**Тауарларды мемлекеттік сатып алудың техникалық ерекшелігі**

**«Желі трафигін тексеру мүмкіндігі бар брандмауэр»**

|  |  |  |
| --- | --- | --- |
| **№**  **п/п** | **Құрылымдық** | **Ескерту** |
| **1.** | **Тауарлардың, жұмыстардың, қызметтердің атауы** | **Желілік трафикті тексеру мүмкіндігі бар шекара, брандмауэр (бұдан әрі - жабдық)** |
| **2.** | **Ұлттық стандарттардың атауы.** | **ГОСТ 30804.3.2-2013** «Техникалық құралдардың үйлесімділігі электромагниттік. Ток шығыны 16 А аспайтын (бір фазада) техникалық құралдармен токтың гармоникалық құрамдас бөліктерін шығару. Нормалар мен сынақ әдістері» |
| **3.** | **Шыққан жылы** | 2021 жылдан кем емес |
| **4.** | **Кепілдік мерзімі** | 12 айдан кем емес |
| **5.** | **Қажетті функционалдық, техникалық сипаттама,**  **сатып алынатын тауардың сапасы, пайдалану және басқа да сипаттамалары** | **Жабдық:**  1. Брандмауэр – 1 жиын;  2. Қуат кабелі 220 В кемінде 1,5 метр;  3. Тірекке орнатуға арналған құлақтар;  4. Құжаттама.  **Пішін факторы:** 1U макс, 19 дюймдік тірекке орнатуға болады;  **Брандмауэрге қойылатын техникалық талаптар:**  - минималды өнімділік:  Брандмауэр өткізу қабілеті (1518/512/64 байт UDP(User Datagram Protocol)): 30/29/23 Гбит/с кем емес;  Сеанстардың бір мезгілдегі саны: кемінде 3,7 миллион;  Жаңа байланыстарды орнату жылдамдығы: секундына 430 000 кем емес;  Өткізу қабілеті IPS Enterprise Mix: кемінде 7,7 Гбит/с;  Қолданбаны басқару өткізу қабілеттілігі (HTTP 64K): кемінде 11 Гбит/с;  Қауіптерден қорғау режиміндегі өткізу қабілеттілігі (барлық қауіпсіздік профильдері қосылған): кемінде 5 Гбит/с;  Негізгі конфигурациядағы виртуалды қауіпсіздік контексттерінің саны: 10-нан кем емес;  Интерфейстердің саны: кемінде 16x GE SFP, 16x GE RJ45;  Бөлінген басқару порттарының саны: 1-ден кем емес;  USB порттарының саны: 1-ден кем емес;  Айнымалы ток 100-ден 240В-қа дейінгі қуат көзі  **Басқару:** SSH, HTTP, HTTPS қолдауы керек;  **Қуат көзі:** 100 - 240 В айнымалы ток (50 - 60 Гц).  **Ақауларға төзімділік:** Белсенді/Белсенді, Белсенді/Пассивті режимдерінде артықшылықты қолдау.  **Интерфейстер:** келесі жұмыс режимдерін қолдайтын кемінде 16 10/100/1000 Base-T RJ-45: L2, L3, Tap, Виртуалды сым (мөлдір режим); кемінде 16 SFP модулі, кем дегенде бір RJ-45 консольдық сериялық порты; кем дегенде бір USB порты; кем дегенде бір жоғары қолжетімді порт; кем дегенде бір 10/100/1000 Base-T RJ-45 басқару порты. |
|  |  | **Брандмауэр бағдарламалық қамтамасыз ету талаптары:**  жүйені лицензиялау пайдаланушылардың шектеусіз саны үшін жүзеге асырылуы тиіс;  - жүйе қауіпсіздік модульдерінің қолтаңбаларының жаңартуларын және өндірушінің серверінен ағымдағы қауіптер тізімін тұрақты түрде алуы керек;  - жүйе кластер түрлерін құру мүмкіндігі бар кем дегенде 4 құрылғыны кластерлеуді қолдауы керек:  • суық резервпен (белсенді/пассивті);  • ыстық күту режимімен (белсенді/белсенді);  • баланстау кластері;  - жүйе брандмауэр функциясына ие болуы керек, яғни IP мекенжайлар, порттар және қосымшалар негізінде желілік трафикті сүзу ережелерін құру мүмкіндігін қамтамасыз етуі керек;  - жүйеде жүктемені теңестіру функциясы болуы керек;  - жүйе трафикті басқарудың интеллектуалды технологиясын SD-WAN (Software-Defined Wide Area Network, software-defined network) қолдауы керек;  - жүйеде трафик өткізу қабілеттілігін басқару (трафикті қалыптастыру) функционалдығы болуы керек;  - жүйе тексерілетін трафикті ICAP протоколы (Internet Content Adaptation Protocol) арқылы сыртқы жүйелерге талдау және беру мүмкіндігімен SSL трафигін тексеруді қамтамасыз етуі керек;  - жүйе ZTNA (Zero Trust Network Access) тұжырымдамасын іске асыру мүмкіндігін қамтамасыз етуі керек;  - жүйе Secure Shell (SSH) трафигінің талдауын қамтамасыз етуі керек (ssh инспекциясы);  - жүйе Internet Protocol v4 және Internet Protocol v6 протоколдарынан төмен емес хаттамалар бойынша динамикалық бағыттауды қамтамасыз етуі керек;  - жүйе Web Cache Communication Protocol (WCCP) төмен емес хаттамада жұмыс істей алуы керек (сервер режимінде де, клиенттік режимде де);  - жүйе кем дегенде Wide Area Network (WAN) қосылымдарын оңтайландыруды қамтамасыз етуі керек;  - жүйеде деректердің ағып кетуін болдырмау (DLP) функционалдығы болуы керек;  - жүйе аппараттық жеделдетілген антивирустық қорғауды қамтамасыз етуі керек;  - жүйе спамнан (антиспам) қорғауды қамтамасыз етуі керек;  - жүйеде аппараттық жеделдетілген интрузияның алдын алу жүйесінен (IPS) төмен емес енудің алдын алу функционалдығы болуы керек;  - жүйе сайттардың белгілі бір санаттарына кіруді шектеу мүмкіндігімен WEB трафикті сүзуді қамтамасыз етуі керек;  - WEB-трафикті сүзгілеу кемінде 85 санат бойынша қамтамасыз етілуі керек;  - танымал іздеу жүйелеріне қауіпсіз іздеу режимін мәжбүрлеп енгізу;  - жүйеде қолданбалы басқару функционалдығы болуы керек;  - жүйеде WEB прокси функциясы болуы керек;  - жүйе әдепкі бойынша қол жетімді кемінде 10 виртуалды доменнің (бір құрылғыдағы толық функционалды виртуалды желіаралық қалқандар) болуын қамтамасыз етуі керек;  - жүйе кем дегенде HTTP, SMTP, POP3, IMAP, FTP және IM трафигі ішінде вирустарды тексере алуы керек;  - жүйе антивирустық деректер базасының жоспарлы жаңартуларын автоматты түрде қабылдау мүмкіндігі болуы керек;  - жүйе жұқтырған хабарламаларды карантинге алу мүмкіндігі болуы керек;  - жүйе өлшемі мен түріне байланысты файлдарды тасымалдауды блоктай алуы керек;  - жүйе бірнеше (Wide Area Network) WAN желілерінің қосылымдарын қолдауы керек;  - жүйе PPPoE және L2TP төмен емес хаттаманы қолдауы керек;  - жүйе «Клиент/Сервер» конфигурациясында DHCP протоколынан төмен емес қолдау көрсетуі керек;  - жүйе саясатқа негізделген маршруттауды қолдауы керек;  - жүйе RIP v1 және v2, OSPF, BGP төмен емес хаттамалар негізінде динамикалық маршруттауды қолдауы керек;  - жүйе қауіпсіздік аймақтарын пайдалануды қолдауы керек;  - жүйе аймақтар арасындағы маршруттауды қолдауы керек;  - жүйе виртуалды желілер арасындағы маршруттауды қолдауы керек;  - жүйе рөлдік басқаруды қолдауы керек;  - жүйе әкімшілер мен пайдаланушылардың бірнеше деңгейін қолдауы керек;  - жүйе TFTP және web-интерфейсінен төмен емес хаттама арқылы орнатылған бағдарламалық қамтамасыз етуді жаңартуды қолдауы керек;  - жүйе енгізілген бағдарламалық қамтамасыз етудің алдыңғы күйіне (нұсқасына) оралу мүмкіндігін қолдауы керек;  - жүйе ішкі деректер базасы арқылы пайдаланушының аутентификациясын қолдауы керек;  - жүйе пайдаланушылар үшін желілік аутентификация протоколын (Kerberos) қолдауы керек;  - жүйе кем дегенде Windows Active Directory арқылы пайдаланушы аутентификациясын қолдауы керек; бұл ретте доменге кіретін Windows 7 және одан жоғары емес операциялық жүйелерді пайдаланушылардың аутентификациясы парольдерді сұраудың қосымша процедураларынсыз автоматты түрде орындалуы тиіс;  - жүйе сыртқы RADIUS/LDAP дерекқоры арқылы пайдаланушының аутентификациясын қолдауы керек;  - жүйе IP/MAC мекенжайын байланыстыру арқылы пайдаланушының аутентификациясын қолдауы керек;  - жүйе пайдаланушылар топтары негізінде аутентификацияны қолдауы керек;  - жүйе NAT, PAT, «мөлдір» (көпір) төмен емес функцияларды қолдауы керек;  - жүйе саясатқа негізделген NAT-тан төмен емес функцияларды қолдауы керек;  - жүйе VLAN Tagging (802.1Q) төмен емес функцияларды қолдауы керек;  - жүйе SIP/H.323 NAT Traversal төмен емес функцияларды қолдауы керек;  - жүйе қауіпсіздік профильдерінің конфигурациясын қолдауы керек;  - жүйе URL/кілт/сөз/фраза бойынша блоктау мүмкіндігі болуы керек;  - жүйе URL мекенжайларының «Ақ» тізімдерін қолдауы керек;  - жүйе Java апплеттерін, Cookie файлдарын, ActiveX басқару элементтерін блоктай алуы керек;  - жүйе желілік шабуылдардың кем дегенде 10 000 түрін болдырмауға қабілетті болуы керек;  - жүйе шабуыл қолтаңбаларының тізімін конфигурациялай алуы керек;  - жүйе шабуылдардың деректер базасын және IPS қолтаңбаларын автоматты түрде жаңартуды қолдауы керек;  - жүйе өндірушінің серверінен спам жіберушілердің және ашық релелердің IP мекенжайларының «қара» тізімін тұрақты түрде алуы керек;  - жүйе MIME тақырыптарын тексеруді қолдауы керек;  - жүйе электрондық поштаны кілт сөздер мен сөз тіркестері бойынша сүзуді қолдауы керек;  - жүйе IP мекенжайларының «қара/ақ» тізімдері бойынша сүзуді қолдауы керек;  - жүйе журналдарды қашықтағы syslog серверіне жібере алуы керек;  - жүйе бастапқы файл пішімін сақтай отырып, Microsoft Office және PDF файлдарынан орындалатын компонентті шығару қызметін қолдауы керек;  - жүйеде желілік трафикті, жүйе күйін және анықталған қауіптерді бақылаудың графикалық құралдары болуы керек;  - жүйе вирустар мен желілік шабуылдар туралы хабарламаларды электронды пошта арқылы жіберу мүмкіндігі болуы керек;  - жүйе VRRP төмен емес хаттаманы қолдауы керек;  - жүйе SIEM-пен интеграцияны қолдауы керек;  - жүйе кепілді, максималды немесе басым өткізу қабілеттілігін белгілей алуы керек;  - жүйе жедел хабар алмасу қызметтерін табуды және пайдалануды бақылауды қолдауы керек;  - жүйе веб-ресурстарға қол жеткізудің өткізу қабілеттілігі мен жылдамдығын оңтайландыру үшін веб-контентті жергілікті сақтау мүмкіндігін қолдауы керек;  - жүйе веб-интерфейс арқылы басқаруды қолдауы керек;  - жүйе орталықтандырылған басқару және есеп беру жүйелерімен интеграциялануы тиіс;  - жүйе NetFlow, sFlow протоколдарынан төмен емес хаттамаларды қолдауы керек;  - жүйе кері прокси режимін қамтамасыз етуі керек;  - жүйе мөлдір прокси сервер режимін қамтамасыз етуі керек (мөлдір прокси);  - жүйе пәрмен жолынан консоль режимінде қауіпсіздік саясатын басқару мүмкіндігін қамтамасыз етуі керек;  - жүйе пайдаланушылар, қолданылатын операциялық жүйенің моделі мен нұсқасы, IP мекенжайы, MAC мекенжайы, анықталған осалдықтар туралы ақпаратты қоса алғанда, телеметриялық ақпаратты алу үшін сыртқы жүйелермен интеграцияны қолдауы керек;  - жүйе жұмыс станцияларының корпоративтік қауіпсіздік саясатына сәйкестігін бағалау үшін сыртқы жүйелермен интеграцияны қолдауы керек. Қауіпсіздік саясатына сәйкес келмеген жағдайда, тексерілген хост желіге кіру шектелген карантинге қойылуы керек;  - жүйе сымсыз кіру нүктелерін басқару мүмкіндігін қамтамасыз етуі керек;  - жүйе ажыратқыштарды басқару мүмкіндігін қамтамасыз етуі керек;  **Брандмауэрде алдын ала орнатылған жазылымдар болуы керек:**  1. IPS енуді анықтау және алдын алу жүйесі күнделікті автоматты түрде жаңартылатын дерекқор негізінде трафикті талдауы және желідегі ауытқуларды анықтауы керек. Теңшелетін қолтаңбаларды жасау мүмкіндігіне қолдау көрсету керек.  2. Антивирус – нақты уақыт режимінде дәстүрлі және мобильді платформаларда вирустар мен зиянды кодтарды анықтауды және бейтараптандыруды қамтамасыз етуі керек. Вирусқа қарсы қолтаңбалар автоматты түрде жаңартылуы керек.  3. Веб және бейнені сүзу жаһандық дерекқор негізінде қажет емес URL мекенжайлары мен бейнелерді сүзуі керек. Деректер базасы күн сайын жаңартылып, тез және оңай теңшеу үшін санаттарға бөлінуі керек. Белгілі бір сайттар мен бейне арналарды пайдалануды шектеу мүмкіндігі болуы керек.  4. Антиспам электрондық пошта қызметтерін (SMTP, POP3, IMAP) тексеруі және IP беделі мен жеке қолтаңбалары негізінде СПАМды бейтараптандыруы керек. Сүзу опциялары үшін параметрлерді және мекенжайлардың ақ және қара тізімдерін жасау мүмкіндігін қамтамасыз етіңіз.  5. Зиянды кодтың құмсалғыш қызметіне жазылу Қызмет эмуляция ортасы күдікті немесе заңды деп белгілейтін белгісіз қауіптерге файлдарды жүктеп алып, талдайды.  6. Тәулік бойы қолдау көрсету қызметіне жазылу бағдарламалық қамтамасыз етуді жаңарту, билеттерді ашу және жүргізу бойынша өндірушінің техникалық қолдау қызметіне хабарласу, жабдықпен жұмыс істеу бойынша техникалық кеңес беру, сондай-ақ істен шыққан жағдайда жабдықты кеңейтілген ауыстыру мүмкіндігін қамтамасыз етуі керек. |
| **6.** | **Ілеспе қызметтер** | Брандмауэр құнына мыналарды қамтуы керек: жеткізу, орнату, сонымен қатар тапсырыс берушінің жауапты қызметкерін оқыту. |
| **7.** | **Жеткізушіге қойылатын талаптар** | Конкурс шеңберінде Әлеуетті жеткізуші өндірушіден немесе оның ресми өкілінен (дилерден немесе дистрибьютордан) Әлеуетті жеткізушінің техникалық ерекшелігінде көрсетілген рұқсат хатын ұсынуы тиіс. |