ТЕХНИКАЛЫҚ СИПАТТАМА

1268964 сатып алу бойынша
Төмендету баға ұсыныстарын сұрату тәсілімен

Лот № (11 У, 4577154) Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер

Тапсырыс беруші: "Самрук-Казына Контракт" ЖШС

Ұйымдастырушы: "Самрук-Казына Контракт" ЖШС

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	11 У
Атауы және қысқаша сипаттамасы	Бағдарламалық жасақтама қолдану құқығына лицензия мерзімін ұзарту бойынша қызмет көрсетулер, Бағдарламалық қымсыздандыруды пайдалану құқығына лицензияны создыру бойынша қызметтер
Қосымша сипаттама	FortiNac
Саны	1.000
Өлшем бірлігі	-
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., район Нура, улица Сығанақ, строение 17/10, БЦ "Зеленый квартал"
Жеткізу шарттары	-
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 10 жұмыс күніішінде
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

2. Сипаттамасы және талап етілетін функционалдық, техникалық, сапалық және пайдалану сипаттамалары

1. Жалпы талаптар.

1.1. Архитектурасы және форм-факторы.

Шешім виртуалды форматта жеткізілуі тиіс.

VMware / Hyper-V / KVM виртуалдандыру жүйелерін қолдауы тиіс.

Шешім істен шығуға төзімділікті қамтамасыз етудің мынадай екі нұсқасын қолдауы тиіс:

- ортақ IP-мекенжаймен (shared IP);

- компоненттердің әртүрлі IP-мекенжайларымен.

Шешім үлестірілген архитектураны қолдауы тиіс.

Шешімде орталықтандырылған басқару жүйесі болуы тиіс.

1.2. Лицензиялау.

Шешім тұрақты қолданыстағы лицензиялар негізінде лицензиялануы тиіс.

Лицензиялау бір мезгілде қосылған сымды және сымсыз соңғы құрылғылардың ең көп санына негізделуі тиіс.

Лицензия «Самұрық-Қазына Контракт» ЖШС (Samruk-Kazyna Contract, LLP) ұйымына тіркелуі тиіс. Қолданыстағы лицензиялар туралы ақпарат жеке кабинетте қолжетімді болуы тиіс.

1.3. Инфрақұрылымды қолдау

Шешім әртүрлі өндірушілердің шешімдерімен, оның ішінде Fortinet, Huawei, HP, Aruba, Cisco және басқа да өндірушілердің шешімдерімен интеграциялануы тиіс.

Шешім мынадай операциялық жүйелермен интеграцияны қолдауы тиіс: Android, Apple macOS және iOS, Linux, Microsoft Windows.

Шешім әртүрлі өндірушілердің үшінші тарап платформаларымен интеграциялауға арналған екіжақты API интерфейсін қолдауы тиіс.

1.4. Жүйеге қойылатын жалпы талаптар.

Шешім мыналарды қамтамасыз етуі тиіс:

- Құрылғылардың сымды және сымсыз желілерге қосылуы туралы ақпаратты алу арқылы желінің көрінуін қамтамасыз ету.

- Желіге қосылған құрылғыларды профильдеу және түгендеу. Бұл ретте тек пайдаланушылардың құрылғылары ғана емес, сонымен қатар Тапсырыс беруші инфрақұрылымының құрамына кіретін принтерлер, IP-телефондар, IP-камералар, желілік жабдықтар және басқа да құрылғылар қамтылуы тиіс.

- Қосылатын құрылғылардың қолжетімділігін басқару үшін желілік инфрақұрылыммен интеграциялану.

- Шешім тіркеген оқиғаларды журналға жазу.

1.5. Желілік құрылғылармен өзара әрекеттесу хаттамалары және инфрақұрылыммен өзара әрекеттесу әдістері.

Шешім желілік инфрақұрылыммен өзара әрекеттесудің мынадай әдістерін қолдауы тиіс:

- SNMP;

- SSH/Telnet (CLI).

Шешім үшінші тарап құрылғыларынан деректерді мынадай тәсілдермен алуды қолдауы тиіс:

- syslog арқылы;

- SNMP traps түрінде.

Шешім мыналарды қолдауы тиіс:

- FortiGate конфигурациялық командаларын жіберу;

- FortiGate құрылғысына мынадай деректерді беру арқылы Fortinet Security Fabric жүйесімен интеграциялану:

- қосылған құрылғының IP-мекенжайы;

- User ID немесе MAC-мекенжайы;

- шешім айқындаған желіаралық экран тобы немесе белгісі.

1.6. Пайдаланушы құрылғыларының қосылуын анықтау және олар туралы ақпарат жинау әдістері.

Шешім пайдаланушылардың құрылғыларын анықтауды және олар туралы ақпарат жинауды мынадай әдістермен жүзеге асыруы тиіс:

- пайдаланушы құрылғысы қосылған нүкте ретінде әрекет ететін құрылғыны сұрау арқылы;

- пайдаланушы құрылғысы қосылған нүкте ретінде әрекет ететін құрылғыдан SNMP traps және SNMP MAC notification traps алу арқылы;

- пайдаланушы құрылғысы қосылған нүкте ретінде әрекет ететін құрылғыдан RADIUS сұрауын алу арқылы;

- DHCP деректерін талдау арқылы.

1.7. Құрылғыларды профильдеу.

Шешім мынадай құрылғыларды профильдеуді жүзеге асыруы тиіс:

- соңғы пайдаланушылардың құрылғылары;

- смартфондар, принтерлер, IP-телефондар, IP-камералар, желілік жабдықтар және басқа да құрылғылар.

Құрылғыларды профильдеу мынадай деректер мен әдістер негізінде жүзеге асырылуы тиіс:

- құрылғының қосылған орны туралы деректерді объектілер дерекқорындағы мәліметтермен салыстыру;

- қосылатын құрылғының OUI идентификаторын OUI дерекқорымен салыстыру;

- NMAP көмегімен белсенді сканерлеу;

- HTTP / HTTPS хаттамалары бойынша сұраулар нәтижелері;

- құрылғының IP-мекенжайының белгілі бір IP-мекенжайлар ауқымына тиесілі болуы;

- 1/2/3 нұсқаларында аутентификацияны қолдайтын SNMP сұрауы;

- SSH хаттамалары арқылы командаларды орындау нәтижелері;

- NMAP көмегімен сканерлеу арқылы TCP ашық порттарын анықтау;

- Telnet хаттамалары арқылы командаларды орындау нәтижелері;

- NMAP көмегімен сканерлеу арқылы UDP ашық порттарын анықтау;

- WinRM хаттамасы арқылы командаларды орындау нәтижелері;

- пайдаланушы құрылғысының WMI профилін талдау арқылы мынадай ақпаратты алу:

- операциялық жүйенің нұсқасы;

- сериялық нөмірі;

- түгендеу нөмірі;

- Windows Security Center деректері;

- іске қосылған процестер;

- орнатылған қолданбалар;

- Windows қызметтері;

- FortiGate құрылғысынан алынған сессиялар туралы ақпаратты талдау;

- желілік трафикті талдау;

- DHCP пакеттерін талдау;

- P0f дерекқорын пайдалана отырып, желілік трафикті пассивті талдау.

1.8. Аутентификация және қолжетімділікті қамтамасыз ету.

Шешім мынадай аутентификация хаттамалары мен каталог қызметтерін қолдауы тиіс:

- RADIUS — Microsoft IAS, Cisco ACS, FreeRADIUS;

- LDAP — Microsoft Active Directory, OpenLDAP, Google SSO.

Шешімде аутентификация әдісі мен каталог қызметін таңдаудың кіріктірілген мүмкіндігі бо луы тиіс:

- 802.1X;

- Non-AAA;

- Captive Portal;

- WebAuth;

- MACauth.

1.9. Құрылғылардың корпоративтік саясаттарға сәйкестігі.

Шешімнің мынадай мүмкіндіктері болуы тиіс:

- Бағдарламалық агенттерді пайдалана отырып, құрылғылардың корпоративтік саясаттарға сәйкестігін сканерлеу.

- Құрылғыда тұрақты орнатылатын агенттерді, сондай-ақ уақытша агенттерді қолдау.

- Мыналарды анықтау:

- қосылатын құрылғының операциялық жүйесін;

- қосылатын құрылғыда орнатылған антивирустық өнімді және антивирустық дерекқорлардың нұсқасын;

- қосылатын құрылғыда іске қосылған процестерді;

- орнатылған бағдарламалық қамтылымды;

- белгілі бір файлдардың болуын;

- сымсыз байланыс модулінде пайдаланылатын драйверлерді;

- жаңартулардың (патчтардың) болуын.

- Корпоративтік саясаттарға сәйкес келмейтін құрылғыларды карантинге автоматты түрде орналастыру.

1.10. Техникалық қолдау.

Шешім өндірушінің жыл бойы тәулік бойы (24×7) көрсетілетін кеңейтілген техникалық қолдауымен қамтамасыз етілуі тиіс.

Бағдарламалық қамтылымды жаңарту, өндірушінің техникалық қолдау қызметіне өтінімдер (тикеттер) ашу және оларды сүйемелдеу, сондай-ақ жабдықты пайдалану мәселелері бойынша техникалық консультациялар алу мүмкіндігі қамтамасыз етілуі тиіс.

1.11. Сандық талаптар.

- FortiNAC Plus License for 100 concurrent endpoint devices FortiNAC Perpetual PLUS License for 100 concurrent endpoint devices – 1 дана;

- FortiCare Support for FortiNAC License 1 Year FortiCare Premium Support (100 Endpoints) for FortiNAC PLUS deployments – 3 дана.

- FortiNAC Control and Application Extended-VM 1 Year FortiCare Premium Support – 2 дана.

2. Қызмет көрсетуге және кепілдікке қойылатын талаптар:

2.1. Жүйе өндірушінің кемінде 1 жыл мерзімге тәулік бойы (24×7) көрсетілетін кеңейтілген техникалық қолдауымен қамтамасыз етілуі тиіс.

3. Өнім берушіге қойылатын талаптар:

3.1. Өнім беруші Қазақстан Республикасының аумағында жабдық өндірушісінің авторизаци яланған серіктесі мәртебесіне ие екенін растауы тиіс (Шартқа қол қойған күннен бастап ғ жұмыс күн ішінде өндірушінің хаты арқылы растау қажет).

3.2. Өнім беруші Тапсырыс берушінің өкілдерімен бірлесіп, өндірушінің интернет-ресурсы а рқылы лицензияны онлайн белсендіруді, баптауды және конфигурациялауды жүзеге асыруы тиіс;

3.3. Өнім беруші көрсетілген қызметтерді көрсетілген қызметтер актісімен растауы тиіс.

4. Өнім берушіге қойылатын қосымша талаптар:

4.1. Өнім беруші лицензияның қолданылу мерзімі ішінде мынадай талаптардың орындалуын қамтамасыз етуі тиіс:

- техникалық қолдауды орыс тілінде көрсету;

- өтініштер санына шектеу қоймау;

- электрондық пошта арқылы қолдау көрсету;

- телефон арқылы қолдау көрсету;

- проблемаларды қашықтан шешу;

- өтініштерді жоғары деңгейге эскалациялау;

- пайдаланылатын бағдарламалық қамтылымды жаңарту (оның ішінде сыни қателерді түзету (патчтар), жоспарлы жаңартулар (сервистік релиздер), жаңа нұсқаға жаңарту және т. б.).

3. Сатып алынатын ТЖҚ жеке әлеуетті жеткізушіге немесе өндірушіге тиістілігін анықтайтын сипаттамалар бар

тауарларды, жұмыстарды және көрсетілетін қызметтерді қосымша жинақтау, қосымша жарақтандыру, біріздендіру немесе қолда бар тауарлармен, жұмыстармен және көрсетілетін қызметтермен үйлесімділігін қамтамасыз ету үшін, сондай-ақ одан әрі техникалық сүйемелдеу, сервистік қызмет көрсету және жөндеу, оның ішінде негізгі (орнатылған) жабдықты жоспарлы жөндеу (қажет болған кезде) үшін сатып алу

Қол қойған	Рахимова Гульбаршин
Қол қойылған күні	05.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1268964
способом Запрос ценовых предложений на понижение

Лот № (11 У, 4577154) Услуги по продлению лицензий на право использования программного обеспечения

Заказчик: Товарищество с ограниченной ответственностью "Самрук-Казына Контракт"
Организатор: Товарищество с ограниченной ответственностью "Самрук-Казына Контракт"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	11 У
Наименование и краткая характеристика	Услуги по продлению лицензий на право использования программного обеспечения, Услуги по продлению лицензий на право использования программного обеспечения
Дополнительная характеристика	FortiNac
Количество	1.000
Единица измерения	-
Место поставки	КАЗАХСТАН, г.Астана, район Нура, улица Сығанақ, строение 17/10, БЦ "Зеленый квартал"
Условия поставки	-
Срок поставки	С даты подписания договора в течение 10 рабочих дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

2. Описание и требуемые функциональные, технические, качественные и эксплуатационные характеристики

1. Общие требования.

1.1. Архитектура и форм-фактор.

Решение должно поставляться в виртуальном исполнении.

Должно поддерживать следующие системы виртуализации: VMWare / Hyper-V / KVM.

Решение должно поддерживать реализацию отказоустойчивости в двух вариантах:

- с общим ip адресом (shared ip);

- с различными ip адресами компонентов.

Решение должно поддерживать распределенную архитектуру.

Решение должно поддерживать центральную систему управления.

1.2. Лицензирование.

Решение должно лицензироваться как решения на основе постоянно действующих лицензий.

Лицензирование должно быть основано на максимальном количестве одновременно подключенных проводных и беспроводных конечных устройств.

Лицензия должна быть зарегистрирована на организацию ТОО Самрук-Казына Контракт. (Samruk-Kazyna Contract, LLP). Информация о действующих лицензиях должна быть доступна в личном кабинете.

1.3. Поддержка инфраструктуры

Решение должно интегрироваться с решениями различных производителей (включая, но не ограничиваясь): Fortinet, Huawei, HP, Aruba, Cisco и др.

Решение должно поддерживать интеграцию со следующими ОС: Android, Apple MAC OSX and iOS, Linux, Microsoft Windows.

Решение должно поддерживать двунаправленный API для интеграции со сторонними платформами различных производителей.

1.4. Общие требования к системе.

Решение должно обеспечить:

- Видимость сети путем получения информации о подключении устройств к проводной и беспроводной сетям.

- Профилирование и инвентаризацию устройств, подключенных к сети, включая не только пользовательские устройства, но и устройства, являющиеся частью инфраструктуры заказчика: принтеры, IP-телефоны, IP-камеры, сетевое оборудование и др.

- Интеграцию с сетевой инфраструктурой для управления доступом подключаемых устройств.

- Журналирование событий, зафиксированных решением.

1.5. Протоколы взаимодействия с сетевыми устройствами, методы взаимодействия с инфраструктурой.

Решение должно поддерживать следующие методы взаимодействия с сетевой инфраструктурой:

- SNMP;

- SSH/Telnet (CLI).

Решение должно поддерживать получение данных от третьих устройств:

- по syslog;

- в виде SNMP traps.

Решение должно поддерживать:

- передачу конфигурационных команд Fortigate;

- интеграцию с Fortinet Security Fabric путем передачи FortiGate следующих данных:

- IP адрес подключенного устройства

- User ID или MAC адрес

- Группа или метка межсетевого экрана, определенный решением

1.6. Методы обнаружения подключения устройств пользователей и сбора информации об устройствах пользователей.

Решение должно осуществлять обнаружение и сбор информации об устройствах пользователей следующими методами:

- путем опроса устройства, выступающего точкой подключения пользовательского устройства;

- путем получения SNMP traps, SNMP MAC notification traps от устройства, выступающего точкой подключения пользовательского устройства;

- путем получения RADIUS запроса от устройства, выступающего точкой подключения пользовательского устройства;

- путем анализа DHCP.

1.7. Профилирование устройств.

Решение должно осуществлять профилирование:

- Устройств конечных пользователей

- Смартфонов, принтеров, IP-телефонов, IP-камер, сетевого оборудования и др.

Устройств на основе:

- сравнения данных о месте подключения устройства с данными в базе данных объектов;

- сравнения OUI подключаемого устройства с базой OUI;

- активного сканирования NMAP;

- результатов запросов по протоколу HTTP / HTTPS;

- принадлежности ip адреса устройства к определенным диапазонам ip адресов;

- SNMP запроса с поддержкой аутентификации версий 1/2/3;

- результатов выполнения команд по протоколам SSH;

- открытых портов TCP путем сканирования с помощью NMAP;

- результатов выполнения команд по протоколам Telnet;

- открытых портов UDP путем сканирования с помощью NMAP;

- результатов выполнения команд по протоколу WinRM;

- анализа WMI профиля пользовательского устройства для получения информации о:

- версии ОС

- серийном номере

- инвентарном номере

- данных Windows Security Center

- запущенных процессах

- установленных приложениях

- сервисах Windows

- анализа информации о сессиях, полученных от FortiGate;

- анализа сетевого трафика;

- анализа пакетов DHCP;

- пассивного анализа сетевого трафика с использованием базы данных P0f.

1.8. Аутентификация и обеспечение доступа.

Решение должно поддерживать следующие протоколы аутентификации и службы каталогов:

- RADIUS — Microsoft IAS, Cisco ACS, Free RADIUS

- LDAP — Microsoft Active Directory, OpenLDAP, Google SSO

Решение должно иметь встроенную возможность выбора метода аутентификации и службы каталогов:

- 802.1x;

- Non-AAA;

- Captive portal;

- WebAuth;

- MACauth.

1.9. Соответствие устройств корпоративным политикам.

Решение должно иметь возможность:

- Осуществлять сканирование устройств на соответствие корпоративным политикам с помощью программных агентов.

- Поддерживать агенты, постоянно установленные на устройстве, а также временные агенты.

- Осуществлять определение:

- ОС подключаемого устройства

- антивирусного продукта, установленного на подключаемом устройстве, версию антивирусных баз

- запущенных на подключаемом устройстве процессов

- установленного ПО

- наличия определенных файлов

- используемых драйверов модуля беспроводной связи

- наличия патчей

- Автоматически добавлять устройства, не соответствующие корпоративным политикам, в карантин.

1.10. Техническая поддержка.

Решение должно обеспечиваться годовой расширенной технической поддержкой производителя в режиме 24x7.

Обеспечивать возможность обновления программного обеспечения, обращения в техподдержку производителя для открытия и сопровождения тикетов, технических консультаций по работе с оборудованием.

1.11. Количественные требования.

- FortiNAC Plus License for 100 concurrent endpoint devices FortiNAC Perpetual PLUS License for 100 concurrent endpoint devices. – 1 шт.;

- FortiCare Support for FortiNAC License 1 Year FortiCare Premium Support (100 Endpoints) for FortiNAC PLUS deployments. – 3 шт.

- FortiNAC Control and Application Extended-VM 1 Year FortiCare Premium Support – 2 шт.

2. Требование к обслуживанию и гарантии:

2.1. Система должна обеспечиваться расширенной технической поддержкой производителя в режиме 24x7 не менее 1 года.

3. Требования к Поставщику:

3.1. Поставщик должен иметь подтвержденный статус авторизованного партнера от производителя оборудования на территории Республики Казахстан (подтвердить письмом от производителя в течение 5 рабочих дней после подписания Договора).

3.2. Поставщик должен провести совместную с представителями Заказчика онлайн активацию, настройку и конфигурирование лицензии с интернет-ресурса производителя;

3.3. Поставщик должен подтвердить услуги актом оказанных услуг.

4. Дополнительные требования к поставщику:

4.1. Поставщик должен обеспечить следующие требования в течении срока действия лицензии:

- Обеспечение технической поддержки на русском языке;

- Неограниченное количество обращений;

- Поддержку по электронной почте;

- Поддержку по телефону;

- Удаленное решение проблем;

- Эскалацию обращений;

- Обновление используемого ПО (такие как исправление критических ошибок (патчи), плановое обновление (сервисные релизы), обновление до новой версии и т.п.).

3. Присутствует указание характеристик, определяющих принадлежность приобретаемого ТРУ отдельному потенциальному поставщику либо производителю на основании

приобретения товаров, работ и услуг для доукомплектования, дооснащения, унификации или обеспечения совместимости с имеющимися товарами, работами и услугами, а также для дальнейшего технического сопровождения, сервисного обслуживания и ремонта, в том числе планового ремонта (при необходимости), основного (установленного) оборудования

Подписал	Рахимова Гульбаршин
Дата подписания	05.11.2026