SPRÁVA ŽELEZNIC

Váš dopis zn.
Ze dne
Naše zn. 2243/2023-SŽ-GŘ-O8
Listů/příloh 2/2

Vyřizuje Miriam Hemzová
Mobil
E-mail

Datum 10. 1. 2023

Žádost o předběžnou tržní konzultaci ve věci přípravy zadávacích podmínek na veřejnou zakázku s názvem „Ochrana perimetru a DMZ – Next Generation Firewall"

(„Žádost")

Vážená paní, vážený pane,

Správa železnic, státní organizace, Vás touto cestou informuje o tom, že připravuje zadávací řízení ve věci **„Ochrana perimetru a DMZ – Next Generation Firewall"**. Vyhlášení této veřejné zakázky bude předcházet předběžná tržní konzultace (dále jen „PTK"), jejímž cílem bude získat relevantní informace pro správné nastavení předmětu plnění, zadávacích podmínek, volby druhu zadávacího řízení či způsobu hodnocení předložených nabídek. Zadavatel usiluje o získání kvalitního plnění, které bude splňovat jeho potřeby, a to za odpovídající cenu.

Cílem veřejné zakázky je uzavření smlouvy, jejímž předmětem bude dodávka čtyř zařízení typu Next Generation Firewall včetně implementace a následné správy.

Zadavatel v rámci PTK žádá o verifikaci požadovaných parametrů uvedených v příloze č. 1 - Parametry Next Generation Firewallu a o zodpovězení dotazů uvedených v příloze č. 2 - Otázky pro písemnou část PTK.

Cílem PTK je transparentním způsobem získat přehled o současné situaci na trhu, možnostech dodavatelů, a ujasnění otázek nezbytných pro realizaci veřejné zakázky.

PTK podle evropské zadávací směrnice (2014/24/EU) je možností zadavatele předtím, než vyhlásí veřejnou zakázku, komunikovat s dodavateli a zjišťovat (případně dalšími relevantními osobami) jejich možnosti a návrhy řešení. V rámci zvoleného modelu bude představen záměr zadavatele, včetně některých navrhovaných detailů jak předmětu veřejné zakázky, tak zadávacího řízení. Dodavatelé se pak budou moci k navrhovaným parametrům zakázky vyjádřit. Dojde tak ke zvýšení transparentnosti zadávacího řízení a získání relevantních a objektivních informací o možnostech trhu, tak aby mohl zadavatel optimálně nastavit zadávací podmínky veřejné zakázky, resp. celkové řešení zadávacího řízení. Vedení PTK je rovněž zcela v souladu s ust. § 33 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „Zákon").

Forma PTK: písemná, případně ústní

Způsob konání PTK:

V prvním kole PTK zašlou dodavatelé, jež projeví zájem o účast na této PTK, vyplněnou přílohu č. 1 - Parametry Next Generation Firewallu a odpovědi na otázky uvedené v příloze č. 2 - Otázky pro písemnou část PTK na e-mailovou adresu: **cnitptk@spravazeleznic.cz**

Svoji odpověď prosím doručte nejpozději do 23. 01. 2023.

Správa železniční dopravní cesty, státní organizace
zapsána v obchodním rejstříku vedeném Městským soudem v Praze, spisová značka A 48384

Sídlo: Dlážděná 1003/7, 110 00 Praha 1
IČ: 709 94 234 DIČ: CZ 709 94 234
www.szdc.cz

Generální ředitelství
Dlážděná 1003/7
110 00 Praha 1

Zadavatel si v případě potřeby vyhrazuje možnost uskutečnit druhé kolo PTK, přičemž v rámci tohoto druhého kola dojde za účelem konzultace zamýšleného řešení k osobnímu setkání s jednotlivými dodavateli. Zadavatel si vyhrazuje právo pozvat do druhého kola libovolný počet účastníků z kola předchozího, přičemž vždy bude postupovat tak, aby nedošlo ke zvýhodnění žádného z účastníků, zejména neposkytne účastníkům druhého kola žádné přídatné informace.

Předpokládaný počátek plnění předmětu veřejné zakázky je 4. kvartál roku 2023 přičemž může být na základě PTK upraven.

V případě Vašeho zájmu o účast na této PTK prosím zašlete vyplněnou přílohu č. 1 - Parametry Next Generation Firewallu a odpovědi na otázky uvedené v příloze č. 2 - Otázky pro písemnou část PTK na e-mailovou adresu: cnitptk@spravazeleznic.cz

Předběžná tržní konzultace nesmí vést k porušení základních zásad Zákona. Průběh i výsledek předběžné tržní konzultace bude zaznamenán ve zprávě vytvořené zadavatelem. Informace z předběžných tržních konzultací užité v zadávacích podmínkách zadané veřejné zakázky budou v souladu s § 36 odst. 4 Zákona v zadávací dokumentaci výslovně označeny, a to včetně osob, které se na výsledku podílely.

Děkuji za spolupráci.

S pozdravem

Ing. David Miklas
11.01.2023 15:06
Podepsáno elektronicky

Ing. David Miklas
ředitel Správy železničních informačních technologií

Přílohy

Příloha č. 1 – Parametry Next Generation Firewallu
Příloha č. 2 – Otázky pro písemnou část PTK

Příloha 1 – Parametry Next Generation Firewallu

Tato příloha obsahuje tabulku technických a realizačních parametrů, které jsou zadavatelem požadovány pro dosažení zamýšleného cílového řešení.

Next Generation Firewall

Uveďte, jakého výrobce a jaký model navrhujete pro požadované vlastnosti Next Generation Firewallu popsaného v níže uvedené tabulce:

Výrobce:

Model:

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Fyzické	
Minimální počet 40 Gbps rozhraní	2	
Minimální počet 25 Gbps nebo 10 Gbps rozhraní	2	
Dosažitelná reálná propustnost při zapnutých funkcionalitách Firewall, IPS, Aplikační kontrola, Web/URL filtering, Antivirus	10 Gbps	
SSL/TLS inspekce až do propustnosti	10 Gbps	
SSL/TLS inspekce podporující TLS 1.3	Ano	
Explicitní proxy	Ano	
Možnost rozdělení na samostatné virtuální kontexty	Ano, minimálně 5	
Sandbox analýza (Cloud)	Ano	
Propustnost IPsec	10 Gbps	
Ochrana proti DoS a DDoS útokům	Ano	
Podpora pravidel na základě identit uživatelů	Ano	
Způsoby ověřování uživatelů či napojení na autentizační systémy	LDAP, RADIUS, Windows AD SSO, NTLMv2, TACACS+	
Módy vysoké dostupnosti klastru	Active-Standby, Active-Active	
Podpora NAT64/DNS64	Ano	
Požadované funcionality	IPS, Aplikační kontrola, Web/URL filtering, DLP, Antiboty, Anti-DoS/DDoS, Ochrana DNS, Sandbox	
Lokální úložiště	100 GB	

Nákladys	Cena v Kč bez DPH
Cena za 4x Next Generation Firewall	
Cena za podporu (8x5 NBD) a aktualizaci požadovaných bezpečnostních služeb celkově po dobu 60 měsíců	

Centrální správa a sběr logů

Předpokládané rozdělení Next Generation Firewallů je na dva klastry po dvou fyzických zařízeních. Z tohoto důvodu jsou zjišťovány možnosti externí správy. Níže uvedenou tabulku prosíme vyplňte pro dvě varianty typu zařízení: fyzické a virtuální.

Uveďte výrobce a model navrhovaného řešení pro centrální správu a sběr logů:

Výrobce:

Model:

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Fyzické	
Podpora počtu spravovaných zařízení/virtuálních kontextů	10 a více	
Příjem logů a práce s nimi přímo na zařízení	10 GB logů za den	
Pokročilá analýza událostí a logů ze spravovaných zařízení	Ano	

Náklady	Cena v Kč bez DPH
Cena za fyzické zařízení na externí správu	
Cena za podporu celkově po dobu 60 měsíců (8x5 NBD)	

Požadovaná vlastnost	Požadovaná hodnota vlastnosti	Hodnota vlastnosti navrhovaného zařízení
Typ zařízení	Virtuální (VMware)	
Podpora počtu spravovaných zařízení/virtuálních kontextů	10 a více	
Příjem logů a práce s nimi přímo na zařízení	10 GB logů za den	
Pokročilá analýza událostí a logů ze spravovaných zařízení	Ano	

Náklady	Cena v Kč bez DPH
Cena za virtuální zařízení na externí správu	
Cena za podporu celkově po dobu 60 měsíců (8x5 NBD)	

*V případě, že respondent definuje vlastnosti na základě jiných parametrů, prosíme uvedení těchto parametrů s doporučenými hodnotami do tabulky.

Příloha 2 – Otázky pro písemnou část PTK

Tato příloha obsahuje seznam otázek za účelem ověření dostupnosti a kvality všech požadovaných vlastností cílového řešení.

Dotazy k technickému řešení pro Ochranu perimetru a DMZ – Next Generation Firewall

1. Jak jsou hodnoceny nabízené firewally posledními porovnáními Gartner Magic Quadrant Network Firewall a The Forrester Wave: Enterprise Firewall včetně historického vývoje?
2. Jakou uvádí výrobce dostupnost v tzv. devítkách při konfiguraci klastru o dvou nodech? (Například 99,999 %)
3. Jakými funkcionalitami disponuje explicitní proxy v rámci řešení? Popřípadě uveďte odkaz na podrobnou dokumentaci.
4. Využití explicitní proxy může přinášet výkonovou zátěž, která se však v produktových listech výrobců neobjevuje. Uveďte, zda využití explicitní proxy zvyšuje zatížení firewallu, popřípadě, jakou lze očekávat propustnost při souběhu s Threat prevention/protection funkcionalitami.
5. V případě využití funkcionality cloud sandbox, lze službu definovat granulárně na určité datové toky nebo komunikaci? Pokud ano, do jaké úrovně?
6. Jaké jsou konfigurační parametry DoS a DDoS ochrany a do jaké úrovně ISO/OSI modelu lze ochranu konfigurovat?
7. Jaká je doporučená architektura pasivního ověřování identit na základě integrace s Active Directory?
8. Jaký protokol je využit pro konfiguraci a běh klastru a na jaké síťové úrovni je implementace realizována (VMAC, VIP, …)?
9. Přibližně kolik IPS signatur obsahuje nabízené řešení a jakým způsobem probíhá stažení a implementace nových signatur. Dochází k nasazení automaticky nebo manuálně správcem. V případě obou možností, která možnost je obvykle realizována.
10. Popište vlastnosti a možnosti využití DLP funkcionality na úrovni perimetrového firewallu.
11. Přibližně kolik aplikací je vedeno ve funkcionalitě aplikační kontrola a jakým způsobem probíhá definice nových aplikací na straně výrobce?
12. Umožňuje řešení centrální správy nebo lokální správy next generation firewallu testování politik před nasazením do produkce? Pokud ano, jaké parametry jsou kontrolovány?
13. Je možné provádět aktualizaci operačního systému firewallu v produkčním provozu bez ztráty navázaných spojení a relací?
14. Jakým způsobem probíhá testování stability, spolehlivosti a funkčnosti nových verzí operačního systému?
15. Jaké „high" a „critical" CVE zranitelnosti byly identifikovány na nabízeném řešení v posledních třech letech?
16. Jaké je podpora pro odesílání záznamů do externích zařízení typu SEM a SIEM? Existují nativní integrace nebo technologické spolupráce?
17. Jaké úrovně podpory výrobce nabízí? Uveďte ke každé úrovni podrobný popis s informacemi o době a způsobu dodání náhradního zařízení, follow the sun podpoře apod.
18. Jaké standardy logování by dané zařízení mělo splňovat.
19. Umožňuje výrobce provozování i virtuální verze NG FW?