РЕПУБЛИКА СРБИЈА
МИНИСТАРСТВО ФИНАНСИЈА
УПРАВА ЗА ИГРЕ НА СРЕЋУ
Број: 404-02-8/2020-03-7
02.04.2020. године
Београд

ПОЈАШЊЕЊЕ У ВЕЗИ СА ПРИПРЕМАЊЕМ ПОНУДЕ ЗА ЈАВНУ НАБАВКУ УСЛУГА У ОТВОРЕНОМ ПОСТУПКУ БРОЈ ЈН 1.1.1/2020

ПИТАЊЕ ПОТЕНЦИЈАЛНОГ ПОНУЂАЧА ЗА ЈАВНУ НАБАВКУ УСЛУГА У ОТВОРЕНОМ ПОСТУПКУ, БРОЈ ЈН 1.1.1/2020 – „ НОВИ ИНФОРМАЦИОНИ СИСТЕМ УПРАВЕ ЗА ИГРЕ НА СРЕЋУ И КОНТРОЛУ ПРИРЕЂИВАЧА“

1. **Питање:**

За Уређај за заштиту информационо - комуникационе мреже на примарној и другој локацији тражите да исти има укључену RAM меморију капацитета од најмање 8 GB. Сходно да различити произвођачи са различитом архитектуром производа могу да обезбеде тражене перформансе уређаја те чак и веће од тражених (Минимални firewall throughtput 4 Gbps или NGFW пропусна моћ (firewall, application controll i IPS) од најмање 1,5 Gbps, да ли је могуће понудити Уређај за заштиту информационо - комуникационе мреже са бољим перформансама од тражених уз укључену RAM меморију капацитета од најмање 4 GB?

Одговор:

Није могуће понудити Уређај за заштиту информационо - комуникационе мреже уз укључену RAM меморију капацитета од најмање 4 GB, зато што количина RAM меморије утиче на број конкурентних конекција као и на број нових конекција у секунди, а самим тим индиректно и на перформансе траженог решења.

2. **Питање:**

За Уређај за заштиту информационо - комуникационе мреже на примарној и другој локацији тражите да исти мора имати могућност креирања безбедносних правила (полиса) на основу идентитета добијених од најмање следећих извора: Microsoft AD, LDAP, RADIUS, Terminal Servers i 3rd parties уређаја кроз Web API integraciju. Сходно да различити произвођачи са различитом архитектуром производа могу да обезбеде тражене перформансе уређаја, да ли је могуће понудити уређај за заштиту информационо -

Омладинских бригада бр. 1
Београд, Република Србија
Тел. (381) (0) (11) 311 76 39 Факс (381) (0) (11) 311 75 72
www.uis.gov.rs

комуникационе мреже који може креирати безбедносна правила (полиса) на основу идентитета добијених од најмање следећих извора: Microsoft AD, LDAP, RADIUS, TACACS или слично, локал, и built-in Portal?

Одговор:
Није могуће понудити уређај за заштиту информационо - комуникационе мреже који може креирати безбедносна правила(полиса) на основу идентитета добијених од најмање следећих извора: Microsoft AD, LDAP, RADIUS, TACACS или слично, локал, и built-in Portal, зато што тражено решење мора да има интеграцију са 3rd parties уређајима кроз Web API интеграцију са циљем постизања аутоматизације процеса.

3. Питање:
За Уређај за заштиту информационо - комуникационе мреже на примарној и другој локацији тражите да исти мора да подржи Anti-Bot функционалност (у наставку могућност детекције и блокирања приступа URL страницама на основу репутације URLa; могућност детекције и блокирања приступа доменима на основу репутације домена; могућност детекције и блокирања сумњивог (малициозног) понашања у мрежи; могућност скенирања мреже са циљем детекције бот активности). Сходно да различити произвођачи са различитом архитектуром производа могу да обезбеде тражене карактеристике описане на другачији начин, да ли је могуће понудити Уређај за заштиту информационо - комуникационе мреже коме експлицитно није наведена Anti-Bot функционалност али подржава тражене детекције и то: могућност детекције и блокирања приступа URL страницама на основу репутације URLa; могућност детекције и блокирања приступа доменима на основу репутације домена; могућност детекције и блокирања сумњивог (малициозног) понашања у мрежи; могућност скенирања мреже са циљем детекције бот активности?

Одговор:
Anti-Bot функционалност спада у post-infection технологије и треба да спречи комуникацију рачунара са C&C (Command & Control Center) сајтовима и изношење осетљивих информација изван корпоративне мреже као и могућност заустављања ширења малвера на друге мрежне сегменте. Могуће је понудити уређај за заштиту информационо - комуникационе мреже у коме експлицитно није наведена Anti-Bot функционалност али подржава тражене методе детекције уз предуслове:

1. да понуђено решење има могућност пресретања малициозних DNS упита и одговарања са DNS Trap ИП адресом,
2. да тражене безбедносне функционалности: могућност детекције и блокирања приступа URL страницама на основу репутације URLa; могућност детекције и блокирања приступа доменима на основу репутације домена; могућност детекције и блокирања сумњивог (малициозног) понашања у мрежи и могућност скенирања мреже са циљем детекције бот активности нису део неког другог безбедносног сервиса као што је антивирус или УРЛ филтеринг.

4. Питање:

За Уређај за заштиту информационо - комуникационе мреже на примарној и другој локацији тражите да исти мора да има могућност препознавања најмање 8000 интернет апликација. Сходно да различити произвиђачи са различитом архитектуром производа могу да обезбеде тражене перформансе уређаја те чак и веће од тражених (Минимални firewall throughtput 4 Gbps или NGFW пропусна моћ (firewall, application controll i IPS) од најмање 1,5 Gbps), да ли је могуће понудити Уређај за заштиту информационо - комуникационе мреже са бољим перформансама од тражених уз могућност препознавања најмање 6000 интернет апликација?

Одговор:

Могуће је понудити Уређај за заштиту информационо - комуникационе мреже који у потпуности задовољава тражене перформансе, хардверске каратеристике и функционалности уз могућност препознавања најмање 6000 интернет апликација уз предуслов да понуђено решење има могућност креирања такозваних custom made сигнатура за детекцију апликација, односно уређај мора омогућити кориснику да прави своје сигнатуре за препознавање интеро развијаних апликација.

5. Питање:

За Централни менаџмент уређаја на примарној локацији тражите да решење мора имати могућност инсталације на Hyper-V (Windows 2016 Server i Windows 2012 Server R2), KVM (REHL 7 / CentOS 7), VMware vSphere 6.5/6.7 као и осталим Open Server платформама. Да ли је могуће понудити решење које има могућност инсталације на KVM (CentOS 7), VMware vSphere 6.5 као и на осталим Open Server платформама?

Одговор:

Није могуће понудити решење које има могућност инсталације на KVM (CentOS 7), VMware vSphere 6.5 као и на осталим Open Server платформама, зато што Централни менаџмент уређаја на примарној локацији мора бити у софтверској варијанти и мора имати могућност инсталације и на Hyper-V окружење. Наручилац жели да има опције инсталирања софтвера и на овој платформи како не би био приморан да користи било коју платформу за виртуализацију.

6. Питање:

За Централни менаџмент уређаја на примарној локацији тражите да решење мора имати могућност креирања свих заштитних функционалности укључујући Anti Bot. Сходно да различити произвођачи уређаја за заштиту информационо-комуникационе мреже са различитом архитектуром производа могу да обезбеде тражене карактеристике Anti-Bot функционалности описане на другачији начин, да ли је могуће понудити Централни менаџмент уређаја на примарној локацији за менаџмент уређај за заштиту информационо - комуникационе мреже коме експлицитно није наведена Anti-Bot функционалност али подржава тражене детекције?

Одговор:
Ако понуђени менаџмент уређај за заштиту информационо - комуникационе у потпуности задовољава тражене функционалности из тендера и задовољава услов из одговора на питање број 3, тада је могуће понудити менаџмент уређај за заштиту информационо - комуникационе мреже у коме експлицитно није наведена Anti-Bot функционалност, али подржава тражене методе детекције бот активности.

7. Питање:
За мрежне свичеве за повезивање менаџмент портова на примарној и другој локацији тражите да исти мора да има подршку за RADIUS и TACACS+ аутентификацију. Како је TACACS+ протокол карактеристичан само за уређаје једног произвођача, да ли је могуће понудити уређај који подржава RADIUS и протокол сличан TACACS+ протоколу?

Одговор:
Потребно је понудити уређај који подржава TACACS+ протокол. Поменути протокол је подржан на уређајима неколико различитих произвођача опреме, и као такав није карактеристичан само за уређаје једног произвођача.

8. Питање:
За сервере на примарној и другој локацији тражите да сервери морају да имају минимално 6 редудантних вентилатора, са могућношћу замене „на живо“ (Hot Swappable). Број вентилатора зависи пре свега од архитектуре сервера и начина на који је произвођач сервера дизајнирао “airf-low” унутар самог сервера како би омогућио адекватно хлађење те број вентилатора не утиче на функционалност истог. Имајући ово у виду, да ли бисте прихватили сервер који има 4 „hot-swappable“ редудантних вентилатора (N+1 redundancy)?

Одговор:
Потребно је понудити сервере који имају најмање 6 редудантних вентилатора, ради постизања веће отпорности на отказ сервера.

9. Питање:
За сервере на примарној и другој локацији тражите да сервери морају да имају минимум 5 x 3.0 USB порта. Да ли бисте прихватили сервер који има већи број USB портова (укупно 6) у конфигурацији 2 x 2.0 USB и 4 x 3.0 USB порта?

Одговор:
Потребно је понудити сервере који имају најмање 5 x 3.0 USB портова. Свакако ће бити прихватљиво, да поред тражених 3.0 USB портова, систем поседује и додатне 2.0 USB портове.

10. Питање:
За систем за складиштење података на примарној и другој локацији тражите да понуђени системи имају минимум два storage контролера у active-active режиму, са могућношћу проширења до минимум четири контролера и међусобно повезивање контролера (независно од броја контролера у конфигурацији) треба да буде реализовано путем

backplane-а или direct-connect каблова, без коришћења свичева. Обзиром да захтевате систем који има подршку до четири контролера, да ли бисте прихватили систем за складиштење података који подржава и већи број контролера од захтеваних и да као такав подржава директно повезивање контролера у конфигурацији четири контролера према захтеву независно од начина на који се повезују системи у конфигурацијама више од четири контролера.

Одговор:
Потребно је понудити систем за складиштење чији контролери су у active-active режиму, што подразумева да сви контролери, било два или више, морају да имају могућност истовременог обрађивања I/O захтева на истом логичком волумену, односно LUN-у. С тим је потребно понудити систем за складиштење података чији контролери су повезани на тражени начин.

11. Питање:
За приступне мрежне свичеве на примарној и другој локацији наводите да се уз понуђене уређаје мора понудити одговарајући број 10Gb SFP+адаптера. Сходно да постоје различити адаптери (MM 100m, MM 300m, SM, Twinax, итд) молим вас да нам специфицирате о којим се адаптерима ради.

Одговор:
Потребно је понудити MM 300m SFP+ адаптере.

12. Питање:
За приступне мрежне свичеве на примарној и другој локацији тражите да понуђени уређаји морају да имају могућност међусобног повезивања до најмање 9 свичева коришћењем IRF технологије. С обзиром да се од произвођача до произвођача разликује технологија међусобног повезивања свичева, да ли је могуће понудити уређаје који имају могућност међусобног повезивања до најмање 9 свичева коришћењем технологије карактеристичне произвођачу опреме.

Одговор:
Могуће је понудити свичеве који користе другачију технологију за повезивање свичева у јединствену целину, али је потребно да технологија понуђених свичева подржава исте карактеристике као и IRF технологија.

13. Питање:
За приступне мрежне свичеве на примарној и другој локацији тражите да исти мора да има подршку за TACACS+ аутентификацију. Како је TACACS+ протокол карактеристичан само за уређаје једног произвођача, да ли је могуће понудити уређај који подржава RADIUS и протокол сличан TACACS+ протоколу?

Одговор:
Потребно је понудити уређај који подржава TACACS+ протокол. Поменути протокол је подржан на уређајима неколико различитих произвођача опреме, и као такав није карактеристичан само за уређаје једног произвођача.

14. Питање:
За CORE мрежни свич на примарној и другој локацији наводите да се уз понуђене уређаје мора понудити одговарајући број 10Gb SFP+адаптера. Сходно да постоје различити адаптери (MM 100m, MM 300m, SM, Twinax, итд) молим вас да нам специфицирате о којим се адаптерима ради.

Одговор:
Потребно је понудити MM 300m SFP+ адаптере.

15. Питање:
За CORE мрежни свич на примарној и другој локацији тражите да исти има укључено минимално 4GB DDR3 RAM меморије. Сходно да различити произвођачи са различитом архитектуром производа могу да обезбеде тражене перформансе уређаја те чак и веће од тражених (switching капацитет од минимално 960Gbps и минималан проток од 570Mpps), да ли је могуће понудити CORE мрежни свич са бољим перформансама од тражених уз укључену RAM меморију капацитета од најмање 2 GB?

Одговор:
Потребно је понудити мрежни свич који има најмање 4GB DDR3 RAM меморије. Свакако ће бити прихваћен и свич који има и боље перформансе од тражених, али је исто потребно да испуни тражени захтев по питању потребне меморије.

16. Питање:
За CORE мрежни свиче на примарној и другој локацији тражите да исти мора да има подршку за RADIUS и TACACS+ аутентификацију. Како је TACACS+ протокол карактеристичан само за уређаје једног произвођача, да ли је могуће понудити уређај који подржава RADIUS и протокол сличан TACACS+ протоколу?

Одговор:
Потребно је понудити уређај који подржава TACACS+ протокол. Поменути протокол је подржан на уређајима неколико различитих произвођача опреме, и као такав није карактеристичан само за уређаје једног произвођача.

Комисија за ЈН

Омладинских бригада бр. 1
Београд, Република Србија
Тел. (381) (0) (11) 311 76 39 Факс (381) (0) (11) 311 75 72
www.uis.gov.rs