ՆԿԱՐԱԳԻՐ

առաջարկվող ապրանքի ամբողջական

Ստեպ Լոջիկ ՍՊԸ-ն ԵՊՀ-ԷԱՃԱՊՁԲ-25/142 ծածկագրով կազմակերպված էլեկտրոնային աճուրդին մասնակցելու շրջանակում ներկայացնում է իր կողմից առաջարկվող ապրանքի ամբողջական նկարագիրը

Չափաբաժնի համար	Առաջարկվող ապրանքի			
	ֆիրմային անվանումը	մակնիշը	արտադրողի անվանումը	տեխնիկական բնութագիրը
1	Palo Alto Networks	PAN-PA-1420	Palo Alto Networks	1.1 Առաջարկվող լուծումները/հարթակները/սարքավորումները արտադրողի կողմից 2 տարի չպետք է հայտարարվեն վաճառքից դուրս (End-of-Sale)՝ մատակարարման պայմանագրի կնքման պահից սկսած: 1.2 Ծրագրի շրջանակներում առաջարկվող լուծումները/հարթակները/սարքավորումները արտադրողի կողմից 4 տարի չպետք է հայտարարվեն սպասարկումից դուրս (End-of-Support) մատակարարման պայմանագրի կնքման պահից սկսած: 1.3 Ամբողջ առաջարկվող սարքավորումների և ծրագրային ապահովման համար տրամադրվում են սպասարկման պայմանագրեր արտադրողի կողմից, որը ներառելու է երաշխիք, ծրագրային ապահովման և ֆունկցիոնալ կախյալ ծրագրային բաղադրիչների

					թարմացումներ 1 տարի ժամկետով(Threat prevention, Advanced URL Filtering, Partner enabled premium support)։ 2. Լուծման ճարտարապետությանը ուղղված պահանջներ Առաջարկվող լուծման առաջարկը պարունակում է 2.1 Թվով 1 բարձր արտադրողականությամբ ապարատային միջցանցային էկրան, որպես ցանցային և անվտանգության ենթահամակարգ: Վերջինս պետք է հնարավոր լինի տեղադրել 19" սերվերային պահարանում և օժտված լինի առնվազն երկու սնուցման աղբյուրով, փոփոխական միաֆազ 220Վ լարմամաբ աշխատանքի հնարավորությամբ։ Պետք է լինի նոր, չօգտագործված։ Միջցանցային էկրանը պետք է ունենա առնվազն 4x10/100/1000(RJ-45), 4x1G/2.5G/5G(RJ-45), 4x1G/2.5G/5G/PoE(RJ-45) և 2x1G SFP, 8x1G/10G SFP/SFP+ պորտեր: 2.2 Լրացուցիչ տրամադրվում է թվով 8 SFP մոդուլներ, որոնցից առնվազն 2-ը 10GBASE-SC-10KM T1310nm համատեղելի առաջարկվող սարքավորման հետ, 2-ը 10GBASE-SC-10KM T1550nm համատեղելի MikroTik սարքավորման հետ, 2-ը 10GBASE-SC-3KM T1310nm համատեղելի առաջարկվող սարքավորման հետ, 2-ը 10GBASE-SC-3KM T1550nm համատեղելի MikroTik սարքավորման հետ: 3. Ցանցային և անվտանգության ենթահամակարգին ուղղված պահանջներ Անվտանգության ենթահամակարգը (ապարատային միջցանցային էկրան) ապահովում է՝ 3.1 Միջցանցային էկրանավորում սեսիաների վերահսկողություն 3.2 Ցանցային էկրանով անցնող ցանցային հավելվածների բացահայտում և

					արգելափակում OSI մոդելի 7-րդ մակարդակում որոնք աշխատում են ընդհանուր պորտով, ներառյալ 80 և 443 , ինչպես նաև դինամիկ պորտեր. 3.3 Threat Prevention (Intrusion Prevention, Anti-Malware, Anti-Virus) և URL filtering ֆունկցիոնալի առկայություն, առնվազն 5 Գբ/վ գումարային արտադրողականությամբ։Անհրաժեշտ լիցենզիաները պետք է առաջարկի մաս կազմեն և ենթարկվեն 1.3 կետի պահանջներին։ 3.4 Առաջարկվող լուծումը ներկայացված է ըստ 2024 թվականի, Gartner –ի կորպորատիվ միջցանցային էկրաններ բաժնի առաջատար կազմակերպություններից մեկի կողմից, (Fortinet, Check Point Quantum, Palo Alto Networks, Cisco)։ 3.5 Ապարատային միջցանցային էկրանը իր մեջ ներառում է կառավարման համար նախատեսված հատուկ առանձնացված ենթահամակարգ, որը թույլ կտա իրականացնել սարքի անխափան ղեկավարում նույնիսկ սարքի ամբողջովին բեռնված լինելու պայմաններում։ 3.6 Սարքի հիմնական ղեկավարումը իրականացվում է HTTPS և ssh պրոտոկոլների միջոցով ղեկավարման կայանում առանց հատուկ ղեկավարման ծրագրային լուծում տեղադրելու անհրաժեշտության։ 3.7 Առաջարկվող միջցանցային էկրանի, արտադրողի կողմից ներկայացված արտադրողականությունը և թողունակությունը պետք է համապատասխանեն հետևյալ պահանջներին. 3.7.1 Միջցանցային էկրանի ռեժիմում, հավելվածների և օգտատերերի իդենտիֆիկացիայով, ոչ պակաս քան 9.5 Գբիտ/վ 3.7.2 Միջցանցային էկրանի ռեժիմում հավելվածների և օգտատերերի իդենտիֆիկացիայով, ցանցային

					վտանգների ստուգմամբ (բոլոր տեսակի signature-ների և հակավիրուսային ենթահամակարգի օգտագործում) ոչ պակաս քան 5 Գբիտ/վ 3.7.3 Վայրկյանի ընթացում նոր սեսիաների մաքսիմալ քանակ - ոչ պակաս քան 150000 հատ: 3.7.4 Սպասարկվող սեսիաների մաքսիմալ քանակ – ոչ պակաս քան 1 400 000 3.8 Միջցանցային էկրանում սպասարկվող պրոտոկոլների և աշխատանքային ռեժիմների հանդեպ պահանջները հետևյալն են. 3.8.1 Ստատիկ երթուղավորում, ինչպես նաև դինամիկ երթուղավորման պրոտոկոլներ BGP, OSPF, RIP v2 3.8.2 Կոմուտացիոն սարքավորումներից ստացվող SPAN ինֆորմացիայի մշակման ցանցային ինտերֆեյսների աշխատանքի ռեժիմ առանց mac հասցեների փոփոխության, տրաֆիկի կոմուտացիայի ռեժիմ, տրաֆիկի երթուղավորման ռեժիմ 3.8.3 Ցանցային տարբեր ինտերֆեյսների թվարկված ռեժիմներում ցանկացած համադրությամբ զուգահեռ աշխատանք առանց սահմանափակումների 3.8.4 Ipv6 աշխատանքի հնարավորություն , հավելվածների և օգտատերերի իդենտիֆիկացիայով 3.8.5 Միջցանցային էկրանում կարգաբերված vlan-ների միջև երթուղավորման հնարավորություն 3.8.6 NAT, DHCP server և DHCP relay հնարավորություն 3.8.7 MAC հասցեների և ARP գրառումների աղյուսակ, ոչ պակաս քան 6000 գրառում 3.8.8 Ինտերֆեյսների ագրեգացիա 802.3ad պրոտոկոլով 3.8.9 Վիրտուալ երթուղիչների հնարավորություն առնվազն 10 հատ 3.8.10 Անվտանգության տիրույթների ստեղծման հնարավորություն առնվազն 50 հատ 3.9 Առաջարկվող

ПОЛНОЕ ОПИСАНИЕ

предлагаемого товара

ООО Стэп Лоджик в качестве участника в рамках участия в электронном аукционе под кодом ԵՊՀ-ԷԱՃԱՊՁԲ-25/142 ниже представляет полное описание предлагаемого им товара.

Номер лота			Предлагаемый товар	
	фирменное наименование	марка	наименование производителя	технические характеристики
1	Пало Альто Нетворкс	PAN-PA-1420	Пало Альто Нетворкс	1.1 Предлагаемые решения/платформы/оборудование не должны быть заявлены производителем как снятые с продаж в течение 2 лет с момента подписания договора поставки. 1.2 Решения/платформы/оборудование, предлагаемые в рамках программы, не должны быть объявлены производителем как неподлежащие обслуживанию (End-of-Support) в течение 4 лет с момента подписания договора поставки. 1.3 Все предлагаемое оборудование и программное обеспечение должно быть обеспечено договорами на обслуживание от производителя, которые будут включать гарантию, обновления программного обеспечения и функционально зависимых программных компонентов сроком на 3 года (предотвращение угроз; լուծումը պետք է ապահովի ցանցային հավելվածներից օգտվող օգտատերերի բացահայտում, վավերացման այնպիսի կորպորատիվ ծառայությունների հետ ինտեգրման միջոցով, ինպիսիք են Microsoft Active Directory: Պետք է ապահովի օգտատերերի հարկադիր վավերացման հնարավորություն վեբ էջի միջոցով (captive portal): 3.10 Միջցանցային էկրանով անցնող տրաֆիկի ստուգում անցման ընթացքում signature-ներով և վարքով, խոցելիությունների, ցանցային հարձակումների և վնասակար ծրագրային ապահովումից պաշտպանություն, ֆայլերի տիպերի բացահայտում ֆայլերի signature-ներով, էլեկտրոնային փոստով , FTP-ով, SMB-ով փոխանցվող վիրուսների հայտնաբերում, լրտեսական ծրագրային ապահովման աշխատանքի կանխում, փոխանցվող տվյալներում նախապես նկարագրված պարունակության հայտնաբերում և կանխում ներառյալ sshv2 ու SSL-ով փոխանցվող տվյալներում: 3.11 Ջեկուլցների աջակցություն, Միջցանցային էկրանը պետք ունենա ավտոմատ ներառվ կամ ըստ ժամանակացույցի ծնավորել տարբեր բնույթի (բացահայտված վտանգներ, փոխանցվածծ ինֆորմացիայի ծավալ ըստ օգտատերների , հավելվածների և այլն) զեկուլցներ, ստեղծվող զեկուլցների անհատական կարգաբերում: Անհրաժեշտ է ունենալ հնարավորություն ստեղծվող զեկուլցները ըիտել գրաֆիկական վեբ ինտերֆեյսի միջոցով ինչպես նաև արտահանել PDF և CSV ֆայլերի տեսքով: 5. Պահանջներ մրցույթին մասնակցող ընկերությունների

				Обнаружение и блокировка сетевых приложений, проходящих через сетевой экран на уровне 7 модели OSI, работающих на общем порту, в том числе 80 и 443, а также динамических портах; 3.3 Наличие

					функции предотвращения угроз (Предотвращение вторжений, Anti-Malware, Anti-Virus) и URL-фильтрации, с общей производительностью не менее 5 Гбит/с. Необходимые лицензии должны быть частью предложения и с учетом требований пункта 1.3. 3.4 Предлагаемое решение должно быть представлено одной из ведущих организаций подразделения корпоративных межсетевых экранов Gartner в соответствии с 2024 г. (Fortinet, Check Point Quantum, Palo Alto Networks, Cisco). 3.5 Аппаратный межсетевой экран должен включать выделенную подсистему управления, которая позволит осуществлять бесперебойное управление устройством даже при полной загрузке устройства. 3.6 Базовое управление устройством должно осуществляться по протоколам HTTPS и ssh на станции управления без необходимости установки специального программного решения для управления. 3.7 Производительность и пропускная способность предлагаемого межсетевого экрана, представленного производителем, должны отвечать следующим требованиям: 3.7.1 В режиме межсетевого экрана, с идентификацией приложения и пользователя, не менее 9,5 Гбит/с. 3.7.2 В режиме межсетевого экрана с идентификацией приложений и пользователей, проверкой сетевых угроз (использование всех типов сигнатур и антивирусной подсистемы) не менее 5 Гбит/с 3.7.3 Максимальное количество новых сессий в секунду – не менее 150 000. 3.7.4 Максимальное количество поддерживаемых

					сессий – не менее 1 400 000. 3.8 Требования к протоколам и режимам работы, поддерживаемым на межсетевом экране, следующие: 3.8.1 Статическая маршрутизация, а также протоколы динамической маршрутизации BGP, OSPF, RIP v2 3.8.2 Режим работы сетевых интерфейсов для обработки SPAN-информации, полученной от коммутационного оборудования, без изменения MAC-адресов, режим коммутации трафика, режим маршрутизации трафика. 3.8.3 Параллельная работа без ограничений в любом сочетании перечисленных режимов различных сетевых интерфейсов 3.8.4 Функциональность IPv6 с идентификацией приложений и пользователей 3.8.5 Возможность маршрутизации между виртуальными локальными сетями, настроенными в брандмауэре 3.8.6 NAT, DHCP-сервер и возможность ретрансляции DHCP 3.8.7 Таблица MAC-адресов и записей ARP, не менее 6000 записей 3.8.8 Агрегация интерфейсов с протоколом 802.3ad 3.8.9 Возможность виртуальных роутеров не менее 10 шт. 3.8.10 Возможность создания не менее 50 доменов безопасности 3.9 Предлагаемое решение должно обеспечивать идентификацию пользователей с помощью сетевых приложений, аутентификацию посредством интеграции с корпоративной информацией, такой как Microsoft Active Directory. Должна обеспечиваться возможность принудительной аутентификации пользователей через веб-страницу (captive-портал). 3.10 Проверка трафика, проходящего через

					межсетевой экран, с сигнатурами и поведением при передаче, защита от уязвимостей, сетевых атак и вредоносного ПО, обнаружение типов файлов с сигнатурами файлов, обнаружение вирусов, передающихся по электронной почте, FTP, SMB, предотвращение шпионской активности, обнаружение и предотвращение заранее определенного содержимого в передаваемых данных, включая данные, передаваемые по sshv2 и SSL. 3.11 Подготовка отчетов. Межсетевой экран должен иметь возможность формировать отчеты различного характера (обнаруженные угрозы, объем информации, переданной пользователями, приложениями и т.п.) автоматически или по расписанию, индивидуальную настройку формируемых отчетов. Необходимо иметь возможность просматривать сформированные отчеты через графический веб-интерфейс, а также экспортировать их в файлы PDF и CSV. 5. Требования к компаниям, участвующим в конкурсе 5.1 Компания обязана иметь сотрудников, имеющих профильный опыт проектирования, монтажа и эксплуатации предлагаемых решений, для бесперебойного выполнения работ по интеграции систем качества. Поставщик должен иметь не менее двух успешных проектов по поставке и монтажу аналогичного оборудования, имеющих соответствующую документацию. Победитель, занявший первое место, должен предоставить копию лицензированного гарантийного сервисного центра, а также письмо-

				сертификат (MAF) от производителя. 5.2 При установке и эксплуатации предлагаемой системы должна быть обеспечена полная работа функций, выполняемых существующей (заменяемой) системой и устройствами. 5.3 Компания обязуется предоставить установленную и полностью работоспособную систему в течение 30 календарных дней после поставки. 5.4 Компания в течение 3-х месяцев после приемки работ обязуется предоставить специалистов, при необходимости, с целью внесения изменений и поддержания текущей конфигурации установленного оборудования.