Zdravotní pojišťovna ministerstva vnitra České republiky
Ředitelství: Vinohradská 2577/178, 130 00 Praha 3, tel. 272 095 111

NAŠE ZNAČKA: ZPMV/0136863/2026
VYŘIZUJE: Mgr. Petr Novák, LL.M., DSc.
TEL: +420272095201
E-MAIL: petr.novak@zpmvcr.cz
DATUM: vizte datum podpisu

Vysvětlení č. 4 zadávací dokumentace veřejné zakázky zadávané v otevřeném řízení

V souladu s ustanovením § 98 odst. 3 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen **„ZZVZ“**), oznamujeme, že jsme obdrželi žádost o vysvětlení zadávací dokumentace veřejné zakázky na dodávky s názvem „***Náhrada firewallů a souvisejících služeb***“, evidované u zadavatele pod č.j.: ZPMV/0136863/2026, evidenčním číslem zakázky ve věstníku veřejných zakázek Z2026-029727.

V souladu s citovaným ustanovením ZZVZ uveřejňujeme anonymizované znění žádosti spolu se zněním naší odpovědi (viz příloha tohoto dopisu) na profilu zadavatele ZP MV ČR.

Tímto sdělením dochází nejen k vysvětlení, ale také ke změně zadávací dokumentace ve smyslu ust. § 99 odst. 1 ZZVZ. Tato změna, vč. upravené Přílohy č.1 -Technická specifikace návrhu smlouvy, která tvoří Přílohu č. I zadávací dokumentace, bude uveřejněna na profilu zadavatele e-zakazky dostupném na adrese:

https://www.e-zakazky.cz/Profil-Zadavatele/9efb23ac-d9c4-4349-b453-2462359b0cba

V souladu s ust. 99 odst. 2 ZZVZ bude také přiměřeně prodloužena lhůta pro podání nabídek.

Příloha: Znění žádosti a vysvětlení

S pozdravem

Miroslav Tůma
Digitálně podepsal Miroslav Tůma
Datum: 2026.07.10 13:58:32 +02'00'

…….……..

Ing. Miroslav Tůma, Ph.D., MBA
předseda komise k veřejné zakázce
Zdravotní pojišťovna ministerstva vnitra
České republiky

Anonymizované znění žádosti o vysvětlení zadávací dokumentace:

Dotaz č. 1

„Síťové funkcionality – podporovat persistentní NAT pro DIPP (Dynamic IP and Port), směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)

Dotaz: Požadavek specifikuje podporu persistentního NAT pro DIPP. Persistentní NAT je relevantní pouze v případě, kdy je zdrojový provoz překládán za pool více veřejných IP adres a je požadováno, aby stejný interní host byl vždy překládán na stejnou veřejnou IP adresu z tohoto poolu. Pokud je překlad realizován za jednu veřejnou IP adresu, je konzistence překladu zajištěna standardním mechanismem Hide NAT bez nutnosti persistence. Stejného výsledku lze dosáhnout i přiřazením dedikované veřejné IP adresy jednotlivým interním sítím nebo segmentům prostřednictvím samostatných NAT pravidel, čímž je konzistence překladu zajištěna staticky na úrovni konfigurace. Žádáme zadavatele o upřesnění, zda je akceptovatelné funkčně ekvivalentní řešení zajišťující konzistentní překlad prostřednictvím statického přiřazení veřejných IP adres jednotlivým interním segmentům?“

Odpověď č. 1

Ano, funkčně ekvivalentní řešení konzistentního překladu je akceptovatelné.

Dotaz č. 2

„Síťové funkcionality – podporovat současně na jednom zařízení na úrovni síťového rozhraní konfigurace Span, Transparent, Layer 3 a Layer 2

Dotaz: Požadavek specifikuje podporu konfigurací SPAN, Transparent, Layer 3 a Layer 2 současně na jednom zařízení na úrovni síťového rozhraní. Vzhledem k tomu, že jednotlivé provozní módy síťového rozhraní se vzájemně vylučují – rozhraní v pasivním módu (SPAN/TAP) nemůže současně aktivně forwardovat provoz a rozhraní v transparentním módu nemůže současně operovat jako routed L3 interface. Prosíme zadavatele o upřesnění, zda je požadavek míněn tak, že zařízení musí podporovat všechny uvedené módy současně na různých fyzických rozhraních, nebo zda se jedná o požadavek na podporu všech uvedených módů na jednom fyzickém rozhraní? V případě druhé interpretace žádáme o technické upřesnění, neboť taková konfigurace není v souladu se standardním chováním síťových rozhraní.“

Odpověď č. 2

Zadavatel souhlasí a upřesňuje, že uvedené módy musí být možné nakonfigurovat současně na stejném boxu, ale ne nutně na stejném rozhraní. Tedy například zároveň SPAN na eth0 a Transparent na eth1.

Dotaz č. 3

„Bezpečnostní funkcionality – obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita

Požadavek specifikuje limitaci počtu spojení pro ochranu proti DoS útokům na úrovni zdrojové IP, cílové IP a uživatelské identity. Vzhledem k tomu, že DoS útoky ze své podstaty s uživatelskou identitou nesouvisejí – jejich cílem je vyčerpání zdrojů napadené služby prostřednictvím záplavy spojení nebo požadavků a cílí na konkrétní služby identifikované IP adresou a portem, nikoliv na uživatelské identity. Mimo to je ve většině případů útočník anonymní (typicky se jedná o provoz generovaný botnety), ochrana proti DoS pracuje standardně na základě zdrojové a cílové IP adresy, případně portu. Uživatelská identita jako dimenze pro detekci a mitigaci DoS útoku není technicky ani prakticky uplatnitelná. Žádáme proto zadavatele o upřesnění, zda je dimenze uživatelské identity v tomto požadavku skutečně

nutná, nebo zda postačuje schopnost systému limitovat počet spojení na úrovni zdrojové a cílové IP adresy (což odpovídá standardním postupům ochrany proti DoS útokům za pomoci limitace počtu spojení)?

Požadavek specifikuje limitaci počtu spojení pro ochranu proti DoS útokům na úrovni zdrojové IP, cílové IP a uživatelské identity. Vzhledem k tomu, že DoS útoky ze své podstaty s uživatelskou identitou nesouvisejí – jejich cílem je vyčerpání zdrojů napadené služby prostřednictvím záplavy spojení nebo požadavků a cílí na konkrétní služby identifikované IP adresou a portem, nikoliv na uživatelské identity – a útočník je ve většině případů anonymní (typicky se jedná o provoz generovaný botnety), ochrana proti DoS spojená s limitaci počtu spojení pracuje standardně na základě zdrojové a cílové IP adresy, případně portu. Uživatelská identita jako dimenze pro detekci a mitigaci DoS útoku není technicky ani prakticky uplatnitelná. Nabízené řešení nicméně umožňuje definovat bezpečnostní pravidla, která řeší i DDOS ochranu s využitím uživatelské identity prostřednictvím Identity Awareness, což lze využít pro širší ochranu sítě nad rámec samotné limitace počtu spojení. Splňuje takto definované řešení požadavek Zadavatele?“

Odpověď č. 3

Uživatelská identita je ve chvíli komunikace typicky svázaná s IP adresou, jinak by uživatel nemohl v síti komunikovat. V tomto smyslu lze tedy uživatelskou identitu použít i v ochraně proti DoS a v tomto smyslu ji zadavatel požaduje. Nejedná se tedy o nakonfigurování DoS na základě uživatelského účtu, ale pouze o možnost spojení uživatelské účtu s konkrétní (externí) IP adresou a portem ve chvíli útoku (pokud by útok souvisel s činností uživatele). Zadavatel umožňuje navrhované řešení.

Dotaz č. 4

„Sandboxing – podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB

Dotaz: Požadavek specifikuje podporu sandboxové inspekce souborů přenášených protokolem IMAPS. Zároveň požadavek na antivirovou kontrolu provozu uvádí mimo jiné pouze protokol IMAP – bez protokolu IMAPS. Je podpora sandboxové inspekce protokolu IMAPS nezbytně nutnou podmínkou plnění, nebo je akceptovatelné nabídnout cenově optimálnější řešení, které pokrývá sandboxovou inspekci pouze pro HTTP, HTTPS, SMTP, SMTPS, IMAP, FTP a SMB?“

Odpověď č. 4

Zadavatel provedl úpravu zadávacích podmínek a požadavek upravil následovně „*Sandboxing – podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, FTP a SMB*.“

Dotaz č. 5

„Sandboxing – aktualizace zero-day signatur musí být instalována do NGFW v reálném čase

Dotaz: Akceptuje zadavatel jako splnění výše uvedeného požadavku i řešení, které místo distribuce signatur využívá real-time sdílení kryptografických hashů nově detekovaných zero-day souborů prostřednictvím threat intelligence platformy, kde výsledný efekt je technicky srovnatelný – tj. okamžité blokování zero-day hrozeb na NGFW v reálném čase?“

Odpověď č. 5

Ano, zadavatel akceptuje tento způsob řešení.

Dotaz č. 6

„Sandboxing – rozpoznat, které závislosti malware potřebuje k tomu, aby se spustil a umí je nasimulovat

Dotaz: Požadavek specifikuje schopnost sandboxového řešení rozpoznat závislosti, které malware potřebuje ke spuštění, a tyto závislosti nasimulovat. Tato technika má však inherentní omezení – závislosti, které sandbox nedokáže rozpoznat, nemůže ani nasimulovat, čímž může dojít k tomu, že malware zůstane nedetekován. Alternativním přístupem je detekce na úrovni CPU instrukcí (CPU-level detection), která analyzuje chování exploitu přímo na úrovni procesoru a paměti ještě předtím, než malware spustí jakýkoliv kód. Tento přístup je nezávislý na konkrétních závislostech malware a dosahuje přinejmenším stejné, zpravidla však vyšší úrovně bezpečnosti. Žádáme zadavatele o odpověď, zda je požadována konkrétní technika simulace závislostí, nebo zda je akceptovatelné řešení dosahující stejné či vyšší úrovně ochrany prostřednictvím CPU-level detekce?“

Odpověď č. 6

Ano, zadavatel akceptuje tento způsob řešení.

Dotaz č. 7

„Sandboxing – podporovat operační systémy Windows, Linux, MacOS

Dotaz: Požadavek specifikuje podporu sandboxové emulace pro operační systémy Windows, Linux a macOS. Námi nabízené řešení zajišťuje ochranu prostřednictvím kombinace dvou komplementárních technologií: OS-level emulace, při níž jsou soubory analyzovány simultánně v několika prostředích (výrobce konkrétní seznam emulovaných operačních systémů nespecifikuje), a CPU-level detekce, která analyzuje hrozby přímo na úrovni procesorových instrukcí nezávisle na cílovém operačním systému. CPU-level detekce je ze své podstaty OS-agnostická technologie – zachycuje exploity na úrovni procesorových instrukcí dříve, než je spuštěn jakýkoliv kód, bez ohledu na to, zda je hrozba cílena na Windows, Linux nebo macOS. Tato kombinace přístupů poskytuje přinejmenším ekvivalentní, v oblasti odolnosti vůči evasion technikám zpravidla vyšší úroveň ochrany oproti přístupu založenému výhradně na dedikovaných emulačních prostředích pro jednotlivé operační systémy. Žádáme zadavatele o odpověď, zda je možné požadavek na podporu dedikovaných emulačních prostředí Windows, Linux a macOS splnit výše popsaným přístupem, a zda je tedy akceptovatelné technologicky ekvivalentní řešení zajišťující OS-agnostickou ochranu prostřednictvím CPU-level detekce v kombinaci s multi-environment OS-level emulací?“

Odpověď č. 7

Ano, zadavatel akceptuje tento způsob řešení.

Dotaz č. 8

„Dotaz k zadávací dokumentaci:

*Dotaz: V rámci kapitoly „Správa řešení" a „Logování a reportování" zadávací dokumentace postrádáme jakýkoliv požadavek na **centrální management server** a **centrální log server** jako samostatné/dedikované komponenty řešení. Aktuálně definované požadavky (spravovatelnost pomocí GUI/CLI, API rozhraní jednotlivé appliance, práce více administrátorů, nástroj pro analýzu logů v rámci GUI apod.) lze u řady řešení na trhu splnit i lokální správou jednotlivých zařízení bez centrální komponenty, což však z pohledu provozu enterprise prostředí s předpokládaným počtem spravovaných gateway představuje zásadní provozní a bezpečnostní riziko (absence jednotného pohledu na politiky, chybějící auditní historie změn napříč zařízeními, omezená škálovatelnost správy a logování, absence disaster recovery scénáře na úrovni správy).*

*HW appliance NGFW jsou primárně dimenzovány pro zpracování, kontrolu a inspekci síťového provozu (firewall, IPS, decryption apod.). Pokud zadávací dokumentace nepožaduje oddělenou komponentu pro management a logování, hrozí, že řešení bude tyto **zdroje spotřebovávat i na zpracování logů, indexaci, korelaci a generování reportů namísto síťové inspekce.***

Mimo uvedené v souladu s doporučeními NÚKIB a mezinárodní iniciativou zaměřenou na bezpečnost hraničních síťových prvků (NÚKIB, únor 2025), která explicitně uvádí zabezpečení rozhraní pro správu jako jedno z klíčových bezpečnostních opatření, doporučujeme, aby centrální management pro správu požadovaného řešení nebyl součástí samotného firewallu, ale byl provozován na dedikovaném management serveru umístěném v odděleném interním síťovém segmentu, nepřístupném z produkční sítě ani z internetu. Tento přístup zajišťuje, že případný bezpečnostní incident na produkční síti neohrozí dostupnost ani integritu management roviny a integrity logů, a zároveň minimalizuje útočnou plochu vyplývající ze správy bezpečnostní infrastruktury.

Chápeme správně, že Zadavatel předpokládá dodání samostatné virtuální appliance pro správu firewallu?

Pokud ano, předpokládá Zadavatel dodání samostatného HW pro provoz takové appliance? Nebo Zadavatel zajistí potřebné prostředí ve vlastní virtualizované infrastruktuře?“

Odpověď č. 8

Požadavek pro správu přímo na zařízení se týká pouze konfigurace síťových rozhraní a směrování. Management server pro správu NGFW jako takového může, ale nemusí být na jednotlivých zařízeních. Zadavatel plně akceptuje i oddělený samostatný management server(y). Ukládání logů může být lokálně na zařízení, na management serveru i na dedikovaném správci logů. Zadavatel v tomto ohledu akceptuje architekturu dodávaného řešení. V případě potřeby dedikovaných serverů pro správu či logy poskytne Zadavatel svoji virtuální infrastrukturu (VMware, Proxmox). Zadavatel předpokládá virtuální appliance, v případě potřeby instalace virtuálního serveru s instalovaným operačním systémem musí být potřebné licence součástí dodávky. Pokud by řešení vyžadovalo dedikovaný HW, musí i tento hw být součástí dodávky.

Dotaz č. 9

„Dobrý den,

rádi bychom se ještě zeptali na následující:

Aktuálně používáte support úrovně Premium, požadujete v nabídce zachovat stejnou úroveň supportu? Pokud ne, mohli byste prosím specifikovat, jaká je požadovaná úroveň supportu?“

Odpověď č. 9

Ano, zadavatel požaduje zachovat stávající úroveň supportu. Požadavky na poskytování Podpory jsou specifikovány v části 9 Přílohy č. 1 Návrhu smlouvy – Technická specifikace.