ТЕХНИКАЛЫҚ СИПАТТАМА

1262177 сатып алу бойынша
Ашық тендер тәсілімен

Лот № 1 (26-2 Т, 4556012) Бағдарламалық-аппараттық кешен

Тапсырыс беруші: "QAZAQGAZ PROCESSING" ЖШС
Ұйымдастырушы: "QazaqGaz" Ұлттық компаниясы" Акционерлік қоғамы

1. ТЖҚ қысқаша сипаттамасы

Атауы	**Мәні**
Жол нөмірі	26-2 Т
Атауы және қысқаша сипаттамасы	Бағдарламалық-аппараттық кешен, серверлік және телекоммуникациялық платформалардың бағдарламалық-аппараттық кешендерін жаңартуға және жөндеуге арналған
ТЖҚЖС санаттың атауы	Бағдарламалық-аппараттық кешендерге арналған жөндеу жинақтары
Қосымша сипаттама	-
Саны	1.000
Өлшем бірлігі	Жиынтық
Жеткізу орны	ҚАЗАҚСТАН, Астана қ., "Есіл" ауданы, ул. Родниковая, 1/1
Жеткізу шарттары	DDP
Жеткізу мерзімі	Шартқа қол қойылған күннен бастап 45 күнтізбелік күні
Төлем шарттары	Алдын ала төлем - 0%, Аралық төлем - 0%, Соңғы төлем - 100%

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

2.1. Жеткізуге қойылатын жалпы талаптар

2.1.1. Бағдарламалық-аппараттық кешен ақпараттық жүйелердің жұмыс істеуін қамтамасыз етуге арналған.

2.1.2. Жеткізу нысаны:

Деректерді сақтау жүйесін, серверлерді, ядро мен қатынау коммутаторларын, сымсыз қатынау нүктелерін, виртуалдандыру бағдарламалық жасақтамасын, жаңа буынның желіаралық экранын (NGFW), лицензияларды, жазылымдарды, оптикалық модульдерді, кәбілдерді және осы техникалық ерекшелікте көрсетілген қызметтерді қамтитын кешенді жеткізу, монтаждау, баптау, пайдалануға беру және кепілді-сервистік демеу.

2.1.3. Өндірушілерді біріздендіру және NGFW үшін ерекшелік:

Деректерді сақтау жүйесі, серверлер, серверлерді басқару құралдары, ядро мен қатынау коммутаторлары, сымсыз қатынау нүктелері, желілік операциялық жүйелер, виртуалдандыру бағдарламалық жасақтамасы, көрсетілген жабдыққа арналған оптикалық трансиверлер мен кәбілдер, сервистік келісімшарттар және инфрақұрылымдық бөлікті техникалық қолдау бірыңғай сауда маркасымен жеткізілуі және бір өндірушімен демеуі тиіс. NGFW, оның операциялық жүйесін, лицензияларын, жазылымдарын, оптикалық модульдерін және техникалық қолдауын қоса алғанда, жеке мамандырылған өндірушіден ұсынуға жол беріледі. Жеткізуде негізгі шешімдердің екі өндірушісінен аспауы тиіс: инфрақұрылымдық бөліктің барлығына арналған біреуі және NGFW үшін біреуі. Инфрақұрылымдық бөліктің ішінде немесе NGFW ішінде әртүрлі өндірушілердің дербес платформаларын біріктіруге жол берілмейді. Бөгде өндірушілердің OEM-компоненттеріне зауыттық интеграция кезінде, жабдық өндірушісінің өнім кодының болуы және оны кепілдік пен қолдаудың толық қамтылуы кезінде ғана жол беріледі.

2.1.4. Біріздендіруді негіздеу:

NGFW-дан басқа инфрақұрылымдық бөлікті біріздендіру зауыттық үйлесімділікті, нұсқалардың бірыңғай матрицасын, түбегейлі диагностиканы, өмірлік циклді орталықтандырылған басқаруды және оқиғаларды жою үшін бірыңғай жауапкершілікті қамтамасыз ету үшін қажет. NGFW желілік қауіпсіздік құралдарының дербес класы болып табылады және жеке өндірушімен жеткізілуі мүмкін. Жеткізуші инфрақұрылымдық бөлікті және NGFW-ны бірыңғай жұмыс істейтін кешенге интеграциялауға жауапты болады.

2.1.5. Зауыттық жеткізу:

Жабдық жаңа, бұрын пайдаланылмаған, қалпына келтірілмеген, демонстрациялық емес және өтінім берілген күнге өндірістен алынбаған болуы тиіс. Барлық компоненттер тиісті өндірушінің зауытында жиналған, интеграцияланған және тестіленген немесе ресми түрде қолдау көрсетілетін зауыттық опциялар түрінде жеткізілуі тиіс. Сериялық нөмірлер тиісті өндірушінің қолдау жүйесінде тіркелуі тиіс.

2.1.6. Техникалық қолдау және өтініштерді үйлестіру:

Инфрақұрылымдық бөлік бойынша өтініштер бірыңғай портал арқылы және оның өндірушісінің қолдау орталығы арқылы тіркелуі тиіс. NGFW үшін жеке порталға және NGFW өндірушісінің қолдау орталығына жол беріледі. Жеткізуші шарт бойынша бірыңғай үйлестіру терезесі болып табылады және Тапсырыс берушіге бастапқы себебін алдын ала анықтауды талап етпей, түбегейлі оқиға кезінде өндірушілердің өзара іс-қимылын дербес ұйымдастырады.

2.1.7. Сәйкестікті растау:

Қатысушы NGFW-ны қоса алғанда, барлық аппараттық компоненттердің, лицензиялардың, жазылымдар мен қызметтердің атаулары, саны және өнім кодтары бар егжей-тегжейлі ерекшелікті ұсынады. Әрбір маңызды талап үшін тиісті өндірушінің ресми құжаттарына немесе хаттарына сілтемелер келтіріледі. Өндірушінің растауы жоқ қатысушының материалдары жеткілікті дәлел болып табылмайды.

2.2. Жинақ мыналардан тұруы керек:

1) масштабталатын all-flash NVMe сақтау жүйесі-1 жинақ:

Жинаққа мыналар кіреді: 16 ядродан тұратын 2 контроллерлік түйін; 10 × 7,68 ТБ NVMe SED; 8 × 25ГБИТ\с SR; бағдарламалық жасақтама, шифрлау, 3 жылдық қолдау, монтаждау және оқыту.

2) екі процессорлы сервер 1U - 2 дана:

Әр серверде: 2 × 86 ядролы процессор; 768 ГБ DDR5-6400; 2 × 480 ГБ NVMe RAID1 аппараттық қорғалған жүктеу құрылғысы; 2 × 25 Гбит\с, 4 × 1 Гбит\с; кеңейтілген қашықтан басқару және 3 жылдық басқару платформасы.

3) ядро/деректер орталығының қосқышы-2 дана:

28 × 1/10/25 Гбит\с SFP28 және 4 × 10/25 Гбит\с sfp28 аппараттық арналарды шифрлаумен; 4 × 40/100 Гбит\с QSFP28; 14 50 Гбит / с портқа дейін қолдау; ақаулыққа төзімді белсенді-белсенді жұп; 2 қуат көзі; 3 желдеткіш; 3 жылдық қолдау.

4) PoE қатынау коммутаторы - 6 дана:

48 × 1 Гбит\с PoE+; 4 × 1/10 Гбит\с SFP+; PoE бюджеті 370 Вт; бір стекке дейін 6 құрылғыны біріктіру; 3 жылдық қолдау.

5) Wi-Fi 6E сымсыз қатынау нүктесі - 10 дана:

2,4/5/6 ГГц бір мезгілде жұмыс істейтін үш радиомодуль; 2×2 MIMO; екі 2,5 Гбит\с порт; ішкі антенналар; монтаждау жиынтықтары; 3 жылдық қолдау.

6) Ядро коммутаторларына арналған оптикалық модульдер мен кәбілдер - кемінде 1 жиынтық:

Жиынтық құрамына мыналар кіреді: 8 × 1ГбЕ SX; 8 × 10 Гбит\с SR; 32 × 25 Гбит\с SR; 2 × 100 Гбит\с DAC ұзындығы 1 м. Барлық компоненттер - желілік жабдық өндірушісінің ресми опциялары.

7) Виртуалдандыру бағдарламалық жасақтамасы - физикалық процессорлық сокеттер саны бойынша кемінде 4 лицензия: жиынтық жабу - кемінде 344 физикалық ядро:

3 жылға жазылу. Лицензиялаудың әрбір бірлігі ядролар санына шектеусіз бір физикалық процессорлық сокетті қамтуы тиіс; KVM-гипервизор және бірыңғай KVM/VMware басқаруы; 24x7 деңгейіндегі техникалық қолдау.

8) Жаңа буынның желіаралық экраны (NGFW) - 1 дана:

NGFW аппараттық платформасы; жеке бөлімде көзделген барлық лицензиялар мен жазылулар, мерзімі 1 жыл; өндірушінің 1 жыл мерзімді техникалық қолдауы; 2 × 1Гбит\сЕ SR және 2 × 10Гбит\сЕ SR; NGFW бөлімінің талаптарына сәйкес кәбілдер мен монтаждау керек-жарақтары жиынтығы.

2.2. Техникалық ерекшеліктің тармағы бойынша саны мен құрамы ең аз. Өндіруші көрсетілген сипаттамаларды төмендетпей, оларсыз жарияланған функционалдықты қамтамасыз ету мүмкін болмаса, қосымша компоненттерді қосуға міндетті.

2.3. жиынтық көлеміндегі масштабталатын All-Flash NVMe деректерді сақтау жүйесіне қойылатын талаптар:

2.3.1. Мақсаты және форма-факторы:

NVMe-накопительдерде толық орындалған, сыни жұмыс жүктемелеріне арналған корпоративтік санаттағы деректерді сақтау жүйесі. Базалық бақылаушы жүйенің форма-факторы - 2U-дан аспайды, стандартты 19-дюймдік тіреуге монтаждау.

2.3.2. Бақылаушылардың архитектурасы:

Бір мезгілде кіріс-шығыс операцияларын өңдеуге қатысатын кемінде екі ыстық ауыстырылатын бақылаушы тораптары. Әрбір тораптың физикалық ядролар саны кемінде 16 x86 архитектурасының кемінде бір процессорын қамтуы тиіс. Жалпы - кемінде 32 физикалық ядро және кемінде 512 ГБ жедел /кэш-память бақылаушылары. Архитектура активті бақылаушымен және резервті бақылаушымен шектелмеуі тиіс: кез келген бақылаушы және оның кез келген фронтальды порты кіріс-шығысты қабылдауы және өңдеуі тиіс, ал әрбір бақылаушының орнатылған барлық накопительдерге тікелей қатынау құқығы болуы тиіс.

2.3.3. Ішкі қосылыстар және ақауларға төзімділік:

Бақылаушы тораптары кемінде екі ішкі жоғары жылдамдықты арналармен RDMA қолдану арқылы қосылуы тиіс, бақылаушылар арасындағы алмасудың жиынтық толық дуплекстік өткізу қабілеті - кемінде 12,5 ГБ/с. Қызметтік алмасу үшін деректерді беру арналарына тәуелді емес жеке резервтелген басқару желісі пайдаланылуы тиіс. Барлық белсенді компоненттер мен жолдар көшірілген болуы тиіс: бақылаушылар, қуат блоктары, желдеткіштер, порттар, ішкі қосылыстар және накопительдерге дейінгі жолдар. Бір бақылаушының, қуат блогының, желдеткіштің, порттың немесе бір жолдың істен шығуы деректердің қолжетімсіздігіне әкеп соқпауы тиіс.

2.3.4. Жинақтағыштар және сыйымдылық:

Әрқайсысы кемінде 7,68 ТБ сыйымдылықтағы корпоративтік кластың кемінде 10 екі портты NVMe SSD жинақтағышы орнатылған. Жиынтық шикі сыйымдылық - кемінде 76,8 ТБ. Барлық жинақтағыштар өзін-өзі шифрлайтын (SED) болуы керек, AES-256-XTS аппараттық шифрлауды және криптографиялық өшіруді қолдау керек. Жинақтағыштарда сақтау жүйесін өндірушінің өнім кодтары болуы керек және бірыңғай сервистік келісімшарт бойынша қызмет көрсетілуі керек.

2.3.5. Сыйымдылықты масштабтау:

Базалық шасси кемінде 24 ішкі NVMe жинақтағышын қолдауы керек. Жүйе базалық платформаны ауыстырмай, кемінде екі кеңейту сөресін қосу арқылы кемінде 72 NVMe жинақтағышына дейін масштабталуы керек. Дискілер ең аз қадаммен екі жинақтағыштан аспайтын, сөрелер - бірден, деректерге қол жеткізуді тоқтатпай қосылуы керек.

2.3.6. Өнімділікті масштабтау:

Платформа өнімділікті және сыйымдылықты тәуелсіз масштабтауды қамтамасыз етуі керек. Деректерді басқа жүйеге көшірмей және томдардың жоспарлы қолжетімсіздігінсіз орнатылған 16-ядролы бақылаушы тораптардан кемінде 32 ядролы тораптарға бұзылмайтын көшу қолдау көрсетілуі керек.

2.3.7. Деректерді жүйелік бөлу:

Деректер мен қызметтік ақпарат барлық қол жетімді жинақтағыштарға, бақылаушыларға, кэш пен порттарға жүйелік деңгейде автоматты түрде бөлінуі керек. Жинақтағыштарды қосу кезінде немесе істен шыққан тасымалдағышты ауыстыру кезінде теңгерімдеу және қалпына келтіру жеке дискілік топтарды қолмен құру және теңгерімдеусіз көптеген жинақтағыштардың ресурстарын пайдалана отырып, автоматты түрде орындалуы керек.

2.3.8. Қосу интерфейстері:

Әрбір бақылаушы торапта деректерді беру үшін кемінде төрт 10/25 Гбит\с SFP28 порты, барлығы кемінде сегіз порт орнатылуы керек. Жинақта - сол өндірушінің кемінде сегіз 25 Гбит\с SFP28 SR көп режимді трансивері. Әрбір бақылаушы торапта әкімшілендірудің және сервистік басқарудың 1Гбит\с RJ-45 жеке порттары болуы керек. iSCSI және NVMe over TCP қолдау көрсетілуі керек; аппараттық платформа бақылаушыларды ауыстырмай, сол жүйеде NFS файлдық қатынауын пайдалануға мүмкіндік беруі керек.

2.3.9. Қуат блоктары:

Резервтеумен жұмыс істейтін әрқайсысы кемінде 1600 Вт қуатты кемінде екі ыстық ауыстырылатын қуат блогы. Жинақта - C13-C14 қуат кабельдері.

2.3.10. Деректерді қорғау:

Кемінде екі жинақтағыштың бір уақытта істен шығуына төтеп беретін, екі еселі жұптылықтан төмен емес, істен шықпайтын деректерді қорғауды қолдау. Деректердің тұтастығын түбегейлі тексеру, ішкі шиналарда, бақылаушылар арасындағы арналарда, хост протоколдарында және жинақтағыштардағы қателерді циклдік бақылау, блоктарды фондық тексеру және тасымалдағыштардың істен шығуын болжау орындалуы керек.

2.3.11. Сыйымдылықты оңтайландыру:

Салынған inline-сығымдау, inline-дедупликация, сыйымдылықты нақты бөлу және босатылған кеңістікті қайтару. Оңтайландыру саясаты жеке томдар/томдар топтары деңгейінде тағайындалуы керек. Қызметтер сыртқы шлюзді немесе жеке құрылғыны талап етпеуі керек.

2.3.12. Жергілікті қорғау және көшірмелер:

Салынған сәттегі суреттерді және томдардың толық/виртуалды көшірмелерін жасау; келісілген томдар топтары; бастапқы сыйымдылықты толық резервтеусіз суреттер жасау; томды немесе жеке виртуалды машиналарды суреттен қалпына келтіру. Суреттерді белгіленген мерзімге рұқсатсыз жоюдан қорғау қолдау көрсетілуі керек.

2.3.13. Репликация және бизнестің үздіксіздігі:

RPO=0 режимін қоса алғанда, өндіруші жүйелері арасындағы ендірілген асинхронды және синхронды репликация, кворуммен алаңдар арасында автоматтандырылған ауыстыру. Платформа екі жақты active-active репликацияны және кемінде үш алаңды қорғау топологиясын қолдауы тиіс. Репликацияның негізгі функциялары әрбір томға жеке лицензияларды сатып алмай жеткізілетін бағдарламалық жасақтама құрамында қол жетімді болуы тиіс.

2.3.14. Қолжетімділік кепілдігі:

Өндіруші бағдарлама шарттары сақталғанда және мәлімделген қолдау деңгейі болғанда осы жүйелер сериясы үшін деректердің 100% қолжетімділігіне кепілдіктің құжатталған бағдарламасын ұсынуы тиіс. Жеткізілетін конфигурацияның бағдарламаға қатысуын растау өндірушінің хатымен немесе ресми құжатпен ұсынылады.

2.3.15. Басқару:

Қорғалған веб-интерфейс, жергілікті интерфейс және REST API арқылы басқару. RBAC, MFA/SSO, әрекеттерді журналдау, сыртқы каталогтармен, Syslog-пен және қауіпсіз басқару хаттамаларымен интеграция қолдау көрсетілуі тиіс. Бір консольден өндірушінің бірнеше массивтерін орталықтандырылған басқару мүмкіндігі болуы тиіс.

2.3.16. AIOps және түбегейлі талдау:

Өндірушінің бұлтты немесе гибридті талдамалық платформасы мыналарды қамтамасыз етуі тиіс: іркілістер мен ресурстардың жетіспеушілігін болжау; БЖ нұсқалары бойынша ұсынымдар; аномалияларды анықтау; сыйымдылық пен өнімділіктің трендтерін талдау; сервистік өтініштерді автоматты түрде ашу.

Виртуалдандырылған орта үшін виртуалды машинадан виртуалды диск, datastore, хост және хост адаптері арқылы томға және сақтау жүйесіне дейінгі ендірілген жол топологиясы көрсетілуі тиіс, соның ішінде CPU/RAM хостының және виртуалды машинаның жүктелуімен кідірістердің корреляциясы. Тарихи деректер кемінде 12 ай қол жетімді болуы тиіс, егжей-тегжейлі талдау - 5 минуттан аспайтын интервалмен.

2.3.17. Кибер қауіптерден қорғау:

Массив деңгейінде аномалдық мінез-құлық пен шифрлау/зияны бар белсенділік белгілерін ендірілген анықтау, хабарламалар мен қалпына келтіру бойынша ұсынымдарды қалыптастыру. Тыныштықтағы деректерді шифрлау өнімділікті айтарлықтай төмендетпей SED-де аппараттық орындалуы тиіс. Стандартты хаттама бойынша кілттерді жергілікті және сыртқы басқаруды, криптографиялық өшіруді және қауіпсіз жүктеуді қолдау.

2.3.18. Виртуалдандырумен интеграция:

Сол өндірушінің жеткізілетін виртуалдандыру платформасымен табиғи интеграция виртуалды машина дискілерін массив томдарымен тікелей салыстыруды, ВМ деңгейінде өнімділік параметрлерін тағайындауды және виртуалдандыру интерфейсінен массивтің аппараттық суреттерін жасауды қамтамасыз етуі тиіс. Сонымен қатар, VMware vCenter, VASA нұсқасы 5-тен төмен емес, vVols, Site Recovery Manager, VAAI және vCenter интерфейсінен сақтауды басқару қолдау көрсетілуі тиіс.

2.3.19. Лицензиялар:

Жинақта - массивтің операциялық жүйесі, шифрлау лицензиясы, барлық орнатылған сыйымдылыққа басқару және бағдарламалық қолдау лицензиялары кемінде 3 жыл мерзімге. Негізгі сақтау, түсірілімдер, сыйымдылықты оңтайландыру, репликация, аналитика және API функцияларының барлығы жеткізілетін көлемге лицензияланған болуы тиіс.

2.3.20. Қолдау:

24×7 деңгейіндегі өндірушінің кемінде 3 жыл техникалық қолдауы. Маманның қайта қоңырау шалудың мақсатты уақыты: 1-деңгейдегі сыни оқиға үшін 15 минуттан аспайды және 2 және 3-деңгейдегі оқиғалар үшін 1 сағаттан аспайды. Инженердің орнату орнына баруы - өндіруші растаған қызметтің географиялық қолжетімділігін ескере отырып, жабылған жабдық үшін 4 сағаттан аспайды. Микрокод пен бағдарламалық жасақтаманы жаңарту кіреді.

2.3.21. Қызметтер және оқыту:

Жинақта - зауыттық/жобалық интеграция, аппараттық бөлікті және операциялық жүйені орнату және бастапқы іске қосу, екі торапты кластерді баптау, басқару платформасына қосылу және ақауларға төзімділікті тексеру. Кемінде 30 оқу кредитін немесе пайдалану мерзімі кемінде 12 ай болатын өндірушінің эквивалентті ресми оқыту көлемін ұсыну.

2.3.22. Жеке массивтердің федерациясы жоқ отбасының масштабталуы:

Отбасының бірыңғай бағдарламалық-аппараттық архитектурасы бір мезгілде 2-ден 4-ке дейінгі белсенді бақылаушы тораптардың конфигурацияларын және бір логикалық жүйе шегінде кемінде 384 екі портты NVMe-накопительдерге және 16 кеңейту сөрелеріне дейін масштабтауды қолдауы тиіс. Барлық бақылаушылардың жалпы накопительдер пулына тікелей қол жеткізуі тиіс; тәуелсіз массивтерді сыртқы федерациямен біріктіру сәйкестік болып саналмайды.

2.3.23. Кепілдендірілген қызмет көрсету сапасы:

Салынған QoS механизмі жеке томдар, томдар топтары, жалгерлер немесе виртуалды машиналар үшін IOPS және өткізу қабілеттілігінің ең аз және ең жоғары мәндерін, сондай-ақ 50 микросекундқа дейінгі кідірістің мақсатты деңгейін белгілеуі тиіс. Саясаттарды өзгерту хосттарға агенттерді орнатпай және накопительдерді физикалық бөлусіз онлайн орындалады.

2.3.24. Өзгертілмейтін түсірілімдер және сақтау мерзімін бақылау:

Сақтау мерзімі көрсетілген WORM/immutable класындағы түсірілімдер қолдау көрсетілуі тиіс. Мұндай түсірілімнің мерзімі аяқталғанға дейін оны ең жоғары құқықтары бар әкімші немесе өндірушінің сервистік қызметі жоюға, мерзімі бойынша қысқартуға немесе бұғаттан шығаруға болмайды. Қорғау жүйенің сағаттарын өзгерту арқылы айналып өтуді болдырмайтын уақытты тәуелсіз бақылауды пайдалануы тиіс.

2.3.25. Мультитенанттылық:

Бір массивтің ішінде бөлек сақтау объектілері, квоталар, QoS саясаттары, журналдар және өкілеттік берілген әкімшілер бар оқшауланған виртуалды домендерді/жалгерлерді құруды қолдау. Бір домен әкімшісінің қатесі немесе әрекеті басқа домен объектілеріне қатынауды ұсынуы тиіс.

2.3.26. Шифрлау кілттерін басқару:

SED-тегі деректерді шифрлау FIPS 140-2 немесе одан кейінгі қолданылатын стандартты валидациядан өткен кілттердің салынған жергілікті менеджерін және сыртқы кілттер менеджерлерін қолдауы тиіс. Жергілікті және сыртқы менеджер арасында, сондай-ақ сыртқы менеджерлер арасындағы ауысу шифрлауды тоқтатпай және деректерді жоғалтпай орындалуы тиіс.

2.3.27. Онлайн-қызмет көрсету және жаңарту:

Бақылаушы тораптарды, жад модульдерін, жүктеуші накопительдерді, адаптерлерді, SFP-модульдерді, қуат блоктарын, желдеткіштерді және накопительдерді онлайн ауыстыруды қамтамасыз етуі тиіс. Массивтің операциялық жүйесін жаңарту барлық бақылаушыларды бір мезгілде қайта жүктеусіз және хосттардың деректерге қатынауын тоқтатпай орындалуы тиіс.

2.4.13. Қашықтан басқару:

Әр сервер үшін енгізілген басқарудың кеңейтілген лицензиясы қосылған, мерзімі кемінде 3 жыл: толық функционалды HTML5 KVM-консолі, виртуалды тасымалдағыштар, ISO қашықтан қосылуы, консоль сеансын жазу және ойнату, бірнеше әкімшілердің бірлескен жұмысы, қуатты басқару, журнал жүргізу және RESTful API.

2.4.14. Серверлік парк басқару платформасы:

Жинақта - өндірушінің орталықтандырылған SaaS/гибридтік басқару платформасына кемінде 3 жыл мерзімге жазылуы. Платформа мыналарды қамтамасыз етуі тиіс: түгендеу; серверлерді топтастыру; микрокодтың автоматты базалық желілері; сәйкестікті бақылау; кесте бойынша және талап бойынша топтық жаңартулар; тізбекті/параллельді режим және қателік кезінде тоқтату; орталықтандырылған BIOS профильдері; қашықтағы HTML5-консоль; сервистік өтініштерді автоматты түрде құру; RBAC/SSO; аудит; REST API; энергия тұтыну, құн және шығарындылар бойынша есептер; микрокодты және драйверлерді жаңарту үшін VMware vCenter және vSphere Lifecycle Manager-мен интеграция.

2.4.15. Қолдау көрсетілетін ОЖ:

Microsoft Windows Server, VMware ESXi, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Canonical Ubuntu, Oracle Linux және негізгі үйлесімді корпоративтік Linux-дистрибутивтердің өзекті нұсқаларын ресми түрде қолдау. Қатысушы ресми қолдау матрицасына сілтеме береді.

2.4.16. Кепілдік және қолдау:

Өндірушінің негізгі кепілдігі бөлшектерге, жұмыстарға және шығуға кемінде 3 жыл. Қосымша жеткізу құрамында - 9×5 деңгейіндегі өндірушінің техникалық қолдауы кемінде 3 жыл, бейінді маманның кері қоңырауымен 2 сағаттан аспайтын және жабылған жабдық үшін келесі жұмыс күніне шығу. Барлық орнатылған зауыттық опциялар сол келісімшарт бойынша қызмет көрсетілуі тиіс.

2.4.17. Қызметтер:

Тіреуге физикалық орнату, қосу, микрокодты келісілген қолдау көрсетілетін нұсқаға дейін жаңарту, қашықтан басқару контроллерін және орталықтандырылған басқару платформасын орнату, жүктеу RAID1-ді тексеру және жабдықтың жай-күйі туралы есеп беру.

2.4.18. Корпустың тереңдігі:

Тұтқаларды, кәбілдерді және жетекшілерді ескермей, әр сервердің тереңдігі 77,5 см-ден аспауы тиіс, бұл стандартты тіреулерде орналастыруды және артқы жағынан коммутация үшін жеткілікті кеңістікті қамтамасыз етеді.

2.4.19. Шасси нұсқалары және әмбебап алдыңғы аймақ:

Серверлік отбасыда 1U шассидің кемінде үш зауыттық нұсқасы болуы керек және бір SFF, LFF, EDSFF E3.S платформасы шеңберінде қолдау көрсетуі керек, M.2 NVMe ішкі жүктеу құрылғысы және OCP желілік адаптерлерін фронтальды көпфункционалды аймақта орналастыру. Нұсқаны таңдау серверлердің басқа отбасына көшуді талап етпеуі тиіс.

2.4.20 Жадының жоғары ақауға төзімділігі:

Платформа жадының режимін қолдауы тиіс, ол жады құрылғыларының ақауларын екі есе түзетуден төмен емес, бірақ барлық көлемді көшірусіз және қол жетімді оперативті жад сыйымдылығын 50% - ға азайтусыз тұрақтылықпен. Режимді сервер өндірушісі іске асыруы және құжаттауы тиіс.

2.4.21 Жұмыс жүктемелерінің профильдері:

UEFI/BIOS-та процессор, жад, энергия тұтыну және виртуалдандыру, дерекқорлар, төмен кідіріс, энергия тиімділігі және басқа сценарийлер үшін кіріс-шығыс параметрлерінің жиынтығын автоматты түрде өзгертетін алдын ала тексерілген жұмыс жүктемелерінің профильдері орнатылуы тиіс. Профиль олардың әрқайсысын қолмен баптаусыз жүздей өзара байланысты параметрлерді оңтайландыруы тиіс.

2.5.21. Кестелер мен маршруттаудың ауқымы

Кемінде 4 094 VLAN, кемінде 212 000 MAC-адрестер, кемінде 145 000 IPv4 host entries, кемінде 145 000 IPv6 host entries, кемінде 600 000 IPv4 және кемінде 600 000 IPv6 маршруттарын қолдау. ECMP кемінде 32 тең бағалы жол бойынша қолдау.

2.5.22. Ағынды телеметрия және диагностика:

OpenConfig модельдерімен gNMI ағынды телеметриясын, аппараттық sFlow-ды, RMON-ды, IP SLA-ны жергілікті талдамалық механизмде тарихты сақтай отырып, сондай-ақ операциялық жүйенің екі тәуелсіз бейнесін және бірнеше конфигурация файлдарын қолдау.

2.5.23. Арналарды агрегациялау:

Кемінде 54 арналарды агрегациялау топтарын қолдау. Бір топта жеке коммутаторда кемінде 16 физикалық қатысушы және екі коммутатордың арасында топты бөлу кезінде кемінде 32 қатысушы қолдау көрсетілуі тиіс. Теңгерімдеу алгоритмі L1-L4 деңгейлерінің өрістері бойынша орнатылуы тиіс.

2.6. PoE қатынау коммутаторларына қойылатын талаптар - 6 дана:

2.6.1 Форм-фактор:

19 дюймдік тіреуге орнату үшін 1U-дан аспайтын басқарылатын қатынау коммутаторы.

2.6.2 Қатынау порттары:

IEEE 802.3at PoE+ (Class 4) қолдауы бар кемінде 48 10/100/1000BASE-T порттары, портқа 30 Вт дейін және кемінде төрт кіріктірілген uplink-порттары 1/10Гбит\с\с SFP/SFP+.

2.6.3 PoE-бюджет:

PoE қуаттандырудың жиынтық бюджеті коммутаторға кемінде 370 Вт. Қуатты басым етуді және әр портта тұтынуды бақылауды қолдау.

2.6.4 Өнімділік:

Блоктаусыз коммутациялық мүмкіндік кемінде 176 Гбит\с/с және кемінде 98 млн пакет/с жіберу өнімділігі.

2.6.5 Стекке біріктіру:

Барлық алты коммутатор арнайы проприетарлық стек модульдерінсіз, штаттық 1/10Гбит\с\с порттар арқылы тізбектік немесе сақиналық топология бойынша бірыңғай логикалық стекке біріктірілуі тиіс. Кемінде 6 қатысушы, бірыңғай конфигурация және бірыңғай басқару нүктесі қолдау көрсетіледі.

2.6.6 Операциялық жүйе:

Ядро және қатынау коммутаторлары конфигурацияның транзакциялық базасы, модулдық архитектурасы және бірыңғай CLI/REST API бар бір өндірушінің бірыңғай заманауи операциялық жүйесін пайдалануы тиіс. Жеке бағдарламалық үдерістің істен шығуы операциялық жүйені толық қайта іске қосуды талап етпеуі тиіс.

2.6.7 Функциялар:

VLAN, LACP, STP/RSTP/MSTP, LLDP/LLDP-MED, ACL, QoS, IPv6, 802.1X, MAC-аутентификация, DHCP Snooping, Dynamic ARP Inspection, Port Security, IGMP/MLD Snooping, статикалық маршруттау және Energy Efficient Ethernet.

2.6.8. Қатынауды автоматтандыру:

Түпкілікті құрылғыны жылжыту VLAN-ға портты қолмен байланыстыруды талап етпеуі үшін пайдаланушыны немесе құрылғыны сәйкестендіру негізінде портқа рөлдерді/саясаттарды динамикалық тағайындауды қолдау. Орталықтандырылған жаппай өзгертуді және конфигурацияны тексеруді қолдау.

2.6.9. Басқару:

Жергілікті Web GUI, CLI, REST API, SNMPv3 және аппараттық қамтамасыз етуді ауыстырмай, бұлтты немесе жергілікті орнатылған өндірушінің платформасы арқылы басқару мүмкіндігі.

2.6.10. Кепілдік және қолдау:

Өндірушінің шектеулі өмірлік кепілдігі сату аяқталғанға дейін кемінде плюс 5 жыл жабумен. Жинақта - 3 жылға ТАС 24×7, БҚ жаңартулары және жабдықты келесі жұмыс күні ауыстырумен қызмет.

2.6.11. Аппараттық сенімді жүктеу:

Әр коммутаторда кіріктірілген сенімді аппараттық модуль болуы тиіс, жүктеушінің және операциялық жүйенің тұтастығын тексеру және қол қойылмаған немесе зақымдалған бағдарламалық бейнені іске қосуды бұғаттау.

2.8.3 KVM және VMware-ді бірлесіп басқару:

Бір веб-консольден жеткізілетін KVM-гипервизорда да, VMware vSphere/ESXi қолданыстағы кластерлерінде де виртуалды машиналарды анықтау, қарау, құру және негізгі басқару операцияларын орындау керек. VMware бейнелерін/виртуалды машиналарын жеткізілетін гипервизор форматына түрлендіру құралы қосылуы тиіс.

2.8.4 Кластер және жоғары қолжетімділік:

Ақауға төзімді кластер құру; торап ақауланғаннан кейін ВМ автоматты түрде қайта іске қосылуы; тоқтатусыз жұмыс істейтін ВМ-ді тораптар арасында тікелей көшіру; жүктеме негізінде ВМ-ді оңтайлы хостқа автоматты түрде орналастыру; жұмыс жүктемесін тоқтатпай торапқа жоспарлы қызмет көрсетуді қолдау.

2.8.5. Сақтауды басқару:

NFS, iSCSI және Fibre Channel бойынша сыртқы сақтау жүйелерін қолдау. ВМ тоқтатусыз datastore арасында виртуалды дискілерді тікелей көшіру. Томдарды виртуалды машиналармен тікелей салыстыру,

өнімділікті баптау және аппараттық суреттерді құру үшін сол өндірушінің жеткізілетін сақтау жүйесімен туаған интеграция.

2.8.6 Желі:

VLAN 802.1Q, trunk, физикалық интерфейстерді біріктіру, Open vSwitch немесе эквивалентті, бөлек басқару/есептеу/сақтау желілерін және виртуалды машиналарға желілерді орталықтандырылған түрде тағайындауды қолдау.

2.8.7 IPAM, DNS және құпиялар:

IP-адрестердің ендірілген пулдарын, есептік деректердің қорғалған қоймасын және әрбір түрдің кемінде екі кең таралған шешімін қоса алғанда, сыртқы IPAM/DNS-жүйелермен интеграция. ВМ-ді орналастыру кезінде A/PTR-жазбаларды автоматты түрде құру және мекенжайларды резервтеу.

2.8.8. Деректерді қорғау:

Құру, қалпына келтіру және жою операциялары бар ВМ-нің ендірілген суреттері мен сақтық көшірмелері. Veeam, Commvault және Rubrik немесе олардың ресми эквиваленттерімен үйлесімді шешімдерді қоса алғанда, кемінде үш сыртқы деректерді қорғау платформасымен интеграция.

2.8.9. Автоматтандыру:

ВМ-ді дайындау және пайдалану кезінде Bash және PowerShell-скрипттерін орындау; орналастыру үлгілері; тегтер; Day-2 операциялары; REST API және CLI.

2.8.10. Консоль және қатынау:

VNC, SSH және RDP қолдауы бар веб-интерфейс арқылы виртуалды машиналардың HTML5-консолі; RBAC; SSO; аудит журналдары; құпияларды қауіпсіз сақтау.

2.8.11. Қонақ ОС-ті қолдау:

Microsoft Windows және негізгі корпоративтік Linux-дистрибутивтерді қолдау. Өндірушінің ресми үйлесімділік матрицасымен растау.

2.8.12. Техникалық қолдау:

Лицензияланған редакция шегінде жаңа нұсқаларды, қауіпсіздік түзетулерін және жаңартуларды қоса алғанда, 1-деңгейдегі күрделі оқиға үшін 15 минуттан аспайтын және 2-3-деңгейлер үшін 1 сағаттан аспайтын мақсатты кері қоңырау уақытымен кемінде 3 жыл 24×7.

2.8.13 Екі торапты кластер:

Платформа Fibre Channel, iSCSI немесе NFS бойынша сыртқы ортақ сақтаумен жеткізілетін екі есептеу торабынан тұратын кластерді ресми түрде қолдауы тиіс. Жоғары қолжетімділікті іске қосу үшін үшінші есептеу серверін сатып алу талап етілмеуі тиіс; кворум функциялары өндіруші қолдайтын тәсілмен іске асырылады.

2.8.14. Жасырын лицензиялық шектеулердің болмауы:

Жаппай сокеттер үшін ядролардың ең аз топтамасына, ядролар санына қосымша коэффициентке, виртуалды машиналар, виртуалды процессорлар, хосттар немесе басқарылатын сыйымдылық санына шектеуге жол берілмейді. Осы бөлімнің барлық функциялары жеке басқару лицензиясын сатып алмай, төленген мерзім ішінде сақталуы тиіс.

2.10. Барлық жеткізілетін брандмауэрлерге арналған жалпы сипаттамалар:

Келесі функционалдығы бар OSI моделінің Layer-2-ден Layer-7-ге дейінгі деңгейлерінде жұмыс істейтін аппараттық брандмауэр:

1. Сеанстардың күйін бақылаумен брандмауэр;

2. Брандмауэр арқылы өтетін трафик бойынша OSI моделінің жетінші деңгейінде желілік қосымшаларды тану және бұғаттау, соның ішінде 80 және 443 ортақ портты пайдаланатын және динамикалық TCP/UDP порттарын пайдаланатын барлық қосымшалар үшін жеке;

3. Ұсынылған NGFW ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSFC, USGV6, ICSA және NEBS стандарттары бойынша сертификатталуы керек

4. Ұсынылған ngfw қауіпсіздік жаңартуларын тексеру және орнату үшін қайта жүктеуді қажет етпеуі керек

5. Ұсынылған NGFW есептерді жасау үшін қосымша жабдықты қажет етпейтін интеграцияланған есеп беру мүмкіндіктеріне ие болуы керек

6. Ұсынылған NGFW портқа, SSL/SSH шифрлауына немесе қолданылатын айналып өту әдістеріне қарамастан қолданбаларды анықтауы керек

7. Ұсынылған NGFW саясатты басқару, қауіп-қатер криминалистикасы немесе қолданбаларды сәйкестендіру технологияларын әзірлеу үшін анықталмаған қолданбаларды жіктеуі керек

8. Ұсынылған NGFW трафикті өңдеуге арналған бір реттік параллельді өңдеу архитектурасы бар толыққанды құрылғы болуы керек.

9. Ұсынылған Ngfw Facebook чатының ажыратымдылығы сияқты қосымшаның әртүрлі бөліктерін ажыратуы керек, бірақ файлдарды тасымалдау мүмкіндігін бұғаттауы керек

10. Ұсынылған NGFW веб-сайттар мен қосымшаларға, соның ішінде SaaS қосымшаларына кіруді бақылап, саясатты қолдануы керек

11. Ұсынылған NGFW барлық форма факторларында бір ОЖ болуы керек

12. Ұсынылған NGFW тіркелгі деректерін ұрлаудың алдын алу үшін қауіпсіздік саясатын құруды қолдауы керек

13. Ұсынылған NGFW ішкі қосымшалар үшін көп факторлы аутентификацияны қолдануды қолдауы керек

14. Ұсынылған NGFW қауіпсіздік саясатының бірыңғай ережесінде стандартты емес порттарды пайдаланатын қолданбалардың көрінуін және шектеу мүмкіндігін қамтамасыз етуі керек

15. Ұсынылған NGFW сыртқы қосылымдарды қажет етпестен тікелей NGFW ден кеңейтілген қорғаныс үшін машиналық оқыту алгоритмдерін ұсына алуы керек

16. Ұсынылған NGFW нұсқаны жаңарту кезінде тұрақтылықты және оңай кері қайтаруды қолдау үшін бірнеше ОЖ кескіндерін сақтау мүмкіндігіне ие болуы керек

17. Ұсынылған NGFW OSI моделінің Layer-7-де тексерілген трафикте келесі қолданба санаттарының қолтаңбалары бойынша тануды қолдауы керек:

17.1. Кәсіпорын қосымшалары:

17.1.1. Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS сияқты аутентификация қызметтері;

17.1.2. ДҚБЖ, соның ішінде Microsoft SQL, Microsoftacle, DB2, Postgres, Sybase;

17.1.3. Файлдық қызметтер, соның ішінде Microsoft SMB;

17.1.4. ERP, CRM, соның ішінде SAP, 1C;

17.1.5. Электрондық құжат айналымы және хабар алмасу жүйелері, соның ішінде EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus;

17.1.6. Электрондық пошта алмасу хаттамалары: SMTP, POP3, IMAP;

17.1.7. SIP, H. 323, H. 245, H. 225, Webex сияқты VoIP және аудио-бейне конференцияларының хаттамалары;

17.1.8. Бағдарламалық жасақтаманы жаңарту қызметтері, соның ішінде Microsoft Update, антивирустық бағдарлама (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple;

17.1.9. Symantec Backup Exec қоса алғанда, сақтық көшірме қызметтері;

17.1.10. VMware, Citrix, Microsoft RDP сияқты виртуалдандыру және терминалға қол жеткізу қызметтері;

17.1.11. Corba, SOAP қоса алғанда, таратылған қосымшаларды жасау үшін қолданылатын өзге де хаттамалар мен технологиялар;

17.1.12. Қашықтан қол жеткізу протоколдары, соның ішінде Telnet, SSH, VNC, Radmin;

17.1.13. Желілік протоколдар, соның ішінде динамикалық маршруттау және SSL протоколдары, IPSec VPN;

17.2. Интернет желісінің қосымшалары:

17.2.1. Электрондық пошта, соның ішінде Gmail, Yandex.Mail, Mail.ru, Hotmail;

17.2.2. Әлеуметтік желілер, соның ішінде Facebook, Google+, LinkedIn, ВКонтакте, Одноклассники, "Менің әлемім";

17.2.3. Жедел хабар алмасу құралдары, соның ішінде ICQ, Jabber, IRC, MSN, тізімделген әлеуметтік желілердегі ұқсас қызметтер;

17.2.4. Аудио-бейне конференция құралдары, соның ішінде Skype;

17.2.5. Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav қоса алғанда, HTTP(S) және peer-to-peer арқылы файл алмасу құралдары;

17.2.6. YouTube, Vimeo, http аудио және бейнені қоса, аудио бейне ағыны (веб-сайтқа қарамастан);

17.2.7. Team-Viewer, LogMeIn сияқты жұмыс үстелін жариялау және қашықтан қол жеткізуді қамтамасыз ету құралдары;

17.2.8. Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy сияқты сыртқы прокси-серверлер мен анонимизаторлар;

17.2.9. FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS сияқты басқа қосымшалардың үстіне жеке VPN құру және туннельдеу құралдары;

18. Брандмауэр қолданбалардың функционалдығын ажыратуды жүзеге асыруы керек, мысалы, файлдарды тасымалдауды бұғаттаған кезде Facebook чатын пайдалануға рұқсат беру мүмкіндігі

19. HTTP(S), FTP, SMB, SMTP, RPC және т. б. декодерлерді, сондай-ақ TCP/UDP пакеттерінің мазмұнына арналған масканы пайдалана отырып, тұрақты өрнектер бойынша жеке қолтаңбаларды жасаудың МЭ-ге ендірілген құралдарын ұсыну;

20. HTTP/2 протоколы арқылы берілетін қосымшаларды тану;

21. Желілік қосымшаларды шифрланған SSL (RSA кілттерін 2048 битке дейін қолдау) және sshv2 арқылы брандмауэр арқылы өтетін трафик (SSL шифрын ашу, SSHv2) арқылы тану - кіріс және шығыс қосылымдар үшін, домендегі пайдаланушылар үшін ашық, қосымшалардың жеке функцияларын,соның ішінде әлеуметтік желілерде хабарлама жіберуді бақылау мүмкіндігі бар, файлды бөлісу, аудио ағыны, бейне;

22. Туннельдерді тексеру:

22.1. Generic Routing Encapsulation (GRE) (RFC 2784);

22.2. Nonencrypted IPSec traffic [NULL Encryption Algorithm for IPSec (RFC 2410);

22.3. Transport mode AH IPSec;

23. Бір сессияда қолданылатын әр түрлі қосымшаларды дәйекті тану;

24. Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix сияқты корпоративтік пайдаланушылардың аутентификация қызметтерімен интеграциялау арқылы желілік қосымшаларды пайдаланатын пайдаланушыларды тану; ашық XML API арқылы басқа аутентификация қызметтерімен (мысалы, сымсыз желі контроллері) интеграциялау мүмкіндігі; пайдаланушылардың мәжбүрлі авторизациясын пайдалану мүмкіндігі web бет – "Captive portal"; Kerberos, tacacs+, SAML V. 2 қолдауы, WMI және NetBIOS сауалнамалары арқылы пайдаланушылардың L3 роумингін қолдау;

25. Қолтаңбалар мен мінез-құлық ағынында нақты уақыт режимінде брандмауэр арқылы Берілетін трафик мазмұнын тексеру, осалдықтардан, желілік шабуылдардан және зиянды бағдарламалардан қорғау, олардың қолтаңбалары бойынша файл түрлерін тану, веб арқылы берілетін вирустарды

электрондық пошта, FTP, SMB, шпиондық бағдарламалар, желілік құрттар арқылы анықтау, белгілі бір мазмұнды беруді бұғаттау SSL және sshv2 шифрлауды қолданатын қосымшаларды қоса алғанда, тұрақты өрнектерді қолдану;

26. Әрбір қосылымның келесі параметрлерін біліктілік ретінде пайдалана отырып, бірыңғай қауіпсіздік саясатында брандмауэр арқылы өтетін трафиктің ережелерін жасау:

26.1. Жіберушінің IP мекенжайы,

26.2. Алушының IP мекенжайы,

26.3. L4 деңгейіндегі қызметтер: TCP және UDP протоколдарына арналған порттар,

26.4. Active Directory пайдаланушы имен немесе пайдаланушы топтары,

26.5. OSI моделінің 7 деңгейлі қосымшалары,

26.6. Категориil санаттары.

27. Жіберушінің, алушының, пайдаланылған қызметтердің (TCP/UDP порттарының) IP мекенжайлары, пайдаланушы имен, пайдаланушы топтары және пайдаланушы немесе қолданба пайдаланушылар тобы немесе белгілі бір қолданба санаттары туралы деректерді біліктілік ретінде пайдалана отырып, бірыңғай қауіпсіздік саясатында ережелер жасау. Құрылатын саясаттарда мынадай іс-әрекеттерді іске асыру мүмкіндігі болуға тиіс:

Рұқсат немесе тыйым салу;

Белгілі бір қолданбаға немесе қолданбалар санатына тек стандартты немесе қатаң анықталған TCP/UDP порттарын пайдалануға рұқсат беру. Бұл ретте бұл порттарды мұндай өзара іс-қимылдарға нақты түрде рұқсат беретін саясатсыз басқа қосымшалар пайдаланбауға тиіс;

Рұқсат беру, бірақ сонымен бірге вирустар мен басқа қауіптерді сканерлеу;

Кестеге, пайдаланушыға немесе пайдаланушылар тобына негізделген рұқсат немесе тыйым салу ережесі;

Декодтау және тексеру. Егер декодтау мүмкін болмаса (стандартты емес крипто-алгоритм, ескірген сертификат және т. б.) – тыйым салу;

Белгілі бір категориil санаттарын және жеке сенімді веб-сайттарды ашпаңыз;

Қолданбаларға, IP мекенжайларына, пайдаланушыларға және пайдаланушы топтарына негізделген QoS саясаттарын пайдалана отырып, dscp таңбалауын және трафикті шектеуді қолдану;

Қолданба деңгейінде анықталған нақты уақыт трафигі үшін qos аппараттық енгізу;

Саясатқа негізделген трафикті қайта бағыттауды қолдану (Policy Based Forwarding);

Қолданбаның жеке функцияларына рұқсат беру;

Жоғарыда келтірілген әрекеттердің кез келген тіркесімі;

28. Брандмауэрде ескірген 4-деңгейдегі саясатты (портқа негізделген) қолданбаға негізделген 7-деңгейдегі саясатқа түрлендіруді қамтамасыз ететін кірістірілген қауіпсіздік саясатын оңтайландыру құралы болуы керек

29. Жүйе антивирустық қорғауды, шпиондық бағдарламадан қорғауды, осалдықтар мен желілік шабуылдардан қорғауды (интрузияны анықтау және алдын алу жүйесі), бір веб-сайттың әртүрлі бөлімдері үшін санаттауды қолдайтын динамикалық бедел базасын қолдана отырып URL сүзгісін, соның ішінде орыс тіліндегі веб-сайттарға санаттарды қолдауды қолдауы керек.. қолтаңбалармен анықталған типтер бойынша файлдарды тасымалдауды бұғаттау. Аталған функционалдылық тиісті жазылымдарды пайдалану кезінде қол жетімді болуы керек;

30. Жүйе хэш емес, пайдалы жүктемеге негізделген қолтаңбалар арқылы кіріктірілген зиянды бағдарламадан қорғауды қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

31. Жүйе сыртқы қосылымдарды қажет етпестен тікелей брандмауэрден кеңейтілген қорғаныс үшін машиналық оқыту алгоритмдерін ұсына алуы керек

32. Брандмауэрде қолданылатын машиналық және терең оқыту модельдері SSL, HTTP және белгісіз UDP және TCP трафигін қоса алғанда, негізгі протоколдар бойынша трафикті талдауды қамтамасыз етуі керек

33. Бұлтты Қызметтер арқылы Машиналық оқыту технологиясын қолдана отырып, трафикті талдау арқылы белгісіз қауіптерге трафикті қосымша тексеру мүмкіндігі. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

34. Брандмауэр қалыпты емес желілік трафикті және күдікті пакеттерді, соның ішінде портты сканерлеу, түйінді сканерлеу және қызмет көрсетуден бас тарту (DoS) шабуылдары сияқты үлгілерді анықтау үшін эвристикалық талдауды қолдауы керек.

35. Брандмауэр шабуылдардан қорғаудың басқа мүмкіндіктерін қолдауы керек, мысалы, жарамсыз немесе бұрмаланған пакеттерді бұғаттау, IP дефрагментациясы және TCP қайта құрастыру, жалтару және шатастыру әдістерінен қорғау.

36. Брандмауэрден жалтару әдістерін ұстап қалу және болдырмау үшін келу тәртібі мен бірнеше пакеттер тізбегімен қамтамасыз етілген контекстті талдауды талап етеді

37. Жүйе Сығылған файлдар мен веб-мазмұнға жасырылған зиянды бағдарламаларды кіріктірілген ағынды анықтау мен алдын-алуды қолдануы керек.

38. Брандмауэр Microsoft Office / Microsoft 365 құжаттары және PDF файлдары сияқты жалпы форматтағы файлдардың ішінде жасырылған зиянды жүктемелерден қорғауды қамтамасыз етуі керек.

39. Брандмауэр функционалдығы ықтимал шабуылды көрсететін бірқатар байланысты қауіп оқиғаларының (мысалы, қауіптің алдын алу журналдарынан) корреляциясын қамтамасыз етуі керек

40. Жүйе белгісіз SQL Injection шабуылдарын, соның ішінде нөлдік күндік шабуылдарды, мінез — құлық талдауын, эвристиканы және машиналық оқытуды қолдана отырып, қолтаңбаларға тәуелді болмай-ақ анықтауға және бұғаттауға мүмкіндік беруі керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

41. Брандмауэр мінез-құлықты талдау және қалыпты әрекеттен ауытқу арқылы қолданба трафигі арқылы зиянды кодты енгізу әрекеттерін анықтау арқылы кодты енгізу түріндегі белгісіз шабуылдардан қорғау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

42. Жүйе осалдықтан қорғау профильдері арқылы транскрипцияланбаған трафикте рұқсат етілмеген постквантты алгоритмдерді (PQC) бұғаттау мүмкіндігін қамтамасыз етуі керек. Транскрипцияланатын трафик үшін тек нақты көрсетілген шифрларға рұқсат беретін және басқалардың барлығын блоктайтын шифрды ашу профилі қолданылуы керек

43. Жүйе ресурстар санатына байланысты Интернет желісіндегі ресурстарға сұраныстарды анықтау және сүзу мүмкіндігін ұсынуы керек, мысалы, зиянды сайттар, әлеуметтік желілер, жарнамалық ресурстар және т. б. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

44. Жүйе әрекеттерді қолдау мүмкіндігін қамтамасыз етуі керек: рұқсат беру, хабарлау, бұғаттау, пайдаланушының растауын сұрау, web-ресурстарға кірген кезде пайдаланушының құпия сөзін сұрау.

45. Жүйе қауіп-қатерге жауап беру уақытын азайту үшін машиналық оқыту технологиясын қолдану арқылы URL сүзу мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

46. Брандмауэрдің функционалдығы маскировка, жалған CAPTCHA және HTML таңбаларын кодтау сияқты жалтару әдістерінен қорғану мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

47. Брандмауэр веб-сайттарды мазмұнға, мүмкіндіктерге және қауіпсіздікке қарай жіктеуге мүмкіндік беруі керек және 70-тен астам қауіпсіз және зиянды мазмұн санаттарын қамтуы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

48. Жүйе рискal мекенжайларын тәуекелді анықтау үшін әртүрлі факторлар бойынша бағалайтын тәуекел рейтингін сақтауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

49. Шешім гибl мекенжайын төрт санатқа бөлетін бірнеше санаттарға қолдау көрсетуі керек, бұл икемді саясатты қолдануға және теңшелетін санаттарды жасауға мүмкіндік береді. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

50. Жүйе пайдаланушының іздеу нәтижелерінде қажетсіз мазмұнның пайда болуын болдырмау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

51. Брандмауэр қауіпсіздік саясаты бұзылған жағдайда Пайдаланушыға хабарлау арқылы теңшелетін құлыптау бетін көрсетуді қолдауы керек.

52. Брандмауэр URL мекенжайын талдау және сүзу мүмкіндігін, соның ішінде веб-беттерде зиянды JavaScript-ті анықтауды қамтамасыз етуі керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

53. Жүйе CAPTCHA қолдану арқылы автоматты талдауды айналып өту механизмдерін пайдаланатын зиянды және фишингтік веб-беттерді анықтау және бұғаттау мүмкіндігін қамтамасыз етуі керек (соның ішінде Google reCAPTCHA сияқты заңды қызметтер, сондай-ақ жалған немесе теңшелетін CAPTCHA интерфейстері). Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

54. Жүйе SNICAT типті айналып өту әдістеріне қарсы тұру үшін HTTP сұрауында URL мекенжайымен бір уақытта TLS Hello да SNI талдау мүмкіндігін қамтамасыз етуі керек;

55. Жүйе күдікті DNS сұрауларын талдау мүмкіндігін қолдауы керек, DGA домендері және вирус жұққан станцияларды DNS sinkhole технологиясымен оқшаулау (DNS серверінің жауабын ауыстыру). Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

56. Жүйе DGA машиналық генерацияланған домендік атауларын, соның ішінде N-Gram жиілік талдауын, энтропияны, сұрау жиілігін талдауды, DNS ішіндегі туннельдерді, DNS сұрау құралдарымен деректерді беру арналарын, соның ішінде ультра баяу DNS туннельдерін пайдалануға тырысатын DNS сұрауларын пайдалану арқылы қорғаныс құралдарын айналып өту әдістерін анықтау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

57. Жүйе DGA домендерін, сөздікте жасалған DGA домендерін, DNS-rebinding, FastFlux айналып өту әдістерін, ілулі DNS жазбаларын, nsnx шабуылдарын, жаңадан тіркелген домендердің с шабуылдарын бұғаттау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

58. Жүйе қауіп-қатерге жауап беру уақытын азайту үшін машиналық оқыту технологиясын қолдана отырып, күдікті DNS сұрауларын талдау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

59. Брандмауэр функциясы белгілі зиянды доменге арналған DNS сұрауына жалған жауап беру мүмкіндігін қолдауы керек және бұл зиянды домен атауын вирус жұққан хосттарды анықтау үшін клиентке берілген анықталатын IP мекенжайына түрлендіруі керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

60. Жүйе зиянды бағдарламалар мен басқа деректерді клиент-сервер моделі арқылы туннельдеу үшін DNS протоколын қолданатын DNS туннелінің қолданылуын болдырмауға мүмкіндік беруі керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

61. Жүйе туннельденген деректер мен эксплуатацияларды бірнеше домендерге тарататын және деректерді анықтауды, ұрлауды немесе желіге қосымша зиянды пайдалы Деректерді жіберуді болдырмау үшін өте төмен жылдамдықты пайдаланатын ультра төмен/баяу DNS туннельдерін бұзу мүмкіндігін қолдауы керек.

62. Жүйе жылдам ағынды домендердің алдын алу мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

63. Жүйе авторитативті домендердің бұзылған DNS аймақтарына жасырын қосылған домендерден қорғау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

64. Жүйе интернеттен кәсіпорын желісіндегі қызметтерге бүйірден жылжу және шабуыл жасау үшін пайдалануға болатын DNS қайта байланыстыру шабуылының алдын алу мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

65. Жүйе DNS сұрауларының немесе жауаптарының бағытын өзгерту нәтижесінде DNS hijacking типті шабуылдарды анықтау және болдырмау — IP мекенжайларын ауыстыру мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

66. Жүйе DNS сұрауларын (DNS Request) және DNS жауаптарын (DNS Response) нақты уақыт режимінде тексеру мүмкіндігін қолдауы керек. Бұл функция зиянды белсенділікті анықтау және зиянды домендерге кірудің алдын алу үшін қажет. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

67. Жүйе жалтару техникасынан қорғау мүмкіндігін қолдауы керек (evasions), мысал MPTCP;

68. Жүйе қолтаңбаға тәуелді емес шабуылдарды анықтауға және алдын алуға мүмкіндік беретін Машиналық оқыту механизмдерін қолдану арқылы бұрын белгісіз қауіптерден жедел қорғаныс мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

69. Жүйе белгісіз ықтимал зиянды файлдарды сканерлеу қызметін Microsoft Windows, Linux операциялық жүйелерімен бірге құжаттарды іске қосу және қарау арқылы эмуляциялау арқылы құм жәшігінде пайдалану мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

70. Құм жәшігі күдікті орындалатын файлдарды (соның ішінде EXE, DLL, SCR, BAT, және т.б.), elf файлдарын, PDF, MS Office 2003, 2007 және одан жоғары форматтағы құжаттарды, Java және Flash, Android APK, Mach-O, DMG және PKG, RAR, ZIP, 7Zip мұрағаттарын тексеруі керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

71. Жүйе http, HTTP, SMTP, POP3, IMAP, SMB, FTP қосымшаларында жіберілген күдікті файлдарды, сондай-ақ егер олар бар болса, оларды SSL арқылы іске асыруды құмсалғышқа жіберу мүмкіндігін қолдауы керек.

72. Құм жәшігі файлды тексеру туралы есепті жасап, брандмауэрге жіберуі керек.

73. Жүйе жасырын бақылау, автоматты түрде орауыштан шығару, тәуелділікті эмуляциялау, зиянды бағдарламаларды басып шығару және жұмыс уақытында жадыны іздеу арқылы жоғары жалтару зиянды бағдарламалардың алдын алу мүмкіндігін қолдауы керек.

74. Құм жәшігі файлды тексеруге алғаннан кейін 5 минут ішінде тізімделген қолданбалардағы компанияның барлық брандмауэрлерінде пайдалану үшін нөлдік күнді блоктау үшін қолтаңбалар жасауы керек.

75. Жүйе құмсалғыштан файлдардың қолтаңбасын алу мүмкіндігін қолдауы керек және бұлтты немесе жергілікті құмсалғыштан алынған жаңа қолтаңбалар бойынша құлыптау қозғалтқышы болуы керек.

76. Бұлтты құмсалғышта барлық тұтынушылар арасында қолтаңба алмасу мүмкіндігі болуы керек.

77. Жүйе құм жәшігінен зиянды кодты пайдаланатын IP, URL, DNS компаға келу индикаторларын алу мүмкіндігін қолдауы керек және зиянды Индикаторлар тізімі бойынша қосылымдарды блоктауы керек.

78. Құм жәшігі SMTP/ POP3 хаттамалары арқылы электрондық поштадағы http:// және https:/ / сілтемелерін тексеруі керек.

79. Құм жәшігі SSL шифрланған қосымшалардағы файлдарды HTTPS протоколында минимуммен тексеруі керек.

80. Құм жәшігі күдікті файлды тексерудің кешігуін азайту үшін нөлдік күндік қауіптерді тексеру кезінде машиналық оқытуды қолдануы керек;

81. Құмсалғыш жеке немесе сыртқы бұлттағы ("құмсалғыш") күдікті файлдар мен сілтемелердің әрекетін талдауды, жаңа зиянды бағдарламаны анықтауды және 5 минут ішінде антивирустық қолтаңбаны автоматты түрде генерациялауды және тиісті жазылымдары бар тапсырыс берушінің барлық құрылғыларына Орнатылатын URL мекенжайының бедел базасын 30 минут ішінде жаңартуды қамтамасыз етуі тиіс;

82. Жүйе Тапсырыс берушінің орталық объектісінде (жеке бұлт) орналастырылатын және 5 минут ішінде Тапсырыс берушінің деректер орталығының алаңында жергілікті бөлінген аппараттық құрылғыда антивирустық қолтаңбаны автоматты түрде жасауға мүмкіндік беретін сол өндірушінің арнайы аппараттық құрылғысының (құмсалғыштың) негізінде іске асырылған "нөлдік" күннің қауіптерін анықтаудың ішкі жүйесімен интеграциялау мүмкіндігін қолдауы тиіс.;

83. Жабдық өндірушісінің жергілікті құм жәшігін пайдаланған кезде, ол брандмауэрлерден де, үшінші тарап қызметтерінен де файлдарды тексеруге қабылдау үшін API болуы керек.

84. Құм жәшігі тексерулер бойынша есептер шығаруы және осы есептерді PDF форматында көре алуы керек.

85. Бұлтты құмсалғыш операциялық жүйенің эмуляциясын қолданбай Bare metal analysis технологиясын қолдануы керек.

86. Жүйе әр түрлі файл түрлерін әр түрлі құм жәшіктеріне жіберу мүмкіндігін қолдауы керек, мысалы exe файлдары бұлтты құмсалғышқа, ал DOC файлдары жергілікті құмсалғышқа.

87. Бұлтты құм жәшігі жазылым болмаған кезде де PE файлдарын тексеруге қабылдауы керек.

88. Жүйе интернет заттарының құрылғыларын анықтау мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

89. Жүйе желідегі құрылғыларды MAC мекенжайын, IP мекенжайын, операциялық жүйені, құрылғы түрін және басқа параметрлерді қоса алғанда, осы деректерге негізделген ақпараттық қауіпсіздік саясаттарын кейіннен қолдану мүмкіндігімен сәйкестендіру мүмкіндігін қолдауы керек. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

90. Жүйе жетілдірілген визуализация функцияларын қамтамасыз етуі керек: қарапайым және ыңғайлы оқылатын форматтағы желілік қосымшалардың белсенділігі, пайдаланушылардың қосымшаларын қолданатын анықталған және бұғатталған желілік қауіптер. Әр түрлі сүзгілерді қолдана отырып, ақпаратты сүзу мүмкіндігі (қолданбалар, қауіптер, пайдаланушылар, IP мекенжайлары, TCP/UDP порттары, қауіпсіздік аймақтары, қауіп түрлері және т. б.);

91. Жүйе бір сессия шеңберінде жасалған әр түрлі типтегі журналдарды (брандмауэр, қауіп-қатерден қорғау, файлдарды жіберуді бақылау, URL-сүзу) автоматты түрде корреляциялау мүмкіндігін қолдауы керек;

92. Жүйе жаңартылатын корреляциялық объектілер арқылы ЭМ-дегі ақпараттық қауіпсіздік оқиғаларын автоматты түрде корреляциялау мүмкіндігін қолдауы керек, олар антивирустық қорғаудан, шпиондық бағдарламадан, осалдықтар мен желілік шабуылдардан қорғаудан, желі деңгейінде және жұмыс станцияларында 0 күндік қауіптер мен вирустардан қорғаудан алынған ақпаратты екі факторлы пайдаланушының аутентификациясын мәжбүрлеу мүмкіндігімен пайдаланады корреляциялық объект жұмыс істеген аутентификация (МФА);

93. Жүйе келесі көп факторлы аутентификация провайдерлерін Multi-Factor Authentication (MFA) (тікелей, аралық өнімдерді пайдаланбай)пайдалану мүмкіндігін қолдауы керек:

Duo,

Okta,

RSA SecureID,

PingID

94. Жүйе көп факторлы аутентификацияны ішкі қосымшаларға мәжбүрлеп қолдану мүмкіндігін қолдауы керек;

95. Жүйе ad интеграциясы, есептік жазбаларды сенімсіз қауіпсіздік аймағына жіберу мониторингі, екі факторлы аутентификация (МФА)көмегімен пайдаланушының мәжбүрлі аутентификациясы есебінен пайдаланушылардың логиндері мен парольдерін ұрлаудан қорғау мүмкіндігін қолдауы тиіс;

96. Жүйе құрылғының ақпараты мен атрибуттарын жинау және есеп беру арқылы хост ақпаратын тексеру (HIP) функциясын ұсыну мүмкіндігін қолдауы керек. Басқарылатын/басқарылмайтын

сертификаттар күйіне, ОЖ түріне, клиент нұсқасына, хост атауына, хост идентификаторына, сериялық нөмірге, ұялы телефон моделіне, телефон нөміріне, Root/Jailbreak күйіне, құпия сөздің болуына, орнатылған қолданбаларға негізделген хост ақпаратын профильдеу атрибуттары., өрт сөндіру агентінің болуы және күйі, зиянды бағдарламалардан қорғау агентінің болуы және күйі, дискінің сақтық көшірме агентінің болуы және күйі, дискіні шифрлау агентінің болуы және күйі, DLP агентінің болуы және күйі, процестер тізімінің болуы және күйі, тізілім кілтінің болуы және күйі, Plist болуы және күйі. Бұл функция тиісті жазылымды пайдалану кезінде қол жетімді болуы керек;

97. Жүйе dos шабуылдарынан қорғау функционалын пайдалану мүмкіндігін қолдауы керек;

98. Жүйе өнімділіктің деградациясынсыз барлық 100% IPS қолтаңбаларын, антивирусты, сүзгілеу URL мекен-жайларын, қолданбаларды басқаруды және Threat Intelligence қосу мүмкіндігін қолдауы керек;

99. Жүйе портты сканерлеудің ICMP/TCP/UDP блоктау функционалын пайдалану мүмкіндігін қолдауы керек;

100. Жүйе осындай файлдарды тасымалдауды бұғаттай отырып, маңызды ақпаратты қамтитын желі арқылы берілетін файлдардағы объектілерді анықтау мүмкіндігін қолдауы тиіс;

101. Жүйе желі арқылы берілетін файлдарда сүзілетін деректердің болуын анықтау мүмкіндігін қолдауы керек, бірақ онымен шектелмейді:

Adobe PDF,

HTML,

Microsoft Office (Excel, Word, PowerPoint),

Rich Text Format

102. Жүйе тұрақты өрнектер негізінде жеке деректер шаблондарын құру мүмкіндігін қолдауы керек;

103. Жүйе әртүрлі тақырыптар бойынша есептер мен кесте бойынша есептерді (анықталған қауіптер, пайдаланушылар, қосымшалар және т.б. бойынша бөлінген берілген ақпарат көлемі), жасалатын есептерді қолмен баптау бойынша функцияларды автоматты түрде жасау мүмкіндігін қолдауы тиіс. Есептерді брандмауэрдің графикалық веб-басқару интерфейсі (GUI) арқылы да, есептерді PDF және CSV форматтарына экспорттау мүмкіндігі де болуы керек;

104. Жүйе орталықтандырылған басқару, логтау, есеп беру, сол өндірушінің брандмауэрлерін жаңарту ішкі жүйесімен интеграциялау мүмкіндігін қолдауы керек;

105. Жүйе SD-WAN функционалдығын орталықтандырылған басқару консолі арқылы теңшеу мүмкіндігін қолдауы керек;

106. Жүйе тиісті лицензияны орнатқан кезде сыртқы құрылғыларға шифрланған SSL трафигін жіберу функционалын пайдалану мүмкіндігін қолдауы керек;

107. Жүйе Сыртқы құрылғылардан трафикті алу функционалдығын пайдалану мүмкіндігін қолдауы керек және шифрлау ішінде SSL Интернет арқылы тасымалдау үшін туннель;

108. Жүйе SaaS типті қосымшалар бойынша жеке есеп құру мүмкіндігін қолдауы керек;

109. Жүйе IPSec VPN функционалдығын қолдауы керек;

110. Жүйе RFC 8784, RFC 9242, RFC 9370 стандарттарын іске асыра отырып, кванттық есептеулерді қолдана отырып шабуылдардан қорғалған алгоритмдерге негізделген кванттық тұрақты криптографияны (Quantum-Resistant Cryptography) пайдалану мүмкіндігі бар IPsec туннельдерін қолдауы керек.

111. Жүйе syslog протоколы бойынша үшінші тарап SIEM/SIM жүйелерімен интеграциялау мүмкіндігін қолдауы керек, бұл лог форматының икемді конфигурациясын қамтамасыз етеді;

112. Жүйе ағымдағы конфигурацияны үміткер конфигурациясымен салыстыру арқылы конфигурация аудитінің мүмкіндігін қолдауы керек.

113. Жүйе белгілі бір пайдаланушылардан өзгерістерді жылдам қайтару және конфигурацияларды қалпына келтіру мүмкіндігін қолдауы керек;

114. Жүйе рөлдік мүмкіндікті қолдауы керек жергілікті әкімшілерге қол жеткізуді басқару:

Бұл жалпы құрылғы деңгейінде, сондай-ақ жеке виртуалды жүйелерде (контексттерде)көру және басқару аймағын шектеу мүмкіндігі;

Өңдеу режимінде немесе тек оқуға рұқсат беру немесе IE веб-интерфейсінің кез келген бөліміне кіруге тыйым салу мүмкіндігі;

Өңдеу режимінде немесе тек оқуға рұқсат беру немесе CLI me-ге кіруге тыйым салу мүмкіндігі.

115. Жүйе толық жүктелген жағдайда да құрылғыны үздіксіз басқаруға мүмкіндік беретін арнайы аппараттық платформаға ие болуы керек. Бақыланатын трафикті өңдеу үшін және басқару мәселелерін шешу үшін бөлек есептеу ресурстары қамтамасыз етілуі керек.

116. Әрбір жеке құрылғыны басқару https және SSH хаттамалары бойынша әкімшінің жұмыс станциясына Қосымша басқару бағдарламасын орнатпай-ақ жүзеге асырылуы керек.

117. Брандмауэрді басқару интерфейсі (веб және CLI) орталықтандырылған басқару, логтау, есеп беру, бағдарламалық жасақтаманы жаңарту ішкі жүйесімен біріктірілуі керек.

118. Жүйе келесі протоколдар мен брандмауэр режимдерін қолдауы керек:

118.1. Статикалық маршруттау және динамикалық маршруттау хаттамалары BGP, OSPF, RIP;

118.2. Қосылатын коммутациялық жабдықтың SPAN-порттарынан "шағылысқан" трафикті тыңдау режимдерінде, MAC және IP-мекенжайларын өзгертпестен мөлдір режимде, трафикті коммутациялау режимінде (Layer 2), трафикті бағыттау режимінде (Layer 3)желілік интерфейстердің жұмысы;

118.3. Әр түрлі желілік интерфейстердің кез келген тізімделген режимдерде кез келген комбинацияда шектеусіз бір уақытта жұмыс істеуі;

118.4. IPv6, соның ішінде қолданбалар мен пайдаланушыларды анықтау;

118.5. Multicast – PIM-SM, PIM-SSM, IGMP v1, v2, v3;

118.6. Брандмауэрде ұйымдастырылған VLAN арасындағы маршруттау;

118.7. NAT, DHCP сервері және DHCP relay мекен-жайларын аудару функциясы;

118.8. 802.1 Q бойынша кадрларды тегтеу (кемінде 4094 VLAN);

118.9. 802.3 ad интерфейстерін біріктіру (lacp қолдауы);

118.10. Үлкен пакеттерді беру (Jumbo frames);

2.11. Брандмауэр саны 1 дана:

2.11.1.Брандмауэр өнімділігінің қажетті параметрлері:

1. Қолданбалар мен пайдаланушыларды сәйкестендіруді қамтамасыз ете отырып, брандмауэр режимінде әрбір құрылғының өндіруші декларациялайтын өткізу қабілеті – кемінде 8,5 Гбит/сек.;

2. Трафикті қауіп-қатердің бар-жоғын тексеру функционалы қосылған қосымшалар мен пайдаланушыларды сәйкестендіруді қамтамасыз ете отырып, (IPS, зиянды бағдарлама және anti-spyware осалдықтарының барлық қолтаңбалары) желіаралық экрандау режимінде құрылғының өндіруші декларациялайтын өткізу қабілеті-кемінде 4,5 Гбит\с/сек;

3. Өндіруші жариялаған IPSec VPN өткізу қабілеті-кемінде 4,1 Гбит/сек;

4. Қолданба деңгейіндегі қолдау көрсетілетін сеанстардың ең көп саны-кемінде 945 000

5. Қолданба деңгейіндегі жаңа қолдау көрсетілетін сеанстар саны-кемінде 100 000

2.11.2. Брандмауэрдің желілік интерфейстеріне қойылатын талаптар:

RJ-45 қосқышы бар 1/100/1000 Ethernet-кемінде 8 порт;

RJ-45/PoE коннекторы бар 1/2. 5/5 Гбит\с Ethernet-кемінде 4 порт;

SFP қосқышы бар 1 Гбит\с-кемінде 6 порт;

SFP + қосқышы бар 10 Гбит\с-кемінде 4 порт;

RJ-45 қосқышы бар 10/100/1000 Мбит Ethernet арнайы брандмауэрді басқару порты-кемінде 1 порт;

RJ-45 коннекторы бар консольді басқару порты-кемінде 1 порт;

USB Micro коннекторы бар консольді басқару порты-кемінде 1 порт;

Брандмауэр желіге қосу үшін барлық қажетті кабельдермен жабдықталуы керек.

Жинаққа бағдарламалық жасақтаманың барлық мүмкін жаңартуларын, қосымшалар мен қауіп-қатерлердің қолтаңбаларын, URL бедел базасын, DNS сұраныстарын, "нөлдік" қауіпті анықтау қызметін, SD-WAN қызметтерін және IOT құрылғыларын қорғау қызметін 1 жыл ішінде пайдалану үшін барлық қажетті лицензиялар мен жазылымдар кіруі керек.

Аппараттық брандмауэрге өндірушіден кемінде 1 жылға техникалық қолдау көрсетілуі керек.

Сондай-ақ, жеткізілім жиынтығына мыналар кіруі керек:

SFP модулі 1Gb SR-2 дана

SFP + 10GB SR модулі-2 дана

2.12. Қосымша талаптар:

2.12.1. Жеткізу тапсырыс берушінің атына бір мезгілде және толық көлемде орындалуы тиіс;

2.12.2. Жеткізілетін жабдықтың құны тауарды жеткізуге және тасымалдауға байланысты барлық шығындарды қамтиды;

2.12.3. Жабдық жаңа болуы керек. Жеткізу зауыттық құрастырумен және барлық компоненттерді алдын ала орнатумен жүзеге асырылуы керек. Жеткізу жиынтығы зауыттың толық жиынтығына сәйкес келуі керек және өндірушінің ресми кепілдігімен бірге жүруі керек;

2.12.4 кепілдік кезеңі және NGFW-ге техникалық қолдау кемінде 12 ай, кешеннің қалған бөліктеріне кемінде 36 ай. Қазақстан Республикасының аумағында сервистік орталықтардың болуы;

2.12.5 Тапсырыс беруші жеткізуші есебінен техникалық ерекшелік талаптарына сәйкестігі тұрғысынан жеткізілетін жабдыққа сараптама жүргізу құқығын өзіне қалдырады;

2.12.6 жабдықтың толық техникалық үйлесімділігін және дұрыс жұмыс істеуін қамтамасыз ету мақсатында шарт шеңберінде жеткізілетін барлық жабдық бір өндіруші болуға тиіс;

2.12.7 өнім беруші шартқа қол қойылған күннен бастап 5 (бес) жұмыс күні ішінде:

- өндірушінің ресми интернет-ресурсында орналастырылған ақпаратпен салыстыру арқылы жеткізілетін Жабдықтың техникалық ерекшелік талаптарына сәйкестігін растау үшін әрбір позиция бойынша өндірушіні, модельді және өнім кодын (Part Number) көрсете отырып, техникалық ерекшелік талаптарына сәйкес жеткізуге ұсынылатын жабдық туралы ақпарат;

- жеткізушінің Қазақстан Республикасының аумағында ұсынылатын жабдықты жеткізуге құқығын растайтын өндірушінің не оның ресми өкілдігінің авторизациялық хаты;

- Қазақстан Республикасының аумағында сервис орталықтарының болуы туралы өндірушіден/Лейден хат.

3. Техникалық стандарттар

№ р/с	ҚР тіркелген	Белгіленуі	Құжат нөмірі	Санаты	Атауы	Қолдану саласы	Әзірлеуші	Беттер	МКС	Мәртебесі	Бұйрық	Енгізу күні бастап	К б
1	Иә	СТ РК ISO 20648-2019	420444	Қазақстан Республикасының ұлттық стандарты	Информационная технология СПЕЦИФИКАЦИЯ TLS ДЛЯ СИСТЕМ ХРАНЕНИЯ	Настоящий стандарт устанавливает требования использования протокола безопасности транспортного уровня (TLS) вместе с	АО "Национальный инфокоммуникационный Холдинг "Зерде" (-)	46	Защита от преступлений	Действует	Приказом Председателя Комитета технического регулированию и метрологии Министерства по инвестициям и развитию Республ	01.01.2021	

					ДАННЫХ	технологиями хранения данных				ики Казахстан от 24 декабря 2019 года № 479-од		
2	Иә	СТ РК ISO/IEC 30134–5-2019	420332	Қазақстан Республикасының ұлттық стандарты	Информационные технологии. Центры обработки данных Ключевые показатели эффективности. Часть 5. Использование IT-оборудования для серверов (ITEUsv)	Настоящий стандарт определяет использование IT-оборудования для серверов (ITEUsv) в качестве ключевого показателя производительности (KPI) для количественной оценки использования серверов в центре обработки данных	АО "Национальный инфокоммуникационный Холдинг "Зерде" (-)	28	Наборы знаков и кодирование информации	Действует		01.01.2021

Қол қойған Изгалиев Аскар Алмасович

Қол қойылған күні 16.10.2026

Құжат «Самұрық-Қазына» АҚ сатып алу веб-порталымен құрылған
Документ сформирован веб-порталом закупок АО «Самрук-Қазына»

ТЕХНИЧЕСКАЯ СПЕЦИФИКАЦИЯ

по закупке 1262177
способом Открытый тендер

Лот № 1 (26-2 Т, 4556012) Комплекс программно-аппаратный

Заказчик: Товарищество с ограниченной ответственностью "QAZAQGAZ PROCESSING"
Организатор: Акционерное общество "Национальная компания "QazaqGaz"

1. Краткое описание ТРУ

Наименование	**Значение**
Номер строки	26-2 Т
Наименование и краткая характеристика	Комплекс программно-аппаратный, для обновления и ремонта программно-аппаратных комплексов серверных и телекоммуникационных платформ
Наименование категории ОКТРУ	Комплекты ремонтные для программно-аппаратных комплексов
Дополнительная характеристика	-
Количество	1.000
Единица измерения	Комплект
Место поставки	КАЗАХСТАН, г.Астана, район "Есиль", ул. Родниковая, 1/1
Условия поставки	DDP
Срок поставки	С даты подписания договора в течение 45 календарных дней
Условия оплаты	Предоплата - 0%, Промежуточный платеж - 0%, Окончательный платеж - 100%

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

2.1. Общие требования к поставке

2.1.1. Комплекс программно-аппаратный предназначен для обеспечения функционирования информационных систем.

2.1.2. Предмет поставки:

Поставка, монтаж, настройка, ввод в эксплуатацию и гарантийно-сервисное сопровождение комплекса, включающего систему хранения данных, серверы, коммутаторы ядра и доступа, точки беспроводного доступа, программное обеспечение виртуализации, межсетевой экран нового поколения (NGFW), лицензии, подписки, оптические модули, кабели и услуги, указанные в настоящей технической спецификации.

2.1.3. Унификация производителей и исключение для NGFW:

Система хранения данных, серверы, средства управления серверами, коммутаторы ядра и доступа, точки беспроводного доступа, сетевые операционные системы, программное обеспечение виртуализации, оптические трансиверы и кабели для указанного оборудования, сервисные контракты и техническая поддержка инфраструктурной части должны поставляться под единой торговой маркой и сопровождаться одним производителем. NGFW, включая его операционную систему, лицензии, подписки, оптические модули и техническую поддержку, допускается предлагать от отдельного специализированного производителя. В поставке допускается не более двух производителей основных решений: один для всей инфраструктурной части и один для NGFW. Объединение самостоятельных платформ разных производителей внутри инфраструктурной части либо внутри подсистемы NGFW не допускается. OEM-компоненты сторонних производителей допускаются только при заводской интеграции, наличии продуктового кода производителя оборудования и полном покрытии его гарантией и поддержкой.

2.1.4. Обоснование унификации:

Унификация инфраструктурной части, за исключением NGFW, необходима для обеспечения заводской совместимости, единой матрицы версий, сквозной диагностики, централизованного управления жизненным циклом и единой ответственности за устранение инцидентов. NGFW является самостоятельным классом средств сетевой безопасности и может поставляться отдельным производителем. Поставщик отвечает за интеграцию инфраструктурной части и NGFW в единый работоспособный комплекс.

2.1.5. Заводская поставка:

Оборудование должно быть новым, ранее не использованным, не восстановленным, не демонстрационным и не снятым с производства на дату подачи заявки. Все компоненты должны быть собраны, интегрированы и протестированы на заводе соответствующего производителя либо поставляться в виде официально поддерживаемых заводских опций. Серийные номера должны регистрироваться в системе поддержки соответствующего производителя.

2.1.6. Техническая поддержка и координация обращений:

По инфраструктурной части обращения должны регистрироваться через единый портал и центр поддержки ее производителя. Для NGFW допускается отдельный портал и центр поддержки производителя NGFW. Поставщик выступает единым координационным окном по договору и самостоятельно организует взаимодействие производителей при сквозном инциденте, не требуя от Заказчика предварительно определять первопричину..

2.1.7. Подтверждение соответствия:

Участник предоставляет детальную спецификацию с наименованиями, количеством и продуктовыми кодами всех аппаратных компонентов, лицензий, подписок и сервисов, включая NGFW. Для каждого существенного требования приводятся ссылки на официальные документы либо письма соответствующего производителя. Материалы участника без подтверждения производителя не являются достаточным доказательством.

2.1.8. Совместимость:

Единый производитель инфраструктурной части должен подтвердить совместимость серверов, системы хранения, проводной и беспроводной сети и программного обеспечения виртуализации единой матрицей, архитектурным документом или проектным письмом. Производитель NGFW подтверждает поддержку заявленных интерфейсов, сетевых режимов и оптических модулей своей подсистемы. Поставщик предоставляет общую схему интеграции. Все версии должны находиться в официальной поддержке соответствующих производителей на дату ввода в эксплуатацию.

2.1.9. Лицензирование:

Все лицензии и подписки должны быть оригинальными, зарегистрированными на Заказчика и поставляться через официальные каналы соответствующих производителей. Не допускаются пробные, демонстрационные, NFR, Community/Free и иные редакции с неуказанными ограничениями. Срок подписок и программной поддержки инфраструктурной части - не менее 36 месяцев. Срок лицензий, подписок и поддержки NGFW определяется отдельным разделом. Для программного обеспечения виртуализации участник отдельно подтверждает покрытие 4 физических сокетов и суммарно не менее 344 физических ядер.

2.1.10. Комплектность:

В стоимость должны быть включены все необходимые лицензии, блоки питания, вентиляторы, крепления, салазки, монтажные комплекты, кабели питания C13-C14, оптические модули, кабели прямого соединения и иные компоненты, необходимые для полной работоспособности заявленного решения.

2.1.11. Монтаж и ввод в эксплуатацию:

Монтаж, пусконаладка и первичная настройка выполняются инженерами, имеющими действующие сертификаты соответствующих производителей по выполняемым направлениям. По завершении предоставляются исполнительная документация, схема подключения, резервные

копии конфигураций, перечень серийных номеров, отчет о тестировании и акт ввода в эксплуатацию.

2.1.12. Регистрация активов и сервисов:

Серийные номера, лицензии, подписки и сервисные контракты инфраструктурной части должны быть зарегистрированы на Заказчика в едином портале ее производителя. NGFW, его лицензии, подписки и поддержка регистрируются на Заказчика в официальном портале производителя NGFW. Порталы должны отображать сроки гарантий и сервисов, уровень поддержки, историю обращений, статус замены и доступные обновления.

2.1.13. Проектные спецификации производителей:

В составе заявки предоставляются официальная проектная спецификация инфраструктурной части и отдельная официальная спецификация NGFW с базовыми изделиями, опциями, лицензиями, подписками и сервисами. Документы должны позволять проверить комплектность и поддерживаемость сочетаний компонентов. Если обе части предлагаются одним производителем, допускается единый документ, явно охватывающий весь состав.

2.1.14. Жизненный цикл продукции:

Предлагаемые модели не должны иметь объявленной даты окончания продаж на момент подачи заявки. Каждый соответствующий производитель должен подтвердить возможность получения обновлений безопасности, запасных частей и технической поддержки на весь заявленный срок обслуживания. Замена на модель с иным жизненным циклом допускается только с письменного согласия Заказчика.

2.1.15. Безопасность цепочки поставки и программного обеспечения:

Каждый производитель основной поставляемой платформы должен применять цифровую подпись микрокодов и программных пакетов, защищенную загрузку и процесс управления уязвимостями. По запросу Заказчика предоставляются уведомления безопасности, перечень исправленных уязвимостей и программный состав поставляемых компонентов (SBOM либо эквивалентный документ), если он выпускается соответствующим производителем.

2.1.16. Матрица регистрации и эскалации:

Производитель инфраструктурной части предоставляет единую схему регистрации и эскалации по хранению, серверам, проводной и беспроводной сети и виртуализации; производитель NGFW - отдельную схему по межсетевому экрану, лицензиям и подпискам. Поставщик передает Заказчику консолидированную матрицу контактов и остается единым ответственным лицом по договору.

2.1.17. Исключение составных OEM-решений:

Инфраструктурная часть не должна формироваться из переименованных OEM-устройств разных исходных производителей, поддерживаемых через разрозненные порталы и договоры. Все ее основные категории должны быть официально представлены в каталоге единого производителя и иметь его продуктовые коды, документацию и сервисное покрытие. Исключение допускается только для самостоятельной подсистемы NGFW, причем аппаратная платформа, операционная система, лицензии, подписки, оптика и поддержка NGFW должны относиться к одному производителю. Исключение не распространяется на серверы, системы хранения, коммутаторы, точки доступа и программное обеспечение виртуализации.

2.2. Комплект должен состоять из:

1) **Масштабируемая All-Flash NVMe система хранения данных – 1 комплект:**

В состав комплекта входит: 2 контроллерных узла по 16 ядер; 10 × 7,68 ТБ NVMe SED; 8 × 25Гбит \с SR; программное обеспечение, шифрование, 3-летняя поддержка, монтаж и обучение.

2) **Двухпроцессорный сервер 1U - 2 штуки:**

В каждом сервере: 2 × 86-ядерных процессора; 768 ГБ DDR5-6400; аппаратно защищенное загрузочное устройство 2 × 480 ГБ NVMe RAID1; 2 × 25 Гбит\с, 4 × 1 Гбит\с; расширенное удаленное управление и 3-летняя платформа управления.

3) **Коммутатор ядра/центра обработки данных - 2 штуки:**

28 × 1/10/25 Гбит\с SFP28 и 4 × 10/25 Гбит\с SFP28 с аппаратным шифрованием каналов; 4 × 40 /100 Гбит\с QSFP28; поддержка до 14 портов 50 Гбит\с; отказоустойчивая active-active пара; 2 блока питания; 3 вентилятора; 3-летняя поддержка.

4) **Коммутатор доступа PoE - 6 штук:**

48 × 1 Гбит\с PoE+; 4 × 1/10 Гбит\с SFP+; бюджет PoE 370 Вт; объединение до 6 устройств в единый стек; 3-летняя поддержка.

5) **Точка беспроводного доступа Wi-Fi 6E - 10 штук:**

Три одновременно работающих радиомодуля 2,4/5/6 ГГц; 2×2 MIMO; два порта 2,5 Гбит\с; внутренние антенны; монтажные комплекты; 3-летняя поддержка.

6) **Оптические модули и кабели для коммутаторов ядра – не менее 1 комплекта:**

В состав комплекта входит: 8 × 1ГбЕ SX; 8 × 10 Гбит\с SR; 32 × 25 Гбит\с SR; 2 × 100 Гбит\с DAC длиной 1 м. Все компоненты - официальные опции производителя сетевого оборудования.

7) **Программное обеспечение виртуализации - Не менее 4 лицензий по числу физических процессорных сокетов; совокупное покрытие - не менее 344 физических ядер:**

Подписка на 3 года. Каждая единица лицензирования должна покрывать один физический процессорный сокет без ограничения количества ядер; KVM-гипервизор и единое управление KVM/VMware; техническая поддержка уровня 24x7.

8) **Межсетевой экран нового поколения (NGFW) - 1 штука:**

Аппаратная платформа NGFW; все лицензии и подписки, предусмотренные отдельным разделом, сроком 1 год; техническая поддержка производителя сроком 1 год; 2 × 1Гбит\сЕ SR и 2 × 10Гбит\с Е SR; комплект кабелей и монтажных принадлежностей согласно требованиям раздела NGFW.

Количество и состав по пункту 2.2. Технической спецификации являются минимальными. Поставщик обязан включить дополнительные компоненты, если без них невозможно обеспечить заявленную функциональность, не уменьшая указанные характеристики.

2.3. Требования к масштабируемой All-Flash NVMe система хранения данных в количестве 1 комплекта:

2.3.1. Назначение и форм-фактор:

Система хранения данных корпоративного класса для критичных рабочих нагрузок, выполненная полностью на NVMe-накопителях. Форм-фактор базовой контроллерной системы - не более 2U, монтаж в стандартную 19-дюймовую стойку.

2.3.2. Архитектура контроллеров:

Не менее двух горячезаменяемых контроллерных узлов, одновременно участвующих в обработке операций ввода-вывода. Каждый узел должен содержать не менее одного процессора архитектуры x86 с количеством физических ядер не менее 16. Совокупно - не менее 32 физических ядер и не менее 512 ГБ оперативной/кэш-памяти контроллеров. Архитектура не должна ограничиваться активным контроллером и резервным контроллером: любой контроллер и любой его фронтальный порт должны принимать и обрабатывать ввод-вывод, а каждый контроллер должен иметь прямой доступ ко всем установленным накопителям.

2.3.3. Внутренние соединения и отказоустойчивость:

Контроллерные узлы должны соединяться не менее чем двумя внутренними высокоскоростными каналами с применением RDMA, совокупная полнодуплексная пропускная способность межконтроллерного обмена - не менее 12,5 ГБ/с. Для служебного обмена должна использоваться отдельная резервированная сеть управления, не зависящая от каналов передачи данных. Все активные компоненты и пути должны быть продублированы: контроллеры, блоки питания, вентиляторы, порты, внутренние соединения и пути к накопителям. Отказ одного контроллера, блока питания, вентилятора, порта или одного пути не должен приводить к недоступности данных.

2.3.4. Накопители и емкость:

Установлено не менее 10 двухпортовых NVMe SSD-накопителей корпоративного класса емкостью не менее 7,68 ТБ каждый. Суммарная сырая емкость - не менее 76,8 ТБ. Все накопители должны быть самошифрующимися (SED), поддерживать аппаратное шифрование AES-256-XTS и криптографическое стирание. Накопители должны иметь продуктовые коды производителя системы хранения и обслуживаться по единому сервисному контракту.

2.3.5. Масштабирование емкости:

Базовое шасси должно поддерживать не менее 24 внутренних NVMe-накопителей. Система должна масштабироваться без замены базовой платформы как минимум до 72 NVMe-накопителей

путем подключения не менее двух полок расширения. Диски должны добавляться минимальным шагом не более двух накопителей, полки - по одной, без остановки доступа к данным.

2.3.6. Масштабирование производительности:

Платформа должна обеспечивать независимое масштабирование производительности и емкости. Должен поддерживаться недеструктивный переход от установленных 16-ядерных контроллерных узлов к узлам не менее 32 ядер без миграции данных на другую систему и без плановой недоступности томов.

2.3.7 Системное распределение данных:

Данные и служебная информация должны автоматически распределяться на системном уровне по всем доступным накопителям, контроллерам, кэшу и портам. При добавлении накопителей или замене отказавшего носителя балансировка и восстановление должны выполняться автоматически с использованием ресурсов множества накопителей, без ручного создания и балансировки отдельных дисковых групп.

2.3.8. Интерфейсы подключения:

На каждом контроллерном узле должно быть установлено не менее четырех портов 10/25 Гбит\с SFP28 для передачи данных, всего не менее восьми портов. В комплекте - не менее восьми совместимых 25 Гбит\с SFP28 SR многомодовых трансиверов того же производителя. Каждый контроллерный узел должен иметь отдельные порты администрирования и сервисного управления 1Гбит\с RJ-45. Должны поддерживаться iSCSI и NVMe over TCP; аппаратная платформа должна допускать использование файлового доступа NFS на той же системе без замены контроллеров.

2.3.9. Блоки питания:

Не менее двух горячезаменяемых блоков питания мощностью не менее 1600 Вт каждый, работающих с резервированием. В комплекте - кабели питания C13-C14.

2.3.10. Защита данных:

Поддержка отказоустойчивой защиты данных не ниже двойной четности, выдерживающей одновременный отказ не менее двух накопителей. Должны выполняться сквозная проверка

целостности данных, циклический контроль ошибок на внутренних шинах, межконтроллерных каналах, хостовых протоколах и накопителях, фоновая проверка блоков и прогнозирование отказов носителей.

2.3.11. Оптимизация емкости:

Встроенные inline-компрессия, inline-дедупликация, тонкое выделение емкости и возврат освобожденного пространства. Политики оптимизации должны назначаться на уровне отдельных томов/групп томов. Функции не должны требовать внешнего шлюза или отдельного устройства.

2.3.12 Локальная защита и копии:

Встроенное создание мгновенных снимков и полных/виртуальных копий томов; согласованные группы томов; создание снимков без полного резервирования исходной емкости; восстановление тома или отдельных виртуальных машин из снимка. Должна поддерживаться защита снимков от несанкционированного удаления на заданный срок.

2.3.13. Репликация и непрерывность бизнеса:

Встроенная асинхронная и синхронная репликация между системами производителя, включая режим RPO=0 и автоматизированное переключение между площадками с кворумом. Платформа должна поддерживать двунаправленную active-active репликацию и топологии защиты не менее трех площадок. Базовые функции репликации должны быть доступны в составе поставляемого программного обеспечения без приобретения отдельных лицензий на каждый том.

2.3.14. Гарантия доступности:

Производитель должен предоставлять документированную программу гарантии 100% доступности данных для данной серии систем при соблюдении условий программы и наличии заявленного уровня поддержки. Подтверждение участия поставляемой конфигурации в программе предоставляется письмом производителя или официальным документом.

2.3.15. Управление:

Управление через защищенный веб-интерфейс, локальный интерфейс и REST API. Должны поддерживаться RBAC, MFA/SSO, журналирование действий, интеграция с внешними каталогами, Syslog и безопасные протоколы управления. Должна быть возможность централизованно управлять несколькими массивами производителя из одной консоли.

2.3.16. AIOps и сквозная аналитика:

Облачная или гибридная аналитическая платформа производителя должна обеспечивать: прогнозирование отказов и дефицита ресурсов; рекомендации по версиям ПО; выявление аномалий; анализ трендов емкости и производительности; автоматическое открытие сервисных обращений.

Для виртуализированный среды должна отображаться сквозная топология пути ввода-вывода от виртуальной машины через виртуальный диск, datastore, хост и хостовый адаптер до тома и системы хранения, включая корреляцию задержек с загрузкой CPU/ОЗУ хоста и виртуальной машины. Исторические данные должны быть доступны не менее 12 месяцев, детальный анализ - с интервалом не более 5 минут.

2.3.17. Защита от киберугроз:

Встроенное обнаружение аномального поведения и признаков шифрования/вредоносной активности на уровне массива, с формированием уведомлений и рекомендаций по восстановлению. Шифрование данных в состоянии покоя должно выполняться аппаратно на SED без существенного снижения производительности. Поддержка локального и внешнего управления ключами по стандартному протоколу, криптографического стирания и безопасной загрузки.

2.3.18. Интеграция с виртуализацией:

Нативная интеграция с поставляемой платформой виртуализации того же производителя должна обеспечивать прямое сопоставление дисков виртуальной машины томам массива, назначение параметров производительности на уровне ВМ и создание аппаратных снимков массива из интерфейса виртуализации. Дополнительно должны поддерживаться VMware vCenter, VASA не ниже версии 5, vVols, Site Recovery Manager, VAAI и управление хранилищем из интерфейса vCenter.

2.3.19. Лицензии:

В комплекте - операционная система массива, лицензия шифрования, лицензии управления и программной поддержки на всю установленную емкость сроком не менее 3 лет. Все заявленные функции базового хранения, снимков, оптимизации емкости, репликации, аналитики и API должны быть лицензированы на поставляемый объем.

2.3.20. Поддержка:

Не менее 3 лет технической поддержки производителя уровня 24×7. Целевое время обратного звонка специалиста: не более 15 минут для критического инцидента уровня 1 и не более 1 часа для инцидентов уровней 2 и 3. Выезд инженера к месту установки - не более 4 часов для покрываемого оборудования, с учетом географической доступности услуги, подтвержденной производителем. Включены обновления микрокода и программного обеспечения.

2.3.21. Услуги и обучение:

В комплекте - заводская/проектная интеграция, установка и первичный запуск аппаратной части и операционной системы, настройка двухузлового кластера, подключение к платформе управления и проверка отказоустойчивости. Предоставить не менее 30 учебных кредитов или эквивалентный объем официального обучения производителя со сроком использования не менее 12 месяцев.

2.3.22. Масштабируемость семейства без федерации отдельных массивов:

Единая программно-аппаратная архитектура семейства должна поддерживать конфигурации от 2 до 4 одновременно активных контроллерных узлов и масштабирование до не менее 384 двухпортовых NVMe-накопителей и 16 полок расширения в пределах одной логической системы. Все контроллеры должны иметь прямой доступ к общему пулу накопителей; объединение независимых массивов внешней федерацией не считается соответствием.

2.3.23. Гарантированное качество обслуживания:

Встроенный механизм QoS должен задавать для отдельных томов, групп томов, арендаторов или виртуальных машин минимальные и максимальные значения IOPS и пропускной способности, а также целевой уровень задержки вплоть до 50 микросекунд. Изменение политик выполняется онлайн, без установки агентов на хосты и без физического разделения накопителей.

2.3.24. Неизменяемые снимки и контроль срока хранения:

Должны поддерживаться снимки класса WORM/immutable с заданным сроком хранения. До истечения срока такой снимок не может быть удален, сокращен по сроку или разблокирован ни администратором с максимальными правами, ни сервисной службой производителя. Защита должна использовать независимый контроль времени, исключающий обход путем изменения системных часов.

2.3.25. Мультитенантность:

Поддержка создания изолированных виртуальных доменов/арендаторов внутри одного массива с раздельными объектами хранения, квотами, политиками QoS, журналами и делегированными администраторами. Ошибка или действие администратора одного домена не должно предоставлять доступ к объектам другого домена.

2.3.26. Управление ключами шифрования:

Шифрование данных на SED должно поддерживать встроенный локальный менеджер ключей и внешние менеджеры ключей, прошедшие валидацию FIPS 140-2 или более позднего применимого стандарта. Переход между локальным и внешним менеджером, а также между внешними менеджерами должен выполняться без остановки шифрования и без потери данных.

2.3.27. Онлайн-обслуживание и обновление:

Должна обеспечиваться онлайн-замена контроллерных узлов, модулей памяти, загрузочных накопителей, адаптеров, SFP-модулей, блоков питания, вентиляторов и накопителей. Обновление операционной системы массива должно выполняться без перезагрузки всех контроллеров одновременно и без прекращения доступа хостов к данным.

2.3.28. Безопасная телеметрия и проактивная поддержка:

Связь массива с сервисной инфраструктурой производителя должна использовать взаимную аутентификацию и шифрованный канал. Передаются только состояние, конфигурация, производительность, события и диагностические метаданные; пользовательские данные не передаются. Критические события должны автоматически создавать обращение и запускать проактивную диагностику.

2.3.29. Миграция данных:

В поставляемом программном обеспечении должна быть предусмотрена онлайн-миграция томов между совместимыми массивами производителя и импорт данных с поддерживаемых сторонних систем без установки специализированного шлюза в тракт ввода-вывода. Должна поддерживаться миграция с минимальным либо отсутствующим простоем приложений.

2.3.30. Автономный режим управления:

Основные операции создания и экспорта томов, настройки хостов, снимков, репликации, QoS, шифрования, мониторинга и обновления должны быть доступны через локальный интерфейс массива, CLI и REST API даже при временной недоступности облачной платформы управления.

2.4. Требования к двухпроцессорным серверам в количестве 2 штук.

2.4.1. Форм-фактор:

Сервер заводской сборки для установки в стандартную стойку 19 дюймов, высота не более 1U. Архитектура – двухпроцессорная x86-64.

2.4.2. Процессоры:

В каждом сервере установлено не менее двух процессоров одного типа. Каждый процессор: не менее 86 физических производительных ядер, не менее 172 потоков, базовая частота не менее 2,0 ГГц, расчетная тепловая мощность не более 350 Вт. Совокупно на сервер - не менее 172 физических ядер и 344 потоков. Поддержка не менее четырех межпроцессорных каналов для установленной модели.

2.4.3 Память:

Не менее 32 слотов DIMM. Максимально поддерживаемый объем - не менее 8 ТБ DDR5. Установлено не менее 768 ГБ DDR5-6400 в виде 24 модулей по 32 ГБ. Память должна быть сертифицирована производителем сервера и поддерживать расширенные режимы ECC и повышенной отказоустойчивости памяти.

2.4.4. Дисковая подсистема:

Сервер должен поддерживать различные варианты шасси и накопителей, включая SFF SAS/SATA /NVMe, LFF и EDSFF E3.S; максимальная поддержка EDSFF - не менее 20 накопителей. В поставляемой конфигурации фронтальные диски не требуются.

2.4.5. Загрузочное устройство:

В каждом сервере установлено отдельное загрузочное устройство, содержащее не менее двух M.2 NVMe SSD емкостью не менее 480 ГБ каждый, с предварительно настроенным аппаратным RAID 1. Устройство должно быть оптимизировано для установки ОС, иметь продуктовый код производителя сервера и не занимать основные фронтальные отсеки.

2.4.6. Поддержка RAID:

Платформа должна поддерживать установку аппаратных Tri-Mode контроллеров SAS/SATA /NVMe с RAID 0/1/5/6/10/50/60, смешанным режимом RAID/HBA, online-расширением томов и миграцией уровней RAID. Поддержка должна обеспечиваться официальными опциями производителя без применения несертифицированных контроллеров.

2.4.7. Сетевые интерфейсы:

В каждом сервере установлены: не менее одного двухпортового адаптера 10/25Гбит\с SFP28 форм-фактора OCP 3.0; не менее двух 25Гбит\с SFP28 SR трансиверов; не менее одного четырехпортового адаптера 1Гбит\с BASE-T OCP 3.0. Платформа должна поддерживать адаптеры Ethernet/InfiniBand не менее 400 Гбит\с/с и Fibre Channel не менее 64 Гбит\с/с.

2.4.8. Слоты расширения:

Не менее двух слотов PCIe 5.0 с возможностью расширения до трех слотов PCIe 5.0 x16. Не менее двух слотов OCP 3.0, с возможностью установки сетевых адаптеров и контроллеров хранения без необоснованного занятия всех стандартных PCIe-слотов.

2.4.9. Порты и индикация:

Не менее: одного выделенного порта удаленного управления; диагностического USB Type-C; пяти портов USB 3.x; одного видеовыхода; световой индикации состояния системы, питания, сети и идентификации. Встроенный видеоадаптер с разрешением не менее 1920×1200 при 60 Гц.

2.4.10. Блоки питания и охлаждение:

Не менее двух горячезаменяемых блоков питания мощностью не менее 1000 Вт каждый, класс энергоэффективности не ниже 80 PLUS Titanium. Полный комплект высокопроизводительных вентиляторов для установленной двухпроцессорной конфигурации. В комплекте - кабели C13-C14 и телескопические направляющие.

2.4.11 Аппаратная безопасность:

Встроенный контроллер удаленного управления должен быть собственной аппаратной разработкой производителя сервера и обеспечивать аппаратный корень доверия на уровне кремния. Проверка цифровой подписи микрокода должна выполняться до его исполнения.

Должно быть отдельное аппаратно защищенное хранилище ключей и секретов внутри контроллера управления, изолированное от основной памяти сервера, а также защищенная эталонная копия микрокода для автоматического или ручного восстановления после компрометации.

2.4.12 Криптографическая готовность:

Платформа должна поддерживать безопасную подпись микрокода с учетом требований NIST и CNSA 2.0 к постквантовой устойчивости, включая применение стандартизованных хэш- и подпись-ориентированных алгоритмов. Подтверждение - официальная документация производителя.

2.4.13. Удаленное управление:

Для каждого сервера включена расширенная лицензия встроенного управления сроком не менее 3 лет: полнофункциональная HTML5 KVM-консоль, виртуальные носители, удаленное подключение ISO, запись и воспроизведение сеанса консоли, совместная работа нескольких администраторов, управление питанием, журналирование и RESTful API.

2.4.14. Платформа управления серверным парком:

В комплекте - подписка производителя сроком не менее 3 лет на централизованную SaaS /гибридную платформу управления. Платформа должна обеспечивать: инвентаризацию; группирование серверов; автоматические базовые линии микрокода; контроль соответствия; групповые обновления по расписанию и по требованию; последовательный/параллельный режим и остановку при ошибке; централизованные профили BIOS; удаленную HTML5-консоль;

автоматическое создание сервисных обращений; RBAC/SSO; аудит; REST API; отчеты по энергопотреблению, стоимости и выбросам; интеграцию с VMware vCenter и vSphere Lifecycle Manager для обновления микрокода и драйверов.

2.4.15. Поддерживаемые ОС:

Официальная поддержка актуальных версий Microsoft Windows Server, VMware ESXi, Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Canonical Ubuntu, Oracle Linux и основных совместимых корпоративных Linux-дистрибутивов. Участник предоставляет ссылку на официальную матрицу поддержки.

2.4.16. Гарантия и поддержка:

Базовая гарантия производителя не менее 3 лет на детали, работы и выезд. Дополнительно в составе поставки - не менее 3 лет технической поддержки производителя уровня 9×5 с обратным звонком профильного специалиста не более 2 часов и выездом на следующий рабочий день для покрываемого оборудования. Все установленные заводские опции должны обслуживаться по тому же контракту.

2.4.17. Услуги:

Физическая установка в стойку, подключение, обновление микрокода до согласованной поддерживаемой версии, настройка контроллера удаленного управления и платформы централизованного управления, проверка загрузочного RAID1 и передача отчета о состоянии оборудования.

2.4.18. Глубина корпуса:

Глубина каждого сервера без учета ручек, кабелей и направляющих должна быть не более 77,5 см, что обеспечивает размещение в стандартных стойках и достаточное пространство для коммутации с тыльной стороны.

2.4.19. Варианты шасси и универсальная передняя зона:

Серверное семейство должно иметь не менее трех заводских вариантов шасси 1U и поддерживать в рамках одной платформы SFF, LFF, EDSFF E3.S, внутреннее загрузочное устройство M.2 NVMe и размещение сетевых адаптеров OCP во фронтальной многофункциональной зоне. Выбор варианта не должен требовать перехода на другое семейство серверов.

2.4.20 Повышенная отказоустойчивость памяти:

Платформа должна поддерживать режим памяти с устойчивостью не ниже двойной коррекции отказа устройств памяти, но без зеркалирования всего объема и без уменьшения доступной емкости оперативной памяти на 50%. Режим должен быть реализован и документирован производителем сервера.

2.4.21 Профили рабочих нагрузок:

В UEFI/BIOS должны быть встроены предварительно проверенные профили рабочих нагрузок, автоматически изменяющие совокупность параметров процессора, памяти, энергопотребления и ввода-вывода для виртуализации, баз данных, низкой задержки, энергоэффективности и других сценариев. Профиль должен оптимизировать сотни взаимосвязанных параметров без ручной настройки каждого из них.

2.4.22. Встроенный программный RAID:

Сервер должен поддерживать встроенный программный RAID уровней 0, 1 и 5 для совместимых накопителей без установки отдельного аппаратного RAID-контроллера и без занятия слота PCIe. Наличие этой возможности не отменяет требования к установленному аппаратно защищенному загрузочному RAID1.

2.4.23. Поддерживаемые форматы накопителей:

Серверное семейство должно поддерживать не менее восьми форматов/типов носителей, включая SFF SAS HDD, SFF SAS SSD, SFF SATA SSD, SFF NVMe SSD, LFF SAS/SATA HDD, LFF SAS /SATA SSD, EDSFF E3.S NVMe SSD и M.2 NVMe SSD.

2.4.24. Унификация блоков питания:

Блоки питания должны иметь единый механический и электрический форм-фактор производителя, устанавливаться и заменяться без инструмента и использоваться в нескольких

моделях серверного семейства. Платформа должна поддерживать линейку блоков питания мощностью не менее чем от 800 до 2200 Вт с эффективностью не ниже 80 PLUS Platinum, включая варианты Titanium.

2.5. Требования к коммутаторам ядра/центра обработки данных - 2 штуки:

2.5.1 Форм-фактор и назначение:

Коммутатор корпоративного класса для ядра сети и подключения серверов/систем хранения. Форм-фактор не более 1U, монтаж в стойку 19 дюймов. Глубина корпуса - не более 410 мм, что обеспечивает установку в стойки с ограниченной монтажной глубиной.

2.5.2. Порты:

Не менее 28 линейных портов 1/10/25 Гбит\с SFP/SFP+/SFP28 и дополнительно не менее 4 линейных портов 10/25 Гбит\с SFP+/SFP28 с аппаратным шифрованием Ethernet-каналов, всего не менее 32 портов со скоростью 25 Гбит\с. Не менее 4 портов 40/100Гбит\с QSFP+/QSFP28. Каждый порт QSFP28 должен поддерживать штатное разделение на 4×10Гбит\с и 4×25Гбит\с.

2.5.3. Производительность:

Коммутационная способность - не менее 2,4 Тбит/с; производительность пересылки - не менее 1 145 млн пакетов/с. Буфер пакетов - не менее 32 МБ. Процессор управления - не менее 4 ядер с частотой не ниже 1,8 ГГц; оперативная память - не менее 16 ГБ; энергонезависимое локальное хранилище - не менее 32 ГБ.

2.5.4. Отказоустойчивость:

Два горячезаменяемых блока питания и не менее трех горячезаменяемых вентиляторов с резервированием и распределением нагрузки. Направление воздушного потока - от портов к блокам питания. Замена блока питания или вентилятора не должна требовать отключения коммутатора. Все вентиляторы и блоки питания должны входить в заводской комплект.

2.5.5. Active-active пара:

Два коммутатора должны формировать отказоустойчивую пару с независимыми плоскостями управления, синхронизацией состояния и active-active пересылкой. Поддержка многосистемного агрегирования каналов к серверам и системам хранения без блокировки резервных линий. Отказ одного коммутатора или его управляющей плоскости не должен останавливать пересылку через второй.

2.5.6 Функции L2/L3:

Поддержка VLAN, 802.1Q, LACP, LLDP/LLDP-MED, STP/RSTP/MSTP, IGMP/MLD Snooping, ACL, QoS, IPv4/IPv6, статической маршрутизации, OSPF, BGP, VRF-Lite, PIM и ECMP.

2.5.7. EVPN-VXLAN:

Аппаратная и программная поддержка VXLAN с BGP EVPN для L2/L3-сегментации, распределенного шлюза и построения фабрики центра обработки данных. Функциональность должна быть доступна в штатной операционной системе коммутатора.

2.5.8. Аналитика и автоматизация:

Встроенная аналитическая система должна поддерживать локальное хранение временных рядов, автоматическое выявление отклонений и запуск программируемых агентов непосредственно на коммутаторе. Поддерживаются REST API, Python-автоматизация, потоковая телеметрия и централизованное управление производителя.

2.5.9. Оптимизация для хранения:

Коммутатор должен иметь официально подтвержденную производителем валидацию как lossless Ethernet fabric для систем хранения и гиперконвергентных решений того же производителя, включая DCBx, PFC/ETS и мониторинг перегрузок. Подтверждение - официальное руководство или матрица совместимости производителя.

2.5.10. Комплект оптики и кабелей:

Для пары коммутаторов в комплекте не менее: 8 × 1Гбит\с SX многомодовых SFP; 8 × 10Гбит\с SR многомодовых SFP+; 32 × 25Гбит\с SR многомодовых SFP28; 2 × 100Гбит\с QSFP28 DAC длиной не менее 1 м. Все модули и кабели должны иметь продуктовые коды производителя коммутаторов, проходить его валидацию и покрываться гарантией/поддержкой.

2.5.11. Управление и безопасность:

CLI, защищенный веб-интерфейс/централизованная система, SSH, SNMPv3, Syslog, TACACS+, RADIUS, LDAP, RBAC, 802.1X, MAC-аутентификация, DHCP Snooping, Dynamic ARP Inspection, защита от подмены адресов, CoPP, безопасная загрузка и подписанные образы ПО.

2.5.12. Гарантия и поддержка:

Ограниченная пожизненная гарантия производителя с покрытием не менее чем до окончания продаж плюс 5 лет. Дополнительно - сервис производителя на 3 года: приоритетный доступ к TAC 24×7, обновления ПО и замена оборудования на следующий рабочий день. Сервис должен быть зарегистрирован на серийные номера Заказчика.

2.5.13. Независимый выбор скорости портов:

Каждый из не менее 28 портов SFP/SFP+/SFP28 должен независимо работать на скорости 1, 10 или 25 Гбит\с/с без объединения портов в группы с общей скоростью и без блокировки соседних портов. Не менее 4 дополнительных защищенных портов должны независимо работать на скорости 10 или 25 Гбит\с/с. Порты 40/100Гбит\с должны поддерживать разделение 100Гбит\с на 4×10Гбит\с и 4×25Гбит\с. Коммутатор должен поддерживать использование до 14 портов 50Гбит\с без замены аппаратной платформы.

2.5.14. Архитектура сетевой операционной системы:

Операционная система должна быть модульной, основанной на базе текущего состояния и конфигурации. Все программные процессы взаимодействуют через эту базу, а не посредством жестких межпроцессных зависимостей; отказ или обновление отдельного модуля не должно требовать полной перезагрузки системы. Должна поддерживаться непрерывная синхронизация состояния между узлами пары.

2.5.15. Встроенная аналитика и временные ряды:

Коммутатор должен иметь локальную базу временных рядов и встроенный механизм аналитики, позволяющий отслеживать события интерфейсов, маршрутизации, очередей, производительности и безопасности, выполнять корреляцию, хранить историю и запускать автоматические действия /скрипты при выполнении заданных условий.

2.5.16. Обновление отказоустойчивой пары:

Должно поддерживаться поочередное обновление программного обеспечения двух коммутаторов active-active пары с сохранением обработки трафика и без одновременного вывода из эксплуатации обоих устройств. Согласованность конфигурации и состояния пары должна проверяться до и после обновления.

2.5.17 Программируемость:

REST API должен предоставлять доступ не только к мониторингу, но и к конфигурации основных функций, доступных через CLI. Поддерживаются встроенные Python-скрипты/агенты, потоковая телеметрия и интеграция с системами автоматизации без установки внешнего проприетарного шлюза.

2.5.18. Единая платформа сетевых операций:

Производитель должен иметь единую облачную или локально развертываемую платформу для инвентаризации, конфигурирования, мониторинга и диагностики коммутаторов ядра, коммутаторов доступа и точек беспроводного доступа, с единой моделью ролей, журналов и API. Требование относится к совместимости платформы; дополнительные подписки включаются только если прямо указаны в составе поставки.

2.5.19. Аппаратное шифрование Ethernet-каналов:

Не менее четырех линейных портов 10/25 Гбит\с/с должны аппаратно поддерживать IEEE 802.1 AE MACsec с шифрованием AES-128 и AES-256. Шифрование должно выполняться на линейной скорости без установки внешних устройств и применяться ко всему Ethernet-трафику защищаемого канала.

2.5.20. Lossless Ethernet и протоколы хранения:

Поддержка Data Center Bridging, включая PFC не менее чем для 7 приоритетов на порт, ETS, DCBX, ECN с настраиваемым профилем, расширенную настройку lossless-пулов и глобальную статистику буферов. Поддержка iSCSI, lossless iSCSI, RoCE v2 и NVMe over Fabrics в штатной операционной системе коммутатора.

2.5.21. Масштаб таблиц и маршрутизации

Поддержка не менее 4 094 VLAN, не менее 212 000 MAC-адресов, не менее 145 000 IPv4 host entries, не менее 145 000 IPv6 host entries, не менее 600 000 IPv4 и не менее 600 000 IPv6 маршрутов. Поддержка ECMP не менее чем по 32 равнозначным путям.

2.5.22. Потоковая телеметрия и диагностика:

Поддержка потоковой телеметрии gNMI с моделями OpenConfig, аппаратного sFlow без снижения производительности пересылки, RMON, IP SLA с сохранением истории в локальном аналитическом механизме, а также двух независимых образов операционной системы и нескольких файлов конфигурации.

2.5.23. Агрегация каналов:

Поддержка не менее 54 групп агрегации каналов. В одной группе должно поддерживаться не менее 16 физических участников на отдельном коммутаторе и не менее 32 участников при распределении группы между двумя коммутаторами отказоустойчивой active-active пары. Алгоритм балансировки должен настраиваться по полям уровней L1-L4.

2.6. Требования к коммутаторам доступа PoE - 6 штук:

2.6.1 Форм-фактор:

Управляемый коммутатор доступа не более 1U для установки в стойку 19 дюймов.

2.6.2 Порты доступа:

Не менее 48 портов 10/100/1000BASE-T с поддержкой IEEE 802.3at PoE+ (Class 4), до 30 Вт на порт, и не менее четырех встроенных uplink-портов 1/10Гбит\с\с SFP/SFP+.

2.6.3 PoE-бюджет:

Совокупный бюджет питания PoE не менее 370 Вт на коммутатор. Поддержка приоритизации питания и мониторинга потребления на каждом порту.

2.6.4 Производительность:

Неблокируемая коммутационная способность не менее 176 Гбит\с/с и производительность пересылки не менее 98 млн пакетов/с.

2.6.5 Объединение в стек:

Все шесть коммутаторов должны объединяться в единый логический стек по цепочной или кольцевой топологии через штатные 1/10Гбит\с\с порты, без специальных проприетарных стековых модулей. Поддерживается не менее 6 участников, единая конфигурация и единая точка управления.

2.6.6 Операционная система:

Коммутаторы ядра и доступа должны использовать единую современную операционную систему одного производителя с транзакционной базой конфигурации, модульной архитектурой и единообразными CLI/REST API. Отказ отдельного программного процесса не должен требовать полного перезапуска операционной системы.

2.6.7 Функции:

VLAN, LACP, STP/RSTP/MSTP, LLDP/LLDP-MED, ACL, QoS, IPv6, 802.1X, MAC-аутентификация, DHCP Snooping, Dynamic ARP Inspection, Port Security, IGMP/MLD Snooping, статическая маршрутизация и Energy Efficient Ethernet.

2.6.8. Автоматизация доступа:

Поддержка динамического назначения ролей/политик порту на основе идентификации пользователя или устройства, чтобы перемещение конечного устройства не требовало ручной привязки порта к VLAN. Поддержка централизованного массового изменения и проверки конфигурации.

2.6.9. Управление:

Локальный Web GUI, CLI, REST API, SNMPv3 и возможность управления через облачную или локально развернутую платформу производителя без замены аппаратного обеспечения.

2.6.10. Гарантия и поддержка:

Ограниченная пожизненная гарантия производителя с покрытием не менее чем до окончания продаж плюс 5 лет. В комплекте - сервис на 3 года с TAC 24×7, обновлениями ПО и заменой оборудования на следующий рабочий день.

2.6.11. Аппаратная доверенная загрузка:

Каждый коммутатор должен иметь встроенный аппаратный модуль доверия, проверять целостность загрузчика и операционной системы и блокировать запуск неподписанного или поврежденного программного образа.

2.6.12. Бессрочные базовые функции:

Базовые функции коммутации, статической маршрутизации, стекирования, ACL, QoS, 802.1X, IPv6, REST API и локального управления должны быть активны бессрочно и не отключаться после окончания подписки на централизованное управление или техническую поддержку.

2.6.13. Автоматизированное развертывание и восстановление:

Поддержка Zero Touch Provisioning, автоматического получения утвержденной конфигурации и восстановления конфигурации на замененном устройстве через платформу производителя. Серийный номер и статус замены должны отслеживаться в том же портале поддержки.

2.6.14. Единые роли проводного и беспроводного доступа :

Операционная система должна поддерживать применение единой роли пользователя/устройства и связанных политик доступа независимо от подключения через проводной порт или беспроводную сеть. Назначение роли выполняется по данным аутентификации, типу устройства и контексту, без ручного создания отдельной VLAN для каждого профиля.

2.6.15. Массовое изменение с проверкой соответствия:

Платформа управления производителя должна поддерживать одновременное редактирование конфигураций нескольких коммутаторов, предварительную проверку синтаксиса и соответствия

корпоративным правилам, протоколирование изменений и возможность отката к сохраненной конфигурации.

2.7. Требования к точкам беспроводного доступа Wi-Fi 6E - 10 штук:

2.7.1 Тип исполнения:

Точка доступа для внутренних помещений с внутренними всенаправленными антеннами. В комплекте - универсальный потолочный/настенный монтажный комплект производителя для каждой точки.

2.7.2 Радиомодули:

Три одновременно работающих радиомодуля диапазонов 2,4 ГГц, 5 ГГц и 6 ГГц. Каждый радиомодуль - не менее 2×2:2 MIMO. Стандарт IEEE 802.11ax в каждом из трех диапазонов, класс Wi-Fi 6E.

2.7.3 Производительность:

Максимальная агрегированная скорость не менее 3,9 Гбит\с/с, включая не менее 574 Мбит/с в 2,4 ГГц, 1,2 Гбит\с/с в 5 ГГц и 2,4 Гбит\с/с в 6 ГГц. Поддержка каналов 160 МГц в диапазоне 6 ГГц, OFDMA, MU-MIMO, beamforming и модуляции до 4096-QAM.

2.7.4 Одновременная работа диапазонов:

Аппаратная фильтрация должна обеспечивать одновременную работу радиомодулей 5 и 6 ГГц без взаимного ограничения доступных каналов и без необходимости отключать один диапазон для работы другого.

2.7.5 Проводные интерфейсы:

Не менее двух портов Ethernet 100/1000/2500BASE-T. Поддержка резервирования подключения и питания с переключением без перезагрузки точки доступа. Питание по IEEE 802.3at PoE+.

2.7.6 Клиентская емкость:

Поддержка не менее 512 ассоциированных клиентских устройств на каждый радиомодуль и не менее 16 BSSID на радиомодуль, при этом для 6 ГГц допускается не менее 4 BSSID.

2.7.7 Безопасность:

WPA3-Enterprise/Personal, Enhanced Open, 802.1X, AES, защищенные управленческие кадры, встроенный межсетевой экран ролей/политик, обнаружение несанкционированных точек доступа и беспроводных угроз.

2.7.8 IoT и позиционирование:

Встроенные Bluetooth Low Energy и IEEE 802.15.4/ZiГбит\с\се либо эквивалентные IoT-радиоинтерфейсы, USB для внешних IoT-устройств. Встроенный GNSS/GPS-приемник и программная функция самоопределения местоположения/использования точки как опорной для координат.

2.7.9 Режимы управления:

Поддержка автономного режима, локального контроллерного управления и облачного централизованного управления одного производителя. Возможность перехода между поддерживаемыми режимами управления без замены точки доступа.

2.7.10 Отказоустойчивость беспроводной сети:

При контроллерном управлении должна поддерживаться кластеризация контроллеров, бесшовное переключение клиентов, обновление программного обеспечения без полного прерывания беспроводного сервиса и автоматическая оптимизация радиосреды.

2.7.11 Гарантия и поддержка:

Ограниченная пожизненная гарантия производителя с покрытием не менее чем до окончания продаж плюс 5 лет. В комплекте - сервис на 3 года: TAC 24×7, обновления ПО и замена точки на следующий рабочий день.

2.7.12 Использование спектра 6 ГГц:

При разрешении соответствующим национальным регулятором точка доступа должна поддерживать до семи неперекрывающихся каналов шириной 160 МГц в диапазоне 6 ГГц и автоматический выбор доступного канала с учетом требований страны эксплуатации.

2.7.13. Интеллектуальная оптимизация радиосреды:

Система управления должна на основе машинного обучения централизованно оптимизировать каналы, ширину каналов и мощность передатчиков, учитывать помехи, плотность клиентов и изменение условий, а также предоставлять рекомендации и историю принятых решений.

2.7.14. Гарантирование ресурсов приложений:

Поддержка политики выделения радиоресурсов критичным пользователям и приложениям с учетом времени доступа к среде, частоты и пространственных потоков, чтобы обеспечить предсказуемую полосу и задержку без установки отдельного оборудования в тракт передачи данных.

2.7.15. Динамическая сегментация:

Политики доступа должны назначаться централизованно по роли пользователя, типу устройства, приложению и местоположению и одинаково применяться в проводной и беспроводной сети. Добавление нового типа клиента не должно требовать ручной настройки отдельных SSID, VLAN и ACL на каждом устройстве.

2.7.16 Обновление и отказоустойчивость без прерывания сеансов:

При контроллерном управлении должны поддерживаться распределение пользовательских сессий между узлами, бесшовное переключение и поэтапное обновление программного обеспечения, при котором активные голосовые вызовы, видео и передача данных продолжаются без повторной аутентификации всех клиентов.

2.8. Требования к программному обеспечению виртуализации - лицензии на 4 физических процессорных сокета (совокупно не менее 344 физических ядер):

2.8.1 Модель лицензирования:

Подписка сроком не менее 3 лет. Основная лицензионная метрика - физический процессорный сокет, без ограничения количества ядер в сокете. Количество - не менее 4 единиц лицензирования, полностью покрывающих два поставляемых двухпроцессорных сервера с суммарным количеством не менее 344 физических процессорных ядер. Замена требуемого покрытия лицензиями, ограниченными меньшим числом ядер, процессоров, виртуальных машин или управляемых хостов, не допускается. В состав каждой единицы лицензирования должна входить техническая поддержка производителя уровня 24x7.

2.8.2. Состав решения:

Единое программное решение должно включать промышленный гипервизор на базе KVM и централизованную систему управления виртуальными машинами. Компонент управления не должен требовать отдельной лицензии для базовых функций, перечисленных в настоящем разделе.

2.8.3 Совместное управление KVM и VMware:

Из одной веб-консоли должны выполняться обнаружение, просмотр, создание и основные операции управления виртуальными машинами как на поставляемом KVM-гипервизоре, так и в существующих кластерах VMware vSphere/ESXi. Должен быть включен инструмент конвертации образов/виртуальных машин VMware в формат поставляемого гипервизора.

2.8.4 Кластер и высокая доступность:

Создание отказоустойчивого кластера; автоматический перезапуск ВМ после отказа узла; живая миграция работающих ВМ между узлами без остановки; автоматическое размещение ВМ на оптимальном хосте на основе загрузки; поддержка планового обслуживания узла без остановки рабочих нагрузок.

2.8.5. Управление хранением:

Поддержка внешних систем хранения по NFS, iSCSI и Fibre Channel. Живая миграция виртуальных дисков между datastore без остановки ВМ. Нативная интеграция с поставляемой системой хранения того же производителя для прямого сопоставления томов виртуальным машинам, настройки производительности и создания аппаратных снимков.

2.8.6 Сеть:

Поддержка VLAN 802.1Q, trunk, объединения физических интерфейсов, Open vSwitch или эквивалента, раздельных сетей управления/вычислений/хранения и централизованного назначения сетей виртуальным машинам.

2.8.7 IPAM, DNS и секреты:

Встроенные пулы IP-адресов, защищенное хранилище учетных данных и интеграция с внешними IPAM/DNS-системами, включая не менее двух распространенных решений каждого типа. Автоматическое создание A/PTR-записей и резервирование адресов при развертывании ВМ.

2.8.8. Защита данных:

Встроенные снимки и резервные копии ВМ с операциями создания, восстановления и удаления. Интеграция не менее чем с тремя внешними платформами защиты данных, включая решения, совместимые с Veeam, Commvault и Rubrik либо их официальные эквиваленты.

2.8.9. Автоматизация:

Выполнение Bash и PowerShell-скриптов при подготовке и в ходе эксплуатации ВМ; шаблоны развертывания; теги; Day-2 операции; REST API и CLI.

2.8.10. Консоль и доступ:

HTML5-консоль виртуальных машин через веб-интерфейс с поддержкой VNC, SSH и RDP; RBAC; SSO; журналы аудита; безопасное хранение секретов.

2.8.11. Поддержка гостевых ОС:

Поддержка гостевых Microsoft Windows и основных корпоративных Linux-дистрибутивов. Подтверждение официальной матрицей совместимости производителя.

2.8.12. Техническая поддержка:

Не менее 3 лет 24×7 с целевым временем обратного звонка не более 15 минут для критического инцидента уровня 1 и не более 1 часа для уровней 2-3, включая обновления, исправления безопасности и новые версии в пределах лицензированной редакции.

2.8.13 Двухузловой кластер:

Платформа должна официально поддерживать кластер из двух поставляемых вычислительных узлов с внешним общим хранилищем по Fibre Channel, iSCSI или NFS. Для запуска высокой доступности не должно требоваться приобретение третьего вычислительного сервера; функции кворума реализуются поддерживаемым производителем способом.

2.8.14. Отсутствие скрытых лицензионных ограничений:

Для покрытых сокетов не допускаются минимальный пакет ядер, дополнительный коэффициент за количество ядер, ограничение числа виртуальных машин, виртуальных процессоров, хостов или управляемой емкости. Все функции настоящего раздела должны сохраняться в пределах оплаченного срока без приобретения отдельной лицензии управления.

2.8.15 Единое управление резервными копиями:

Из основной консоли должны выполняться создание, просмотр, восстановление и удаление резервных копий виртуальных машин как поставляемого KVM-гипервизора, так и подключенной среды VMware. Поддерживаются нативная защита и интеграция с внешними системами резервного копирования.

2.8.16. Проброс устройств:

Гипервизор должен поддерживать безопасный прямой проброс в виртуальные машины совместимых GPU, USB-, PCIe- и NVMe-устройств с документированными ограничениями и сохранением управляемости хоста.

2.8.17 Интеграция с сетевой инфраструктурой:

Платформа должна использовать Open vSwitch или эквивалент и предоставлять API для создания, изменения и удаления сетей/порт-групп виртуальных машин. Должна поддерживаться документированная интеграция с поставляемыми коммутаторами того же производителя для автоматизации сетей виртуализации.

2.8.18 Защищенная эксплуатация:

Гипервизор и система управления должны иметь документированное безопасное усиление конфигурации, защищенные репозитории обновлений, RBAC с разграничением по ресурсам, SSO, централизованный журнал аудита и возможность экспортировать события в Syslog/SIEM.

2.9. Требования к внедрению, приемке и документации:

2.9.1. Проектирование:

До начала работ Поставщик согласовывает схему размещения, адресный план управления, VLAN, схему резервирования, версии микрокода и программного обеспечения, перечень подключений и план испытаний.

2.9.2. Монтаж:

Установка оборудования в стойку, подключение питания и коммуникаций, маркировка, проверка направления воздушных потоков, установка всех лицензий и регистрация сервисных контрактов на Заказчика.

2.9.3. Настройка системы хранения:

Создание отказоустойчивой конфигурации, настройка 25Гбит\с\с интерфейсов, MPIO, пулов /томов, шифрования, снимков, аналитики и интеграции с виртуализацией. Проверка отказа контроллера, порта и блока питания без потери доступа к данным.

2.9.4. Настройка серверов:

Актуализация микрокода, настройка загрузочного RAID1, BIOS-профилей, контроллеров управления, платформы управления серверным парком, сетевых интерфейсов и установка /подготовка гипервизора.

2.9.5. Настройка сети:

Формирование active-active пары коммутаторов ядра, настройка VLAN/LAG/маршрутизации /EVPN-VXLAN по согласованному проекту; создание стека из шести коммутаторов доступа; проверка отказа одного устройства/линка. Установка и проверка всех трансиверов и DAC.

2.9.6. Настройка беспроводной сети:

Монтаж точек доступа, обновление ПО, присоединение к выбранному режиму управления, настройка радиопараметров и безопасности, проверка 2,4/5/6 ГГц и резервирования Ethernet/PoE.

2.9.7. Настройка виртуализации:

Создание двухузлового кластера, подключение внешней системы хранения, настройка сетей, тестовая ВМ, проверка live migration, HA, live storage migration, снимков и интеграции с массивом.

2.9.8. Приемо-сдаточные испытания:

Поставщик предоставляет и выполняет программу испытаний. Минимально проверяются: комплектность; серийные номера и регистрации; версии ПО; доступность управления; отказоустойчивость хранения и сети; загрузочный RAID1 серверов; производительность интерфейсов; миграция и HA ВМ; доступность Wi-Fi 6E; открытие тестового обращения в поддержку; восстановление конфигураций из резервной копии.

2.9.9. Документация:

Передать на русском или английском языке: исполнительную схему, таблицу портов и кабелей, адресный план, конфигурации и их резервные копии, учетные записи в запечатанном /защищенном виде, перечень лицензий, серийных номеров и сроков поддержки, протокол испытаний, инструкции по эскалации и контактные данные сервисных центров.

2.9.10. Начало гарантийного срока:

Гарантийные и сервисные сроки должны исчисляться не ранее даты поставки/регистрации на Заказчика и не сокращаться временем нахождения оборудования на складе поставщика. Все сервисы и подписки активируются по согласованию с Заказчиком.

2.9.11. Ответственность за совместимость:

Поставщик несет ответственность за полную совместимость и работоспособность всей конфигурации, включая корректную интеграцию инфраструктурной части и NGFW разных производителей. Выявленные при внедрении недостающие лицензии, подписки, кабели, оптика, монтажные элементы или поддерживаемые заводские опции предоставляются Поставщиком без увеличения стоимости договора.

2.9.12. Проверка архитектуры производителями:

До поставки Поставщик предоставляет письмо или отчет единого производителя инфраструктурной части о проверке ее проектной конфигурации, а также официальное подтверждение производителя NGFW по составу межсетевого экрана, лицензий, подписок, оптики и поддержки. Документы должны подтверждать комплектность, поддерживаемость сочетания аппаратных средств, версий ПО и лицензий, а также соответствие мощности блоков питания, охлаждения, оптики и кабелей.

2.9.13. Матрица версий

До ввода в эксплуатацию согласовывается единая матрица версий микрокода серверов, контроллеров управления, сетевых адаптеров, системы хранения, коммутаторов, точек доступа, гипервизора, драйверов и плагинов. Все версии должны находиться в официальной поддержке производителя и быть совместимы между собой.

2.9.14. Доказательная матрица соответствия:

Участник заполняет построчную матрицу соответствия настоящему ТЗ с точным указанием модели, продуктового кода, значения характеристики, названия официального документа, номера страницы/раздела и действующей ссылки. Формулировки только «соответствует» без проверяемого подтверждения не принимаются.

2.9.15. Демонстрация или стендовая проверка:

По запросу Заказчика до подведения итогов или до окончательной приемки участник должен продемонстрировать на действующем стенде производителя либо удаленно: единый портал поддержки, управление оборудованием, отказоустойчивую пару коммутаторов, live migration, HA, интеграцию виртуализации с массивом, неизменяемые снимки и аналитические функции.

2.9.16. Испытания безопасности:

При приемке проверяются доверенная загрузка серверов и коммутаторов, статус шифрования SED, создание неизменяемого снимка с невозможностью досрочного удаления, RBAC, MFA/SSO при наличии, журнал аудита и отправка тестового события в Syslog/SIEM. Результаты фиксируются в протоколе.

2.9.17. Испытания отказоустойчивости под нагрузкой:

Отказ контроллера массива, сетевого линка, одного коммутатора ядра, блока питания и перенос виртуальной машины должны проверяться при активной тестовой нагрузке ввода-вывода и сетевого трафика. Не допускаются потеря данных, повреждение файловой системы или необходимость ручного переподключения томов.

2.9.18. Проверка сервисных прав:

До подписания итогового акта Заказчик совместно с Поставщиком проверяет в официальных порталах соответствующих производителей регистрацию всех серийных номеров, сроков поддержки, подписок и лицензий, доступ к обновлениям и возможность открытия тестовых обращений. Отсутствующие или неверно зарегистрированные сервисные права устраняются за счет Поставщика.

2.10. Общие характеристики для всех поставляемых межсетевых экранов:

Аппаратный межсетевой экран, работающий на уровнях с Layer-2 по Layer-7 модели OSI, имеющий следующий функционал:

1. Межсетевое экранирование с контролем состояния сессий;

2. Распознавание и блокировка сетевых приложений на седьмом уровне модели OSI по трафику, проходящему через межсетевой экран, в том числе индивидуально для всех приложений, использующих общий порт, в том числе 80 и 443, и использующих динамические TCP/UDP-порты;

3. Предлагаемый NGFW должен быть сертифицирован по стандартам ISO 27001, ISO 27017, ISO 27018, ISO 27701, SOC2, Common Criteria, FIPS 140-2, CMVP, NCSC Foundation, ANSSI, DoDIN, CSfC, USGV6, ICSA и NEBS

4. Предлагаемый NGFW не должен требовать перезагрузки для проверки и установки обновлений безопасности

5. Предлагаемый NGFW должен иметь интегрированные возможности отчетности, не требующие дополнительного оборудования для создания отчетов

6. Предлагаемый NGFW должен идентифицировать приложения независимо от порта, шифрования SSL/SSH или используемых методов обхода

7. Предлагаемый NGFW должен классифицировать неидентифицированные приложения для управления политиками, криминалистики угроз или разработки технологий идентификации приложений

8. Предлагаемый NGFW обязан быть полноценным устройством с архитектурой однопроходной параллельной обработки для обработки трафика.

9. Предлагаемый NGFW должен разграничивать различные части приложения, такие как разрешение чата Facebook, но блокирование возможности передачи файлов

10. Предлагаемый NGFW должен контролировать доступ и применять политики для веб-сайтов и приложений, включая приложения SaaS

11. Предлагаемый NGFW должен иметь единую ОС во всех форм-факторах

12. Предлагаемый NGFW должен поддерживать создание политик безопасности для предотвращения кражи учетных данных

13. Предлагаемый NGFW должен поддерживать применение многофакторной аутентификации для внутренних приложений

14. Предлагаемый NGFW должен обеспечивать видимость и возможность ограничения приложений, использующих нестандартные порты, в едином правиле политики безопасности

15. Предлагаемый NGFW должен быть способен предоставлять алгоритмы машинного обучения для расширенной защиты непосредственно из NGFW без необходимости внешних подключений

16. Предлагаемый NGFW должен иметь функцию хранения нескольких образов ОС для поддержки устойчивости и легкого отката во время обновления версии

17. Предлагаемые NGFW должен поддерживать распознавание в инспектируемом трафике на Layer-7 модели OSI по сигнатурам, хранимым на нём, следующих категорий приложений:

17.1. Корпоративные приложения:

17.1.1. Сервисы аутентификации, включая Microsoft Active Directory, Netlogon, LDAP, RADIUS, TACACS;

17.1.2. СУБД, включая Microsoft SQL, Oracle, DB2, Postgres, Sybase;

17.1.3. Файловые сервисы, включая Microsoft SMB;

17.1.4. ERP, CRM, включая SAP, 1C;

17.1.5. Системы электронного документооборота и обмена сообщениями, в том числе EMC Documentum, Microsoft SharePoint, Exchange, Lync, Office 365, Google Docs, Lotus;

17.1.6. Протоколы обмена электронной почтой: SMTP, POP3, IMAP;

17.1.7. Протоколы VoIP и аудио-видео-конференций, включая SIP, H.323, H.245, H.225, Webex;

17.1.8. Сервисы обновления программного обеспечения, включая Microsoft Update, антивирусное ПО (Kaspersky, Symantec, TrendMicro, McAfee, ESET), Adobe, Java, Apple;

17.1.9. Сервисы резервного копирования, включая Symantec Backup Exec;

17.1.10. Сервисы виртуализации и терминального доступа, включая VMware, Citrix, Microsoft RDP;

17.1.11. Прочие протоколы и технологии, применяемые для создания распределенных приложений, включая CORBA, SOAP;

17.1.12. Протоколы удаленного доступа, включая Telnet, SSH, VNC, Radmin;

17.1.13. Сетевые протоколы, включая протоколы динамической маршрутизации и SSL, IPsec VPN;

17.2. Приложения сети Интернет:

17.2.1. Электронная почта, включая Gmail, Yandex.Mail, Mail.ru, Hotmail;

17.2.2. Социальные сети, включая Facebook, Google+, LinkedIn, ВКонтакте, Одноклассники, «Мой Мир»;

17.2.3. Средства мгновенного обмена сообщениями, включая ICQ, Jabber, IRC, MSN, аналогичные сервисы в составе перечисленных социальных сетей;

17.2.4. Средства аудио-видео-конференций, включая Skype;

17.2.5. Средства файлового обмена по HTTP(S) и peer-to-peer, включая Dropbox, BitTorrent, eMule, Google Drive, Yandex Disk, Gnutella, Boxnet, SkyDrive, WebDav;

17.2.6. Потоковое аудио-видео (вне зависимости от веб-сайта), включая YouTube, Vimeo, аудио и видео по HTTP;

17.2.7. Средства публикации рабочего стола и предоставления удаленного доступа, включая Team-Viewer, LogMeIn;

17.2.8. Внешние прокси-серверы и анонимайзеры, включая Tor, Ultrasurf, FreeGate, SOCKS, PHP Proxy;

17.2.9. Средства построения частных VPN и туннелирования поверх других приложений, включая FreeNet, Open-VPN, VTun, RDP-to-TCP, TCP-over-DNS;

18. В межсетевом экране должно быть реализовано разграничение функциональности приложений, например, возможность разрешать использование чата Facebook при одновременной блокировке передачи файлов

19. Предоставление встроенных в МЭ средств создания собственных сигнатур приложений по регулярным выражениям с использованием декодеров HTTP(S), FTP, SMB, SMTP, RPC и др., а также по маске для содержимого TCP/UDP-пакетов;

20. Распознавание приложений, передаваемых средствами протокола HTTP/2;

21. Распознавание сетевых приложений по зашифрованному SSL (поддержка ключей RSA до 2048 бит) и SSHv2 трафику, проходящему через межсетевой экран (дешифрация SSL, SSHv2), - как для входящих, так и для исходящих подключений, прозрачно для пользователей в домене, с возможностью контроля отдельных функций приложений, включая отправку сообщений в социальных сетях, файловый обмен, потоковое аудио, видео;

22. Инспекция туннелей:

22.1. Generic Routing Encapsulation (GRE) (RFC 2784);

22.2. Nonencrypted IPSec traffic [NULL Encryption Algorithm for IPSec (RFC 2410);

22.3. Transport mode AH IPSec;

23. Последовательное распознавание различных приложений, используемых в рамках одной сессии;

24. Распознавание пользователей, использующих сетевые приложения, за счет интеграции с корпоративными сервисами аутентификации пользователей, такими как Microsoft Active Directory, Microsoft Exchange, Novell eDirectory, LDAP, Citrix; возможность интеграции с другими сервисами аутентификации (например, контроллерами беспроводных сетей) через открытый XML API; возможность использования принудительной авторизации пользователей, используя WEB страницу – “Captive portal”; поддержка Kerberos, Tacacs+, SAML v.2, поддержка L3-роуминга пользователей с помощью WMI и NetBios опросов;

25. Инспекция передаваемого через межсетевой экран содержимого трафика в реальном режиме времени в потоке по сигнатурам и поведению, защита от уязвимостей, сетевых атак и

вредоносного ПО, распознавания типов файлов по их сигнатурам, определение вирусов, передаваемых по веб, через электронную почту, FTP, SMB, шпионского ПО, сетевых червей, блокировка передачи определенного содержимого с использованием регулярных выражений, в том числе для приложений, использующих шифрование SSL и SSHv2;

26. Создание правил для проходящего через межсетевой экран трафика в единой политике безопасности, используя в качестве квалификаторов следующие параметры каждого соединения:

26.1. IP-адрес отправителя,

26.2. IP-адрес получателя,

26.3. используемые сервисы уровня L4: порты для протоколов TCP и UDP,

26.4. имена пользователей или групп пользователей из Active Directory,

26.5. приложения 7 уровня модели OSI,

26.6. URL категории.

27. Создание правил в единой политике безопасности, используя в качестве квалификаторов данные об IP-адресах отправителя, получателя, используемых сервисов (TCP/UDP-портов), имена пользователей, групп пользователей и используемых пользователем или группой пользователей приложений или определенных категорий приложений. В создаваемых политиках должна иметься возможность реализации следующих действий:

Разрешения или запрета;

Разрешения конкретному приложению или категории приложений использовать только стандартные или строго определенные TCP/UDP-порты. При этом эти порты не должны быть использованы другими приложениями без политики, разрешающей такие взаимодействия в явном виде;

Разрешения, но при этом сканирования на вирусы и другие угрозы;

Разрешения или запрета, основанного на расписании, пользователе или группе пользователей;

Расшифровать и проверить. Если не удалось расшифровать (в случае нестандартного крипто-алгоритма, устаревшего сертификата и др.) – запретить;

Не расшифровывать определенные категории URL и отдельные доверенные веб-сайты;

Применить маркировку DSCP и ограничение по трафику, используя политики QoS на основе приложений, IP-адресов, пользователей и групп пользователей;

Аппаратная реализация QoS для трафика real-time, идентифицируемого на уровне приложений;

Применить перенаправление трафика на основе политик (Policy Based Forwarding);

Разрешить отдельные функции приложения;

Любая комбинация из вышеприведенных действий;

28. Межсетевой экран должен иметь встроенный инструмент оптимизации политик безопасности, обеспечивающий преобразование устаревших политик уровня 4 (основанных на портах) в политики уровня 7, основанные на приложениях

29. Система должна поддерживать возможность использования антивирусной защиты, защиты от шпионского ПО, защиты от уязвимостей и сетевых атак (система обнаружения и предотвращения вторжений), URL-фильтрацию с использованием динамической репутационной базы, поддерживающей категоризацию для разных разделов одного и того же веб-сайта, включая поддержку категорий для веб-сайтов на русском языке, блокировку передачи файлов по типам, определенных сигнатурами. Перечисленный функционал должен быть доступен при использовании соответствующих подписок;

30. Система должна поддерживать встроенную защиту от вредоносного ПО — с помощью сигнатур на основе полезной нагрузки, а не хэша. Данный функционал должен быть доступен при использовании соответствующей подписки;

31. Система обязана иметь возможность предоставлять алгоритмы машинного обучения для расширенной защиты непосредственно из межсетевого экрана без необходимости внешних подключений

32. Модели машинного и глубокого обучения, используемые в межсетевом экране, должны обеспечивать анализ трафика по ключевым протоколам, включая SSL, HTTP, а также неизвестный UDP- и TCP-трафик

33. Возможность дополнительной проверки трафика на предмет неизвестных угроз путём анализа трафика с применением технологии машинного обучения через облачные сервисы. Данный функционал должен быть доступен при использовании соответствующей подписки;

34. Межсетевой экран должен поддерживать эвристический анализ для выявления аномального сетевого трафика и подозрительных пакетов, включая такие шаблоны, как сканирование портов, сканирование узлов и атаки типа «отказ в обслуживании» (DoS).

35. Межсетевой экран должен поддерживать другие возможности защиты от атак, такие как блокировка недопустимых или искаженных пакетов, дефрагментация IP и повторная сборка TCP, защита от методов уклонения и запутывания.

36. Требуется, чтобы межсетевой экран анализировал контекст, обеспечиваемый порядком прибытия и последовательностью нескольких пакетов, чтобы перехватывать и предотвращать методы уклонения

37. Система должна использовать встроенное потоковое обнаружение и предотвращение вредоносных программ, скрытых в сжатых файлах и веб-контенте.

38. Межсетевой экран должен обеспечивать защиту от вредоносной полезной нагрузки, скрытой внутри файлов распространённых форматов, таких как документы Microsoft Office / Microsoft 365 и PDF-файлы.

39. Функционал межсетевого экрана должен обеспечивать корреляцию ряда связанных событий угроз (например, из журналов предотвращения угроз),которые в совокупности указывают на вероятную атаку

40. Система должна предоставлять возможность обнаружения и блокировки неизвестных атак SQL Injection, включая атаки нулевого дня, с использованием поведенческого анализа, эвристик и машинного обучения — без зависимости от сигнатур. Данный функционал должен быть доступен при использовании соответствующей подписки;

41. Межсетевой экран должен поддерживать возможность защиты от неизвестных атак типа Code Injection, выявляя попытки внедрения вредоносного кода через трафик приложений с помощью анализа поведения и отклонений от нормальной активности. Данный функционал должен быть доступен при использовании соответствующей подписки;

42. Система должна предоставлять возможность блокировки несанкционированных постквантовых алгоритмов (PQC) в не расшифровываемом трафике с помощью профилей защиты от уязвимостей. Для расшифровываемого трафика должен использоваться профиль дешифрования, разрешающий только явно указанные шифры и блокирующий все остальные

43. Система должна предоставлять возможность детектирование и фильтрация запросов к ресурсам в сети Интернет в зависимости от категории ресурсов, например, вредоносные сайты, социальные сети, рекламные ресурсы и т.д. Данный функционал должен быть доступен при использовании соответствующей подписки;

44. Система должна предоставлять возможность поддержки действий: разрешить, уведомить, заблокировать, запросить подтверждение пользователя, запросить пароль пользователя при доступе к Web-ресурсам.

45. Система должна поддерживать возможность URL-фильтрации с применением технологии машинного обучения для уменьшения времени реагирования на угрозу. Данный функционал должен быть доступен при использовании соответствующей подписки;

46. Функционал межсетевого экрана должен поддерживать возможность защиты от методов уклонения, таких как маскировка, поддельные CAPTCHA и кодирование символов HTML. Данный функционал должен быть доступен при использовании соответствующей подписки;

47. Межсетевой экран должен позволять классифицировать веб-сайты на основе содержимого, функций и безопасности и включать более 70 категорий безопасного и вредоносного контента. Данный функционал должен быть доступен при использовании соответствующей подписки;

48. Система должна поддерживать рейтинг риска, который оценивает URL-адреса по различным факторам для определения риска. Данный функционал должен быть доступен при использовании соответствующей подписки;

49. Решение должно обеспечивать поддержку нескольких категорий, которая классифицирует URL-адрес до четырех категорий, что позволяет использовать гибкую политику и создавать настраиваемые категории. Данный функционал должен быть доступен при использовании соответствующей подписки;

50. Система должна поддерживать возможность предотвращения появления нежелательного контента в результатах поиска пользователя. Данный функционал должен быть доступен при использовании соответствующей подписки;

51. Межсетевой экран должен поддерживать отображение настраиваемой страницы блокировки с уведомлением пользователя в случае нарушения политик безопасности.

52. Межсетевой экран должен обеспечивать возможность анализа и фильтрации URL, включая выявление вредоносных JavaScript внутри веб-страниц. Данный функционал должен быть доступен при использовании соответствующей подписки;

53. Система должна обеспечивать возможность выявления и блокировки вредоносных и фишинговых веб-страниц, которые используют механизмы обхода автоматического анализа за счёт применения CAPTCHA (включая как легитимные сервисы, такие как Google reCAPTCHA, так и поддельные или кастомные CAPTCHA-интерфейсы). Данный функционал должен быть доступен при использовании соответствующей подписки;

54. Система должна обеспечивать возможность анализа SNI в TLS Hello одновременно с URL в запросе HTTP для противодействуя техникам обхода типа SNIcat;

55. Система должна поддерживать возможность анализа подозрительных DNS-запросов, DGA доменов и локализация зараженных станций с помощью технологии DNS sinkhole (подмена ответа DNS-сервера). Данный функционал должен быть доступен при использовании соответствующей подписки;

56. Система должна поддерживать возможность детектирования техник обхода средств защиты при помощи DNS-запросов пытающихся использовать машинносгенерированные доменные имена DGA, в том числе n-gram частотный анализ, анализ энтропии, частоты запросов, туннелирования внутри DNS, каналов передачи данных средствами DNS-запросов, в том числе ультра-медленных DNS-туннелей. Данный функционал должен быть доступен при использовании соответствующей подписки;

57. Система должна поддерживать возможность блокировки DGA-доменов, DGA-доменов, созданных по словарю, техник обхода DNS-rebinding, FastFlux, обращения к подвисшим записям DNS, атакам NSNX, атакам с недавно зарегистрированных доменов. Данный функционал должен быть доступен при использовании соответствующей подписки;

58. Система должна поддерживать возможность анализа подозрительных DNS-запросов с применением технологии машинного обучения для уменьшения времени реагирования на угрозу. Данный функционал должен быть доступен при использовании соответствующей подписки;

59. Функционал межсетевого экрана должен поддерживать возможность подделывать ответ на DNS-запрос для известного вредоносного домена и заставлять это вредоносное доменное имя преобразовываться в определяемый IP-адрес, предоставленный клиенту для идентификации зараженных хостов. Данный функционал должен быть доступен при использовании соответствующей подписки;

60. Система должна поддерживать возможность предотвращать использование туннелирования DNS, которое использует протокол DNS для туннелирования вредоносных программ и других данных через модель клиент-сервер. Данный функционал должен быть доступен при использовании соответствующей подписки;

61. Система должна поддерживать возможность нарушения сверхнизких/медленных туннелей DNS, которые распространяют туннелированные данные и эксплойты по нескольким доменам и используют очень низкие скорости, чтобы избежать обнаружения, кражи данных или отправки дополнительных вредоносных полезных данных в вашу сеть.

62. Система должна поддерживать возможность предотвращения доменов с быстрым потоком. Данный функционал должен быть доступен при использовании соответствующей подписки;

63. Система должна поддерживать возможность защиты от доменов, тайно добавленных во взломанные зоны DNS авторитативных доменов. Данный функционал должен быть доступен при использовании соответствующей подписки;

64. Система должна поддерживать возможность предотвращения атаки повторной привязки DNS, которые можно использовать для бокового перемещения и атак на службы внутри корпоративной сети из Интернета. Данный функционал должен быть доступен при использовании соответствующей подписки;

65. Система должна поддерживать возможность обнаружения и предотвращения атак типа DNS hijacking — подмены IP-адресов в результате изменения маршрута DNS-запросов или ответов. Данный функционал должен быть доступен при использовании соответствующей подписки;

66. Система должна поддерживать возможность инспекции DNS-запросов (DNS Request) и DNS-ответов (DNS Response) в реальном времени. Данный функционал необходим для выявления вредоносной активности и предотвращения обращений к вредоносным доменам. Данный функционал должен быть доступен при использовании соответствующей подписки;

67. Система должна поддерживать возможность защиты от техник уклонения (evasions), пример MPTCP;

68. Система должна поддерживать возможность мгновенной защиты от ранее неизвестных угроз за счёт использования механизмов машинного обучения, позволяющих выявлять и предотвращать атаки без зависимости от сигнатур. Данный функционал должен быть доступен при использовании соответствующей подписки;

69. Система должна поддерживать возможность использования сервиса сканирования неизвестных потенциально вредоносных файлов в песочнице с операционными системами Microsoft Windows, Linux методом эмуляции запуска и просмотра документов. Данный функционал должен быть доступен при использовании соответствующей подписки;

70. Песочница должна проверять подозрительные исполняемые файлы (в том числе EXE, DLL, SCR, BAT, и др.), ELF файлы, документы форматов PDF, MS Office 2003, 2007 и выше, Java и Flash, Android APK, Mach-O, DMG и PKG, архивы RAR, ZIP, 7Zip. Данный функционал должен быть доступен при использовании соответствующей подписки;

71. Система должна поддерживать возможность отправлять на проверку в песочницу подозрительные файлы, передаваемые в приложениях HTTP, HTTP, SMTP, POP3, IMAP, SMB, FTP, а также их реализации через SSL, если они существуют.

72. Песочница должна генерировать и присылать в межсетевой экран отчет о проверке файла.

73. Система должна поддерживать возможность предотвращать вредоносные программы с высокой уклончивостью, используя скрытое наблюдение, автоматическую распаковку, эмуляцию зависимостей, снятие отпечатков вредоносных программ и интеллектуальный анализ памяти во время выполнения.

74. Песочница должна генерировать сигнатуры для блокирования zero-day для использования на всех межсетевых экранах компании в перечисленных приложениях в течение 5 минут после получения файла на проверку.

75. Система должна поддерживать возможность получения из песочницы сигнатуры файлов и иметь движок блокировки по новым сигнатурам, которые получены от облачной или локальной песочницы.

76. Облачная песочница должна иметь возможность обмена сигнатурами между всеми заказчиками.

77. Система должна поддерживать возможность получать из песочницы индикаторы компрометации: IP, URL, DNS, которые использует вредоносный код и блокировать соединения по списку вредоносных индикаторов.

78. Песочница должна проверять ссылки http:// и https:// в электронной почте по протоколам SMTP/POP3.

79. Песочница должна проверять файлы в приложениях, зашифрованных SSL, минимум в HTTPS протоколе.

80. Песочница должна использовать машинное обучение при инспектировании угроз нулевого дня для уменьшения задержки на инспектирование подозрительного файла;

81. Песочница должна обеспечивать анализ поведения подозрительных файлов и ссылок в частном или внешнем облаке («песочнице»), обнаружение нового вредоносного ПО и автоматическую генерацию антивирусной сигнатуры в течение 5 мин. и обновление репутационной базы URL в течение 30 мин., устанавливаемые на все устройства Заказчика, имеющие соответствующие подписки;

82. Система должна поддерживать возможность интеграции с подсистемой обнаружения угроз «нулевого» дня, реализованной на базе выделенного аппаратного устройства того же производителя (песочницей), размещаемого на центральном объекте Заказчика (частное облако) и позволяющего автоматическую генерацию антивирусной сигнатуры локально на выделенном аппаратном устройстве на площадке ЦОД Заказчика в течение 5 мин.;

83. При использовании локальной песочницы от производителя оборудования она должна иметь API для приема файлов на проверку как от межсетевых экранов, так и сторонних сервисов.

84. Песочница должна создавать отчеты по выполненным проверкам и иметь возможность просмотра этих отчетов в формате PDF.

85. Облачная песочница должна использовать технологию Bare metal analysis без использования эмуляции операционной системы.

86. Система должна поддерживать возможность отправки разных типов файлов в разные песочницы, например, exe файлы в облачную песочницу, а DOC файлы в локальную песочницу.

87. Облачная песочница должна принимать PE файлы на проверку, даже в отсутствии подписки.

88. Система должна поддерживать возможность идентификации устройств Интернет вещей. Данный функционал должен быть доступен при использовании соответствующей подписки;

89. Система должна поддерживать возможность идентификации устройств в сети по множеству признаков, включая MAC-адрес, IP-адрес, операционную систему, тип устройства и прочие параметры, с возможностью последующего применения политик информационной безопасности на основе этих данных. Данный функционал должен быть доступен при использовании соответствующей подписки;

90. Система должна предоставлять развитые функции визуализации: визуализация в простом и удобно читаемом формате активности сетевых приложений, обнаруженных и блокированных сетевых угроз, использующих приложения пользователей. Возможность фильтрации информации, используя различные фильтры (по приложениям, по угрозам, по пользователям, IP-адресам, TCP/UDP-портам, зонам безопасности, типам угроз и др.);

91. Система должна поддерживать возможность автоматической корреляции логов различного типа (межсетевое экранирование, защита от угроз, контроль передачи файлов, URL-фильтрация), сгенерированных в рамках одной сессии;

92. Система должна поддерживать возможность автоматической корреляции событий информационной безопасности на МЭ посредством обновляемых корреляционных объектов, которые задействуют информацию, полученную от антивирусной защиты, защиты от шпионского ПО, защиты от уязвимостей и сетевых атак, защиты от угроз и вирусов 0-ого дня на уровне сети и рабочих станциях с возможностью принудительной аутентификацию пользователя при помощи двухфакторной аутентификации (МФА), для которого сработал корреляционный объект;

93. Система должна поддерживать возможность использования следующих провайдеров многофакторной аутентификации Multi-Factor Authentication (MFA) (напрямую, без использования промежуточных продуктов):

Duo,

Okta,

RSA SecureID,

PingID

94. Система должна поддерживать возможность принудительного применения многофакторной аутентификации к внутренним приложениям;

95. Система должна поддерживать возможность защита от кражи логинов и паролей пользователей за счет интеграции с AD, мониторингом пересылки учетных записей в недоверенную зону безопасности, принудительную аутентификацию пользователя при помощи двухфакторной аутентификации (МФА);

96. Система должна поддерживать возможность предлагать функцию проверки информации о хосте (HIP), собирая и сообщая информацию и атрибуты устройства. Атрибуты профилирования информации о хосте на основе статуса управляемых/неуправляемых сертификатов, типа ОС, версии клиента, имени хоста, идентификатора хоста, серийного номера, модели мобильного телефона, номера телефона, статуса Root/Jailbreak, наличия пароля, установленных приложений, присутствие и состояние агента фаерволла, присутствие и состояние агента защиты от вредоносных программ, присутствие и состояние агента резервного копирования диска, присутствие и состояние агента шифрования диска, присутствие и состояние агента DLP, наличие и состояние списка процессов, наличие и состояние ключа реестра, присутствие и состояние Plist. Данный функционал должен быть доступен при использовании соответствующей подписки;

97. Система должна поддерживать возможность использования функционала защиты от DoS атак;

98. Система должна поддерживать возможность включить все 100% сигнатур IPS, антивируса, URL фильтрации, Application Control и Threat Intelligence без деградации производительности;

99. Система должна поддерживать возможность использования функционала по блокированию ICMP/TCP/UDP сканирования портов;

100. Система должна поддерживать возможность детектирования объектов в файлах, передаваемых по сети, содержащих важную информацию, с блокировкой передачи таких файлов;

101. Система должна поддерживать возможность детектирования наличия фильтруемых данных в файлов, передаваемых по сети, включая, но не ограничиваясь:

Adobe PDF,

HTML,

Microsoft Office (Excel, Word, PowerPoint),

Rich Text Format

102. Система должна поддерживать возможность создания собственных шаблонов данных на базе регулярных выражений;

103. Система должна поддерживать возможность по автоматической генерации отчетов и отчетов по расписанию по различным тематикам (обнаруженные угрозы, объемы переданной информации с разбиением по пользователям, приложениям и пр.), функции по ручной настройке создаваемых отчетов. Должна иметься возможность просмотра отчетов как непосредственно через графический веб-интерфейс управления (GUI) межсетевым экраном, так и возможность экспортирования отчетов в форматы PDF и CSV;

104. Система должна поддерживать возможность интеграции с подсистемой централизованного управления, логирования, отчетности, обновления ПО межсетевых экранов того же производителя;

105. Система должна поддерживать возможность настройки функционала SD-WAN через консоль централизованного управления;

106. Система должна поддерживать возможность использования функционала отправки расшифрованного SSL трафика на внешние устройства, при установки соответствующей лицензии;

107. Система должна поддерживать возможность использования функционала забора трафика с внешних устройств и шифрование в SSL туннель для передачи через Интернет;

108. Система должна поддерживать возможность генерации отдельного отчета по приложениям типа SaaS;

109. Система должна поддерживать функционала IPSec VPN;

110. Система должна поддерживать IPsec-туннели с возможностью использования квантово-устойчивой криптографии (Quantum-Resistant Cryptography), основанной на алгоритмах, защищённых от атак с применением квантовых вычислений, с реализацией стандартов RFC 8784, RFC 9242, RFC 9370.

111. Система должна поддерживать возможность интеграции со сторонними SIEM/SIM-системами по протоколу Syslog с обеспечением гибкой настройки формата логов;

112. Система должна поддерживать возможность аудита конфигурации путем сравнения текущей конфигурации с конфигурацией-кандидатом.

113. Система должна поддерживать возможность быстрого отката изменений от конкретных пользователей и восстановления конфигураций;

114. Система должна поддерживать возможность ролевого управление доступом локальных администраторов:

Возможность ограничить область просмотра и управления на уровне устройства в целом, а также отдельных виртуальных систем (контекстов);

Возможность предоставить доступ в режиме правки или только для чтения, либо запретить доступ к любому разделу веб-интерфейса МЭ;

Возможность предоставить доступ в режиме правки или только для чтения, либо запретить доступ к CLI МЭ.

115. Система должна иметь специализированную аппаратную платформу, позволяющую беспрепятственно управлять устройством даже в случае его полной загрузки. Должны быть обеспечены выделенные вычислительные ресурсы для обработки контролируемого трафика и отдельно для решения задач управления.

116. Управление каждым отдельным устройством должно осуществляться по протоколам HTTPS и SSH без необходимости установки какого-либо дополнительного ПО управления на рабочую станцию администратора.

117. Интерфейс управления межсетевыми экранами (веб и CLI) должен быть унифицирован с подсистемой централизованного управления, логирования, отчетности, обновления ПО.

118. Система должна поддерживать следующие протоколы и режимы функционирования межсетевого экрана:

118.1. Статическая маршрутизация и протоколы динамической маршрутизации BGP, OSPF, RIP;

118.2. Работа сетевых интерфейсов в режимах прослушивания «зеркалированного» трафика со SPAN-портов подключаемого коммутационного оборудования, в прозрачном режиме без

изменения MAC и IP-адресов, в режиме коммутации трафика (Layer 2), в режиме маршрутизации трафика (Layer 3);

118.3. Одновременную работу разных сетевых интерфейсов в любых перечисленных режимах в любой комбинации без ограничений;

118.4. IPv6, включая идентификацию приложений и пользователей;

118.5. Multicast – PIM-SM, PIM-SSM, IGMP v1, v2, v3;

118.6. Маршрутизацию между VLAN, организованными на межсетевом экране;

118.7. Функционал трансляции адресов NAT, сервера DHCP и DHCP relay;

118.8. Тегирование фреймов по 802.1Q (не менее 4094 VLAN);

118.9. Агрегирование интерфейсов по 802.3ad (поддержка LACP);

118.10. Передачу больших пакетов (Jumbo frames);

2.11. Межсетевой экран в количестве 1 штуки:

2.11.1.Требуемые параметры производительности межсетевого экрана:

1. Декларируемая производителем пропускная способность каждого устройства в режиме межсетевого экранирования с обеспечением идентификации приложений и пользователей – не менее 8,5 Гбит\с/сек.;

2. Декларируемая производителем пропускная способность устройства в режиме межсетевого экранирования с обеспечением идентификации приложений и пользователей с включенным функционалом проверки трафика на наличие угроз (всех сигнатур уязвимостей IPS, вредоносного ПО и Anti-spyware) – не менее 4,5 Гбит\с/сек;

3. Декларируемая производителем пропускная способность IPSec VPN – не менее 4,1 Гбит\с /сек;

4. Максимальное количество поддерживаемых сессий уровня приложений – не менее 945 000

5. Количество новых поддерживаемых сессий уровня приложений – не менее 100 000

2.11.2. Требования к сетевым интерфейсам межсетевого экрана:

1/100/1000 Ethernet с разъемом RJ-45 – не менее 8 портов;

1/2.5/5 Гбит\с Ethernet с разъемом RJ-45/PoE – не менее 4 портов;

1 Гбит\с с разъемом SFP– не менее 6 портов;

10 Гбит\с с разъемом SFP+– не менее 4 портов;

Выделенный порт управления межсетевым экраном 10/100/1000 Мбит Ethernet с разъемом RJ-45 – не менее 1 порта;

Консольный порт управления с разъемом RJ-45 – не менее 1 порта;

Консольный порт управления с разъемом USB Micro – не менее 1 порта;

Межсетевой экран должен комплектоваться всеми необходимыми кабелями для включения в сеть электропитания.

В комплект должны входить все необходимые лицензии и подписки для получения всех возможных обновлений программного обеспечения, сигнатур приложений и угроз, репутационной базы URL, DNS запросов, использования сервиса обнаружения угроз «нулевого», сервисы SD-WAN и сервиса защиты IoT устройств в течение 1 года.

На аппаратный межсетевой экран должна быть предоставлена техническая поддержка от производителя на не менее 1 года.

Так же в комплект поставки должны входить:

Модуль SFP 1Gb SR – 2 штуки

Модуль SFP+ 10Gb SR - 2 штуки

2.12. Дополнительные требования:

2.12.1. Поставка должна быть выполнена единовременно и в полном объеме в адрес Заказчика;

2.12.2. Стоимость поставляемого оборудования включает все расходы, связанные с поставкой и транспортировкой товара;

2.12.3. Оборудование должно быть новым. Поставка должна осуществляться с заводской сборкой и предустановкой всех компонентов. Комплект поставки должен соответствовать полной заводской комплектации и сопровождаться официальной гарантией производителя;

2.12.4 Гарантийный период и техническая поддержка на NGFW не менее 12 месяцев, на остальные части комплекса не менее 36 месяцев. Наличие сервисных центров на территории Республики Казахстан;

2.12.5 Заказчик оставляет за собой право проведения экспертизы поставляемого оборудования на предмет соответствия требованиям технической спецификации за счет поставщика;

2.12.6 В целях обеспечения полной технической совместимости и корректного функционирования оборудования все оборудование, поставляемое в рамках Договора, должно быть одного производителя;

2.12.7 Поставщик обязан в течение 5 (пяти) рабочих дней с даты подписания Договора предоставить:

- информацию о предлагаемом к поставке оборудовании в соответствии с требованиями технической спецификации с указанием производителя, модели и продуктового кода (Part Number) по каждой позиции для подтверждения соответствия поставляемого оборудования требованиям технической спецификации посредством сопоставления с информацией, размещенной на официальном интернет-ресурсе производителя;

- авторизационное письмо от производителя либо его официального представительства, подтверждающее право Поставщика на поставку предлагаемого оборудования на территории Республики Казахстан;

- письмо от производителя/лей о наличии сервис центров на территории Республики Казахстан.

3. Технические стандарты

№ п/п	Зарегистрирован в РК	Обозначение	Номер документа	Категория	Наименование	Область применения	Разработчик	Страницы	МКС	Статус	Приказ	Дата введения с
						Настоящий стандарт устанавливает требован					Приказом Председателя Комитета технического регулировани	

1	Да	СТ РК ISO 20648-2019	420444	Национальный стандарт Республики Казахстан	Информационная технология СПЕЦИФИКАЦИЯ TLS ДЛЯ СИСТЕМ ХРАНЕНИЯ ДАННЫХ	ия использования протокола безопасности транспортного уровня (TLS) вместе с технологиями хранения данных	АО "Национальный инфокоммуникационный Холдинг "Зерде" (-)	46	Защита от преступлений	Действует	ю и метрологии Министерства по инвестициям и развитию Республики Казахстан от 24 декабря 2019 года № 479-од	01.01.2021
2	Да	СТ РК ISO/IEC30134–5-2019	420332	Национальный стандарт Республики Казахстан	Информационные технологии. Центры обработки данных Ключевые показатели эффективности. Часть 5. Использование IT-оборудования для серверов (ITEUsv)	Настоящий стандарт определяет использование IT-оборудования для серверов (ITEUsv) в качестве ключевого показателя производительности (KPI) для количественной оценки использования серверов в центре обработки данных	АО "Национальный инфокоммуникационный Холдинг "Зерде" (-)	28	Наборы знаков и кодирование информации	Действует		01.01.2021

Подписал Изгалиев Аскар Алмасович

Дата подписания 16.10.2026