ТЕХНИКАЛЫҚ СИПАТТАМА

1266782 , Желіаралық экран сатып алу бойынша
Ашық тендер тәсілімен

Лот № 1 (2362-2 Т, 4569628) Арнайы экран

Тапсырыс беруші: "Болат Нұржанов атындағы Екібастұз ГРЭС-1" жауапкершілігі шектеулі серіктестігі
Ұйымдастырушы: "Болат Нұржанов атындағы Екібастұз ГРЭС-1" жауапкершілігі шектеулі серіктестігі

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	2362-2 Т
Атауы және қысқаша сипаттамасы	Арнайы экран, желі аралық
ТЖҚЖС санаттың атауы	Межжелілік экрандар (жиынтықта)
Қосымша сипаттама	Сипаттама: Желіаралық экран
Саны	1.000
Өлшем бірлігі	Жиынтық
Жеткізу орны	ҚАЗАҚСТАН, Павлодар облысы, Екібастұз Қ.Ә., Екібастұз қ., Павлодарская область, г. Экибастуз, Промышленная зона ГРЭС-1, строение 2
Жеткізу шарттары	DDP
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап (қоса алғанда) 12.2026 дейін.
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

Жүйенің жалпы ережелері мен қолданылуы:

Құрылған ақпараттық қауіпсіздік жүйесі ұйымның желілік инфрақұрылымын орталықтандырылған қорғауды, бақылауды, мониторингті және басқаруды қамтамасыз ететін бірыңғай архитектура қағидаты бойынша құрылған кешенді, интеграцияланған шешім болуы тиіс.

Шешім келесілерді қамтамасыз етуі керек:

- желінің периметрі мен ішкі сегменттерін қорғауды;
- барлық деңгейдегі желілік трафикті бақылауды және сүзуді;
- заманауи киберқауіптерді, соның ішінде мақсатты шабуылдар мен нөлдік күндік қауіптерді анықтауды және алдын алуды;
- ақпараттық қауіпсіздік оқиғаларын орталықтандырылған жинауды, корреляциялауды және талдауды;
- пайдаланушылар мен құрылғылардың желілік ресурстарға қолжетімділігін бақылауды;
- Zero Trust принциптеріне негізделген қауіпсіз қашықтан қолжетімділікті;
- барлық компоненттерді масштабтау мүмкіндігі бар бірыңғай басқару жүйесіне біріктіруді.

Жүйе ұзақ мерзімді пайдалануға, функционалдылықтың кеңеюін қолдауға және барлық негізгі компоненттер деңгейінде ақауларға төзімділікті қамтамасыз етуге бағытталған болуы керек.

Қауіпсіздік шлюзіне қойылатын талаптар:

1. **Қауіпсіздік шлюзі** (жаңа буындағы желіаралық экран, NGFW) – желілік периметрді қорғауды, трафикті сүзуді, кірулерді болдырмауды, антивирустық қорғауды, қосымшаларды басқаруды және веб-сүзуді қамтамасыз ететін бағдарламалық-аппараттық кешен.

2. **Оқиғаларды орталықтандырылған жинау және есептерді құру жүйесі** – ақпараттық қауіпсіздік оқиғаларының журналдарын біріктіру, сақтау, талдау, сондай-ақ оқиғалардың есептілігі мен мониторингін қалыптастыру үшін арналған.

3. **Zero Trust Network Access (ZTNA) технологиясын қамтамасыз ету үшін лицензия** кемінде 100 бірлік мөлшерінде – пайдаланушының контекстін және құрылғының жай-күйін есепке алумен Zero Trust принциптері негізінде пайдаланушылардың корпоративтік ресурстарға қауіпсіз қолжетімділікті ұйымдастыру үшін арналған Zero Trust Network Access қамтамасыз

ету үшін.

Әлеуетті өнім берушіге қойылатын талаптар:

Желіаралық экрандауға қойылатын функционалдық талаптар.

Желінің үздіксіз қауіпсіздігін қамтамасыз ету үшін бірге жұмыс істейтін екі аппараттық құрылғыдан тұрады.

Жүйені лицензиялау пайдаланушылардың шектеусіз саны үшін жүзеге асырылуы керек.

Жүйе қауіпсіздік модульдері сигнатураларының жаңартуларын және өндірушінің серверінен өзекті қауіптердің тізбесін үнемі алып отыруы керек.

Жүйе кластерлердің түрлерін құру мүмкіндігімен кластерге кемінде 4 құрылғыны біріктіруді қолдауы керек:

- суық резервпен (active/passive);
- ыстық резервпен (active/active);
- теңдестіру кластері.

Жүйе желіаралық экрандау функционалдығына ие болуы керек, яғни IP мекенжайлары, порттар және қосымшалар негізінде желілік трафикті сүзу қағидаларын құру мүмкіндігін қамтамасыз етуі керек.

Жүйеде жүктемені теңестіру функционалдығына ие болуы керек.

Жүйе SD-WAN технологиясын қолдауы және интеллектуалды трафикті басқаруды қамтамасыз етуі керек (Software-Defined Wide Area Network, бағдарламалық-конфигурацияланатын желі).

Жүйеде трафикті өткізу жолағын басқару функциясы болуы керек (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 трафиктің SSH талдауын (ssh inspection) қамтамасыз етуі керек.

Жүйе IPv4, IPv6 динамикалық маршруттауды қамтамасыз етуі керек.

Жүйе WCCP хаттамасы бойынша жұмыс істеу мүмкіндігіне ие болуы керек (сервер режимінде де, клиент режимінде де).

Жүйе WAN қосылыстарды оңтайландыруды қамтамасыз етуі керек.

Жүйеде DLP деректерінің жылыстауынан қорғау функционалы болуы керек.

Жүйе аппараттық жеделдетумен антивирустық қорғауды қамтамасыз етуі керек.

Жүйе спамнан қорғауды қамтамасыз етуі керек (антиспам).

Жүйе аппараттық жеделдетумен IPS шабуылының алдын алу функционалдығына ие болуы керек.

Жүйе сайттардың белгілі бір санаттарына қолжетімділікті шектеу мүмкіндігімен WEB трафикті сүзуді қамтамасыз етуі керек.

Трафикті кемінде 85 санат бойынша WEB сүзу қамтамасыз етілуі тиіс.

Танымал іздеу жүйелерінде қауіпсіз іздеу режимін мәжбүрлеп іске қосу.

Жүйе қосымшаларды басқару функционалдығына ие болуы керек.

Жүйе WEB proxy функционалдығына ие болуы керек.

Жүйе әдепкі қалпы бойынша қолжетімді кемінде 10 виртуалды доменнің (бір құрылғының ішінде толық жұмыс істейтін виртуалды МСЭ) болуын қамтамасыз етуі керек.

Жүйе HTTP, SMTP, POP3, IMAP, FTP және IM трафиктің ішінде вирустарды тексеру мүмкіндігіне ие болуы керек.

Жүйе кесте бойынша антивирустық базалардың жаңартуларын автоматты түрде ала мүмкіндігіне ие болуы керек.

Жүйе жұқтырған хабарламаларды карантинге орналастыру мүмкіндігіне ие болуы керек.

Жүйе көлеміне байланысты файлдарды тасымалдауды бұғаттау мүмкіндігіне ие болуы керек.

Жүйе түріне байланысты файлдарды тасымалдауды бұғаттау мүмкіндігіне ие болуы керек.

Жүйе көптеген WAN желілерінің қосылыстарын қолдауы керек.

Жүйе PPPoE және L2TP хаттамаларын қолдауы керек.

Жүйе «Клиент/Сервер» конфигурациясында DHCP хаттамасын қолдауы керек.

Жүйе саясаттар негізіндегі маршруттауды қолдауы керек.

Жүйе RIP v1 және v2, OSPF, BGP хаттамалары 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 рөлдер негізінде әкімшілендіруді қолдауы керек.

Жүйе әкімшілер мен пайдаланушылардың бірнеше деңгейлерін қолдауы керек.

Жүйе TFTP хаттамасы мен web-интерфейс арқылы кіріктірілген БЖ жаңартуды қолдауы керек.

Жүйе кіріктірілген БЖ алдыңғы күйіне (нұсқасына) оралу мүмкіндігін қолдауы керек.

Жүйе ішкі деректер базасы арқылы пайдаланушылардың аутентификациясын қолдауы керек.

Жүйе Kerberos пайдаланушыларының аутентификациясын қолдауы керек.

Жүйе Windows Active Directory арқылы пайдаланушылардың аутентификациясын қолдауы керек; бұл ретте доменге енгізілген Windows 7 және одан жоғары операциялық жүйелер пайдаланушыларының аутентификациясы қосымша құпиясөзді сұрау процедураларынсыз автоматты түрде орындалуы керек.

Жүйе сыртқы RADIUS/LDAP деректер базасы арқылы пайдаланушының аутентификациясын қолдауы керек.

Жүйе IP/MAC-мекенжайын байланыстыру арқылы пайдаланушылардың аутентификациясын қолдауы керек.

Жүйе пайдаланушылардың топтары негізінде аутентификацияны қолдауы керек.

Жүйе NAT, PAT, «мөлдір» (көпір) функцияларын қолдауы керек.

Жүйе саясаттар негізіндегі NAT функцияларын қолдауы керек.

Жүйе VLAN Tagging (802.1Q) функцияларын қолдауы керек.

Жүйе SIP/H.323 NAT Traversal функцияларын қолдауы керек.

Жүйе қауіпсіздік профильдерін теңшеуді қолдауы керек.

Жүйе URL/кілт сөз/сөз тіркесі арқылы бұғаттау мүмкіндігіне ие болуы керек.

Жүйе «Ақ» URL тізімдерін қолдауы керек.

Жүйе Java, Cookies аплеттерін, ActiveX басқару элементтерін бұғаттау мүмкіндігіне ие болуы керек.

Жүйе желілік шабуылдардың кемінде 10000 түрін болдырмауы керек.

Жүйе шабуыл сигнатураларының тізімін теңшеу мүмкіндігіне ие болуы керек.

Жүйе IPS шабуылдар мен сигнатуралар базасын автоматты түрде жаңартуды қолдауы керек.

Жүйе өндірушінің серверінен спамерлер мен ашық релелердің IP-мекенжайлардың «қара» тізімін үнемі алып отыруы керек.

Жүйе MIME тақырыптарын тексеруді қолдауы керек.

Жүйе электрондық поштаны кілт сөздер мен сөз тіркестері бойынша сүзуді қолдауы керек.

Жүйе IP-мекенжайлардың «қара/ақ» тізімдері бойынша сүзуді қолдауы керек.

Жүйе қашықтағы syslog серверіне логтарды жіберу мүмкіндігіне ие болуы керек.

Жүйе файлдың бастапқы форматын сақтай отырып, Microsoft Office және PDF форматындағы файлдардан орындалатын құралатын шығару сервисін қолдауы керек.

Жүйе желілік трафикті, жүйенің жай-күйін және анықталған қауіптерді мониторингілеу үшін графикалық құралдарға ие болуы керек.

Жүйе вирустар мен желілік шабуылдар туралы электрондық пошта хабарландыруларын жіберу мүмкіндігіне ие болуы керек.

Жүйе «0-day» класындағы белгісіз қауіптерді анықтау үшін файлдарды және URL-ды cloud sandbox талдауына жіберуді қолдауы керек.

Жүйе cloud sandbox-та талдау үшін күніне (24 сағат) кемінде 10 000 нысанды (файлдар мен URL-ды) лицензиялауға ие болуы керек.

Жүйе VRRP хаттамасын қолдауы керек.

Жүйе SIEM-мен интеграцияны қолдауы керек.

Жүйе кепілдендірілген, максималды немесе басымдықты өткізу қабілеттілігін орнату мүмкіндігіне ие болуы керек.

Жүйе жедел хабар алмасу қызметтерін анықтауды және пайдалануды бақылауды қолдауы керек.

Жүйе өткізу қабілеттілігін және Web ресурстарға қолжетімділік жылдамдығын оңтайландыру үшін Web контентті жергілікті сақтау мүмкіндігін қолдауы керек.

Жүйе WEB интерфейс арқылы басқаруды қолдауы керек.

Жүйе орталықтандырылған басқару және есеп беру жүйелерімен интеграциялану мүмкіндігіне ие болуы керек.

Жүйе NetFlow, sFlow хаттамаларын қолдауы керек.

Жүйе кері прокси-сервер режимін (reverse proxy) қамтамасыз етуі керек.

Жүйе мөлдір прокси-сервер (transparent proxy) режимін қамтамасыз етуі керек.

Жүйе командалық жолдан консоль режимінде қауіпсіздік саясатын басқару мүмкіндігін қамтамасыз етуі керек.

Жүйе телеметрия туралы ақпаратты, пайдаланылған модель мен амалдық жүйенің нұсқасын, IP мекенжайды, MAC мекенжайды, анықталған осалдықтар туралы ақпаратты қамтитын сыртқы жүйелермен интеграцияны қолдауы керек.

Жүйе жұмыс станцияларының корпоративтік қауіпсіздік саясатына сәйкестігін бағалау үшін сыртқы жүйелермен интеграцияны қолдауы керек. Қауіпсіздік саясатына сәйкес келмеген жағдайда, тексерілетін хост желілік қолжетімділікті шектейтін карантинге орналастырылуы керек.

Жүйе сымсыз қолжетімдідік нүктелерін басқару мүмкіндігін қамтамасыз етуі керек.

Жүйе коммутаторларды басқару мүмкіндігін қамтамасыз етуі керек.

Қауіпсіздік шлюздері 1 жыл ішінде сервистерге жазылымдарға ие болуы керек:

- Қосымшаларды бақылау;
- IPS;
- AV;
- Web Filtering;
- Antispam;
- Sandbox Cloud;
- Security Rating;
- IoT Device Detection.

Желіаралық экрандауға қойылатын техникалық талаптар:

- Firewall Throughput (1518/512/64 byte UDP): кемінде 79/78/69 Gbps;
- Сессиялардың бір уақыттағы саны: кемінде 7.7 Млн;
- Жаңа қосылыстарды орнату жылдамдығы: кемінде 490 000 в сек;
- IPS Throughput Enterprise Mix: кемінде 11.5 Gbps;
- Application Control Throughput (HTTP 64K): кемінде 27.5 Gbps;
- Threat Protection Throughput: кемінде 8.9 Gbps;
- Базалық жиынтықтылаудағы қауіпсіздіктің виртуалды контекстерінің саны: кемінде 10;
- Интерфейстер саны: кемінде 8x GE SFP, 18x GE RJ45, 8x10GE SFP+
- Жоғары қолжетімділіктегі белгіленген порт: кемінде 1;
- USB порттар саны: кемінде 1;
- Консольдық порт: кемінде 1;
- Қуат беру блогы 100–240V AC, 50–60 Hz: кемінде 2.

Қызмет көрсетуге және кепілдікке қойылатын талаптар:

Жүйе өндірушінің 24x7 режимінде кемінде 1 жыл кеңейтілген техникалық қолдауымен қамтамасыз етілуі керек.

Оқиғаларды орталықтандырылған жинау және есептерді құру жүйесіне қойылатын талаптар:

Функционалдық талаптар.

Желіаралық экрандау жүйелерімен, электрондық поштаны қорғау жүйелерімен, жеткізілім жиынтығына кіретін мақсатты бағытталған шабуылдардан қорғау жүйелерімен үйлесімділік;

Журналдардың оқиғаларын жинауды және талдауды, желіаралық экрандау жүйелерінен алынған мәліметтер негізінде есептер құруды қамтамасыз ету;

Талданатын құрылғылардан жиынтық графикалық есептерді құру мүмкіндігі;

Желілік белсенділік, жүйелік оқиғалар, вирустар, шабуылдар, web сүзу туралы есептерді құруды қолдау;

Ең көп сұранысқа ие есептерді жылдам құру үшін кіріктірілген шаблондардың болуы;

Есептердің шаблондарын импорттау және экспорттауды қолдау;

Нақты уақытта логтарды көру мүмкіндігі;

Логтарда деректерді іздеу және сүзу мүмкіндігі;

Логтарда белгілі бір оқиғалар болған кезде хабарламалар құру мүмкіндігі;

Хабарламаларды электрондық пошта бойынша жіберу немесе Syslog хаттамасы бойынша жіберу мүмкіндігі;

Құпиялылығы бұзылған тораптарды ретроспективті анықтау үшін қауіпсіздіктің бұзылу индикаторларының сервисін қолдау;

Виртуалды машина түрінде іске асыру (VMware vSphere, Xen, KVM, Hyper-V қолдайтын гипервизорлар);

Бұл логтардың өнімділігі: кемінде 5 Гб/күніне;

Деректер қоймасының қолжетімді көлемі: кемінде 3 ТБ;

24х7 режимінде өндірушінің жылдық кеңейтілген техникалық қолдауымен жиынтықтылау;

Өндірушінің қолдау мерзімі: кемінде 1 жыл.

Zero Trust Network Access қамтамасыз ету үшін лицензияларға қойылатын талаптар:

Функционалдық талаптар.

100 клиентке Zero Trust Network Access лицензиясы келесі талаптарға сәйкес болуы керек:

- Жүйе клиенттік құрылғыларға мамандандырылған БЖ орнату жолымен шешімнің жұмысын қамтамасыз етуі керек.
- Жүйе ресурстарға қолжетімділікті қамтамасыз етудің алдында құрылғыны егжей-тегжейлі тексеруді қамтамасыз етуі керек:

- Комплаенсты тексеру: Қолжетімділік берілген критерийлерді қанағаттандыратын құрылғыларға ғана рұқсат етілуі керек.

- Корпоративтік құрылғыларды сәйкестендіру: AD доменінде құрылғылардың болуын міндетті түрде тексеру және/немесе бірегей сертификатты тексеру.
- Тегтер бойынша тексеру (ZTNA Tags): Жүйе құрылғыларға олардың жай-күйінің негізінде тегтерді автоматты түрде тағайындауы керек (мәселен, Critical_Vulnerability немесе Non-Compliant) және құрылғының мәртебесі өзгерген кезде белсенді сессияларды дереу тоқтатуы керек.

- Жүйе сайттардың белгілі бір санаттарына қолжетімділікті шектеу мүмкіндігімен трафикті web сүзуді қолдауы керек.
- Жүйе екі факторлы аутентификация жүйесімен, оның ішінде бір реттік уақытша құпиясөздері бар токендерді қолданумен интеграцияны қамтамасыз етуі керек.
- Жүйе осалдық сканерін қолдауы керек.
- Жүйе нақты уақыт режимінде соңғы түйіндердің жай-күйін мониторингілеуді қамтамасыз етуі керек.
- Жүйе әкімшінің бірыңғай консолінен (графикалық интерфейстен) қашықтан орналастыруды, конфигурацияны және орталықтандырылған басқаруды қолдауы керек.
- Жүйе кіріктірілген функционалға ие болуы керек немесе телеметрия ақпаратын беру үшін сыртқы жүйелермен интеграцияны қолдауы керек, оның ішінде пайдаланушылар туралы ақпарат, операциялық жүйенің моделі мен нұсқасы, IP мекенжайы, MAC мекенжайы, тиісті қосымша лицензияны орнату кезінде анықталған осалдықтар туралы ақпарат.
- Жүйе жұмыс станцияларының корпоративтік қауіпсіздік саясатына сәйкестігін бағалау үшін кіріктірілген функционалға ие болуы немесе сыртқы жүйелермен интеграцияны қолдауы керек.
- Оқиғаларды орталықтандырылған жинау жүйесімен интеграциялау және барлық тіркелген клиенттер туралы ақпаратты осы жүйеге беру мүмкіндігі.
- Жүйе мақсатты бағытталған және бұрын белгісіз шабуылдардан қорғау үшін сыртқы мамандандырылған жүйемен интеграцияны қолдауы керек.
- Орталықтандырылған басқару жүйесі жеткізілім жиынтығында лицензияға ие болуы керек және 100-ге дейін клиенттік құрылғыларды орталықтандырылған басқаруға қолдау көрсетуі керек.
- Жүйе масштабталған болуы керек және лицензияны кеңейту арқылы 100 мыңға дейін клиенттік құрылғыларға қолдау көрсетуі керек.
- Топтпо негізінде басқаруды қолдау және Microsoft Active Directory-мен жұмыс станцияларында, соның ішінде GPO көмегімен клиенттерді орталықтандырылған орналастыру үшін интеграция.
- Клиенттік, серверлік және мобильді операциялық жүйелерді қолдау:

- Microsoft Windows 10/8.1/8/7 (32-bit, 64-bit), XP (32-bit);
- Windows Server 2008 R2/2012/2012 R2;

- Жүйе виртуалды жеке желілердің (VPN) – SSL және IPSec қосылыстарын, соның ішінде екі факторлы аутентификация мен сертификаттарды қолданумен орнату мүмкіндігін қолдауы керек.
- Жүйе Windows logon жүйесіне VPN қосылымын орнатуды қолдауы керек.
- Жүйе сертификаттарды орталықтандырылған басқаруды қолдауы керек.
- Жүйе пайдаланушылардың ашық аутентификациясын жүзеге асыру үшін ағымдағы Active Directory пайдаланушысының есептік жазбасы туралы ақпаратты беру мүмкіндігін қолдауы керек.
- Жүйе ботнет-желілермен желілік өзара әрекеттесуді қадағалау мүмкіндігін қолдауы керек.
- Жүйе келесі хаттамалар үшін WAN оңтайландыруын қолдауы керек: CIFS, FTP, HTTP, MAPI.
- Жүйе қосылған функцияларды, НҚЖ, түйін атауын, IP мекенжайын және басқа жүйелік ақпаратты қарауды қамтамасыз етуі керек.
- Жүйе әрбір түйін үшін клиенттік бағдарламаның мәртебесін көрсетуі керек.
- Жүйе XML конфигурациясының таралуын қолдауы керек.

Лицензияның әрекет ету мерзімі кемінде 1 жыл.

Қол қойған	Закирьянов Данияр Бактыбекович
Қол қойылған күні	03.11.2026

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1266782 , Межсетевой экран
способом Открытый тендер

Лот № 1 (2362-2 Т, 4569628) Экран специальный

Заказчик: Товарищество с ограниченной ответственностью "Экибастузская ГРЭС-1 имени Булата Нуржанова"

Организатор: Товарищество с ограниченной ответственностью "Экибастузская ГРЭС-1 имени Булата Нуржанова"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	2362-2 Т
Наименование и краткая характеристика	Экран специальный, межсетевой
Наименование категории ОКТРУ	Межсетевые экраны, в комплекте
Дополнительная характеристика	Описание: Межсетевой экран
Количество	1.000
Единица измерения	Комплект
Место поставки	КАЗАХСТАН, Павлодарская область, Экибастуз Г.А., г.Экибастуз, Павлодарская область, г. Экибастуз, Промышленная зона ГРЭС-1, строение 2
Условия поставки	DDP
Срок поставки	С даты подписания договора по (включительно) 12.2026
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

Общие положения и назначение системы:

Создаваемая система информационной безопасности должна представлять собой комплексное, интегрированное решение, построенное по принципу единой архитектуры, обеспечивающее централизованную защиту, контроль, мониторинг и управление сетевой инфраструктурой организации.

Решение должно обеспечивать:

- защиту периметра сети и внутренних сегментов;
- контроль и фильтрацию сетевого трафика на всех уровнях;
- выявление и предотвращение современных киберугроз, включая целенаправленные атаки и угрозы нулевого дня;
- централизованный сбор, корреляцию и анализ событий информационной безопасности;
- контроль доступа пользователей и устройств к сетевым ресурсам;
- безопасный удалённый доступ на основе принципов Zero Trust;
- интеграцию всех компонентов в единую систему управления с возможностью масштабирования.

Система должна быть ориентирована на долгосрочную эксплуатацию, поддерживать расширение функциональности и обеспечивать отказоустойчивость на уровне всех ключевых компонентов.

Состав системы:

1. **Шлюз безопасности** (межсетевой экран нового поколения, NGFW) – программно-аппаратный комплекс, обеспечивающий защиту сетевого периметра, фильтрацию трафика, предотвращение вторжений, антивирусную защиту, контроль приложений и веб-фильтрацию.
2. **Система централизованного сбора событий и построения отчетов** – предназначена для агрегирования, хранения, анализа журналов событий информационной безопасности, а также формирования отчетности и мониторинга инцидентов.
3. **Лицензии для обеспечения технологии Zero Trust Network Access (ZTNA)** в количестве не менее 100 единиц – предназначены для организации защищённого доступа пользователей к корпоративным ресурсам на основе принципов Zero Trust с учетом контекста пользователя и состояния устройства для обеспечения Zero Trust Network Access.

Требования к шлюзу безопасности:

Функциональные требования к межсетевому экранированию.

Состоит из двух аппаратных устройств, функционирующих совместно для обеспечения непрерывности сетевой защиты.

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 SD-WAN и обеспечивать интеллектуальное управление трафиком (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 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 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 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 1 года:

- Контроль приложений;
- IPS;
- AV;
- Web Filtering;
- Antispam;
- Sandbox Cloud;
- Security Rating;
- IoT Device Detection.

Технические требования к межсетевому экранированию:

- Firewall Throughput (1518/512/64 byte UDP): не менее 79/78/69 Gbps;
- Одновременное количество сессий: не менее 7.7 Млн;
- Скорость установки новых соединений: не менее 490 000 в сек;
- IPS Throughput Enterprise Mix: не менее 11.5 Gbps;
- Application Control Throughput (HTTP 64K): не менее 27.5 Gbps;
- Threat Protection Throughput: не менее 8.9 Gbps;
- Количество виртуальных контекстов безопасности в базовой комплектации: не менее 10;
- Количество интерфейсов: не менее 8x GE SFP, 18x GE RJ45, 8x10GE SFP+
- Выделенный порт высокой доступности: не менее 1;
- Количество USB портов: не менее 1;
- Консольный порт: не менее 1;
- Блок питания 100–240V AC, 50–60 Hz: не менее 2.

Требование к обслуживанию и гарантии:

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

Требования к системе централизованного сбора событий и построения отчетов:

Функциональные требования.

Совместимость с системами межсетевого экранирования, системами защиты электронной почты, системами защиты от целенаправленных атак, входящими в комплект поставки;

Обеспечение сбора и анализа событий журналов, создания отчётов на основе данных, получаемых с систем межсетевого экранирования;

Возможность построения сводных графических отчётов с анализируемых устройств;

Поддержка создания отчётов по сетевой активности, системным событиям, вирусам, атакам, web фильтрации;

Наличие встроенных шаблонов для быстрого создания наиболее востребованных отчётов;

Поддержка импорта и экспорта шаблонов отчётов;

Возможность просмотра логов в реальном времени;

Возможность поиска и фильтрации данных в логах;

Возможность создания оповещений при возникновении определённых событий в логах;

Возможность рассылки оповещений по электронной почте или передачи по протоколу Syslog;

Поддержка сервиса индикаторов компрометации, для ретроспективного выявления скомпрометированных узлов;

Реализация в виде виртуальной машины (поддерживаемые гипервизоры VMware vSphere, Xen, KVM, Hyper-V);

Производительность данных логов: не менее 5 Гб/день;

Доступный объём хранилища данных: не менее 3 ТБ;

Комплектация годовой расширенной технической поддержкой производителя в режиме 24x7;

Срок поддержки производителем: не менее 1 года.

Требования к лицензиям для обеспечения Zero Trust Network Access:

Функциональные требования.

Лицензии Zero Trust Network Access на 100 клиентов, должны соответствовать следующим требованиям:

- Система должна обеспечивать работу решения путем установки специализированного ПО на клиентские устройства.
- Система должна обеспечивать гранулярную проверку устройства перед предоставлением доступа к ресурсам:

- Проверка комплаенса: Доступ должен разрешаться только устройствам, удовлетворяющим заданные критерии.
- Идентификация корпоративных устройств: Обязательная проверка наличия устройства в домене AD и/или проверка уникального сертификата.
- Проверка по тегам (ZTNA Tags): Система должна автоматически присваивать теги устройствам на основе их состояния (например, тег Critical_Vulnerability или Non-Compliant) и немедленно терминировать активные сессии при изменении статуса устройства.

- Система должна поддерживать web фильтрацию трафика с возможностью ограничения доступа к определённым категориям сайтов.
- Система должна обеспечивать интеграцию с системой двухфакторной аутентификации в том числе с применением токенов с одноразовыми паролями временного действия.
- Система должна поддерживать сканер уязвимостей.
- Система должна обеспечивать мониторинг состояния конечных узлов в реальном времени.
- Система должна поддерживать удалённое развертывание, настройку и централизованное управление из единой консоли (графического интерфейса) администратора.
- Система должна иметь встроенный функционал или поддерживать интеграцию с внешними системами для передачи информации телеметрии, включающей информацию о пользователях, используемой модели и версии операционной системы, IP адрес, MAC адрес, информацию об обнаруженных уязвимостях при установке соответствующей дополнительной лицензии.
- Система должна иметь встроенный функционал или поддерживать интеграцию с внешними системами для оценки соответствия рабочих станций корпоративной политике безопасности.
- Возможность интеграции с системой централизованного сбора событий и передача информации обо всех зарегистрированных клиентах в данную систему.
- Система должна поддерживать интеграцию с внешней специализированной системой для защиты от целенаправленных и ранее не известных атак.
- Система централизованного управления должна иметь в комплекте поставки лицензию и обеспечивать поддержку централизованного управления до 100 клиентских устройств.
- Система должна быть масштабируемой и обеспечивать поддержку до 100 тысяч клиентских устройств методом лицензионного расширения.
- Поддержка управления на основе групп и интеграция с Microsoft Active Directory для централизованного развертывания клиентов на рабочих станциях в том числе с помощью GPO.
- Поддержка клиентских, серверных и мобильных операционных систем:

- Microsoft Windows 10/8.1/8/7 (32-bit, 64-bit), XP (32-bit);
- Windows Server 2008 R2/2012/2012 R2;

- Система должна поддерживать возможность устанавливать соединения виртуальных частных сетей (VPN) – SSL и IPSec, в том числе с применением двухфакторной аутентификации и сертификатов.
- Система должна поддерживать установление VPN подключения до Windows logon.
- Система должна поддерживать централизованное управление сертификатами.
- Система должна поддерживать возможность передачи информации об учетной записи текущего пользователя Active Directory для реализации прозрачной аутентификации пользователей.
- Система должна поддерживать возможность отслеживания сетевого взаимодействия с ботнет-сетями.
- Система должна поддерживать WAN оптимизацию для следующих протоколов: CIFS, FTP, HTTP, MAPI.
- Система должна обеспечивать просмотр включенных функций, ОС, имени узла, IP адреса и иной системной информации.
- Система должна отображать статус клиентского ПО для каждого узла.

- Система должна поддерживать распространение XML конфигурации.

Срок действия лицензии не менее 1-го года.

Подписал	Закирьянов Данияр Бактыбекович
Дата подписания	03.11.2026