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. 2 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 a doplnění 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: 2026.07.01 09:50:00 +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

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW – všeobecné požadavky požaduje zadavatel: „výrobce NGFW se musí nacházet v "Leaders" kvadrantu Enterprise Network Firewalls v posledním aktuálním reportu společnosti GARTNER“.

Dodavatel upozorňuje na skutečnost, že uvedený požadavek nepředstavuje technickou podmínku vyjádřenou prostřednictvím výkonových nebo funkčních parametrů předmětu plnění, ale fakticky váže splnění zadávací podmínky na jedinou konkrétní komerční hodnoticí metodiku soukromého subjektu. Takto nastavená podmínka je z pohledu § 89 ZZVZ problematická, neboť technické podmínky mají být zásadně stanoveny prostřednictvím:

- *parametrů vyjadřujících požadavky na výkon nebo funkci,*
- *popisu účelu a potřeb zadavatele,*
- *případně odkazem na normy nebo technické dokumenty v režimu § 90 ZZVZ.*

Současně platí, že zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže (§ 36 odst. 1 ZZVZ) a zadavatel je povinen dodržet zásadu rovného zacházení a zákazu diskriminace (§ 6 odst. 2 ZZVZ).

Dodavatel současně upozorňuje, že podle veřejně dostupných informací společnost GARTNER v minulém roce ustoupila od vydávání Magic Quadrant pro oblast NGFW a dále vydává zejména tzv.Peer Insights analýzy (odkaz), do kterých zařazuje renomovaná, doporučovaná a ověřená řešení. Dodavatel tímto tedy upozorňuje, že došlo ke změně přístupu k hodnocení této oblasti a předmětný report již nemusí být vydáván ve stejné podobě, v jaké je na něj v zadávací dokumentaci odkazováno. Pokud by tomu tak bylo, vzniká otázka:

- *jak má být tento požadavek dodavateli vůbec splněn a prokazován,*
- *a zda není zadávací podmínka v této části neurčitá nebo nepřiměřeně restriktivní.*

Dále dodavatel upozorňuje na existenci dalších reportů, které se zabývají hodnocení pokročilých NGFW jako například SE LABS (odkaz).

Využití jedné jediné metodiky hodnocení NGFW, navíc vydávané soukromým subjektem, vykazuje známky porušení §6 odst. 2. Zákona, z důvodu zvýhodňování určitých konkrétních dodavatelů.

Pro zajištění transparentního soutěžního prostředí a rovného zacházení ve vztahu k dodavatelům by měl Zadavatel připustit i jiné, obdobné metodiky hodnocení výrobců.

Pro takové posouzení je obdobně relevantní také IDC MarketScape Worldwide Enterprise Hybrid Firewall Vendor Assessment a to konkrétně sekce Leaders (odkaz) viz.obrázek dále.

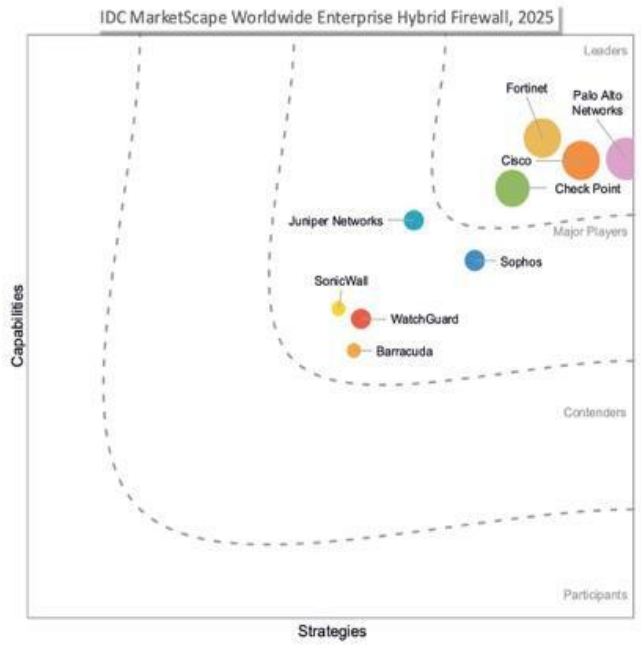
Dodavatel má za to, že pokud zadavatel stanoví podmínku, která fakticky zvýhodňuje pouze řešení odpovídající jedné konkrétní externí metodice, musí být schopen konkrétně a přesvědčivě odůvodnit, proč požadovaný standard nelze vyjádřit obecněji a proč nepostačuje použití objektivních technických, bezpečnostních a výkonových parametrů.

Judikatura správních soudů přitom opakovaně zdůrazňuje, že:

- *odkaz na konkrétní výrobek či selektivní vymezení předmětu plnění je přípustné jen výjimečně a musí být konkrétně věcně odůvodněno, přičemž obecná tvrzení nepostačují – viz rozsudek NSS 9 Afs 30/2010-182,*
- *pokud nejde o situaci, kdy zadavatel objektivně potřebuje jediné konkrétní plnění, musí připustit rovnocenné řešení – viz rozsudek NSS 1 As 57/2025-27,*
- *nepřiměřeně nastavené požadavky, které předem vylučují objektivně způsobilé dodavatele, mohou představovat skrytou diskriminaci — viz rozsudek NSS 7 Afs 44/2013-37*

FIGURE 1

IDC MarketScape Worldwide Enterprise Hybrid Firewall Vendor Assessment



Source: IDC, 2025

Dodavatel je přesvědčený, že zařazení výrobce NGFW v sekci Leaders IDC MarketScape Worldwide Enterprise Hybrid Firewall Vendor Assessment je dostatečné pro účely posouzení kvality nabízeného řešení.

Odpověď na Dotaz č. 1:

Byla upravena zadávací dokumentace a uvedený požadavek byl odstraněn.

Dotaz č. 2

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW – síťové funkcionality požaduje zadavatel: „umět nakonfigurovat IPSec tunel v transportním módu pro šifrování komunikace mezi hosty.“

Dle zkušeností Uchazeče se od využití IPSec tunelu v transportním módu v poslední době upouští z důvodu bezpečnostních limitů a využívá se řešení IPSec v tunelovém modu, které poskytuje vyšší bezpečnost, protože šifruje kompletně celý paket včetně IP hlavičky. 3

Umožní zadavatel předložit nabídku pomocí řešení IPSec v tunelovém modu, které poskytuje vyšší bezpečnost?“

Odpověď na Dotaz č. 2:

Zadavatel nemůže vždy ovlivnit, s kým potřebuje vytvořit tunelované spojení a jaké technické prostředky bude mít druhá strana k dispozici. Proto je třeba mít k dispozici širší prostředky.

Zadavatel na požadavku IPSec tunelu v transportním módu trvá.

Dotaz č. 3

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW – bezpečnostní funkcionality požaduje zadavatel: „obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita“.

Podle uživatelské identity lze efektivně řídit např. šířku pásma komunikace, ale typické DoS protekce jsou ve spojení s identitou principiálně technologicky neřešitelné. V okamžiku tohoto útoku není totiž typicky uživatelská identita k dispozici. Proto pokročilá NGFW řešení pracují na principu ochrany publikovaných i interních služeb proti DoS útokům na základě konfigurovatelných limitů spojení, limitů neúplně navázaných spojení a dalších mechanismů ochrany proti zahlcení služeb.

Umožní zadavatel naplnění tohoto požadavku, pokud NGFW umožňuje ochranu publikovaných i interních služeb proti DoS útokům pomocí konfigurovatelných limitů spojení, limitů neúplně navázaných spojení a dalších mechanismů ochrany proti zahlcení služeb?“

Odpověď na Dotaz 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. Zadavatel umožňuje navrhované řešení, pokud ho bude možné navázat na zdroje určené uživatelskou identitou tzn. za podmínek dodržení zadávací dokumentace.

Dotaz č. 4

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW - QoS požaduje zadavatel: „poskytovat možnost prioritizace provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)“

Ze zkušenosti Uchazeče je časové řízení prioritizace provozu neefektivní a zbytečně komplikuje bezpečnostní politiky. Při nasazení NGFW je vhodnějším řešením aplikace tzv. Zero Trust Network Access (ZTNA) konceptu. Toto znamená, že konkrétní aplikace jsou přístupné pouze pro konkrétní uživatele, jejichž role, ale i stav koncového zařízení splňuje firemní bezpečnostní požadavky. Pokud mají mít nějaké aplikace nastavenou šířku pásma, konfigurujeme toto typicky permanentně. Časové plány, pokud jsou nasazovány, pracují s řízením přístupu jako takovým, nikoliv s řízením šířky pásma. Koncept ZTNA poskytuje přístup k prostředkům, které má mít uživatel dostupné, dochází k trvalé eliminaci přístupu na rizikové aplikace a zároveň je umožněno dostatečné pásmo pro bezpečný přístup na „business critical“ aplikace.

Umožní zadavatel nabídnout řešení, které poskytuje popsanou možnost nastavení pomocí principu Zero Trust, to znamená požadavek formulovaný takto: „Firewall musí být schopen pracovat se ZTNA konceptem - tj. aplikovat kontinuální politiky řízení přístupu na odpovídající zdroje podle role uživatele a stavu jeho stanice. Pro konkrétní aplikace musí být možné definovat šířku pásma, a tak je prioritizovat nebo naopak umožnit dostatečný prostor pro „business critical aplikace“. Firewall musí podporovat časové řízení přístupu na konkrétní aplikace.“

Odpověď na Dotaz č. 4:

Zadavatel provozuje systém, kde jsou v různých časech různé datové toky, tedy i jiné potřeby prioritizace. Zadavatel definoval zadávací podmínky tak, aby v co nejširší možné míře naplnily jeho požadavky.

Zadavatel trvá na požadavku na časové nastavení pravidel.

Dotaz č. 5

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW – sandboxing požaduje zadavatel: „schopen detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod.“

Uchazeč považuje za srovnatelné, ne-li efektivnější využití detekčních mechanismů přímo na FW, pracující s klasifikací souborů, detekcí polymorfních útoků, verifikací oproti reputačním databázím, detekcemi s využitím strojového učení a dalšími mechanismy reagujícími na nové a pokročilé formy útoků (0-day,…). Nutno podotknout, že pro analýzu souborů je potřeba provádět důsledně SSL dekrypci. Pro detekci nebezpečných komunikací, které principiálně nemusí být jednoduché dešifrovat potom existují strojovým učením vybavené metody analýzy šifrovaného provozu. Vlastní Sandbox platforma poskytuje analýzu neznámých souborů a předává verdikty integrovaným bezpečnostním komponentám jako např. NGFW, Email gateway, Web gateway, EDR, apod. Ale z principu je potřeba počítat s tím že vlastní Sandboxing proces má časovou režii typicky několik minut a není efektivní pro blokaci škodlivého souboru v reálném čase. Tudíž samotný Sandbox není inline blokovací technologie a pokud nebudeme po uživateli chtít aby např. na stažení souboru, dokumentu apod. čekal několik minut, nelze jej jako samotnou platformu uvažovat pro blokaci doručení škodlivého souboru na koncový bod. Měl by tedy být nasazen spolu s prvky klasifikace, real-time detekce a analýzy – tj. např. mechanismy přímo na NGFW.

Akceptuje Zadavatel pro blokaci stahovaného souboru v reálném čase využít paralelní efektivní vrstvu inline protekce (na zde poptávaném NGFW)?“

Odpověď na Dotaz č. 5:

Zadavatel požaduje "detekovat a zablokovat stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod" a to v sekci Sandboxing. Zadavatel na funkcionalitě jako takové trvá, ovšem netrvá na tom, aby ochrana v reálném čase byla řešena nutně funkcí sandboxu, pokud požadované funkcionality bude dosaženo jinou technologií. Akceptuje tedy i jinou formu řešení, pokud vyhovuje požadavku.

Dotaz č. 6

„V dokumentu VZ_Náhrada_firewallů_P1_SML_Technická_specifikace v části HW – sandboxing požaduje zadavatel: „podporovat operační systémy Windows, Linux, MacOS“

Uchazečem uvažované řešení se opírá o nejrozsáhlejší znalostní databázi updatovanou průběžně z Threat Intelligence báze a mechanismem porovnání vzorků s bází zachycuje vzorky před vlastním sandboxingem (ten je typicky jen „doplňkovou“ analýzou a nelze jej nazvat on-line analýzou pokud trvá v řádech minut). Uvažované řešení pracuje s ML analýzou přímo na NGFW tak, aby on-line způsobem odchytil útoky nulového dne. Sandbox se následně využívá pro detonaci neznámých souborů pro validaci výsledku, avšak ne pro on-line blokaci souboru – to před odesláním do sandboxu udělá již samotný NGFW. Threat báze je online způsobem aktualizována a vzorky sbírá globálně ze všech zařízení připojených do této služby a zpětně je poskytuje všem připojeným zařízením. Připojenými zařízeními se rozumí platformy jako NGFW, Email gateway, Web gateway, Endpoint Detection and Response pro koncové stanice, servery a mobily (s různými operačními systémy jako Windows, MacOS, linux, Android).

Umožní zadavatel předložit nabídku, která řeší uvedený požadavek zmiňovaným způsobem, a tedy není nezbytná podpora všech zmiňovaných operačních systémů v rámci sandboxu?“

Odpověď na Dotaz č. 6:

Zadavatel trvá na tom, že požaduje sandbox ověření pro všechny relevantní operační systémy používané ve své infrastruktuře, tedy MS Windows, Linux i MacOS. Neumožňuje žádné řešení, které by nepodporovalo sandbox pro všechny tři systémy.

Na základě výše uvedeného dotazu zadavatel přistoupil ke změně zadávací dokumentace veřejné zakázky. Tato změna, tedy upravená Příloha 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.