Odpovědi na dotazy dodavatelů – veřejná zakázka malého rozsahu na službu „Globální AntiDDoS ochrana“

Zadavatel: CESNET, zájmové sdružení právnických osob
Zikova 1903/4, 160 00 Praha 6
IČO: 63839172
Odkaz na adresu VZMR na profilu zadavatele: https://zakazky.cesnet.cz/contract_display_272.html

Vážení dodavatelé,

zadavatel v minulých dnech obdržel několik dotazů k zadávacím podmínkám předmětné veřejné zakázky malého rozsahu. V souladu se zadávací dokumentací zadavatel níže uvádí odpovědi na obdržené dotazy.

Č. dotazu	Znění dotazu	Odpověď zadavatele
1	Dobry den, nase spolecnost ma ve svem produktovem portfoliu a v provozu u rady zakazniku jiz nekolik let plne funkcni a profesionalni sluzbu DDoS Mitigation. Podminkou nasazeni teto sluzby, je z technickeho (nikoliv z obchodniho) hlediska odber sluzby IP Transit Global IPv4 a IPv6 (tedy zahranicni IP konektivita). Vsechny pozadavky uvedene v bodu 2.3 zadavaci dokumentace jsme schopni splnit v pripade, ze by spol. CESNET soucasne vyuzila sluzbu IP Transit Global, ktera vsak neni predmetem teto VZ. Byl by akceptovan fakt, ze by nase spolecnost nabidla jak reseni Anti DDoS, tak i sluzbu IP Transit? A pokud ano, jake parametry sluzby IP Transit by spol. CESNET pozadovala?	Služba IP Transit není součástí předmětu plnění veřejné zakázky (tuto službu již zadavatel má zajištěnou). Pokud je však poskytnutí této služby nezbytnou podmínkou poskytnutí požadované služby AntiDDoS, zadavatel nijak nebrání dodavateli jí společně s požadovanou službou nabídnout / poskytnout, trvá nicméně na požadovaných parametrech požadovaného předmětu plnění veřejné zakázky - služby AntiDDoS ochrany, jak jsou specifikovány v poptávce. Požadujeme technické předání způsobem uvedeným v bodě 2.3.3. poptávky) umožňující poskytnutí služby AntiDDoS služby v kapacitě až 4 Gbps (2.3.4. poptávky). Je možný i model „burst“ například s minimálním commit 1 Gbps až do kapacity optických propojů (10 Gbps).
2	V bodě 2.3.3. žádáte optické 10G propojení do dvou lokalit. Služba ******, kterou bychom vám rádi nabídli, umožnuje doručení provozu do těchto lokalit pouze skrze GRE tunel ukončený na vašich routerech v daných lokalitách, nikoliv fyzické propojení. Naše otázka zní, zda to z hlediska nabídky je zásadní problém.	Služba může být poskytnuta prostřednictvím GRE tunelu, musí však být předána na fyzických portech a v lokalitách uvedených v bodě 2.3.3 poptávky.
3	Aktuálně máte DDoS řešení „on premise“ – má poptávané řešení sloužit pro mitigaci DDoS útoku nad kapacitní možnosti on premise řešení.	Poptávané řešení má sloužit pro mitigaci DDoS útoků na úrovni globálního routingu, tedy ještě před „vstupem“ IP trafficu do AS sítě CESNET. On-premise řešení provádí

		mitigaci DDoS útoku na hraně AS sítě CESNET. Otázka „kapacitních možností“ není proto relevantní, protože se jedná o jiný stupeň ochrany. Tyto systémy ochrany mají být komplementární.
4	Na základě „historie“ DDoS útoků lze odhadnout, ke kolika přesměrování a mitigaci ve scrubbing centru by docházelo (měsíčně / ročně)?	V „běžném provozu“ může přesměrování a mitigace probíhat v jednotkách případů měsíčně. V „kritickém provozu“ může přesměrování a mitigace probíhat řádově intenzivněji. Z bezpečnostních důvodů zadavatel nebude zveřejnovat historii nebo další detailní informace o očekávané četnosti využití. Z bezpečnostních důvodů požadujeme poskytnutí služby, která bude flexibilně využitelná podle aktuálních potřeb bez omezení četnosti využití, nebo limitující dobu využití. S ohledem na zadávací dokumentaci požadujeme poskytnutí služby bez dalších (variabilních) nákladů (např. podle četnosti užití, limitující dobu využití atp.). Pro správné nastavení očekávání, lze sdělit odhad fair-policy use využíti služby přibližně 100+ hodin / měsíčně.
5	Od jaké velikosti útoků by docházelo k přesměrování?	Z bezpečnostních důvodů nebude zadavatel zveřejnovat informace o předpokládané velikosti mitigovaných útoků. Poptáváme řešení, které budeme schopní využít flexibilně podle potřeby.
6	Má byt součástí služby i detekce útoků?	Detekce útoků bude prováděná nástroji CESNET, na základě kterých bude probíhat konfigurace služby způsobem definován v bodě 2.3.2. zadávací dokumentaci.
7	Předpokládá se automatické přesměrování během útoku nebo bude přesměrování manuální na základě rozhodnutí operátora dohledu?	Automaticky, nicméně s možností ruční konfigurace do konfigurace automatu.
8	Je možné zvážit i jiný typ konektivity - např. GRE ev. Konektivitu přímo ve scrubbing centru?	Služba může být poskytnuta prostřednictvím GRE tunelu, musí však být předána na fyzických portech a v lokalitách uvedených v bodě 2.3.3 poptávky. Předání služby ve Scrubbing centru není součástí předmětu plnění veřejné zakázky (tuto službu zadavatel nepožaduje). Pokud je však poskytnutí této služby nezbytnou podmínkou poskytnutí požadované služby AntiDDoS, zadavatel nijak nebrání dodavateli jí společně s požadovanou službou nabídnout / poskytnout, trvá nicméně na požadovaných parametrech

		služby AntiDDoS ochrany, jak jsou specifikovány v poptávce.
9	V zadávací dokumentaci je požadovaná kapacita konektivity „Limit „vyčištěného“ (clean) IP provozu: 4 Gbps.“ Může legitimní provoz pro jednotlivé subnety dosáhnout 4 Gbps pro příchozí provoz (Lze předpokládat, že bude docházet k přesmérování pouze jednotlivých subnetů)? Dávalo by smysl zvážit i menší kapacitu legitimního provozu?	Ano, lze předpokládat přesměrování jednotlivých subnetů o granularitě nejméně velikosti CIDR / 24. V „běžném provozu“ mohou být kapacity menší. Indicií může být odpověď na dotaz č.1. Službu je však nutné kalibrovat pro „krizový režim“, kde menší garance parametrů definované v bodě 2.3.4 poptávky nepřipouštíme.

S ohledem na rozsah dotazů a odpovědí zadavatel prodlužuje lhůtu pro podání nabídek do 9. 4. 2021, 12:00.

Dne 31. 3. 2021 zpracovali: Ing. Radovan Igliar, Mgr. Vojtěch Široký