ТЕХНИКАЛЫҚ СИПАТТАМА

1024760 сатып алу бойынша
Төмендету бойынша ашық тендер тәсілімен

Лот № 1 (10104-2 Т, 3744290) Бағдарламалық-аппараттық кешен

Тапсырыс беруші: АО "Казахтелеком"

Ұйымдастырушы: "Қазақтелеком" акционерлік қоғамының филиалы "Телеком Жинақтау" дирекциясы"

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	10104-2 Т
Атауы және қысқаша сипаттамасы	Бағдарламалық-аппараттық кешен, қызметтік ақпаратты жинау үшін
Қосымша сипаттама	Сипаттама: ДИТ_Закуп в рамках проекта ЦА "Организация ОЦИБ и услуг ИБ для B2B /B2G"
Саны	1.000
Өлшем бірлігі	Жиынтық
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., "Есіл" ауданы, г.Астана, район "Есиль", г.Астана, АТС-33, пр. Абая 26. (ДИТ)
Жеткізу шарттары	DDP
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 180 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 100%, Соңғы төлем - 0%

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

ТЕХНИКАЛЫҚ СПЕЦИФИКАЦИЯ

Потенциалды жеткізуші міндетті түрде техникалық спецификацияны ұсынуы қажет, ол төменде көрсетілген техникалық талаптарға, сондай-ақ төменде көрсетілген жабдық конфигурацияларына сәйкес келуге тиіс. Поставкаға жататын жабдықтың спецификациясы жабдық құрамына кіретін барлық комплектушілер мен төменде көрсетілген жабдық конфигурацияларында белгіленген барлық қызмет түрлерін қамтуы тиіс. Спецификацияны Конкурс құжаттамасына қосымша ретінде Кесте түрінде ұсынуға болады.

1. Закупка пәні.

Закупка пәні - кіруді қорғау жүйесіне арналған аппараттық-бағдарламалық кешен (әрі қарай - АПК).

2. Жеткізушіге қойылатын талаптар.

Жеткізуші келесі ақпаратты ұсынуы қажет:

2.1. Ақпараттық қауіпсіздік саласындағы жобаларды іске асыру тәжірибесі мен іске асырылған жобаларды растайтын құжат.

2.2. Ұсынылған шешімнің өндірушісінің сериктестік мәртебесінің болуы.

2.3. Әлеуетті өнім беруші шарт жасасу сәтінде Тапсырыс берушінің талаптарына сәйкес басып кіруден қорғау жөніндегі аппараттық-бағдарламалық кешенді орнату және баптау үшін Қазақстан Республикасының аумағында желілік технологиялар және кәсіби деңгейден төмен емес деңгейде жұмыс тәжірибесі 1 жыл болатын 2 білікті инженерді ұсынуы тиіс.

3. Кіруге қарсы қорғау бойынша АПК талаптары

3.1. Кіру қорғау жүйесін құру мақсаттары:

3.1.1. Кіру қорғау жүйесін құру мақсаты - хакерлік шабуылдарға, зиянды бағдарламаларға және басқа да кибер қауіптерге қарсы тұру арқылы пайдаланушылар мен ақпараттық жүйелерді қорғау. Желілік инфрақұрылымның, серверлердің, құрылғылардың және бағдарламалық қамтамасыз етудің қауіпсіздігін қамтамасыз ету. Операциялық қауіпсіздікті қамтамасыз ету.

3.2. Кіруге қарсы қорғаудың АПК құрамына мыналар кіреді:

3.2.1. Кіруді қорғау жүйесі келесі элементтерді қамтуы тиіс:

3.2.1.1. Жаңа буынды қауіпсіздік шлюзі, интеграцияланған функционал:

a) Межсетевые экранирования

b) Кіруден қорғау (IPS);

c) Ағынды антивирус (flow-based antivirus);

d) Қосымша деңгейдегі межсетевой экранирование (Application Control);

e) Желілік ресурстарға қолжетімділікті бақылау жүйесі (Webfilter);

3.3. Кіруге қарсы қорғау жүйесіне қойылатын талаптар:

3.3.1. Барлық компоненттер біртұтас экожүйе болу керек, хатар туралы мәліметтермен алмасып, құрылғыларды қосу мен интеграциялауға дайын коннекторлары болуы керек.

3.3.2. Жүйе тапсырыс берушінің басқару/бақылау жүйелерімен және оқиғаларды жинау мен есептер құру жүйелерімен үйлесімді болуы керек.

3.3.3. Жаңа буынды қауіпсіздік шлюзіне қойылатын талаптар:

a) Өнімділік (UDP пакеттері 1518 байт және 512 байт) кемінде 190 Gbps;
b) Өткізу қабілеті кемінде 195 Mpps;
c) Бір уақытта сессия саны: кемінде 7,5 млн;
d) Жаңа TCP байланыстарын орнату жылдамдығы: кемінде 630 000 секундта;
e) Application Control өткізу қабілеттілігі (HTTP 64K): кемінде 40 Gbps;
f) IPsec VPN өткізу қабілеттілігі: кемінде 50 Gbps;
g) IPS өткізу қабілеттілігі: кемінде 18 Gbps;
h) Threat Protection өткізу қабілеттілігі: кемінде 13 Gbps;
i) SSL VPN өткізу қабілеттілігі: кемінде 5 Gbps;
j) SSL Inspection өткізу қабілеттілігі: кемінде 10 Gbps;
k) SSL Inspection бір уақытта сессиялар саны (IPS, HTTPS): кемінде 580,000;
l) Бір уақытта SSL VPN пайдаланушылары саны: кемінде 10,000;
m) Поставляетін конфигурациядағы виртуалды қауіпсіздік контекстілерінің саны: кемінде 25;
n) Интерфейстер саны: кемінде 8x 10GE/5GE/2.5GE RJ45, 8x 25 GE SFP28/10 GE SFP+/GE SFP, 2x 100 GE QSFP28/40 GE QSFP+;
o) Аппараттық жеделдетумен жоғары қолжетімдік интерфейстер саны 2.5 GE/ GE HA: кемінде 1;
p) USB порттарының саны: кемінде 2;
q) Консоль порты: кемінде 1;
r) Басқару порттары 10GE/GE RJ-45: кемінде 1;
s) AC қуат көзі 100–240V, 50–60 Гц: кемінде 2 блок қуаттау;

3.3.4. Межсетевое экранирование функционалдық талаптары:

a) лицензиялауды шектеусіз пайдаланушылар үшін жүзеге асыру;
b) Подсистема өндірушінің серверінен қауіпсіздік модульдері мен өзекті қауіптер тізімінің қолжетімділігін тұрақты түрде жаңартып отыруы тиіс;
c) Подсистема 4 құрылғыдан тұратын кластерлерді құру мүмкіндігін қамтамасыз етуі керек;

· Суық резервпен (active/passive);

· Ыстық резервпен (active/active);

· Теңгерім кластері;
d) Подсистема межсетевое экранирование функционалдылығын қолдауы тиіс;
e) Подсистема жүктемені теңестіру функционалдылығын қолдауы тиіс;
f) Подсистема трафиктің өткізу қабілетін басқару функционалдылығын қолдауы тиіс;
g) Подсистема SSL трафигін инспекциялау мүмкіндігін және ICAP (Internet Content Adaptation Protocol) протоколы бойынша инспекцияланған трафикті сыртқы жүйелерге

жіберу мүмкіндігін қамтамасыз етуі тиіс;
h) Подсистема ZTNA (Zero Trust Network Access) шлюзінің іске асырылуын қамтамасыз етуі тиіс;
i) Подсистема SSH трафигінің анализі (SSH инспекция) мүмкіндігін қамтамасыз етуі тиіс;
j) Подсистема IPv4, IPv6 динамикалық маршрутизациясына ие болуы тиіс;
k) Подсистема WCCP протоколымен жұмыс істеу мүмкіндігін қамтамасыз етуі тиіс;
l) Подсистема аппараттық жеделдетумен антивирустық қорғауды қамтамасыз етуі тиіс;
m) Подсистема спамнан қорғауды (антиспам) қамтамасыз етуі тиіс;
n) Подсистема IPS аппараттық жеделдетуімен кіруден қорғау функционалын қолдауы тиіс;
o) Подсистема сайттарды веб-фильтрациялау, кейбір сайттарға қолжетімділікті шектеу мүмкіндігін қамтамасыз етуі тиіс;
p) Веб-фильтрация 85 категориядан кем емес болуы тиіс;
q) Подсистема веб-прокси функциясымен қолдау көрсетуі тиіс;
r) Подсистема кем дегенде 10 виртуалды домендерді (бір құрылғы ішінде толық функционалды виртуалды МСЭ) қолдау көрсетуі тиіс;
s) Подсистема HTTP, SMTP, POP3, IMAP, FTP және IM трафигінің ішінде вирус тексеру мүмкіндігін қамтамасыз етуі тиіс;
t) Подсистема антивирустық базалардың автоматты түрде кесте бойынша жаңартылу мүмкіндігін қамтамасыз етуі тиіс;
u) Подсистема жұқтырылған хабарламаларды карантинге орналастыру мүмкіндігін қамтамасыз етуі тиіс;
v) Подсистема файлдарды көлемі бойынша шектеу мүмкіндігін қамтамасыз етуі тиіс;
w) Подсистема файлдарды түрі бойынша шектеу мүмкіндігін қамтамасыз етуі тиіс;
x) Подсистема бірнеше WAN желілерімен жұмыс істеуді қолдауы тиіс;
y) Подсистема PPPoE және L2TP протоколдарын қолдауы тиіс;
z) Подсистема DHCP протоколын "Клиент/Сервер" конфигурациясында қолдауы тиіс;
aa) Подсистема саясаттан негізделген маршрутизацияны қолдауы тиіс;
bb) Подсистема RIP v1 және v2, OSPF, BGP протоколдары негізінде динамикалық маршрутизацияны қолдауы тиіс;
cc) Подсистема қауіпсіздік зоналарын қолдануды қолдауы тиіс;
dd) Подсистема зоналар арасындағы маршрутизацияны қолдауы тиіс;
ee) Подсистема виртуалды желілер арасындағы маршрутизацияны қолдауы тиіс;
ff) Подсистема әкімшілеудің рөлдік негізін қолдауы тиіс;
gg) Подсистема бірнеше әкімші мен пайдаланушы деңгейлерін поддерживает;
hh) Подсистема TFTP протоколы және веб-интерфейс арқылы бағдарламалық қамтамасыз етуді жаңартуды қолдауы тиіс;
ii) Подсистема енгізілген бағдарламалық қамтамасыз етуді алдыңғы күйге (нұсқаға) қайтару мүмкіндігін қолдауы тиіс;
jj) Подсистема пайдаланушыларды аутентификациялауды ішкі деректер базасы арқылы қолдауы тиіс;
kk) Подсистема Kerberos аутентификациясын қолдауы тиіс;
ll) Подсистема Windows Active Directory сыртқы деректер базасы арқылы пайдаланушыларды аутентификациялау мүмкіндігін қолдауы тиіс;
mm) Подсистема IP/MAC-адресі бойынша байланыстыру негізіндегі аутентификацияны қолдауы тиіс;

nn) Подсистема пайдаланушы топтары негізіндегі аутентификацияны қолдауы тиіс;
oo) Подсистема NAT, PAT, "прозрачный" (көпір) функцияларын қолдауы тиіс;
pp) Подсистема саяси NAT функцияларын қолдауы тиіс;
qq) Подсистема VLAN Tagging (802.1Q) функцияларын қолдауы тиіс;
rr) Подсистема SIP/H.323 NAT Traversal функцияларын қолдауы тиіс;
ss) Подсистема қауіпсіздік саясаттарын конфигурациялау мүмкіндігін қолдауы тиіс;
tt) Подсистема URL/кілт сөз/дәл/фраза бойынша блоктау мүмкіндігін қамтамасыз етуі тиіс;
uu) Подсистема URL бойынша "Ақ" тізімді қолдауы тиіс;
vv) Подсистема Java апплеттерін, Cookies, ActiveX элементтерін блоктау мүмкіндігін қамтамасыз етуі тиіс;
ww) Подсистема шабуылдардың сигнатураларын конфигурациялау мүмкіндігін қамтамасыз етуі тиіс;
xx) Подсистема шабуылдар мен IPS сигнатураларының базасын автоматты түрде жаңартуды қамтамасыз етуі тиіс;
yy) Подсистема өндірушінің серверінен "қара" тізімді спамшылар мен ашық рельс IP-адрестерінен алуы тиіс;
zz) Подсистема MIME заголовковын тексеру мүмкіндігін қолдауы тиіс;
aaa) Подсистема электрондық поштада кілт сөздер мен фразалар бойынша фильтрация жүргізу мүмкіндігін қамтамасыз етуі тиіс;
bbb) Подсистема "қара" және "ақ" IP-адрес тізімдері бойынша фильтрация жүргізу мүмкіндігін қамтамасыз етуі тиіс;
ccc) Подсистема логтарды алысты syslog серверіне жіберу мүмкіндігін қамтамасыз етуі тиіс;
ddd) Подсистема Microsoft Office және PDF форматтарының файлдарынан атқарушы бөлшекті қамтамасыз ету үшін жұқпалы элементтерді алып, файлдың бастапқы форматында сақтауы тиіс;
eee) Подсистема желілік трафик, жүйе жағдайы және табылған қауіптерді бақылау үшін графикалық құралдармен қамтамасыз етуі тиіс;
fff) Подсистема вирустар мен желілік шабуылдар жөнінде электрондық хаттар жіберу мүмкіндігін қамтамасыз етуі тиіс;
ggg) Подсистема "0-day" сыныбындағы белгісіз қауіптерді анықтау үшін cloud sandbox талдауына файлдар мен URL-дерді жіберу мүмкіндігін қамтамасыз етуі тиіс;
hhh) Подсистема cloud sandbox-тық талдауға кемінде 10 000 объектіні (файлдар мен URL) күніне (24 сағат) қолдау көрсетуі тиіс;
iii) Подсистема VRRP протоколына қолдау көрсетуі тиіс;
jjj) Подсистема үшінші тараптың SIEM жүйесімен интеграциялану мүмкіндігін қолдауы тиіс;
kkk) Подсистема қызметтердің жылдамдығын белгілеуді, максималды немесе басым өткізу қабілеттілігін қамтамасыз етуі тиіс;
lll) Подсистема жедел хабар алмасу қызметтерін пайдалану мен бақылау функцияларын қамтамасыз етуі тиіс;
mmm) Подсистема веб-контенттің жедел қолжетімділігі мен таратылуын жақсарту мүмкіндігін қолдауы тиіс;
nnn) Подсистема веб-интерфейс арқылы басқару мүмкіндігін қамтамасыз етуі тиіс;
ooo) Подсистема орталықтандырылған басқару мен есептер құру жүйелерімен интеграциялану мүмкіндігін қолдауы тиіс;

ppp) Подсистема NetFlow, sFlow протоколдарын қолдауы тиіс;
qqq) Подсистема кері прокси-сервер режимін қамтамасыз етуі тиіс;
rrr) Подсистема "прозрачный" прокси-сервер режимін қамтамасыз етуі тиіс;
sss) Подсистема команда жолымен қауіпсіздік саясатын басқаруды қамтамасыз етуі тиіс;
ttt) Подсистема телеметрия ақпаратын, пайдаланушылар, моделі мен операциялық жүйенің версиясы, IP адресі, MAC адресі, табылған осалдықтар туралы ақпаратты сыртқы жүйелермен интеграциялану мүмкіндігін қамтамасыз етуі тиіс;
uuu) Подсистема корпоративтік қауіпсіздік саясатына сай жұмыс станцияларын тексеру үшін құжаттарды интеграциялауды қамтамасыз етуі тиіс. Саясатқа сәйкес келмеген жағдайда тексерілген хост карантинге орналастырылуы тиіс, желілік қатынау шектеледі;
vvv) Қауіпсіздік шлюзі кемінде 12 айлық жазылыммен келесі қызметтерді қамтуы тиіс:

· Қосымшаларды бақылау

· IPS

· Антивирус

· Веб-фильтрация

· Спамнан қорғау (Antispam)

· Облачная песочница

4. Жалпы техникалық қолдау мен жабдықты жөндеу талаптары

4.1. АПК ұсынысы 24/7 техникалық қолдауды және бағдарламалық қамтамасыз ету мен сигнатураларды кемінде бір жыл бойы жаңарту мен кепілдікті қамтуы тиіс.
4.2. Гарантия мерзімі жабдықты қабылдау актісін ресімдеген сәттен бастап басталады және бір жылға созылады.
4.3. Жеткізуші АО «Казахтелеком» ұйымына жабдықты пайдалану мерзімі ішінде техникалық қолдау көрсету қызметтерін жеке сервис контрактан ұсынуы тиіс.
4.4. Техникалық қолдау жабдықты жеткізуді және жөндеуді, бағдарламалық қамтамасыз етуді (қателерді жою, бағдарламалық қамтамасыз етудің жаңа нұсқаларын жүктеу және т.б.) қоса алғанда, апаттарды жоюды қамтуы тиіс.
4.5. Гарантия мерзімі ішіндегі техникалық қолдау қызметтері олардың деңгейі бойынша жіктеледі.

4.5.1. Трафиктің толық немесе і ج ұпайызды жоғалуы (БІРІНШІ ДӘРЕЖЕ ПРОБЛЕМАСЫ);
4.5.2. Трафиктің жоғалуы қаупі (ЕКІНШІ ДӘРЕЖЕ ПРОБЛЕМАСЫ);
4.5.3. Трафикке әсер етпейтін проблемалар (ҮШІНШІ ДӘРЕЖЕ ПРОБЛЕМАСЫ).

4.5.4. Проблемаларды жоюға арналған нормативтік уақыт:

· Бірінші дәрежелі проблема - 4 сағат;

· Екінші дәрежелі проблема - 48 сағат;

· Үшінші дәрежелі проблема - 1 ай.

4.5.5. Гарантия кезеңінде Бірінші дәрежелі проблемаларды шешу бойынша қызмет көрсету уақытын бұзу жағдайында, Компания Заказшыға жабдық құнының 0,05% мөлшерінде зиян өндіріп, жабдықтың құнының 10% - дан аспайтын сомаға өндіруге міндетті.
4.5.6. Ақаулықтар жойылғаннан кейін, қызмет көрсетуші жабдықты 45 күн ішінде жөндеуге жіберуі тиіс (гарантия кезеңінде). Егер жабдық осы мерзімде қайтарылмаса, күнделікті 0,1% (бір оннан бір) көлемінде айыппұл мөлшеріндегі санкциялар қолданылатын болады.

5. Жұмыстық құжаттаманы әзірлеу, монтаж жасау және іске қосу қызметтеріне қойылатын талаптар.

5.1. Көрсетілетін қызметтер мыналарды қамтуы тиіс:

· Жабдық орнату орындары бойынша талаптарды әзірлеу, байланыс жолдары және маршруттаушы жабдық конфигурациясы;

· Тапсырыс беруші объектілерінің тексеруі (Site Survey);

· Жұмыстық құжаттаманы әзірлеу;

· Жүйенің жұмыс қабілеттілігі мен функционалдылығын тестілеу бағдар бағдарламасын және әдістемесін әзірлеу;

· Жабдықтың орнатудан өтуі;

· АО «Казахтелеком» өндірістік алаңында жабдық консольдарына конфигурировать және баптау;

· Конфигурацияланған шаблондарды орнату және конфигурацияланған комплекттерді орнында тестілеу;

· Жүйенің кешенді конфигурациясы және АО «Казахтелеком» жөніндегі маршруттаушы жабдықпен интеграциялау;

· Қабылдау сынақтарын өткізу.

6. Құжаттамаларға қойылатын талаптар

6.1. Жалпы талаптар:
6.1.1. Барлық құжаттар орыс тілінде болуы тиіс.
6.1.2. Құжаттама қағаз және электронды түрде ұсынылуы тиіс.

6.2. Пайдалану құжаттамасының құрамына:

· Әкімшілер үшін жүйені пайдалану жөніндегі нұсқаулық.

6.3. Объектте жұмысшы құжаттама жинағына:

· Байланыс ұйымының сызбасы;

· Жабдықты бөлмеде орналастыру сызбасы;

· Телекоммуникациялық шкафтарда жабдықты орналастыру жоспары;

· Жабдықты электрмен жабдықтауға қосылу сызбасы немесе кестесі;

· Жабдық, кабель өнімдері мен материалдардың спецификациясы;

· Жүйе құрамындағы компоненттердің сипаттамасы мен функционалдық мүмкіндіктері;

· Жүйедегі IP адресацияның сипаттамасы;

· Жүйедегі маршрутизацияны ұйымдастыру сипаттамасы;

· Жабдықта типтік қызметтерді баптау сипаттамасы;

· Жүйемен интеграциялау және тарихтық схемалар;

· Жалпы жүйе топологиясы;

· Жүйе объектілерінің құрылымдық схемалары;

· Жүйе объектілеріндегі жабдықтардың байланысу схемалары мен кестелері;

· Жүйе объектілеріндегі жабдықтың қуат тұтыну кестелері;

· Жүйе жабдығының фасадтары;

· Жүйе тораптарындағы жабдықтың стелаждары;

6.4. Жұмысшы жүйенің жұмыс қабілеті мен функционалдылығын тестілеу бағдарламасы мен әдістемесі:

· Тестілеуге жататын объектілердің тізімі;

· Жүйе мен оның бөліктерін қабылдау критерийлері;

· Сынақтарды өткізу ережелері мен шарттары;

· Сынақтарды материалдық-техникалық сипаттамасы;

· Тестілеуге өтетін барлық тест науқандарының (тексерулерінің) тізімі;

· Тестілеу және нәтиже өңдеу әдістемелері.

7. Жабдықты монтаждау, іске қосу, конфигурациялау, тестілеу және жүйенің кешенді конфигурациясы

7.1. Жабдық монтаждау, іске қосу, конфигурациялау және жүйенің тестілеу қызметтері жеткізуші тарапынан сатып алушы объектілерінде көрсетіледі. Осы кезде байланыс арналарын, электрмен жабдықтауды, жерлеуді және сатып алушы жабдығымен интеграциялау үшін қажетті мамандар тартылады.
7.2. Сатып алушы объектілерінде қызмет көрсету процесі мыналарды қамтиды:

· Жабдықты пакетін ашу, дайындау және монтаждау;

· Жабдықты ішкі шкаф шегінде қосып, электрмен жабдықтау жүйесіне және, мүмкін, ішкі кросс жабдығына қосу;

· Объектілер электрмен жабдықтау және жерлеу жүйесіне қосылу (сатып алушының жауапкершілігі бар персоналмен);

· Байланыс арналарымен қосылу (сатып алушының жауапкершілігі бар персоналмен);

· Жабдыққа қажетті конфигурациялау;

· Жабдықтың технологиялық нұсқаулықтарына сәйкес жұмыс қабілеттілігін тестілеу;

7.3. Жабдық орнату және тестілеу аяқталғаннан кейін, жүйенің кешенді конфигурациясы мен АО «Казахтелеком» маршруттаушы жабдықпен интеграциясы жүргізіледі.

8. Қабылдау-тапсыру сынақтары

8.1. Жабдықты монтаждау және бағдарламалық қамтамасыз етуді барлық орнату орындарында, жабдықты тестілеу мен жүйенің кешенді конфигурациясы аяқталғаннан кейін, жүйенің кешенді қабылдау-тапсыру сынақтары өткізіледі, олар Жүйенің жұмыс істейтіндігін растауы тиіс.
8.2. Қабылдау-тапсыру сынақтары жеткізуші тарапынан әзірленген Жұмыс бағдарламасы мен жүйенің қызмет қабілетін тестілеу әдістемесі бойынша тапсырыс берушінің өкілдерімен бірге өткізіледі.

ТЕХНИКАЛЫҚ ЖАБДЫҚТАРДЫҢ КОНФИГУРАЦИЯСЫ

Жабдықтар мен монтаждау және іске қосу қызметтері желілік қауіпсіздік қызметтерін ұсыну үшін.

Межсетевые экраны: Жаңа буынды қауіпсіздік шлюзі, интерфейстің саны кемінде 8 x 10GE /5GE/2.5GE RJ45, 8 x 25 GE SFP28/10 GE SFP+/GE SFP, 2 x 100 GE QSFP28/40 GE QSFP+ жабдықтарын, деректерді жіберу желісіне және осы шешім аясында ұсынылатын басқа жабдықтарға қосу үшін қажетті оптикалық трансиверлермен. Саны - 2 дан.

1. Жеткізуші барлық қажетті монтаж материалдарын қамтамасыз етуі тиіс.

2. Жеткізуші айтылған жоба шеңберінде сатып алушының кемінде 10 (он) инженері үшін оқыту өткізуі тиіс.

3. Жеткізуші жабдықты монтаждау мен пуско-наладка бойынша қызметтерді ұсынуы тиіс.

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	Кожакапанов Айхан Нурланханулы
Қол қойылған күні	29.08.2024

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1024760
способом Открытый тендер на понижение

Лот № 1 (10104-2 Т, 3744290) Комплекс программно-аппаратный

Заказчик: Акционерное общество "Казахтелеком"

Организатор: "Дирекция "Телеком Комплект" - филиал Акционерного общества "Казахтелеком"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	10104-2 Т
Наименование и краткая характеристика	Комплекс программно-аппаратный, для сбора служебной информации
Дополнительная характеристика	Описание: ДИТ_Закуп в рамках проекта ЦА "Организация ОЦИБ и услуг ИБ для B2B /B2G"
Количество	1.000
Единица измерения	Комплект
Место поставки	КАЗАХСТАН, г.Астана, район "Есиль", г.Астана, район "Есиль", г.Астана, АТС-33, пр. Абая 26. (ДИТ)
Условия поставки	DDP
Срок поставки	С даты подписания договора в течение 180 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 100%, Окончательный платеж - 0%

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

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ.

Потенциальный поставщик в обязательном порядке должен предоставить Техническую спецификацию, которая должна соответствовать нижеприведенным техническим требованиям, предъявляемым к оборудованию, услугам и составу, указанному в нижеприведенных конфигурациях оборудования. Спецификация на поставляемое оборудование должна включать все комплектующие, входящие в состав оборудования и весь перечень оказываемых услуг, указанных в конфигурациях оборудования. Спецификация может быть представлена в виде Таблицы Приложения к Конкурсной документации.

1. Предмет закупки.

Предметом закупки является аппаратно-программный комплекс (далее - АПК) по защите сетевой инфраструктуры от вторжений.

2. Требования к Поставщику.

Поставщик должен предоставить следующую информацию:

2.1. Опыт реализации проектов в сфере обеспечения информационной безопасности с подтверждением реализации.

2.2. Наличие партнерского статуса от производителя/-ей предлагаемого решения

2.3. Потенциальный поставщик в момент заключения Договора должен предоставить 2х квалифицированных инженеров с опытом работы 1 год в области сетевых технологий и уровня не ниже Professional на территории Республики Казахстан для установки и настройки аппаратно-программный комплекса по защите от вторжений в соответствии с требованиями Заказчика.

3. Требования АПК по защите сетевой инфраструктуры от вторжений

3.1. Цели создания системы защиты от вторжений

3.1.1. Целью создания системы защиты от вторжения, является - защита от хакерских атак, вредоносных программ и других киберугроз, которые могут нанести вред пользователям и информационным системам. Обеспечение безопасности сетевой инфраструктуры, серверов, устройств и программного обеспечения. Обеспечение операционной безопасности.

3.2. Состав АПК по защите от вторжений

3.2.1. АПК по защите от вторжений должен включать в себя следующие элементы:

3.2.1.1. Шлюз безопасности нового поколения со встроенным функционалом

a) Межсетевое экранирование

b) Предотвращения вторжений (IPS);

c) Потоковый антивирус (flow-based antivirus);

d) Система межсетевого экранирования на уровне приложений (Application Control);

e) Система контроля доступа к сетевым ресурсам (Webfilter);

3.3. Требования к Системе защиты от вторжений

3.3.1. Все компоненты Системы должны представлять из себя единую экосистему, которая обменивается данными об угрозах и имеет готовые коннектора для подключения и интеграции устройств.

3.3.2. Система должна быть совместима с существующими у Заказчика системами управления/мониторинга и системами сбора событий и построения отчетов.

3.3.3. Требования к шлюзу безопасности нового поколения:

a) Производительность (UDP пакеты размером как 1518 байт, так и 512 байт) не менее 190 Gbps;

b) Пропускная способность не менее 195 Mpps;

c) Одновременное количество сессий: не менее 7.5 млн;

d) Скорость установки новых TCP соединений: не менее 630 000 в сек;

e) Application Control Throughput (HTTP 64K): не менее 40 Gbps;

f) IPsec VPN Throughput: не менее 50 Gbps;

g) IPS Throughput: не менее 18 Gbps;

h) Threat Protection Throughput: не менее 13 Gbps;

i) SSL VPN Throughput: не менее 5 Gbps;

j) SSL Inspection Throughput: не менее 10 Gbps;

k) SSL Inspection Concurrent Session (IPS, HTTPS): не менее 580000;

l) Количество одновременных SSL VPN пользователей: не менее 10 000;

m) Количество виртуальных контекстов безопасности в поставляемой комплектации: не менее 25;

n) Количество интерфейсов: не менее 8x 10GE/5GE/2.5GE RJ45, 8x 25 GE SFP28/10 GE SFP+/GE SFP, 2x 100 GE QSFP28/40 GE QSFP+.

o) Количество интерфейсов высокой доступности с аппаратным ускорением 2.5 GE/ GE HA: не менее 1;

p) Количество USB портов: не менее 2;

q) Консольный порт: не менее 1;

r) Порты управления 10GE/GE RJ-45: не менее 1;

s) Питание от сети переменного тока 100–240V AC, 50–60 Hz: не менее 2 блоков питания в комплекте;

3.3.4. Функциональные требования к межсетевому экранированию:

a) лицензирование должно осуществляться для неограниченного количества пользователей;

b) подсистема должна регулярно получать обновления сигнатур модулей безопасности и перечень актуальных угроз с сервера производителя;

c) подсистема 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;

a) подсистема должна иметь функциональность межсетевого экранирования, то есть обеспечивать возможность создания правил фильтрации сетевого трафика на основе IP адресов, портов и приложений;

b) подсистема должна иметь функциональность балансировки нагрузки;

c) подсистема должна иметь функциональность управления полосой пропускания трафика (traffic shaping);

d) подсистема должна обеспечивать инспекцию SSL трафика с возможностями анализа и передачи проинспектированного трафика во внешние системы по протоколу ICAP (Internet Content Adaptation Protocol);

e) подсистема должна обеспечивать возможность реализации шлюза ZTNA (Zero Trust Network Access);

f) подсистема должна обеспечивать анализ SSH трафика (ssh inspection);

g) подсистема должна обеспечивать динамическую маршрутизацию IPv4, IPv6;

h) подсистема должна иметь возможность работы по протоколу WCCP (как в режиме сервера, так и в режиме клиента);

i) подсистема должна обеспечивать антивирусную защиту с аппаратным ускорением;

j) подсистема должна обеспечивать защиту от спама (антиспам);

k) подсистема должна иметь функциональность предотвращения вторжения IPS с аппаратным ускорением;

l) подсистема должна обеспечивать WEB фильтрацию трафика с возможностью ограничения доступа к определенным категориям сайтов;

m) должна обеспечиваться WEB фильтрация трафика по не менее 85 категориям;

n) подсистема должна иметь функциональность WEB proxy;

o) подсистема должна обеспечивать наличие не менее 10 виртуальных доменов (полнофункциональных виртуальных МСЭ внутри одного устройства), доступных по умолчанию;

p) подсистема должна иметь возможность проверки на наличие вирусов внутри HTTP, SMTP, POP3, IMAP, FTP и IM трафика;

q) подсистема должна иметь возможность автоматически по расписанию получать обновления антивирусных баз;

r) подсистема должна иметь возможность помещать инфицированные сообщения в карантин;

s) подсистема должна иметь возможность блокировки передачи файлов в зависимости от размера;

t) подсистема должна иметь возможность блокировки передачи файлов в зависимости от типа;

u) подсистема должна поддерживать соединения множества WAN сетей;

v) подсистема должна поддерживать протокол PPPoE и L2TP;

w) подсистема должна поддерживать DHCP протокол в конфигурации “Клиент /Сервер”;

x) подсистема должна поддерживать маршрутизацию на основе политик;

y) подсистема должна поддерживать динамическую маршрутизацию на основе протоколов RIP v1 и v2, OSPF, BGP;

z) подсистема должна поддерживать использование зон безопасности;

aa) подсистема должна поддерживать маршрутизацию между зонами;

bb) подсистема должна поддерживать маршрутизацию между виртуальными сетями;

cc) подсистема должна поддерживать администрирование на основе ролей;

dd) подсистема должна поддерживать несколько уровней администраторов и пользователей;

ee) подсистема должна поддерживать обновление встроенного ПО через протокол TFTP и web-интерфейс;

ff) подсистема должна поддерживать возможность возврата к предыдущему состоянию (версии) встроенного ПО;

gg) подсистема должна поддерживать аутентификацию пользователей посредством внутренней базы данных;

hh) подсистема должна поддерживать Kerberos аутентификацию пользователей;

ii) подсистема 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;

jj) подсистема должна поддерживать аутентификацию пользователей посредством внешней базы данных RADIUS/LDAP;

kk) подсистема должна поддерживать аутентификацию пользователей через привязку по IP/MAC-адресу;

ll) подсистема должна поддерживать аутентификацию на основе групп пользователей;

mm) подсистема должна поддерживать функции NAT, PAT, «прозрачный» (мост);

nn) подсистема должна поддерживать функции NAT на основе политик;

oo) подсистема должна поддерживать функции VLAN Tagging (802.1Q);

pp) подсистема должна поддерживать функции SIP/H.323 NAT Traversal;

qq) подсистема должна поддерживать настройку профилей безопасности;

rr) подсистема должна иметь возможность блокировки по URL/ключевому слову /фразе;

ss) подсистема должна поддерживать «Белые» списки URL;

tt) подсистема должна иметь возможность блокировки аплетов Java, Cookies, элементов управления ActiveX;

uu) подсистема должна иметь возможность настройки списка сигнатур атак;

vv) подсистема должна поддерживать автоматическое обновление базы атак и сигнатур IPS;

ww) подсистема должна регулярно получать с сервера производителя «черный» список IP адресов спамеров и открытых релеев;

xx) подсистема должна поддерживать проверку заголовков MIME;

yy) подсистема должна поддерживать фильтрацию электронной почты, по ключевым словам, и фразам;

zz) подсистема должна поддерживать фильтрацию по «черным/белым» спискам IP-адресов;

aaa) подсистема должна иметь возможность отсылки логов на удаленный syslog сервер;

bbb) подсистема должна поддерживать сервис извлечения исполняемой составляющей из файлов форматов Microsoft Office и PDF, сохраняя исходный формат файла;

ccc) подсистема должна иметь графические средства для мониторинга сетевого трафика, состояния системы и обнаруженных угрозах;

ddd) подсистема должна иметь возможность отправки уведомлений по электронной почте о вирусах и сетевых атаках;

eee) подсистема должна поддерживать отправку файлов и URL на анализ в cloud sandbox для обнаружения неизвестных угроз класса “0-day”;

fff) подсистема должна иметь лицензирование в комплекте поставки для анализа в cloud sandbox не менее 10 000 объектов (файлов и URL) в день (24 часа);

ggg) подсистема должна поддерживать протокол VRRP;

hhh) подсистема должна поддерживать интеграцию с SIEM стороннего производства;

iii) подсистема должна иметь возможность установления гарантированной, максимальной или приоритетной пропускной способности;

jjj) подсистема должна поддерживать обнаружение и контроль использования служб мгновенных сообщений;

kkk) подсистема должна поддерживать возможность локального хранения Web контента для оптимизации полосы пропускания и скорости доступа к Web ресурсам;

lll) подсистема должна поддерживать управление через Web интерфейс;

mmm) подсистема должна иметь возможность интеграции с системами централизованного управления и построения отчетов;

nnn) подсистема должна поддерживать протоколы NetFlow, sFlow;

ooo) подсистема должна обеспечивать режим обратного прокси-сервера (reverse proxy);

ppp) подсистема должна обеспечивать режим прозрачного прокси-сервера (transparent proxy);

qqq) подсистема должна обеспечивать возможность управления политиками безопасности в консольном режиме из командной строки;

rrr) подсистема 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;

sss) подсистема 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;

ttt) Шлюз безопасности должен иметь в комплекте подписки на следующие сервисы сроком на 12 месяцев:

- Контроль приложений
- IPS
- Антивирус
- Web фильтрация
- Защита от спама Antispam
- Облачная песочница

3. ПУНКТ 4 Общие требования по технической поддержке и ремонту оборудования

3.3. Предложение для АПК должно включать 24x7 техническую поддержку и гарантию, программное обеспечение и обновление сигнатур минимум на один год.

3.4. Гарантийный период начинается с момента подписания Акта окончательной приемки оборудования и составляет один год.

3.5. Поставщик должен предоставлять АО «Казахтелеком» услуги по технической поддержке на весь период эксплуатации оборудования, которые будут предоставляться по отдельному сервисному контракту.

3.6. Техническая поддержка должна включать в себя поставку и ремонт оборудования, сопровождение программного обеспечения (устранение ошибок, загрузка новых версий ПО и др.), устранение аварий.

3.7. Услуги по технической поддержке в гарантийный период классифицированы в зависимости от их степени.

4.9.1. Полная или частичная потеря трафика (ПРОБЛЕМА ПЕРВОЙ СТЕПЕНИ);

4.9.2. Опасность потери трафика (ПРОБЛЕМА ВТОРОЙ СТЕПЕНИ);

4.9.3. Проблемы, не влияющие на трафик (ПРОБЛЕМА ТРЕТЬЕЙ СТЕПЕНИ).

4.9.4. Нормативное время на устранение проблем:

- Проблема первой степени – 4 часа;
- Проблема второй степени – 48 часов;
- Проблема третьей степени – 1 месяц.

4.9.5. В случае нарушения нормативного времени оказания услуг по технической поддержке в гарантийный период по устранению проблем ПЕРВОЙ СТЕПЕНИ, Фирма возмещает Заказчику убытки, равные 0,05% в день от стоимости поставляемого оборудования, но не более 10% стоимости данного оборудования.

4.9.6. Неисправное оборудование должно быть восстановлено и возвращено фирмой производителя в течение 45 дней со дня отправки на ремонт (в гарантийный период). Если оборудование не будет возвращено в течение этого срока, будут применены штрафные санкции в размере 0,1 % (одна десятая) от стоимости оборудования за каждый день просрочки.

5. Требования к услугам по разработке рабочей документации, монтажу и пусконаладке.

5.9. Оказываемые услуги должны включать в себя:

- разработку требований к местам установки оборудования, линиям связи и конфигурации маршрутизирующего оборудования;
- обследование объектов Покупателя (Site Survey);

- разработку рабочей документации;
- разработку программы и методики тестирования работоспособности и функциональности системы;
- приемку мест установки под монтаж оборудования;
- наладку и конфигурирование комплектов оборудования на производственных площадях АО «Казахтелеком»;
- установку и пусконаладку предконфигурированных комплектов и тестирование оборудования на местах установки;
- комплексную настройку системы и интеграцию с существующим маршрутизирующим оборудованием АО «Казахтелеком»;
- проведение приемочных испытаний.

6. Требования к документации

6.9. Общие требования

6.9.1. Вся документация должна быть на русском языке.

6.9.2. Документация должна быть представлена в бумажном и электронном видах.

6.10. Состав эксплуатационной документации:

- Инструкция по эксплуатации системы для администраторов.

6.11. Рабочая документация на объект, в составе:

- Схема организации связи;
- Схема размещения оборудования в помещении;
- План размещения оборудования в телекоммуникационных шкафах;
- Схема или таблица подключения оборудования к электропитанию;
- Спецификация оборудования, кабельных изделий и материалов;
- Описание состава компонент системы и их функциональных возможностей;
- Описание IP адресации в системе;

- Описание организации маршрутизации на сети;
- Описание настроек типовых сервисов на оборудовании;
- Описание и схемы интеграции существующей сети с системой;
- Общая топологическая схема системы;
- Структурные схемы объектов системы;
- Схемы и таблицы соединений оборудования на объектах системы;
- Таблицы потребления мощности оборудованием на объектах системы;
- Фасады оборудования системы;
- Фасады стоек с оборудованием на узлах системы;

6.12. Состав программы и методики тестирования работоспособности и функциональности системы

- перечень объектов, подлежащих испытаниям;
- критерии приемки системы и ее частей;
- условия и порядок проведения испытаний;
- материально-техническое обеспечение испытаний;
- перечень тестов (проверок), по которым проводятся испытания;
- методики проведения испытаний и обработки их результатов;

7. Монтаж, запуск, наладка, тестирование оборудования и комплексная настройка системы

7.9. Услуги по монтажу, запуску, наладке и тестированию системы оказываются Поставщиком на объектах Покупателя. При этом для оказания услуг по подключению к каналам связи, электропитанию, заземлению и интеграции с прочим оборудованием Покупателя привлекаются соответствующие специалисты Покупателя.

7.10. Процесс оказания услуг на объектах Покупателя включает:

- распаковку, подготовку и монтаж оборудования;

- выполнение всех внутри-шкафных соединений оборудования с подключением его к системам распределения электропитания и, возможно, к внутреннему кроссовому оборудованию;

- подключение к объектовым системам электропитания и заземления (с привлечением ответственного персонала Покупателя);

- подключение к каналам связи (с привлечением ответственного персонала Покупателя);

- необходимое конфигурирование оборудования;

- тестирование работоспособности оборудования в соответствии с технологическими инструкциями Поставщика.

7.11. По завершении настройки и тестирования оборудования в местах установки, производится комплексная настройка системы и интеграция с существующим маршрутизирующим оборудованием АО «Казахтелеком».

8. Приемо-сдаточные испытания

8.9. После завершения монтажа Оборудования и установки Программного обеспечения на всех Местах установки, тестирования оборудования и комплексной настройки системы проводятся приёмо-сдаточные испытания Системы в комплексе, которые должны подтвердить, что Система работоспособна и функционирует в полном соответствии с Техническими требованиями.

8.10. Приёмо-сдаточные испытания проводятся Поставщиком согласно разработанной Поставщиком Программе и методике тестирования работоспособности и функциональности системы с участием представителей Покупателя.

ТЕХНИЧЕСКАЯ КОНФИГУРАЦИЯ ОБОРУДОВАНИЯ

Оборудование и услуги по монтажу и пуско-наладке для систем предоставления услуг сетевой безопасности

Межсетевые экраны в составе: Шлюз безопасности нового поколения с интерфейсами не менее 8 10GE/5GE/2.5GE RJ45, 8 25 GE SFP28/10 GE SFP+/GE SFP, 2 100 GE QSFP28/40 GE QSFP+ в комплекте с оптическими трансиверами необходимыми для подключения к сети передачи данных и к остальным системам поставляемым в рамках данного решения. Количество – 2 шт.

1. Поставщик должен предусмотреть поставку всех необходимых инсталляционных материалов.

2. Поставщик в рамках данного проекта должен провести обучение не менее 10 (десяти) инженеров Покупателя.

3. Поставщик должен предоставить услуги монтажа и пуско-наладки оборудования.

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	Кожакапанов Айхан Нурланханулы
Дата подписания	29.08.2024