ПРИЛОГ 2

ПОЗИВА ЗА ПОДНОШЕЊЕ ПОНУДЕ ЗА НАБАВКУ СИСТЕМА ЗА УНАПРЕЂЕЊЕ РЕШЕЊА ЗА НЕСПЕЦИФИЦИРАНЕ СИСТЕМЕ
број: С32-2-6497 од 19.12.2025.године
(Техничка спецификација)

Обавезни захтеви за NG firewall уређаје:

Предмет набавке је испорука и имплементација решења за унапређења система за неспецифициране системе засновано на (PAN-PA-3440 или еквивалент)

1. Понуђени уређаји морају бити специјализовани мрежни хардверски уређаји, који морају имати подршку за рад у моделу високе доступности (HA - *High Availability*), у начинима рада Активно/Пасивно и Активно/Активно.
2. Понуђени уређаји морају имати могућност рада у следећим начинима:
   - *routing* (тј. у слоју 3 ISO OSI модела),
   - *bridging* (тј. у слоју 2 ISO OSI модела),
   - у транспарентном начину,
   - у начину пасивног слушања (тзв. *sniffer/tap*).
3. Понуђено решење мора моћи радити у свим горе наведеним модовима истовремено, на различитим интерфејсима инспекције, у једној логичкој инстанци firewall система.
4. Понуђени уређаји морају бити опремљени с најмање једним, RJ45 базираним, серијским конзолним прикључком, као и са најмање једним наменским управљачким (*management*) интерфејсом имплементираним као Ethernet RJ45 10/100/1000 Mbps прикључак.
5. Уређаји морају бити опремљени с најмање 2 x AC 230V напајања, која раде редундантно. Напајања морају бити замењива, уз могућност замене оштећеног напајања док уређај ради.
6. Понуђени уређаји морају имати логичку раздвојеност ресурса који се користе за обраду саобраћаја (*data plane*) од ресурса који се користе за управљање уређајем (*management plane*). Логичко одвајање ресурса може бити реализовано додељивањем наменског броја језгара ресурса процесора (*CPU cores*) обема функцијама, или алтернативно коришћењем засебних наменских процесора (*CPU*) за сваку функцију.
7. Понуђено решење мора бити у стању да обезбеди алгоритам машинског учења за напредну заштиту директно у оквиру платформе, без потребе за екстерним конекцијама.
8. Понуђени уређаји морају подржавати Ethernet протокол, с подршком за VLAN *tagging*, компатибилног са стандардом IEEE 802.1q. VLAN подинтерфејси могу се креирати на мрежним интерфејсима који раде u L2 i L3 modu. Уређај мора подржавати минимално 4000 VLAN-ova.
9. Понуђени уређаји морају подржавати LACP протокол.
10. Понуђени уређаји морају, сходно утврђеној политици конфигурације, контролисати мрежни саобраћај између мрежних подручја (сигурносних зона) на мрежном, транспортном и апликацијском слоју (L3, L4, L7).

11. Понуђено решење морају радити по моделу, и функционално обезбедити подршку за исти, нултог поверења безбедности (*Zero Trust Security*). Мора имати могућности блокирања свих апликације и мрежног саобраћаја, осим оних који су означени као дозвољени у правилима сигурносне политике конфигурисаној на уређају.
12. Сигурносна политика firewall мора узети у обзир приликом конфигурације тражених сигурносних полиса:
    a. изворне и дестинационе IP adrese,
    b. мрежне протоколе и услуге,
    c. апликације,
    d. URL категорије,
    e. кориснике и групе апликација,
    f. сигурносне одговоре,
    g. *logging* подршка (почетак и крај сесије),
    h. долазна и одлазна зона саобраћаја.
13. Понуђени уређаји морају аутоматски идентификовати апликације, без обзира на бројеве порта (укључујући P2P и IM тип апликација). Препознавање мора бити идентификовано барем путем потписа тј. адекватне апликационе сигнатуре. Уређај мора имати подршку за најмање 3500 унапред дефинисаних апликација које подржава произвођач, укључујући тунелирање апликација у HTTP или HTTPS, као и индустријске апликације (тзв. ICS/OT), нпр. DNP3, Modbus.
14. Додатно, ради скалабилности, понуђено решење мора омогућити и мануелно креирање препознавања и за нове апликације, директно кроз GUI система (без коришћења екстерних алата).
15. Понуђени firewall уређаји морају омогућити блокирање преноса датотека одабране врсте, укључујући минимално: *.pif, .scr, .cpl, .dll, .ocx, .exe, .class, .jar, vbe, .hta, .wsf, .torrent, .7z, .rar, .bat, .cab, .msi, .lnk*, kriptovani MS Office, kriptovani *RAR*, kriptovani *ZIP*. Препознавање датотеке мора се заснивати на садржају и метаподацима саме датотеке.
16. Понуђеним уређајима мора се управљати кроз интерфејс командне линије (*Command Line Interface*) и графичке, Web базиране, GUI конзоле. Није дозвољено постојање потребе за инсталирањем или преузимањем наменског софтвера/клијента на администраторској станици за управљање решењем.
17. Понуђени firewall уређаји морају бити опремљени API интерфејсом које је саставни део сигурносне платформе, путем којег је могуће конфигурисати и пратити статус уређаја без коришћења управљачке конзоле или *CLI* интерфејса.
18. Приступ решењу и удаљено управљање мора бити криптографски осигурано (путем енкрипције саме комуникације). Сигурносни систем и решење мора омогућити дефинисање више врста администраторских корисника, са различитим привилегијама у оквиру платформе.
19. Понуђени уређаји морају омогућити аутентификацију администратора користећи минимално: локалну базу података, Radius server, TACACS+ server, AD/LDAP server. Аутентификација помоћу SSH кључева мора бити подржана за SSH административни приступ.
20. Понуђени уређаји морају осигурати могућност аутоматског и транспарентног одређивања идентитета корисника мреже и интеграцију са следећим системима:
    a. Microsoft AD ili Open LDAP,
    b. *Captive Portal*-a,
    c. VPN,
    d. *Network Admission Control* sistema (kroz XML ili API)
    e. *Terminal Services*,
    f. Syslog поруке,

g. XFF заглавља,
h. Server monitoring
i. Испитивање клијента (client probing)

21. Понуђено решење мора омогућити локално прикупљање лог записа (на диску уређаја) и анализу, повезивање прикупљених информација и израду извештаја на темељу њих. Прикупљени подаци морају садржати најмање информације о: мрежном саобраћају, апликацијама, безбедносним претњама, URL филтрирању, SSL декрипцији, VPN везама.
22. Понуђени системи морају омогућити израду извештаја прилагођених захтевима Наручиоца, смештај истих на уређај и покретање ручно или аутоматски у одређеним временским интервалима. Формат излазног извештаја мора бити доступан у најмање PDF, CSV и XML форматима. Уређај такође мора бити у могућности да креира извештаје о активностима одабраног корисника или групе корисника у наведеном временском периоду.
23. Понуђени уређаји морају имати могућност креирања динамичких корисничких група. Чланство у групи мора се темељити на ознакама, а процес означавања мора омогућити коришћење:
    a. одговор на догађај (нпр. појава претње)
    b. API
24. Понуђено решење мора да подржава могућност динамичког и аутоматског прегруписавања корисника/е на основу безбедносних догађаја који се односе на тог корисника, при чему није потребна мануелна интервенција
25. Понуђени уређаји морају имати функцију динамичког преузимања и освежавања информација о ВМ ресурсима и њиховим IP адресама и ознакама (таговима) за окружења VMware ESXi и VMware vCenter. IP адресе прикупљене на овај начин морају омогућити стварање динамичких објеката који се затим могу користити у сигурносним политикама уређаја.
26. Понуђени уређаји морају подржавати протоколе динамичког рутирања, минимално: BGP и OSPF.
27. Понуђени уређаји морају подржавати статичку и динамичку транслацију (*Network Address Translation*) IP адреса.
28. Понуђени уређаји морају имати засебан скуп правила која дефинишу правила транслације IP адреса, одвојена од сигурносних правила.
29. Понуђени уређаји морају омогућити селективно слање записа зависно о њиховој врсти. Потребно је подржати Syslog протокол користећи UDP, TCP, SSL транспорт и подршку за IETF и BSD формате.
30. Понуђено решење мора да подржава могућност креирања безбедносних политика како би се спречила крађа корпоративних кредендијала
31. Понуђени уређаји морају подржавати могућност декриптовања корисничког саобраћаја у сврху инспекције за HTTP/2, SSL, TLS 1.2, TLS 1.3 протоколе.
32. Понуђени уређаји морају имати могућност дефинисања SSL/TLS саобраћаја који би требао бити подвргнут или искључен из операција декрипције и инспекције - одвојено од сигурносних правила.
33. Понуђени уређаји морају имати могућност дефинисања SSL/TLS саобраћаја који се не декриптује, али се проверава валидност сертификата издаваоца у смислу истека и валидног потписника. У том случају уређај мора имати могућност блокирања такве корисничке сесије.
34. Операције декрипције саобраћаја морају бити забележене у записима уређаја у одељку намењеном за ту сврху. Мора садржати податке који олакшавају дијагнозу, укључујући: информације о грешци, тип и величина кључа, TLS верзија. Мора

постојати механизам за аутоматско искључивање проблематичних страница из енкрипције на темељу ових информација.

35. Операције декрипције промета морају омогућити коришћење механизама за филтрирање URL-ova (ако је потребно) или могућност коришћења властитог пописа URL-ova уређаја који се декриптују или изузимају од овог процеса.
36. За дешифровање TLS 1.3 саобраћаја потребна је подршка за X25519, X448 и минимум следећих скупова протокола: TLS_AES_128_GCM_SHA256, TLS_AES_256_GCM_SHA384, TLS_CHACHA20_POLI1305_SHA256.
37. Понуђени уређаји морају имати функцију заштите од DoS напада заједно са могућношћу ограничавања броја сесија у односу на изворну или одредишну IP адресу.
38. Понуђени уређаји морају подржавати управљање пропусним опсегом (QoS - *Quality of Service*) за апликације и кориснике.
39. Понуђени уређаји морају омогућити успостављање криптографски заштићених VPN тунела заснованих на IPSec и IKE стандардима у конфигурацији од локације до локације. VPN конфигурација мора да се заснива на подешавањима рутирања (тзв. VPN заснован на рутирању).
40. За IKE, потребна је подршка за AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, Diffie-Hellman групе 14,19,20.
41. За IPsec, потребна је подршка за AES-256-CBC, AES-256-GCM, HMAC-SHA-384, HMAC-SHA-512, Diffie-Hellman групе 14,19,20.
42. Понуђени уређаји морају да обезбеде излазну SSH (*Secure Shell*) инспекцију, ради блокирања формирања SSH тунела.
43. Понуђени уређаји морају да подржавају функцију DNS проксија.
44. Понуђено решење мора бити у стању да омогући било који нов безбедносни сервис, кроз постојећу или докупљену лиценцу, без утицаја на перформансе саобраћаја који пролази кроз њега
45. Претплате, лиценце и гаранције које се испоручују са уређајима морају да важе 36 месеци.

Додатни захтеви за NG firewall:

Уз уређаје се морају испоручити следеће врсте и количине прикључних модула и система - количина за сет од 2 главне јединице:

- за HA: DAC кабл минималне дужине 5m за директно 10Gbps повезивање између уређаја – 1 ком.
- за LAN: 10Gbps SFP+ SR модул – 4 ком.
- за повезивање са core мрежом:
    - 25Gbps SFP+ SR модул - 4 ком.
    - 10Gbps SFP+ SR модулl (Cisco компатибилни) - 4 ком.
- додатни on site spare уређај на локацији Корисника, за потребе инстант замене у случају отказа примарних NGFW уређаја

Сваки уређај мора, поред општих услова наведених изнад, да испуни следеће додатне захтеве:

1. Мора имати најмање:
    a. 10 RJ45 Ethernet порта који подржавају 10GE/5G/2.5G/1GE
    b. 8 SFP+ Ethernet порта(прихватају 10GE SFP+ и 1GE SFP модуле)
    c. 4 SFP28 Ethernet порта (прихватају 25G SFP28, 10GE SFP+ i 1GE SFP модуле)

d. 2 QSFP+/QSFP28 40Gbps/100Gbps Ethernet porta
e. 2 порта дедицирана за повезивање уређаја у HA 10/100/1000Mbps RJ45. Ови портови се морају третирати као додатни у односу на горе наведене. Портови захтевани изнад нису дозвољени да се рачунају као HA.
f. Мора бити опремљен дисковним ресурсом (осим ротирајућих HDD-a), минимално 400 GB за потребе оперативног система и евиденције.

2. Мора да испуњава најмање следеће параметре перформанси:
   a. минимум 30 Gbps за препознавање и контролу апликација – за трансакције од 64 KB,
   b. минимум 20 Gbps за препознавање контроле апликација са омогућеним безбедносним функцијама: сви IPS потписи су омогућени, антивирусни програм, *antispy*, блокирање типа датотеке, DNS заштитом, са омогућеним логовањем на дискове уређаја - за трансакције од 64 KB.
   c. Најмање 14 Gbps IPSec VPN перформансе.
   d. Најмање 250.000 нових сесија у секунди.
   e. Најмање 2.8 милиона истовремених сесија

- Мора да подржава најмање 10 виртуелних рутера са одвојеним табелама рутирања, као и да може да покрене више од једне табеле рутирања у једној инстанци безбедносног система.
- Уређај мора имати могућност откривања и блокирања напада/упада на слоју 7 OSI modela (koji se često naziva i IPS). База података IPS потписа мора бити ускладиштена на уређају, редовно аутоматски ажурирана и долази од истог произвођача као и произвођач безбедносног система.
- Уређај мора имати функцију *anti-spyware* подршке. База података потписа мора бити ускладиштена на уређају, редовно аутоматски ажурирана и долази од истог произвођача као и систем безбедносног система.
- Уређај мора имати активирану функцију антивирусне инспекције по апликацији/политици и минимално одабрани протокол: http, http2, smtp, imap, pop3, ftp, smb. База података антивирусних потписа мора да се чува на уређају, да се редовно ажурира аутоматски (најмање једном на сваких 48 сати) и да долази од истог произвођача као и уређај.
- Понуђени уређај мора да подржи функционалности откривања и класификације осетљивих података, инспекције података у реалном времену, креирања грануларних DLP (Data Loss Prevention) политика заснованих на типу података, корисницима, групама, дестинацијама и апликацијама, уз константну видљивост, мониторинг и извештавање у оквиру понуђене платформе.
- Уређај мора да подржи, без потребе за инсталацијом додатног агента у окружењу Наручиоца, идентификацију и класификацију уређаја, процену ризика и безбедносног стања уређаја, праћење и анализу понашања, препоруке и аутоматизацију сигурносних политика на самом понуђеном систему.
- Уређај мора да открије и блокира DNS претње у саобраћају који пролази кроз уређај без потребе да се поново конфигурише DNS сервер и без потребе да се понуђени систем постави као DNS сервер. Откривање и блокирање саобраћаја ка доменима за које се сматра да су злонамерни морају се контролисати (преусмерити) коришћењем DNS *sinkholing* методе.
- Подршка за понуђени уређај и укључене безбедносне претплате мора бити у трајању од 3 године.
- Уређај мора бити намењен за уградњу у 19" rack орман.

Централизован менаџмент за NG firewall:
Уз понуђене firewall системе испоручити и систем за централно управљање и менаџмент у виду виртуелног appliance система, са свим потребним лиценцама и подршком у трајању од 3 године. Понуђено решење мора имати подршку за имплементацију на актуленим виртуелним платформама типа VMware, Hyper-V, KVM И слично. Понуђене лиценце морају имати подршку за управљање са минимално 4 firewall система, ради планираног проширења на DR локацији Корисника.

Тренинг кредити за понуђено решење:
У сврху адекватне обуке запослених Наручиоца неопходно је понудити потребан број тренинг кредита, који се могу искористити у року од 1 године, у ауторизованом центру понуђеног вендорског решења на територији Републике Србије. Циљ је оперативно и техничко оспособљавање запослених Наручиоца, зарад максималног искоришћења функционалности понуђеног решења, како на нивоу firewall уређаја, тако и на нивоу безбедносних сервиса и централизованог менаџмента за управљање.

Испорука и имплементација

У оквиру имплементације је потребно да се уради испорука и монтажа уређаја на локацији корисника, иницијална конфигурација уређаја, инсталација и повезивање firewall-a на централну конзолу за управљање, као и усклађивање конфигурације са архитектуром за контролу и приступ IoT уређаја интернету и другим ресурсима компаније.

Посебан акценат биће на конфигурацији и активирању лиценце, која омогућава аутоматску идентификацију IoT уређаја, категоризацију, праћење понашања и дефинисање политика приступа на основу ризичности уређаја. Потребно је интегрисати IoT модул са постојећом безбедносном политиком и обезбедити да се све детекције и препоруке аутоматски прослеђују ка централној конзоли и SOC-u Наручиоца.

Такође, у оквиру пројекта биће извршена имплементација и подешавање заштите DNS инфраструктуре, која омогућава блокирање малвер комуникације, Command&Control домена, као и превенцију DNS tunelinga. Обухвата подешавање DNS сигурносних политика, праћење упита и интеграцију са системима за корелацију догађаја.

Потребно је да се ради подршка при детекцији проблема, анализа забележених грешака, логова и аларма, отклањање проблема и помоћ при пријави инцидената.

Потребна је и подршка приликом ажурирања система према препорукама произвођача, анализа и праћење перформанси система или опреме ради благовременог уочавања потенцијалних ризика, као и унапређивање конфигурације и функционалности, у складу са захтевима Наручиоца.

Понуђач је у обавези да изврши испоруку и имплементацију решења у року од 90 (деведесет) дана од ступања уговора на снагу.

Место испоруке и имплементације је на локацији Наручиоца у Београду.

Техничка подршка

Понуђач је у обавези да пружи техничку подршку у трајању од 36 месеци по принципу 8x5 (од понедељка до петка, од 8.30 то 16.30 часова) у складу са параметрима датим у наставку

Приоритет проблема дефинише Наручилац, а верификује понуђач, у тренутку пријаве квара. Време одзива техничке подршке зависи од класификације пријављеног нивоа приоритета инцидента.

Критичан: Индикује стање када цела мрежа или мрежна компонента није операбилна, када се догоди тотални испад у мрежи или се испад понавља више пута узастопно, што за последице има отказ или смањену функционалност успостављених сервиса у мрежи.

Озбиљан: Означава стање када у мрежи или њеном одређеном делу постоји неправилност, али сервиси нису угрожени (нпр. губитак мрежног менаџмента, губитак редундансе итд.)

Низак: Представља стање у којем је мрежа операбилна, али постоји упозорење који индицира постојање грешке у систему. Евентуалне техничке консултације као захтев за додатним информисањем се такође овако класификују.

Дефиниције времена:

Време одзива: време које протекне од тренутка када Наручилац пријави проблем (отвори сервисни захтев) до тренутка када техничка подршка Понуђача контактира Наручиоца у циљу размене информација у вези проблема и почетка рада на његовом отклањању.

Време опоравка: време које протекне од тренутка пријаве проблема (подизања сервисног захтева) до тренутка потпуног решења проблема или опоравка основних функционалности неопходних за рад сервиса или мрежну управљивост.

Време затварања случаја: време које протекне од тренутка пријаве проблема (подизања сервисног захтева) до тренутка када су успостављене све функционалности, односно стање као пре проблема (коначно решење).

У случају да је сервисни захтев узрокован отказом опреме која није предмет одржавања, онда претходни временски интервали нису применљиви.

Ескалациона табела приоритета:

	Време одзива	**Време опоравка**	**Време затварања случаја**
Критичан ниво	1x	2x	7 дана
Озбиљан ниво	4x	6x	14 дана
Низак ниво	8x	72x	30 дана

Време одзива се односи на системске конфигурације и хардверске проблеме код уређаја, док се софтверски проблеми који се примете код уређаја решавају у складу са дефиницијама и прописима произвођача. Сервисни захтеви приоритета Критичан ниво се обавезно пријављују и телефонским позивом. У случају потребе за истовременом пријавом више проблема, сваки сервисни захтев се засебно пријављује.