Veřejná zakázka

Dodávka HW, SW a služeb v oblasti infrastruktury datových center

Ev.č.: 499467

Zadavatel veřejné zakázky:

Česká republika – Ministerstvo práce a sociálních věcí

se sídlem Na Poříčním právu 1/376, 128 01 Praha 2

IČO: 00551023

(dále jen „**zadavatel**“ nebo „**MPSV**“)

Dodatečné informace k zadávacím podmínkám č. X

dle § 49 odst. 1 zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „**ZVZ**“).

MPSV, jako zadavatel shora uvedené veřejné zakázky, obdrželo dne 24. 2. 2015 žádost o poskytnutí dodatečných informací k zadávacím podmínkám.

Na níže uvedené dotazy poskytuje zadavatel následující odpovědi:

Dotaz č. 1:

V Příloze ZD č. 6_Funkčni a technické požadavky – kapitola 3.13.2.5.1 Kategorizace incidentů jsou definovány požadované parametry Reakční doby a požadované doby vyřešení incidentů pro jednotlivé priority takto:

Priorita	Popis	Reakční doba na incident	Doba vyřešení incidentu
1	Nejvyšší priorita na odstranění chyby	0,5 hodiny	do 4 hodin
2	Vysoká priorita na odstranění chyby	0,5 hodiny	NBD
3	Střední až nízká priorita na odstranění chyby	0,5 hodiny	72 hodin

Dle kapitoly 3.13.2.5.2 jsou tyto priority přiřazeny jednotlivým kategoriím Incidentů (A, B, C).

V závazném vzoru Smlouvy je v odstavci 14.4. uvedeno:

Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak:

14.4.1 Poskytovatel zahájí řešení odstranění vady kategorie A, tj. vady, která zcela nebo podstatným způsobem znemožňuje užívání Infrastruktury, okamžitě po jejím nahlášení, s tím, že vadu do 8 hodin od jejího nahlášení odstraní nebo poskytne akceptovatelné náhradní řešení,

14.4.2 Poskytovatel zahájí řešení odstranění vady kategorie B, tj. vady, která nebrání užívání Infrastruktury, ale omezuje její provoz, maximálně do 4 hodin od jejího nahlášení s tím, že vadu do 5 dnů od jejího nahlášení odstraní nebo poskytne akceptovatelné náhradní řešení,

14.4.3 Poskytovatel zahájí řešení odstranění vady kategorie C, tj. vady, která není vadou kategorie A ani B, maximálně do 2 dnů od jejího nahlášení s tím, že termín odstranění vady bude předmětem dohody smluvních stran, nepřekročí však dobu 10 dnů od jejího nahlášení

Dle našeho názoru jsou požadavky uvedené ve Funkční specifikaci a návrhu Smlouvy nejednoznačné.

Může k tomu Zadavatel podat vysvětlení a pokud se případně jedná o chybu, žádáme o upřesnění a sjednocení parametrů „Reakční doba“ a „Doba vyřešení“ dle jednotlivých priorit a kategorií Incidentů.

Odpověď zadavatele:

Zadavatel k tomuto uvádí, že tato otázka je zcela jednoznačně řešena v odst. 14.3 Závazného vzoru Smlouvy – příloha č. 2 zadávací dokumentace (dále jen „**Smlouva**“), v němž je uvedeno, že **po dobu poskytování Služeb podpory provozu budou veškeré záruční i mimozáruční vady Infrastruktury řešeny plněním Poskytovatele poskytovaným v rámci těchto Služeb podpory provozu a ustanovení odst. 14.4, odst. 19.2.1 a odst. 19.2.2 Smlouvy se po tuto dobu nepoužijí**.

V žádném případě se tedy nejedná o jakýkoli rozpor mezi Smlouvou a Přílohou č. 6 zadávací dokumentace – Funkční a technické požadavky, zadavatel tedy nebude zadávací podmínky jakkoli upravovat.

Dotaz č. 2:

Dne 12. 2. 2015 jsme pokládali následující dotaz k zakázce: „V příloze č. 6 Zadávací dokumentace v kapitole 3.3.1.6. – Funkční a technické požadavky je požadován minimální technický požadavek „nezávislost výkonu firewallu na velikosti paketu“. Tento parametr splňuje pouze jediný výrobce (zdroj. NNS Labs 2014). Je nesplnění tohoto kritéria důvodem k vyloučení nabídky z výběrového řízení?“

Odpověď zadavatele byla následující: „Technickým požadavkem na „„nezávislost výkonu firewallu na velikosti paketu“ je myšleno zajištění požadovaného výkonu u packetu, které specifikuje tabulka č. 2. Pokud uchazeč dodá řešení splňující minimální požadavky na „Firewall Throughput“ uvedené v tabulce č. 2 a v některých oblastech jej bude překonávat (např. Firewall Throughput 1518 Bytes = 25 Gbps Firewall Throughput 512 Bytes = 20 Gbps), pak je požadavek nezávislost výkonu firewallu na velikosti paketu splněn, neboť požadovaná šířka pásma 20 Gbps je zajištěna i při různé velikosti paketů.

Zadavatel dále uvádí, že tabulka v kapitole „3.3.1.6 – Požadavky na firewall“ jsou minimální technické požadavky uvedeny agregovaně pro celý firewallový cluster. Nejedná se o požadavky na I uzel clusteru“.

Dotaz:

Požadované minimální výkonové parametry pro firewalový cluster uvedené v odpovědi Zadavatele (např. propustnost 20Gbps pro velikosti paketů: 64 byte, 128 byte, 256 byte) splňuje, dle výsledku testů nezávislé společnosti NSS Labs (viz přiložená tabulka níže), pouze jediný výrobce (FORTINET). **Tento požadavek považujeme za striktně diskriminační pro všechny ostatní technologie. Trvá zadavatel na uvedených parametrech a bude jejich nesplnění důvodem vyloučení nabídky dodavatele z výběrového řízení?**

Figure 4 and figure 5 depict the maximum UDP throughput (in megabits per second) achieved by each device using different packet sizes.

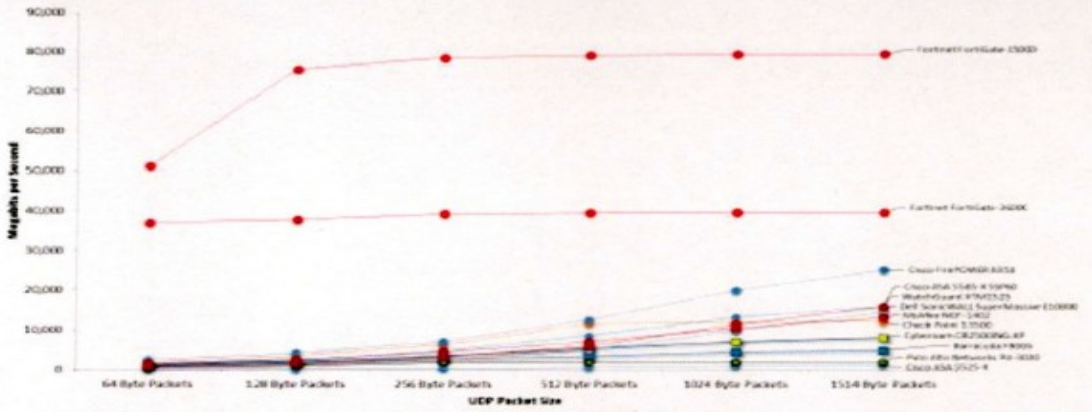

Figure 4 – UDP Throughput by Packet Size (Mbps)

This type of test was considered "table stakes" for legacy firewalls, but it can often cause significant problems for NGFW (and IPS) devices because of the amount of deep inspection they are expected to perform.

Product	64 Byte Packets	128 Byte Packets	256 Byte Packets	512 Byte Packets	1024 Byte Packets	1514 Byte Packets
Barracuda F800b	1,200	1,900	2,700	3,500	4,600	5,000
Check Point 13500	1,986	3,522	6,342	11,700	12,120	12,270
Cisco ASA 5525-X	80	200	400	680	1,040	1,320
Cisco ASA 5585-X SSP60	1,480	2,500	4,950	8,600	13,300	16,000
Cisco FirePOWER 8350	2,600	4,250	7,100	12,570	19,990	25,250
Cyberoam CR2500iNG-XP	1,200	2,200	3,600	5,300	7,100	8,200
Dell SonicWALL SuperMassive E10800	780	1,380	2,570	5,040	9,990	14,650
Fortinet FortiGate-15000	51,200	75,600	78,500	79,100	79,400	79,500
Fortinet FortiGate-3600C	37,000	37,800	39,200	39,500	39,700	39,700
McAfee NGF-1402	1,600	2,700	4,500	7,100	10,500	13,300
Palo Alto Networks PA-3020	600	1,040	1,960	2,000	2,000	2,000
WatchGuard XTM1525	880	1,600	3,400	5,900	11,400	16,000

Odpověď zadavatele:

Výše uvedená tabulka odkazuje na test firewallů uvedených v tabulce, provedené v rámci NSS LAB v roce 2014. **Nejedená se však o test všech dostupných produktů na trhu, pouze o vzorek.** Navíc nejsou zde ani zastoupeni všichni velcí výrobci firewallů, natož jejich portfolio produktů. Tabulka také odkazuje na „Legacy Firewalls“, neboli **pouze fyzické firewally. Virtuální firewally nebyly do testu nikterak zahrnuty.**

Zadavatel v zadávací dokumentaci uvádí:

Zadavatel nestanovuje podmínky, zda-li řešení firewallu má být provozováno na fyzickém hardware výrobce firewallu nebo formou virtualizace. V případě volby virtualizace je uchazeč povinen v nabídce k ceně softwarového řešení započítat hardware nutný pro provoz virtuálních appliance s požadovaným výkonem.

Pakliže by Uchazeč chtěl nabídnout některé zařízení uvedené v obrázku uchazeče, jednou z možností by byla realizace za pomocí většího počtu uzlů v rámci firewall clusteru.

Zadavatel dále upozorňuje dodavatele, že NSS LABS neprovedli pouze jeden dodavatelem zmíněný test firewallu.

Vzhledem k výše uvedenému je tvrzení dodavatele o diskriminaci ze strany zadavatele zcela nedůvodné a zadavatel trvá na splnění požadavku.

Dotaz č. 3:

V dokumentu Příloha č. 6 ZD, odstavec 3.3.4.1 v tabulce č. 8 – minimální parametry diskového pole TYP A, číslo řádku 1 je uvedeno

Číslo řádku	Požadavek na funkcionalitu nebo parametr	Minimální požadavky
	Celkový počet kontroléru (jak pro přístup k datům, tak souborovým systémům)	4

Dle názoru uchazeče je tento požadavek formulován nejednoznačně v tom smyslu, že jej lze vyložit následujícími způsoby:

a) Celkový počet kontrolérů diskového pole musí být alespoň 4, nezávisle na tom zda poskytují blokový nebo souborový přístup k datům - např. 2 SAN a 2 NAS kontroléry

b) Celkový počet kontrolérů poskytujících blokový přístup k datům musí být alespoň 4, a současně celkový počet kontrolérů poskytujících souborový přístup k datům musí být alespoň 4 – například:

celkem 8 kontrolérů - 4 pouze SAN kontroléry a 4 pouze NAS kontroléry, nebo

celkem 4 kontroléry s oběma funkcionalitami SAN i NAS

Chtěli bychom požádat o jednoznačný výklad tohoto požadavku.

Odpověď zadavatele:

Dodavatelem uvedený výklad v bodě a) je správný.

Pro vyvrácení jakýchkoliv pochybností, zadavatel dále uvádí, že uchazečem navržené řešení musí splňovat požadavky na vysokou dostupnost (Tabulka č. 8 – řádek č. 3 – příloha zadávací dokumentace č. 6 - Funkční a technické požadavky). Řešení s 1x SAN a 3x NAS kontroléry je neakceptovatelné, neboť pouze 1x SAN by nesplňoval požadavky na vysokou dostupnost.

Dotaz č. 4:

Dle Zákona 137/2006 Sb. §46 odst. 4-7) jsou technické podmínky stanovené v Zadávací dokumentaci brány jako požadavky na výkon a funkci. V tomto smyslu chápeme tento požadavek RAID jako metodu zabezpečení dat proti selhání pevného disku. Dle uvedeného paragrafu připouští zákon plnění i obdobnou technologií při zachování požadované funkce a výkonu.

Jelikož výrobce zařízení nabízí RAID-DP jako standardní funkcionalitu již v základní konfiguraci zařízení při zachování všech ostatních funkčních a výkonnostních parametrů zařízení, považuje podporu méně výhodných úrovní RAID (zejména RAID10) za zbytečnou, neboť ekvivalentní funkcionality s vyšší mírou zabezpečení dat proti výpadku lze dosáhnout právě za použití RAID-DP.

Podle názoru uchazeče taxativně vymezený požadavek na konkrétní úrovně RAID může znevýhodňovat některé soutěžitele, tím vytvářet nerovné soutěžní prostředí a tudíž znemožňovat

rovnou hospodářskou soutěž. Zároveň znemožňuje zadavateli získat nejvýhodnější technickou nabídku.

Chtěli bychom požádat o odpověď, zda zadavatel připouští zařízení pouze s RAID-DP jako odpovídající a vyhovující požadavku č. 39 z kap. 3.3.4.1 Přílohy č. 6 ZD.

Odpověď zadavatele:

Zadavatel nesouhlasí s tvrzením dodavatele, že svazek typu RAID-DP zachová veškeré výkonnostní parametry při srovnání se svazkem typu RAID10.

Při zápisu do svazku RAID10 dochází k paralelnímu zápisu dat do několika diskových jednotek, kdy zapisovaná data jsou navíc vždy zrcadlena (zapisována do dvou různých diskových jednotek pro zajištění odolnosti proti selhání hardware). Zjednodušeně řečeno, ve svazku RAID10 jsou data uložena vždy ve dvou místech (diskové jednotky). Při selhání diskové jednotky jsou data v identické kopii dostupná na jiné diskové jednotce.

Při zápisu do svazku RAID-DP musí řadič diskového pole nejprve dopočítat horizontální paritu a poté diagonální paritu (pro zajištění odolnosti proti svazku proti výpadku). Tyto výpočty zatěžují řadič diskového pole a dochází tak k degradaci výkonu při zápisu dat ve srovnání se svazkem typu RAID10, neboť u svazku RAID10 žádnou paritu není třeba počítat.

Při selhání diskové jednotky ve svazku RAID-DP musí řadič diskového pole nejprve data „dopočítat“ (dle horizontální a diagonální parity). U svazku RAID10 se provede pouhé zrcadlení disků.

Zadavatel definoval na řádku č. 39 požadavky na RAID svazky z důvodu zajištění svých potřeb, kdy:

RAID 10 – svazek disků pro zajištění maximálního výkonu

RAID 5,6 – svazek disků s preferencí použitelné čisté kapacity

Dle průzkumu zadavatele podporu standardních svazků RAID uvedených na řádku č. 39 mají disková pole min. 8 výrobců. Nejedná se tedy o proprietární technologii směřující k jednomu výrobci, jako dodavatelem zmíněný nestandardní svazek RAID-DP. Z těchto důvodů nelze požadavek č. 39 vnímat jako jakkoliv diskriminační nebo podporující nerovné soutěžní prostředí.

Uchazeč může navrhnout zařízení přesahující požadavky určené na řádku č. 39 (v souladu s kapitolou 3.1.2). Např. zařízení podporující RAID 1, 5, 6, 10 a další nestandardní RAID svazky, kdy RAID svazky jsou pojmenovaný komerčním (technologickým) názvem výrobce zařízení, avšak jejich funkce je obdobná.

Z výše uvedených důvodů nepřipouští zařízení pouze s RAID-DP. Pro odstranění všech pochybností, pod pojmem RAID-DP zadavatel chápe technologii popsanou v tomto odkaze:

https://en.wikipedia.org/wiki/Non-standard_RAID_levels#DOUBLE-PARITY

Dotaz č. 5:

V hlavním textu zadávací dokumentace, v kapitole 3. Podmínky veřejné zakázky, uvádíte v podkapitole 3.1 následující podmínku: „Cílem této veřejné zakázky je rovněž zajištění dodržení požadavků na bezpečnostní opatření a bezpečnostní dokumentaci dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů, a souvisejících předpisů.“ Znamená

uvedení této podmínky požadavek zadavatele, aby jako nedílná součást nabízeného plnění byly dodány nástroje pro ochranu, zaznamenávání, detekci, sběr a vyhodnocování ve smyslu § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, přestože v příloze ZD č. 6 nejsou takové nástroje blíže specifikovány? Pokud je odpověď na uvedenou otázku kladná, žádáme o uvedení konkrétních ustanovení zákona č. 181/2014 Sb., která zadavatel požaduje dodat jako nedílnou součást plnění zakázky, včetně uvedení nezbytných technických parametrů, jejichž nedodržení by zadavatel považoval za vadné plnění.

Odpověď zadavatele:

Zadavatel k tomuto uvádí, že pokud z Bezpečnostního projektu jakožto výstupu Poskytovatele zpracovaného dle odst. 3.1.1 Smlouvy (příloha zadávací dokumentace č. 2), požadujícího zpracování bezpečnostní dokumentace reflektující (všechny) požadavky zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů a souvisejících předpisů, vyplyne požadavek na dodání nástrojů pro ochranu, zaznamenávání, detekci, sběr a vyhodnocování ve smyslu § 5 odst. 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti, v rámci zajištění výkonu bezpečnostního dohledu a realizace bezpečnostních opatření dle KS1.4 ve smyslu přílohy č. 6 Zadávací dokumentace, pak je Poskytovatel povinen toto plnění poskytnout.

S ohledem na výše uvedené a očekávanou znalost Poskytovatele parametrů a vlastností navrhovaného řešení, považuje zadavatel druhou část dotazu za zodpovězenou.

V Praze dne 2. 3. 2015