Конкурстық құжаттамаға сатып алынатын тауарлардың техникалық ерекшелігі

Сатып алудың нөмірі:	№ 17959090-1
Сатып алудың атауы:	Басқа тауарларды сатып алу (техникалық шарттарға сәйкес) Жеткізушінің есебінен жеткізу, түсіру.
Лоттың нөмірі:	№ 83404878-ЗЦП1
Лоттың атауы:	Бағдарламалық-аппараттық кешен
Лоттың сипаттауы:	желілік инфрақұрылымның қауіпсіздігі және қауіпсіздік оқиғалары, оқиғаларды талдау процесін автоматтандыру туралы ақпаратты басқару үшін
Лоттың қысқаша сипаттауы:	желілік инфрақұрылымның қауіпсіздігі және қауіпсіздік оқиғалары, оқиғаларды талдау процесін автоматтандыру туралы ақпаратты басқару үшін
Саны, көлемі:	1
Өлшем бірлігі:	Дана
Жеткізу орны:	391010000, Қостанай облысы, Қостанай қ. Қостанай облысы, Қостанай қаласы, Көбеева көшесі, 2;
Жеткізу мерзімі:	30 шартқа қол қойылған күннен бастап
Функционалдық, техникалық, сапалық және пайдалану мінездемесін сипаттау:	Аппараттық желіаралық қалқанның техникалық сипаттамасы (NGFW) Тауардың атауы Аппараттық желіаралық экран (NGFW) Үлгі Өлшем бірлігі Дана Саны (көлемі) Жеткізу мерзімі 90 күнтізбелік күннен артық емес Шығарылған жылы 2026 жылдан ерте емес Кепілдік мерзімі (айлармен) Кемінде 36 ай Сатып алынатын тауардың талап етілетін функционалдық, техникалық, сапалық, пайдалану және өзге де сипаттамаларының сипаттамасы. Жалпы талаптар Жаңа буынның аппараттық желіаралық қалқаны (NGFW) жаңа, зауыттық қаптамада болуы керек. Жаңа буын аппараттық желіаралық қалқанды жеткізу (NGFW) жиынтықта толық көлемде және осы техникалық сипаттамада көрсетілген мерзімде орындалуы тиіс. Барлық ұсынылған сипаттамалар осы техникалық сипаттамада көрсетілген ең төменгі техникалық сипаттамаларға сәйкес келуі немесе асып кетуі керек. Өтінімдегі өнім сипаттамасында өндірушінің веб-сайтында тексеру үшін нақты үлгілер немесе жұмыс үстелінің нөмірлері болуы керек. Жабдыққа қойылатын талаптар. Корпус түрі Үстел үсті Интерфейстер Қол қойылған микробағдарламаны ауыстырып қосқыш; Кем емес: 1 консольді порт; Кем емес: 1 - USB порты; Кем емес: 2 - GE RJ45 WAN-порты; Кем емес: 2 - GE RJ45 сілтеме порттары; Кемінде: 6 - GE RJ45 Ethernet порттары; Желіаралық экрандауға қойылатын техникалық талаптар Firewall Throughput (1518/512/64 byte UDP): емес аздау 10/10/10 Gbps; Сессиялардың бір мезгілде саны: кемінде 1.4 млн; Жаңа қосылыстарды орнату жылдамдығы: секундына кемінде 100 000; Application Control Throughput (HTTP 64K): емес аздау 3.6 Gbps; IPsec VPN Throughput:емес аздау 7 Gbps; Базалық жиынтықтағы қауіпсіздіктің виртуалды мәнмәтіндерінің саны: кемінде 10; Техникалық қызмет көрсету талаптары мен кепілдіктер: жүйе өндірушінің 24x7 режимінде кемінде 3 жыл бойы кеңейтілген техникалық қолдауымен қамтамасыз етілуі керек. Желіаралық экранға қойылатын функционалдық талаптар: жүйені лицензиялау пайдаланушылардың шектеусіз саны үшін жүзеге асырылуы тиіс; жүйе қауіпсіздік модульдерінің қолтаңбалары туралы жаңартуларды және өндірушінің серверінен ағымдағы қауіптер тізімін жүйелі түрде алып отыруы керек; жүйе кластер типтерін құру мүмкіндігімен кем дегенде 4 құрылғының кластерленуін қолдауы керек: суық резервпен (белсенді/пассивті); ыстық резервпен (белсенді/белсенді); теңгерім кластері; жүйе IP мекенжайларына, порттарына және қолданбаларына негізделген желілік трафикті сүзу ережелерін жасау мүмкіндігін қамтамасыз етуі керек;

	жүйеде жүктемені теңестіру функциясы болуы керек; жүйе SDWAN (Software-Defined Wide Area Network, Software-Configurable Network) интеллектуалды трафикті басқару технологиясын қолдауы керек.; жүйеде трафиктің өткізу қабілеттілігін басқару (traffic shaping) функционалдығы болуы керек; жүйе SSH трафигін талдауды қамтамасыз етуі керек (ssh инспекциясы); жүйе IPv4, IPv6 динамикалық маршруттауын қамтамасыз етуі керек; жүйе аппараттық жеделдетілген антивирустық қорғанысты қамтамасыз етуі керек; жүйе спамнан (антиспамнан) қорғауды қамтамасыз етуі тиіс.; жүйеде аппараттық жеделдетілген IPS енуінің алдын алу функционалдығы болуы керек; жүйе сайттардың белгілі бір санаттарына кіруді шектеу мүмкіндігімен трафикті веб-сүзуді қамтамасыз етуі керек; трафикті кемінде 85 санат бойынша веб-сүзгілеу қамтамасыз етілуі керек; танымал іздеу жүйелерінде қауіпсіз іздеу режимін қосуға мәжбүрлеу; жүйеде қолданбаларды басқару функционалдығы болуы керек; жүйенің функционалдығы болуы керек web proxy; жүйе әдепкі бойынша қолжетімді кемінде 10 виртуалды доменді (бір құрылғының ішінде толық жұмыс істейтін виртуалды МӘС) қамтамасыз етуі керек; жүйе HTTP, SMTP, POP3, IMAP, FTP және IM трафигі ішінде вирустардың бар-жоғын тексере алуы керек; жүйе кесте бойынша антивирустық мәліметтер базасының жаңартуларын автоматты түрде ала алатындай болуы керек; жүйе жұқтырған хабарламаларды карантинге қою мүмкіндігіне ие болуы керек; жүйе көлеміне қарай файлдарды тасымалдауды блоктау мүмкіндігіне ие болуы керек; жүйе түріне байланысты файлдарды тасымалдауды блоктау мүмкіндігіне ие болуы керек; жүйе көптеген WAN желілерінің қосылымдарын қолдауы керек; жүйе DHCP протоколын "Клиент" конфигурациясында қолдауы керек/ Сервер"; жүйе саясатқа негізделген маршруттауды қолдауы керек; жүйе RIP v1 және v2, OSPF, BGP протоколдары негізінде динамикалық маршруттауды қолдауы керек; жүйе қауіпсіздік аймақтарын пайдалануды қолдауы керек; жүйе аймақтар арасындағы маршруттауды қолдауы керек; жүйе виртуалды желілер арасындағы маршруттауды қолдауы керек; жүйе рөлге негізделген басқаруды қолдауы керек; жүйе әкімшілер мен пайдаланушылардың бірнеше деңгейлерін қолдауы керек; жүйе TFTP протоколы және web интерфейсі арқылы микробағдарламаны жаңартуды қолдауы керек; жүйе микробағдарламаның алдыңғы күйіне (нұсқасына) оралу мүмкіндігін қолдауы керек; жүйе ішкі дерекқор арқылы пайдаланушылардың аутентификациясын қолдауы керек; жүйе Kerberos пайдаланушы аутентификациясын қолдауы керек; жүйе Windows Active Directory арқылы пайдаланушылардың аутентификациясын қолдауы керек; бұл жағдайда доменге кіретін Windows 7 және одан жоғары операциялық жүйелер пайдаланушыларының аутентификациясы парольдерді сұраудың қосымша процедураларынсыз автоматты түрде жүзеге асырылуы керек; жүйе RADIUS/LDAP сыртқы дерекқоры арқылы пайдаланушылардың аутентификациясын қолдауы керек; ; жүйе байланыстыру арқылы пайдаланушылардың аутентификациясын қолдауы керек IP/MAC мекенжайы бойынша; жүйе пайдаланушылар 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) функцияларын қолдауы керек; жүйе SIP/H функцияларын қолдауы керек.323 NAT Traversal; жүйе қауіпсіздік профильдерін орнатуды қолдауы керек; жүйе URL/кілт сөз/сөз тіркесі арқылы блоктау мүмкіндігіне ие болуы керек; жүйе URL мекенжайларының "Ақ" тізімдерін қолдауы керек; жүйе шабуылдардың қолтаңбаларының тізімін теңшеу мүмкіндігіне ие болуы керек; жүйе шабуылдар базасын және IPS қолтаңбаларын автоматты түрде жаңартуды қолдауы керек; жүйе өндірушінің серверінен спамерлердің және ашық релелердің IP мекенжайларының "қара" тізімін жүйелі түрде алып тұруы керек; жүйе электрондық поштаны кілт сөздер мен сөз тіркестері бойынша сүзуді қолдауы керек;

	жүйе IP мекенжайларының "қара/ақ" тізімдері бойынша сүзуді қолдауы керек; жүйе журналдарды қашықтағы syslog серверіне жібере алатындай болуы керек; жүйеде желілік трафикті, жүйенің күйін және анықталған қауіптерді бақылауға арналған графикалық құралдар болуы керек; жүйе вирустар мен желілік шабуылдар туралы хабарламаларды электрондық пошта арқылы жібере алатындай болуы керек; жүйе "0-day" класындағы белгісіз қауіптерді анықтау үшін файлдарды және URL мекенжайларын талдау үшін cloud sandbox жүйесіне жіберуді қолдауы керек.; жүйе VRRP протоколын қолдауы керек; жүйе кепілдендірілген, максималды немесе басымдықты өткізу қабілеттілігін белгілей алатындай болуы керек; жүйе лездік хабар алмасу қызметтерін пайдалануды анықтауды және бақылауды қолдауы керек; жүйе Web интерфейсі арқылы басқаруды қолдауы керек; жүйе орталықтандырылған басқару жүйелерімен интеграциялануға және есептер шығаруға қабілетті болуы керек; жүйе консольдық режимдегі қауіпсіздік саясаттарын пәрмен жолынан басқару мүмкіндігін қамтамасыз етуі керек; жүйе телеметрия ақпаратын, соның ішінде пайдаланушы ақпаратын, операциялық жүйенің пайдаланылған моделі мен нұсқасын, IP мекенжайын, MAC мекенжайын, анықталған осалдықтар туралы ақпаратты алу үшін сыртқы жүйелермен интеграцияны қолдауы керек; жүйе жұмыс станцияларының кәсіпорынның қауіпсіздік саясатына сәйкестігін бағалау үшін сыртқы жүйелермен интеграцияны қолдауы керек. Қауіпсіздік саясатына сәйкес келмеген жағдайда, тексерілетін хост желіге кіруді шектеу арқылы карантинге жатқызылуы керек; жүйе сымсыз кіру нүктелерін басқару мүмкіндігін қамтамасыз етуі керек; жүйе коммутаторларды басқару мүмкіндігін қамтамасыз етуі керек; Брандмауэрлерде жазылым белсендірілген күннен бастап кемінде 3 жыл бойы қызметтерге жазылымдар болуы керек: Бақылау қосымшалардың IPS Antivirus URL Filtering/DNS Filtering/Video Filtering Antispam Cloud Sandbox Ілеспе қызметтер қажет болған жағдайда көрсетіледі: тауарларды монтаждау, баптау, оқыту, тексеру және сынау Жеткізу шеңберінде Жеткізуші жеткізілетін жабдықты конфигурациялау бойынша барлық қажетті жұмыстарды, оның ішінде қолданыстағы желілік инфрақұрылыммен интеграциялауды қашықтықтан жүзеге асыруы керек. Тауарды жеткізу орнына дейін жеткізуді Жеткізуші жүзеге асырады. Әлеуетті өнім беруші жеңімпаз болып анықталған және онымен мемлекеттік сатып алу туралы шарт жасалған жағдайда оған қойылатын талаптар қажет болған жағдайда көрсетіледі. Контрафактілік өнімдердің жеткізілуіне жол бермеу үшін әлеуетті Өнім беруші конкурсқа қатысуға өтінімде әлеуетті өнім берушінің Қазақстан Республикасында ұсынылатын жабдықтың сауда маркасының ресми өкілінен сатып алынатын тауарларды жеткізуге және сатуға құқығын растайтын рұқсат қағазын ұсынуы керек.

Приложение 2
к конкурсной документации

Техническая спецификация закупаемых товаров к конкурсной документации

Номер закупки:	№ 17959090-1
Наименование закупки:	Приобретение прочих товаров (согласно технической спецификации) Доставка, разгрузка за счет средств Поставщика.
Номер лота:	№ 83404878-ЗЦП1
Наименование лота:	Комплекс программно-аппаратный
Описание лота:	для управления информацией о безопасности и событиях безопасности, автоматизации процесса анализа событий сетевой инфраструктуры
Дополнительное описание лота:	для управления информацией о безопасности и событиях безопасности, автоматизации процесса анализа событий сетевой инфраструктуры
Количество:	1
Единица измерения:	Штука
Места поставки:	391010000, Костанайская область, г.Костанай Костанайская область, г.Костанай, ул.Кубеева,2 ;
Срок поставки:	30 календарных дней с момента подписания договора
Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики закупаемых товаров:	Техническая спецификация на аппаратный межсетевой экран (NGFW) Наименование товара Аппаратный межсетевой экран (NGFW) Модель Единица измерения Штука Количество (объем) Срок поставки Не более 90 календарных дней Год выпуска Не ранее 2026 года Гарантийный срок (в месяцах) Не менее 36 месяцев Описание требуемых функциональных, технических, качественных, эксплуатационных и иных характеристик закупаемого товара. Общие требования Аппаратный межсетевой экран нового поколения (NGFW) должен быть новым, в заводской упаковке. Поставка Аппаратного межсетевого экрана нового поколения (NGFW) в комплекте должна быть осуществлена в полном объеме и в сроки, указанные в данной технической спецификации. Все предложенные характеристики должны соответствовать или превосходить минимальные технические характеристики, указанные в данной технической спецификации. Описание товара в заявке должно содержать конкретные модели или парт номера для проверки их на сайте производителя. Требования к оборудованию. Тип корпуса Настольный Интерфейсы Переключатель подписанной прошивки; Не менее: 1 - консольный порт; Не менее: 1 - USB-порт; Не менее: 2 - GE RJ45 WAN-порта; Не менее: 2 - GE RJ45 Link-порта; Не менее: 6 - GE RJ45 Ethernet-портов; Технические требования к межсетевому экранированию Firewall Throughput (1518/512/64 byte UDP): не менее 10/10/10 Gbps; Одновременное количество сессий: не менее 1.4 млн; Скорость установки новых соединений: не менее 100 000 в сек; Application Control Throughput (HTTP 64K): не менее 3.6 Gbps; IPsec VPN Throughput: не менее 7 Gbps; Количество виртуальных контекстов безопасности в базовой комплектации: не менее 10; Требование к обслуживанию и гарантии: система должна обеспечиваться расширенной технической поддержкой производителя в режиме 24x7 не менее 3 лет. 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 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 управление трафиком SDWAN (Software-Defined Wide Area Network, программно-конфигурируемая сеть); система должна иметь функциональность управления полосой пропускания трафика (traffic shaping); система должна обеспечивать анализ SSH трафика (ssh inspection); система должна обеспечивать динамическую маршрутизацию IPv4, IPv6; 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 веб-фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов; должна обеспечиваться веб-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 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 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 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 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 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 иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности; система должна поддерживать обнаружение и контроль использования служб мгновенных сообщений; система должна поддерживать управление через Web интерфейс; система должна иметь возможность интеграции с системами централизованного управления и построения отчетов; 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; Межсетевые экраны должны иметь подписки на сервисы в течение не менее 3 лет с момента активации подписки: Контроль приложений IPS Antivirus URL Filtering/DNS Filtering/Video Filtering Antispam Cloud Sandbox Сопутствующие услуги указываются при необходимости: монтаж, наладка, обучение, проверки и испытания товаров В рамках поставки Поставщик должен удаленно произвести все необходимые работы по настройке поставляемого оборудования, включая его интеграцию с существующей сетевой инфраструктурой. Доставка товара до места поставки осуществляется Поставщиком. Условия к потенциальному поставщику в случае определения его победителем и заключения с ним договора о государственных закупках указываются при необходимости. Во избежание поставки контрафактной продукции, потенциальный Поставщик в заявке на конкурс должен предоставить авторизационное письмо, подтверждающее право потенциального поставщика на поставку и реализацию закупаемых товаров от официального представителя торговой марки предлагаемого оборудования в Республике Казахстан.