

V Bratislave, dňa 24.10.2022

VEC: Vysvetlenie súťažných podkladov č. 5

Verejný obstarávateľ Slovenská agentúra životného prostredia, Tajovského 28, 97590 Banská Bystrica (ďalej len „**Verejný obstarávateľ**“) vyhlásil v súlade so zákonom č. 343/2015 Z.z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov, v platnom znení (ďalej len „**Zákon**“) oznámením o vyhlásení verejného obstarávania uverejneným v Dodatku k Úradnému vestníku Európskej únie zo dňa 19.09.2022 pod zn. 2022/S 180-508852 a vo Vestníku verejného obstarávania č. 204/2022 zo dňa 20.09.2022 pod značkou 41159 - MST (obe oznámenia ďalej spoločne ako „**Oznámenie**“) verejnú súťaž na obstaranie nadlimitnej zákazky s názvom „Nákup hardvéru“ (ďalej len „**Verejná súťaž**“).

Spoločnosť Tatra Tender s. r. o., so sídlom Krčméryho 16, 811 04 Bratislava, Slovenská republika realizuje pre Verejného obstarávateľa predmetnú Verejnú súťaž a na základe jeho poverenia vykonáva v jeho mene niektoré úkony spojené s jej realizáciou.

Dňa 19.10.2022 bola Verejnému obstarávateľovi jedným zo záujemcov doručená žiadosť o vysvetlenie podmienok uvedených v súťažných podkladoch. V súlade s ust. § 48 Zákona Vám týmto v mene Verejného obstarávateľa poskytujeme nižšie uvedené vysvetlenie.

Žiadosti o vysvetlenie / doplnenie súťažných podkladov	
Číslo	Otázka / obsah žiadosti a odpoveď
	Otázka č. 1: V položke 8.1.1 pri parametri Rozhrania verejný obstarávateľ požaduje: RDMA (RoCE, RoCE v2, iWARP). Trvá verejný obstarávateľ na podpore všetkých spomenutých protokolov alebo stačí podpora aspoň jedného z uvedených protokolov ?
	Odpoveď: Verejný obstarávateľ trvá na podpore všetkých spomenutých protokolov v rámci položky 8.1.1 pri parametri Rozhrania z dôvodu spätnej kompatibility s existujúcimi servermi MUSES.
	Otázka č. 2: V položke Položka č. 7.1.3: Disky pre existujúce diskové polia, vie pre správne nacenenie verejný obstarávateľ poskytnúť sériové číslo zariadenia Huawei OceanStore, do ktorého sa disky obstarávajú?



TATRATENDER

	Odpoveď: V serverovej časti pripojenie rs232 db9 je vhodné, ale nie potrebné. Takže na pripojení konektorom rs232 db9 Verejný obstarávateľ netrvá.
	Otázka č. 3: Radi by sme verejného obstarávateľa poprosili o vysvetlenie technickej špecifikácie Pri položka č. 9.1.1: Ochrana sieťových prístupov na pracoviskách SAŽP, nakoľko navrhovaná technická špecifikácia obmedzuje uchádzačov z dôvodu, že je možné ponúknuť konkrétne zariadenie iba jedného výrobcu a. Pre Firewall č.1 je požadované „Rackmount zariadenie“ pričom v základných technických vlastnostiach je uvedené „Virtuálny firewall“. Poprosíme vysvetliť, čoho sa týka požiadavka na virtuálny firewall. b. Pre Firewall č.1 je požadovaná vlastnosť „Mail gateway“. Poprosíme vysvetliť, čo je touto požiadavkou požadované. c. Požiadavka je na automatické vypnutie IPS ochrany firewallu v prípade preťaženia HW (utilizácia CPU alebo fyzickej pamäte) nad definovanú prahovú hodnotu. Z bezpečnostného hľadiska je takéto správanie firewallu diskutabilné. Bude verejný obstarávateľ akceptovať riešenie, kde pri preťažení HW začne firewall radšej zahadzovať packety ako by mal vypnúť IPS ochranu? d. Požiadavka je, že VPN IPSec musí podporovať nasledujúce šifrovacie protokoly: AES-128, AES-256, CAST, DES. Trvá verejný obstarávateľ na podpore algoritmu CAST, ktorý je z roku 1999 a je podporovaný na minimálnom počte zariadení? Ako štandardy sú definované napríklad AES-128 a AES-256, ktoré sú podporované na všetkých relevantných zariadeniach? e. Požiadavka je, že VPN IPSec musí podporovať dátovú integritu pre MD5, SHA1, SHA-256, AES-XCBC. Trvá verejný obstarávateľ na podpore algoritmu AES-XCBC, ktorý nie je bežne využívaný pre dátovú integritu? Dokonca ani „NIST Guide to IPsec VPNs (SP 800-77)“ tento algoritmus neuvádza medzi odporúčanými algoritmami. Odporúčané algoritmy sú z kategórie SHA-X. f. Požiadavka je na podporu linux nástrojov (min. SCP, BASH, VI, TOP), spúšťania linuxových BASH skriptov a nástrojov tretích strán. Požiadavka je značne špecifická a môže poukazovať na konkrétneho výrobcu. Trvá verejný obstarávateľ na tejto požiadavke a plánuje túto funkcionálnu využívať? g. Požiadavka je na podporu IP compression pre S2S VPN. Požiadavka je značne špecifická a môže poukazovať na konkrétneho výrobcu. Trvá verejný obstarávateľ na tejto požiadavke a plánuje túto funkcionálnu využívať? h. Požiadavka je na minimálny počet rozpoznávaných aplikácií, minimálne 7500. Bude verejný obstarávateľ akceptovať aj menšiu granularitu rozpoznávania aplikácií (napríklad 4000), ktorá ale pokrýva porovnateľné množstvo aplikácií? i. Požiadavka je na minimálny počet aplikácií / pluginov pre sociálne siete, minimálne 300.000. Trvá verejný obstarávateľ na tejto požiadavke, nakoľko táto požiadavka je čiastočne pokrytá už v predchádzajúcej požiadavke a požiadavka na počet 300 000 aplikácií/pluginov pre sociálne siete je značne nadhodnotený a v reálnych situáciách nevyužiteľný.



TATRATENDER

j. Požiadavka je na blokovanie komunikácie na IP riadiacich centier botnetov pomocou behavior analýzy. Trvá verejný obstarávateľ na tejto požiadavke? Máme za to, že behaviour analýza komunikácie prebieha u výrobcu bezpečnostného riešenia na základe zozbierania komunikácie z celého sveta a tým dôjde k oveľa rýchlejšiemu odhaleniu IP adres botnetov, ktoré sú následne pomocou aktualizácií distribuované na všetky relevantné zariadenia v dostatočnom predstihu.

k. Je požadovaná možnosť granularného riadenie HTTPs (inšpekcia spojenia alebo bypass), pričom je uvedená presná kombinácia: src IP + username + dst IP + service + aplikácia / URL / URL kategória.

Trvá verejný obstarávateľ na takto exaktne zadanej kombinácii alebo bude postačovať riadenie HTTPs spojení na základe potrebnej kombinácie podmienok?

l. Verejný obstarávateľ požaduje aby každá virtuálna firewall inštancia mala vlastnú bezpečnostnú politiku, stavové, routovacie a ARP tabuľky. Bude verejný obstarávateľ akceptovať, keď budú splnené podmienky len na vlastnú bezpečnostnú politiku, stavové a routovacie tabuľky?

m. Verejný obstarávateľ požaduje pridelovanie hardware zdrojov pre jednotlivé virtuálne firewall inštalácie (CPU, pamäť), monitorovanie využívania zdrojov pre jednotlivé virtuálne firewall inštalácie (CPU, pamäť) a dynamické riadenie zdrojov pomocou nastavenia priorít pre jednotlivé virtuálne firewall inštalácie. Bude verejný obstarávateľ akceptovať, ak bude možné pridelovať zdroje ako počet užívateľov, SSL-VPN, IPSec VPN, Active Sessions, Policies, Addresses, Address groups,... Pridelovanie hardvérových zdrojov (CPU, pamäť,...) je riadené dynamicky priamo firewallom podľa požiadaviek na výkon.

n. Verejný obstarávateľ požaduje možnosť vytvoriť dedikované virtuálne prepínače a smerovače na zabezpečenie prepínania a smerovanie paketov medzi virtuálnymi firewallmi a externými segmentami. Táto požiadavka nám nie je úplne jasná. Bude verejný obstarávateľ akceptovať riešenie, kde bude umožnené jednotlivé virtuálne FW prepájať tak, aby spolu komunikovali a posielali si dáta?

o. Požiadavka je na rozkladanie záťaže virtuálnych firewallov medzi fyzickými členmi firewall klastra. Bude verejný obstarávateľ akceptovať riešenie, ktoré umožňuje rozklad záťaže virtuálnych FW na úrovni fyzického FW, na ktorom sú jednotlivé virtuálne FW definované.

p. Verejný obstarávateľ požaduje minimálne 32 GB operačnej pamäte. Bude verejný obstarávateľ akceptovať aj nižšiu veľkosť operačnej pamäte, ak budú zachované ostatné výkonové požiadavky?

q. Verejný obstarávateľ požaduje minimálne 1xUSB-C serial konsole port. Bude verejný obstarávateľ akceptovať aj klasický USB serial console port?

Odpoveď:

a. Verejný obstarávateľ požaduje Rackmount zariadenie, ktoré podporuje virtualizáciu, teda oddelenie jednotlivých bežiacich virtuálnych inštancií firewallu, tak aby pre ne bolo možné použiť samostatné fyzické porty a aby boli pre vyššiu dostupnosť a bezpečnosť oddelené aj manažmentovo.

b. Funkcionalitou „Mail gateway“ je myslená požadovaná funkcionálna na SMTP/MTA pre kontrolu prichádzajúcej a odchádzajúcej mailovej komunikácie, minimálne s AV/antispam kontrolou, ktoré je integrované do FW funkcionality, tak aby nevyžadovalo samostatný manažment alebo zariadenie.



TATRATENDER

c. Verejný obstarávateľ požaduje vysokú dostupnosť poskytovaných služieb a preto je táto funkcionality požadovaná, tak aby nebola degradovaná dostupnosť služby. V prípade neočakávaného vyťaženia firewallu je pre verejného obstarávateľa akceptovateľná dočasná degradácia zabezpečenia ale nie výpadok služby. Túto funkcionality verejný obstarávateľ požaduje najmä na fázu nasadenia a odladenia IPS modulu a následne zväži jej vypnutie. d. Verejný obstarávateľ netrvá na podpore CAST algoritmu e. Verejný obstarávateľ netrvá na podpore AES-XCBC algoritmu f. Verejný obstarávateľ plánuje pomocou linuxových nástrojov vykonávať automatické zálohovanie a konfiguráciu obstarávaných zariadení. Verejný obstarávateľ ma za to, že väčšina FW zariadení je postavená na linuxovom jadre a prístupnosť týchto nástrojov uľahčí automatizované úlohy a ladenie problémov. Verejný obstarávateľ netrvá na BASH podpore ale bude vyžadovať adekvátnu náhradu za tento skriptovací jazyk a uchádzač musí uviesť ponukovanú náhradu s popisom podpory pre požadovanú funkcionality: spustanie vzdialenej CLI konfigurácie, spustanie automatických a automatizovaných skriptov vzdialene cez CLI, zber výkonostných štatistík vzdialne cez CLI. g. Verejný obstarávateľ túto funkcionality vyžaduje vzhľadom na kapacitu existujúcich liniek. Verejný obstarávateľ ma vedomosť o min. 3 výrobcov ktorý túto funkcionality ponúkajú a preto nemá za to že je značne špecifická. h. Áno i. Verejný obstarávateľ má za to, že väčšina renomovaných FW riešení ponúka rozoznávajúce najčastejšie používaných aplikácií a pluginov pre sociálne siete, preto vyžaduje, aby riešenie umožňovalo použitie nielen kontroly obsahu sociálnych aplikácií ale aj ich pluginov. Verejný obstarávateľ netrvá na počte 300000, ale trvá na preukázaní takejto granularity a teda riešenie musí podporovať kontrolu pluginov. j. Verejný obstarávateľ má pod „blokovanie komunikácie na IP riadiacich centier botnetov pomocou behavior analýzy“ na mysli rovnakú funkcionality ako popisujete. k. Verejný obstarávateľ nevie posúdiť čo je Vami definovaná potrebná kombinácia podmienok. Na zdroji musí byť definovateľné src IP alebo username na základe údaje IDFW. Cieľ musí byť definovateľný kombináciou destination IP a service a aplikácia/URL/URL kategória. l. Verejný obstarávateľ bude akceptovať aj takéto riešenie. m. V takomto prípade bude verejný obstarávateľ požadovať aby dynamické riadenie zdrojov pre FW obsahovalo prioritizáciu jednotlivých virtuálny FW na základe ktorého budú pridelené HW zdroje n. Verejný obstarávateľ bude akceptovať aj takéto riešenie, avšak na takéto riešenie nesmie byť využitý iný hardvér obstarávateľa. o. Nie, virtuálne FW musia byť rozložiteľné rovnomerne na všetkých fyzických členoch klastra. p. Áno. V takomto prípade bude obstarávateľ požadovať zmluvnú garanciu od dodávateľa, že v prípade nedostatočného výkonu pri použití všetkej požadovanej funkcionality



TATRATENDER

	dodávateľ tento hardvér bez zmeny vysúťaženej ceny vymení za HW s minimálne 32GB operačnej pamäte. q. Verejný obstarávateľ bude akceptovať aj klasický USB serial console port.
--	---

JUDr. Jakub Hošo
Tatra Tender s.r.o.