімділікті қамтамасыз ету және аппараттық құрал құрамдастарын біріктіруге қажетті уақытты азайту үшін қосқыш пен қауіпсіздік шлюзі бір өндірушіден болуы керек. Қауіпсіздік шлюзіне қойылатын талаптар Брандмауэрге қойылатын функционалдық талаптар: жүйе пайдаланушылардың шектеусіз саны үшін лицензияланған болуы керек; жүйе қауіпсіздік модулі қолтаңбаларының жаңартуларын және өндірушінің серверінен ағымдағы қауіптер тізімін тұрақты түрде алуы керек; жүйе 4 құрылғыға дейін тұратын кластер түрлерін құру мүмкіндігі бар кластерлеуді қолдауы керек: суық резервпен (белсенді/пассивті); ыстық резервпен (белсенді/белсенді); баланстау кластері; жүйе брандмауэр функциясына ие болуы керек, яғни IP мекенжайлары, порттар және қосымшалар негізінде желілік трафикті сүзу ережелерін құру мүмкіндігін қамтамасыз етуі керек; жүйеде жүктемені теңестіру функциясы болуы керек; жүйе SD-WAN трафикті басқарудың интеллектуалды технологиясын бөлек лицензиясыз қолдауы керек (Software-Defined Wide Area Network, бағдарламалық қамтамасыз етумен анықталған желі); трафик өткізу қабілеттілігін басқару функциясы болуы керек (traffic shaping); жүйе тексерілген трафикті талдау және ICAP протоколы арқылы сыртқы жүйелерге жіберу мүмкіндігімен SSL трафигін тексеруді қамтамасыз етуі керек (Internet Content Adaptation Protocol); жүйе ZTNA шлюзін іске асыру мүмкіндігін бөлек лицензиясыз қамтамасыз етуі керек (Zero Trust Network Access); жүйе SSH трафигінің талдауын қамтамасыз етуі керек (ssh inspection); жүйе IPv4, IPv6 динамикалық маршруттауын қамтамасыз етуі керек; WCCP хаттамасы арқылы жұмыс істей алуы керек (сервер және клиенттік режимде); жүйе WAN қосылымдарын оңтайландыруды қамтамасыз етуі керек; жүйеде DLP деректерінің ағып кетуіне қорғау функциясы болуы керек; жүйе аппараттық жеделдету арқылы антивирустық қорғауды қамтамасыз етуі керек; жүйе спамнан қорғауды қамтамасыз етуі керек (антиспам); жүйеде аппараттық жеделдету арқылы IPS енуді болдырмау функционалдығы болуы керек; жүйе сайттардың белгілі бір санаттарына кіруді шектеу мүмкіндігімен WEB трафикті сүзуді қамтамасыз етуі керек; жүйе танымал іздеу жүйелерінде қауіпсіз іздеу режимін мәжбүрлеп қосуды қолдауы қажет; жүйеде қосымшаларды басқару функциясы болуы керек; жүйеде WEB прокси функциясы болуы керек; жүйе әдепкі бойынша қолжетімді кемінде 10 виртуалды доменді (бір құрылғыдағы толық функционалды виртуалды брандмауэр) қамтамасыз етуі керек; жүйе HTTP, SMTP, POP3, IMAP, FTP және IM трафигі ішіндегі вирустарды тексере алуы керек; жүйеде кесте бойынша антивирустық дерекқор жаңартуларын автоматты түрде алу мүмкіндігі болуы керек; жүйе жұқтырылған хабарламаларды карантинге алу мүмкіндігіне ие болуы керек; жүйе өлшеміне байланысты файлдарды тасымалдауды бұғаттай алуы керек; жүйе түріне байланысты файлдарды тасымалдауды бұғаттай алуы керек; жүйе бірнеше WAN желілерінен қосылымдарды қолдауы керек; жүйе PPPoE және L2TP протоколын қолдауы керек; жүйе «Клиент/Сервер» конфигурациясында DHCP протоколын қолдауы керек; жүйе саясатқа негізделген маршруттауды қолдауы керек; жүйе RIPv1 және v2, OSPF, BGP хаттамаларына негізделген динамикалық бағыттауды қолдауы керек; жүйе қауіпсіздік аймақтарын пайдалануды қолдауы керек; жүйе аймақтар арасындағы маршруттауды қолдауы керек; жүйе виртуалды желілер арасындағы маршруттауды қолдауы керек; жүйе рөлдік басқаруды қолдауы керек; жүйе әкімшілер мен пайдаланушылардың бірнеше деңгейін қолдауы керек; жүйе TFTP протоколы және веб интерфейс арқылы микробағдарламаны жаңартуды қолдауы керек; микробағдарламаның алдыңғы күйіне (нұсқасына) оралу мүмкіндігін қолдауы керек ; жүйе ішкі деректер базасы арқылы пайдаланушының аутентификациясын қолдауы керек; жүйе Kerberos пайдаланушы аутентификациясын қолдауы керек; жүйе Windows Active Directory арқылы пайдаланушы аутентификациясын қолдауы; бұл жағдайда доменге енгізілген Windows 7 және одан жоғары операциялық жүйелерді пайдаланушылардың аутентификациясы парольдерді сұрауынсыз процедураларынсыз автоматты түрде орындалуы керек; жүйе сыртқы RADIUS/LDAP дерекқоры арқылы пайдаланушының аутентификациясын қолдауы керек; жүйе IP/MAC мекенжайын байланыстыру арқылы пайдаланушының аутентификациясын қолдауы керек; жүйе пайдаланушы топтары негізінде аутентификацияны қолдауы керек; жүйе NAT, PAT, «мөлдір» (көпір) функцияларын қолдауы керек; жүйе саясатқа негізделген NAT функцияларын қолдауы керек; жүйе VLAN Tagging (802.1Q) қолдауы керек; жүйе SIP/H.323 NAT Traversal функцияларын қолдауы керек; жүйе қауіпсіздік профильдерін орнатуды қолдауы керек; жүйеде URL/кілт сөз/фраза бойынша блоктау мүмкіндігі болуы керек; жүйе URL «ақ» тізімдерін қолдауы керек; жүйе Java апплеттерін, Cookie файлдарды, ActiveX басқару элементтерін бұғаттай алуы керек; жүйе шабуыл қолтаңбаларының тізімін конфигурациялай алуы керек; жүйе шабуыл деректер базасын және IPS қолтаңбаларын автоматты түрде жаңартуды қолдауы керек; жүйе өндірушінің серверінен спам жіберушілердің және ашық релелердің IP мекенжайларының «қара» тізімін үнемі алуы керек; жүйе MIME тақырыбын тексеруді қолдауы керек; жүйе электрондық поштаны кілт сөздер мен сөз тіркестері бойынша сүзуді қолдауы керек; жүйе IP мекенжайларының «қара/ақ» тізімдері бойынша сүзуді қолдауы керек; жүйе логтарды syslog серверіне жібере алуы керек; жүйе Microsoft Office және PDF файл пішімдерін сақтай отырып орындалатын құрамдастарды шығару қызметін қолдауы керек; жүйеде желілік трафикті, жүйе күйін және анықталған қауіптерді бақылауға арналған графикалық құралдар болуы керек; жүйе вирустар мен желілік шабуылдар туралы электрондық пошта хабарламаларын жібере алуы керек; жүйе «0-day» қауіп сынығын анықтау үшін файлдар мен URL-дерді cloud sandbox-қа жіберуді қолдауы керек; жүйе VRRP протоколын қолдауы керек; жүйе SIEM-мен интеграцияны қолдауы керек; жүйе кепілді, максималды немесе басым өткізу қабілеттілігін белгілей алуы керек; жүйе жедел хабар алмасу қызметтерін пайдалануды және анықтауды және бақылауды қолдауы керек; веб ресурстарға қол жеткізу жылдамдығын оңтайландыру үшін веб мазмұнды жергілікті түрде сақтау мүмкіндігін қолдауы керек ; жүйе веб интерфейс арқылы басқаруды қолдауы керек; жүйе орталықтандырылған басқару және есеп беру жүйелерімен интеграциялануы тиіс; жүйе NetFlow, sFlow протоколдарын қолдауы керек; жүйе кері прокси режимін қамтамасыз етуі керек (reverse proxy); жүйе мөлдір прокси сервер режимін қамтамасыз етуі керек (transparent proxy); жүйе пәрмен жолынан консоль режимінде қауіпсіздік саясатын басқару мүмкіндігін қамтамасыз етуі керек; жүйе пайдаланушылар туралы ақпаратты, қолданылатын операциялық жүйенің моделі мен нұсқасын, IP мекенжайын, MAC мекенжайын, анықталған осалдықтар туралы ақпаратты қоса алғанда, телеметриялық ақпаратты алу үшін сыртқы жүйелермен интеграцияны қолдауы керек; жүйе жұмыс станцияларының корпоративтік қауіпсіздік саясаттарына сәйкестігін бағалау үшін сыртқы жүйелермен интеграцияны қолдауы керек. Қауіпсіздік саясатына сәйкес келмеген жағдайда сканерленген хост желіге шектеулі қолжетімділікпен карантинге қойылуы керек; жүйе сымсыз кіру нүктелерін басқару мүмкіндігін қамтамасыз етуі керек; жүйе коммутаторларды басқару мүмкіндігін қамтамасыз етуі керек; Қауіпсіздік шлюзінде кем дегенде 12 ай қызметтерге жазылым болуы керек: Қосымшаларды басқару IPS AV Web Filtering Antispam Sandbox Cloud Желіаралық экранға қойылатын техникалық талаптар: Ең аз өнімділік: Брандмауэр Өткізу қабілеті (1518/512/64 байт UDP): кем дегенде 27/27/11 Гбит/с ; SSL тексеру өткізу қабілеті: кем дегенде 4 Гбит/с; Сеанстардың бір мезгілдегі саны: кемінде 3 миллион; Жаңа қосылулар орнату жылдамдығы: кемінде 280 000/сек; IPS өткізу қабілеті: кемінде 5 Гбит/с NGFW өткізу қабілеті: кемінде 3,5 Гбит/с Брандмауэр саясаттарының саны: кемінде 10 000 Қауіптерден қорғау өткізу қабілеті: кемінде 3 Гбит/с SSL-VPN өткізу қабілеті: кемінде 2 Гбит/с Қолданбаны басқару өткізу қабілеті: кемінде 13 Гбит/с IPsec VPN өткізу қабілеті (пакет өлшемі 512 байт): кемінде 13 Гбит/с Негізгі конфигурациядағы виртуалды қауіпсіздік контексттерінің саны: кемінде 10; Интерфейстердің саны: 4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP Бөлінген басқару порттарының саны: кемінде 1; Қуат көзі 100–240 В Ыстық ауыстырылатын айнымалы ток, 50–60 Гц : кемінде 2; Қызметке қойылатын талаптар және кепілдік: жүйе кем дегенде 12 ай бойы өндірушіден 24x7 режимінде кеңейтілген техникалық қолдаумен қамтамасыз етілуі керек; Қол жеткізу коммутаторына қойылатын талаптар: Порттардың саны/түрі: кемінде 48x 1GE RJ 45 порты; кемінде 4x 10 GE SFP+ слоттары; кемінде 1x RJ 45 консоль порты; өткізу қабілеттілігі - кемінде 176 Гбит/ с; Пакеттердің секундына өткізу қабілеті – кемінде 260 Мп/сек ; Коммутатор Multi-Chassis Link Aggregation (MCLAG)ақауларына төзімділік технологиясын қолдауы керек; Web және CLI арқылы коммутаторларды басқару; Коммутатор 19 дюймдік байланыс шкафында және биіктігі 1 RU орнатуға арналған болуы керек; Коммутатор L2 деңгейіне арналған Virtual-Wire технологиясын қолдауы керек; Пакетті жүйеде өңдеуге жұмсалатын кідіріс – 1 µs аспайды ; Коммутатор бұғатталмаған архитектураға ие болуы керек, коммутатордың барлық порттары жарияланған жылдамдықта бір уақытта жұмыс істеуі керек; Коммутатордың коммутация кестесінде сақталған MAC мекенжайларының максималды саны кемінде 32 000 болуы керек ; Коммутатор саясатқа негізделген маршруттауды басқаруды қолдауы керек (Policy-based Routing). IGMP snooping протоколдарын қолдауы керек ; Коммутатор IEEE 802.1x аутентификация протоколын қолдауы керек (Порт негізінде, MAC негізінде, MAB); Коммутатор SNMP 2c және 3 нұсқаларын, Syslog стандарттарын қолдауы керек; Коммутатор sFlow технологиясын қолдауы керек; Коммутатор желіаралық қалқан контроллерінің ACL басқару және анықтау мүмкіндігін қолдауы керек; ACL максималды саны - кемінде 640; Ақаулар арасындағы уақыт кемінде 10 жыл; Жедел жад мөлшері - кемінде 512 МБ; Флэш жад көлемі - кемінде 64 МБ; Кіріктірілген қуат AC 100–240 В AC, 50–60 Гц; Сақтау температурасының диапазоны -20 - 70 С ; Жұмыс температурасының диапазоны 0 - 45 С; Жұмыс кезінде (конденсациясыз) салыстырмалы ылғалдылық диапазоны 10-нан 90% дейін; Стандартты қолдау: IEEE 802.1D MAC Bridging/STP; IEEE 802.1w Rapid Spanning Tree Protocol (RSTP); IEEE 802.1s Multiple Spanning Tree Protocol (MSTP); IEEE 802.1Q VLAN Tagging; IEEE 802.3ad Link Aggregation with LACP IEEE 802.1AX Link Aggregation IEEE 802.3x Flow Control and back-pressure IEEE 802.3z 1000Base-SX/LX IEEE 802.3ab 1000Base-T IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications Storm control; Port Mirroring; Өндіруші бір жыл бойы 24x7 тәртібінде техникалық қолдау көрсетуі керек; Өтінімнің құрамына қойылатын талаптар/Әлеуетті жеткізушіге қойылатын талаптар: 1. Әлеуетті жеткізушілердің өтінімдерін салыстыру және олардың техникалық ерекшелік талаптарына сәйкестігін анықтау үшін Әлеуетті жеткізуші оны қолдану бөлігі ретінде өндірушінің (және/немесе өндіруші зауытының) атауын және жабдықтың үлгісін көрсетуі керек. Ұсынылған жабдық туралы ақпарат ашық көздерде болуы керек. 2. Контрафактілік өнімді жеткізуді болдырмау үшін әлеуетті өнім беруші өтінім шеңберінде жабдықты өндірушіден немесе оның Қазақстан Республикасының аумағындағы ресми өкілінен жабдықты жеткізу құқығына рұқсат беру хатын ұсынуы қажет. Берілген хаттарда келесі мәліметтер көрсетілуі керек: Тұтынушы, Жеткізуші және сатып алу нөмірі. Жеткізушіге қойылатын талаптар: 1. Жабдықты жеткізу кезінде (жабдықты тапсырған кезде), ауыстыру жағдайында (өндіруші және/немесе үлгіні өтінімде көрсетілгеннен өзгерткен кезде) Жабдықтаушы жабдықты өндірушіден немесе оның Қазақстан Республикасының аумағындағы ресми өкілінен жеткізу құқығына берілген жабдыққа рұқсат қағазын ұсынуы керек. Берілген хаттарда келесі мәліметтер көрсетілуі керек: Тұтынушы, Жеткізуші. 2. Жабдықты өндіруші немесе оның Қазақстан Республикасының аумағындағы ресми өкілі Жабдықтаушының жарамдылығын растамаса немесе жеткізілетін жабдықтың импорты заңсыз болса, Тапсырыс беруші Жеткізушіге қабылдаудан бас тарту құқығын өзіне қалдырады. 3. Кепілдік міндеттемелері шеңберінде Жеткізуші өз есебінен кепілдік кезеңінде анықталған барлық ақаулар мен ақаулықтарды жояды. Бір жыл ішінде бұзылған немесе ақаулық болған жағдайда жабдықты ауыстыру.

Ілеспе қызметтер (қажет болған жағдайда көрсетіледі тауарларды монтаждау, баптау, оқыту, тексеру және сынау)	1. Ағымдағы инфрақұрылымды талдау. 2. Жабдықты орнату: Сөреде немесе басқа дайындалған жерде брандмауэр мен кіру қосқышын орнату; Электр желісіне және желілік инфрақұрылымға қосылу. 3. Брандмауэр конфигурациясы: Негізгі параметрлерді конфигурациялау (IP мекенжайы, шлюз, DNS); Трафикті сүзу саясатын жасау (брандмауэр ережелер); VPN орнату (қажет болса); IPS/IDS, веб-сүзгілеу және DDoS қорғау функцияларын қосу және конфигурациялау. 4. Кіру қосқышының конфигурациясы: Желіні сегменттеу үшін VLAN конфигурациялау; Негізгі қатынас параметрлерін орнату. 5. Тестілеу және жөндеу : Жабдықтың функционалдығын тексеру; Сүзу ережелерін және басқа функцияларды тексеру; Анықталған проблемаларды жою.
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 "Департамент полиции Атырауской области Министерства внутренних дел Республики Казахстан"
Наименование организатора	Государственное учреждение "Департамент полиции Атырауской области Министерства внутренних дел Республики Казахстан"
№ конкурса:	№ 14515895-2
Наименование конкурса:	Приобретение коммуникационного оборудование/согласно технической спецификации
Номер лота:	№ 74037017-ОК1
Наименование лота:	Модуль коммуникационный
Наименование кода Единого номенклатурного справочника товаров, работ, услуг*:	265145.200.000009
Наименование товара*:	Модуль коммуникационный
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*:	Комплект
Количество (объем)*:	8
Цена за единицу, без учета налога на добавленную стоимость*:	6660714.28
Общая сумма, выделенная для закупки, без учета налога на добавленную стоимость*:	53285714.24
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*:	Срок поставки товара в течение 16 (шестнадцать) календарных дней после обязательной регистрации договора в территориальном подразделении Казначейства.
Место поставки товара*:	231010000, Атырауская область, г.Атырау г.Атырау, пр.Абулхайыр хана 55
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	Коммуникационного оборудования (коммутатор, межсетевой экран для УП г.Атырау и 7 РОП) Базис поставки: Управление полиции города Атырау и районные отделения Департамента полиции Атырауской области Министерства внутренних дел Республики Казахстан (Отдел полиции Жылыойского района, Отдел полиции Махамбетского района, Отдел полиции Макатского района, Отдел полиции Курмангазинского района, Отдел полиции Кызылкогинского района, Отдел полиции Исатайского района, Отдел полиции Индерского района). Срок поставки товара в течение 90 (девяносто) календарных дней после обязательной регистрации договора в территориальном подразделении Казначейства. Количество: 8 (восемь) комплектов. Состав комплекта: Коммутатор доступа – 1 (одна) штука; Шлюз безопасности – 1 (одна) штука. В целях обеспечения совместимости и сокращения затрат времени для интеграции компонентов оборудования, коммутатор и шлюз безопасности должны быть одного производителя. 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 до 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) без отдельного лицензирования; 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) без отдельного лицензирования; 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; система должна поддерживать 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 помещать инфицированные сообщения в карантин; 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 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 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; Шлюз безопасности должен иметь подписку на сервисы в течение не менее 12 месяцев: Контроль приложений IPS AV Web Filtering Antispam Sandbox Cloud Технические требования к межсетевому экранированию: Минимальная производительность: Firewall Throughput (1518/512/64 byte UDP): не менее 27/27/11 Gbps; SSL Inspection Throughput: не менее 4 Gbps; Одновременное количество сессий: не менее 3 млн; Скорость установки новых соединений: не менее 280 000 в сек; Пропускная способность IPS: не менее 5 Gbps Пропускная способность NGFW: не менее 3.5 Gbps Количество политик брандмауэра: не менее 10 000 Пропускная способность защиты от угроз: не менее 3 Gbps Пропускная способность SSL-VPN: не менее 2 Gbps Пропускная способность контроля приложений: не менее 13 Gbps Пропускная способность IPsec VPN (размер пакета 512 байт): не менее 13 Gbps Количество виртуальных контекстов безопасности в базовой комплектации: не менее 10; Количество интерфейсов: 4x 10 GE SFP+, 18x GE RJ45, 8x GE SFP Количество выделенных менеджмент портов: не менее 1; Блок питания 100–240V AC с возможностью горячей замены, 50–60 Hz: не менее 2; Требование к обслуживанию и гарантии: система должна обеспечиваться расширенной технической поддержкой производителя в режиме 24x7 не менее 12 месяцев; Требования к коммутатору доступа: Количество/тип портов: - не менее 48 портов 1GE RJ45; - не менее 4 слотов 10 GE SFP+; - не менее 1 консольного порта RJ45; Пропускная способность Гбит/ - не менее 176 Гбит/с; Пропускная способность пакетов в секунду – не менее 260 Mpps; Коммутатор должен поддерживать технологию отказоустойчивости Multi-Chassis Link Aggregation (MCLAG); Управление коммутатором по Web и CLI; Коммутатор должен быть предназначен для монтажа в 19-ти дюймовый коммуникационный шкаф и высотой 1 RU; Коммутатор должен поддерживать технологию Virtual-Wire для уровня L2; Задержка пакетов при обработке системой - не более 1 µs; Коммутатор должен иметь неблокируемую архитектуру, все порты коммутатора должны работать одновременно на заявленной скорости; Максимальное количество хранимых MAC адресов в таблице коммутации коммутатора должно быть - не менее 32 000; Коммутатор должен поддерживать управление маршрутизацией при помощи политик (Policy-based Routing). Коммутатор должен поддерживать протоколы IGMP snooping; Коммутатор должен поддерживать протокол IEEE 802.1x Authentication (Port-based, MAC-based, MAB); Коммутатор должен поддерживать стандарты SNMP версий 2c и 3, Syslog; Коммутатор должен поддерживать технологию sFlow; Коммутатор должен поддерживать возможность управления и определения ACL контроллером межсетевого экрана; Максимальное количество ACL - не менее 640; Время между отказами - не менее 10 лет; Размер оперативной памяти - не менее 512 Мб; Размер флеш-памяти - не менее 64 Мб; Блок питания встроенный AC 100–240V AC, 50–60 Hz; Диапазон температуры хранения -20 - 70 C ; Диапазон температур в рабочем режиме 0 - 45 C; Диапазон относительной влажности при эксплуатации (без образования конденсата) от 10 до 90%; Поддержка стандартов: IEEE 802.1D MAC Bridging/STP; IEEE 802.1w Rapid Spanning Tree Protocol (RSTP); IEEE 802.1s Multiple Spanning Tree Protocol (MSTP); IEEE 802.1Q VLAN Tagging; IEEE 802.3ad Link Aggregation with LACP IEEE 802.1AX Link Aggregation IEEE 802.3x Flow Control and back-pressure IEEE 802.3z 1000Base-SX/LX IEEE 802.3ab 1000Base-T IEEE 802.3ae 10 Gigabit Ethernet IEEE 802.3 CSMA/CD Access Method and Physical Layer Specifications Storm control; Port Mirroring; Коммутатор должен поддерживаться годовой технической поддержкой производителя в режиме 24x7; Требования к составу заявки/требования к Потенциальному поставщику: 1. Для сопоставления заявок Потенциальных поставщиков и определения их соответствия требованиям технической спецификации, Потенциальный поставщик должен в составе своей заявки указать наименование производителя (и/или завод-изготовитель) и модель оборудования. Информация о предлагаемом оборудовании должна быть доступна в открытых источниках. 2. Во избежание поставки контрафактной продукции Потенциальный поставщик в составе заявки должен предоставить авторизационное письмо на право поставки оборудования от производителя оборудования либо его официального представителя на территории Республики Казахстан. В предоставленных письмах должны быть указаны следующие реквизиты: Заказчик, Поставщик и номер закупки. Требования к Поставщику: 1. При поставке оборудования (при сдаче оборудования), в случае замены (изменение производителя и/или модели от указанной в заявке), Поставщик должен предоставить авторизационное письмо на поставляемое оборудование на право поставки от производителя оборудования либо его официального представителя на территории Республики Казахстан. В предоставленных письмах должны быть указаны следующие реквизиты: Заказчик, Поставщик. 2. В случае не подтверждения правомочности Поставщика от производителя оборудования либо его официального представителя на территории Республики Казахстан или незаконности импорта поставляемого оборудования, Заказчик оставляет за собой право отказать Поставщику в приемке. 3. В рамках гарантийных обязательств поставщик за свой счет устраняет все дефекты и неисправности выявление в период гарантии. Замена оборудования в случае поломки или неисправности в течении одного года.

Сопутствующие услуги (указываются при необходимости) (монтаж, наладка, обучение, проверки и испытания товаров)	1. Анализ текущей инфраструктуры. 2. Монтаж оборудования: Установка межсетевого экрана и коммутатора доступа в стойку или на другое подготовленное место; Подключение к электрической сети и сетевой инфраструктуре. 3. Конфигурация межсетевого экрана: Настройка базовых параметров (IP-адрес, шлюз, DNS); Создание политик фильтрации трафика (firewall rules); Настройка VPN (при необходимости); Включение и настройка функций IPS/IDS, веб-фильтрации, DDoS-защиты. 4. Конфигурация коммутатора доступа: Настройка VLAN для сегментации сети; Установка базовых параметров доступа . 5. Тестирование и отладка: Проверка работоспособности оборудования; Тестирование правил фильтрации и других функций; Устранение выявленных проблем.
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).