Príloha č. 2

Návrh na plnenie kritéria

„Zriadenie primárneho a záložného bezpečného pripojenia na adresu verejného obstarávateľa vrátane poskytovania súvisiacich služieb“ - (na obdobie 24 mesiacov)

Identifikačné údaje uchádzača

Obchodné meno: Slovanet, a.s.
Sídlo/Miesto podnikania: Galvaniho 19, 821 04 Bratislava
IČO: 35 954 612
DIČ: 2022059094
IČ DPH: SK2022059094
Telefón: 02 / 208 28 111
E-mail: vo@slovanet.net
Kontaktná osoba: Ing. Dominik Podmanický, KEY Account Manager

Pol.	Predmet zákazky	J. c. bez DPH/ mesačne	Cena spolu v EUR bez DPH 24 mes.	Cena spolu v EUR s DPH 24 mes.
1.	Bezpečný centrálny prístup do verejnej siete Internet	700,00 €	16 800,00 €	20 664,00 €
2.	Služby zabezpečenia úrovne bezpečnosti sieťovej prevádzky	1 800,00 €	43 200,00 €	53 136,00 €
3.	Služby viacstupňového overenia prístupu do siete	550,00 €	13 200,00 €	16 236,00 €
4.	Služby elektronickej pošty	200,00 €	4 800,00 €	5 904,00 €
5.	Služby podpory a prevádzky	200,00 €	4 800,00 €	5 904,00 €
	Cena spolu za celý predmet zákazky	**3 450,00 €**	**82 800,00 €**	**101 844,00 €**

** Ak uchádzač nie je platcom DPH, uvedie pre sadzbu DPH slovné spojenie „Neaplikuje sa“.*
Ak uchádzač nie je platcom DPH, týmto vyhlasuje, že berie na vedomie, že ak sa neskôr stane platcom DPH, nie je oprávnený fakturovať k ponúknutej cene DPH, pretože skutočnosť, že sa stal platcom DPH nie je dôvodom na zmenu ponuky, či zmluvy a ním pôvodne ponúknutá cena sa považuje za cenu vrátane DPH.

čestné vyhlásenie uchádzača

Dolu podpísaný čestne vyhlasujem, že :

a) Riešenie uvedené v tejto cenovej ponuke zodpovedá špecifikácii a požiadavkám verejného obstarávateľa na predmet zákazky.
b) Cena predmetu zákazky za obstarávaný predmet je uvedená na základe vlastných prepočtov, berie do úvahy všetky skutočnosti, ktoré sú nevyhnutné na úplné a riadne plnenie, pričom do ceny sú zahrnuté všetky náklady spojené s požadovaným predmetom zákazky.

V Bratislave, dňa 07.02.2025

Podpis a pečiatka oprávnenej osoby/štatutára uchádzača: .....
RNDr. Lukáš Karlík, PhD.

ŠPECIFIKÁCIA PRE VYPRACOVANIE CENOVEJ PONUKY

v zmysle Opisu predmetu zákazky (príloha č.1)

Parameter	Požadovaný parameter	Požadujeme uviesť, či požiadavku spĺňa áno/nie resp. uviesť konkrétny parameter
1. Bezpečný centrálny prístup do verejnej siete		
Požiadavky na primárne pripojenie do verejnej siete Internet		
Minimálna požadovaná kapacita pripojenia: 500/500 Mbit/s	500/500 Mbit/s	Áno
Možnosť navýšenia kapacity	Primárne pripojenie musí umožniť navýšenie prístupovej kapacity minimálne na hodnotu 1Gbit/s bez potreby zmeny HW prístupovej platformy výlučne prostredníctvom zmeny konfigurácie prístupovej platformy bez prerušenia prevádzky, resp. s minimálnym vopred vzájomne dohodnutým a oznámeným prerušením prevádzky v rámci tolerovanej doby nedostupnosti služby.	Áno
Symetrickosť linky	Prístupová kapacita primárneho pripojenia musí byť symetrická, garantovaná a spĺňať minimálne uvedené parametre garancie kvality poskytovaných služieb („SLA“) uvedených v časti služby podpory a prevádzky.	Áno
Konektivita 500/500 Mbps do internetu v datacentre poskytovateľa	500/500 Mbps	Áno
Konektivita 500/500 Mbps do MPLS	500/500 Mbps	Áno
Optické pripojenie s kapacitou 500/500 Mbps s možnosťou navýšenia na 1/1 Gbps - Nemocnica Nové Zámky	500/500 Mbps	Áno
Rozhrania	Prístup do siete Internet bude ukončený na rozhraní Ethernet 10/100/1000 alebo optickom rozhraní 1000 Mbit/s. Súčasťou služby bude dodávka a správa aktívnych prvkov ktoré zodpovedajú výkonovým parametrom požadovaným v tomto dokumente.	áno
Požiadavky na záložné pripojenie do verejnej siete Internet		
Záložné pripojenie	4G LTE 10/10 Mbps	áno
Konfigurácia	Riešenie pripojenia do siete internet bude konfiguračne realizované tak, že v prípade výpadku pripojenia na primárnej linke dôjde k automatickému presmerovaniu sieťovej prevádzky na záložnú linku bez potreby vykonania akéhokoľvek konfiguračného zásahu Verejným obstarávateľom.	áno
Parametre záložnej linky	Prístupová kapacita záložného pripojenia musí byť symetrická, garantovaná a spĺňať minimálne uvedené parametre garancie kvality poskytovaných služieb („SLA“) uvedených v časti služby podpory a prevádzky. Záložné pripojenie bude realizované inou, nezávislou prístupovou technológiou, ktorá je plne nezávislá od primárneho pripojenia.	Áno
Ukončenie liniek	Prístup do verejnej siete internet má byť realizovaný ako primar/backup – obe linky primar/backup – ukončené na spoločnom smerovači.	áno
2. Služby zabezpečenia úrovne bezpečnosti sieťovej prevádzky		
Služby NGFW	V rámci tejto služby Verejný obstarávateľ požaduje poskytnutie služby Next Generation Firewall-u („NGFW“) s licenciou UTM pre účely online vyhodnocovania novovzniknutých zraniteľností. Verejný	Áno

	obstarávateľ požaduje, aby bolo použité zariadenie formou služby certifikované podľa medzinárodných štandardov ISO 27001.	
Funkcoionalita NGFW	Minimálne požiadavky na zriadenie a poskytovanie služby zabezpečenia úrovne bezpečnosti sieťovej prevádzky: - podpora VPN (virtuálne privátne siete IPSec a SSL VPN), Traffic Shaping; - Intrusion Prevention System – IPS (prevencia prieniku do systému); - Intrusion Detection System – IDS (detekcia prieniku do systému); - Funkcionalita Web Filtering pre účely možnosti riadenia kontroly webového obsahu; - Geo - blokovanie (blokovanie prístupu do systémov z vybraných krajín sveta); - DDoS ochrana; - Application Control; - Smerovanie na 2/3 vrstve; - Dual WAN (záloha alebo load balancing primárneho pripojenia do internetu so sekundárnym); - Zabezpečenie aktualizácie signatúr, databáz a firmware; - Antispam; Nastavenie vstupných parametrov riešenia: - monitoring zariadenia; - záloha konfigurácií; - zriadenie webového prístupu pre administráciu; - logovanie; Nastavenie minimálnych pravidiel sieťovej bezpečnosti: - ochrana pred útokmi na L3 vrstve ISO OSI; - ochrana a monitoring manažmentu prístupu; - monitoring dostupnosti zariadenia; - monitoring vyťaženia zariadenia a poskytovanie UTM štatistík; Služby definície UTM profilov a následné otestovanie nastavení: DNS UTM profil; - Antimalware UTM profil; - Webfilter UTM profil; - IPS UTM profil; - UTM profil pre aplikačnú kontrolu; Minimálne požiadavky na zariadenie NGFW: - Počet RJ45 slotov: min. 12; - Počet GE SFP slotov: min. 12; - Počet RJ45 manažment portov: min. 2; - IPv4 priepustnosť pri 1518/ 512 / 64 (UDP): min. 32 Gbit/s; - Priepustnosť firewallu (paket/s): min. 30 Mp/s - Minimálny počet súčasných TCP spojení: 4 000 000; - Minimálny počet nových TCP spojení: min. 250 000; - Minimálny počet NGFW politík: min. 10 000; - IPsec VPN priepustnosť: min. 20 Gbit/s; - SSL VPN priepustnosť: min. 2,5 Gbit/s; - Počet súčasných SSL-VPN používateľov: min. 500; - Priepustnosť SSL inšpekcie: min. 6 Gbit/s; - Priepustnosť IPS: min. 11 Gbit/s; - NGFW priepustnosť: min. 3 Gbit/s; - Možnosť prevádzky v režime vysokej dostupnosti „HA“; - Možnosť osadenia do racku – rozmer 1 U; - Prenájom zariadenia v prostredí dátového centra poskytovateľa;	Áno

	- zapojenie NGFW v režime vysokej dostupnosti „HA“ s funkcionalitou automatického presmerovania komunikácie na sekundárny NGFW	
Správa a údržba	Verejný obstarávateľ ako súčasť poskytovaných služieb požaduje súčasne vykonávať nepretržitú správu a údržbu požadovaných základných nastavení, tak aby boli dodržané východiskové nastavenia služby nastavené počas spustenia služby do prevádzky.	Áno
Dodatočná správa	Verejný obstarávateľ zároveň súčasne požaduje, aby uchádzač v rámci pravidelného mesačného paušálu poskytol služby dodatočnej správy a to v rozsahu minimálne 10 človekohodín mesačne. Služby dodatočnej správy zahŕňajú predovšetkým úkony súvisiace so zmenou nastavení parametrov služby nad rámec úvodných základných nastavení ako sú: - Nastavenia VPN SSL; - Správa certifikátov; - IPSEC VPN nastavenia; - Správa používateľov LAN; - Pokročilá správa IDS/IPS, Web Filtra, AntiSpam; - Geo - blokovanie; - Firewall pravidiel.	Áno
riešenie pre centralizované zhromažďovanie prevádzkových logov	Minimálne požiadavky: - Zhromažďovanie a ukladanie logov z navrhnutého NGFW riešenia; - Zasielanie logov poskytovateľovi do dátového centra v kryptovanej forme moderných neprelomených kryptovacích riešení; - Konsolidácia a centralizácia logov na jednom mieste za účelom efektívnej správy a analýz stavu sieťovej prevádzky; - Možnosť analýzy logov s cieľom odhaľovania anomálií a bezpečnostných hrozieb v sieti; - Možnosť generovania podrobných reportov o aktivite v sieti; - Možnosť vytvárania vlastných šablón pre reportovanie na základe potrieb Verejného obstarávateľa. Minimálne požiadavky na zariadenie pre zber a analýzu logov: - Počet RJ45 slotov: min. 2; - Kapacita úložiska zariadenia: min. 4 TB; - Denná kapacita spracovania logov: min: 100 GB; - Kapacita analyzovaných logov: min. 2500/s; - Kapacita zberu logov: min. 4000/s; - Kompatibilita s nasadeným NGFW riešením; - Kapacita počtu pripojených zdrojov logov: min. 100; - Možnosť osadenia do racku – rozmer 1 - 2U; - Prenájom zariadenia v prostredí dátového centra poskytovateľa; - Riešenie v režime HA (postačuje jedno zariadenie)	Áno
3. Služby viacstupňového overenia prístupu do siete		
Dvojfaktorové overovanie	Požaduje sa realizovať riešenie založené na SW tokenoch, ktoré bude generovať „ONE TIME PASSWORDS“ („OTP“) pre používateľov, ktorí sa prihlasujú do siete. Užívateľ bude získavať OTP prostredníctvom softvérového tokenu, ktorý bude nainštalovaný na koncovom zariadení Verejného obstarávateľa. Po zadaní OTP systém vykoná overovaciu procedúru a po	áno

	úspešnom overení bude užívateľ pripustený k sieťovým aktívam Verejného obstarávateľa. Minimálne požiadavky na systém dvojfaktorovej autentifikácie: - Počet tokenov: 200 používateľov ; - Klient pre generovanie OTP kompatibilný pre iOS, Android a Windows; - Jednoduché, používateľsky prívetivé prostredie, ktoré dokáže plnohodnotne využívať aj používateľ bez pokročilých technických zručností a znalostí; - možnosť prenosnej (perpetuálnej licencie) po výmene koncového zariadenia; - možnosť škálovateľnosti riešenia do budúcnosti bez nutnosti deaktivácie a/alebo zmeny nasadeného riešenia až do 200 používateľov; - možnosť kopírovania OTP; - viditeľnosť intervalu platnosti OTP; - 30 sekundový kód, ktorý sa po uplynutí zmení;	
FortiAuthenticator VM + FortiTokenMobile + priestor v cloude	Pre 200 používateľov	Áno
4. Služby elektronickej pošty		
Virtuálny mailový server v datacentre	Áno	Áno
Možnosť jednorazového zasielania elektronickej pošty min. v kapacite: 2 500 mailov za hodinu v rámci domény obstarávateľa	2500 aliasov	Áno
Riešenie disponuje samostatným administrátorským rozhraním pre účely výkonu základnej administrácie mailových účtov s možnosťou vytvárania vlastných aliasov	Áno	Áno
Zasielanie automatických notifikácií o nedoručenej pošte	Áno	Áno
Nasadenie formou „SAAS“	Áno	Áno
Funkcionalita zálohovania a obnovy mailov (obnova celej mailovej schránky so 100% obsahom podľa retencie - 2 týždne)	Áno	Áno
Webový klient	Áno	Áno
Minimálna kapacita úložiska mailov: 1,5 TB s možnosťou dynamického navýšenia	Min. 1,5 TB	Áno
Podpora pre IMAP, POP a SMTP protokoly	Áno	Áno
Podpora šifrovania TLS	Áno	Áno
Webové administrátorské rozhranie	Áno	Áno
Podpora štandardných API	Áno	Áno
Možnosť nastavovania užívateľom automatickej odpovede cez webové rozhranie, jednoduchý spôsob, napr.. v čase neprítomnosti	Áno	Áno
AntiSpam	Áno	Áno
Autodiscovery, AutoConfig	Áno	Áno
E-mailové kontá prepojené s AD a povolený LDAP	Áno	Áno
Monitoring a logovanie	Áno	Áno
Migrácia aktuálnej e-mailovej pošty a e-mailových schránok na nový hosting dodávateľa	Áno	Áno
Prenájom mailového servera v prostredí dátového centra poskytovateľa	Áno	Áno
5. Služby podpory a prevádzky		
Dostupnosť služby min: 99,95%;	99,95 %	Áno
Maximálna doba reakcie na nahlásený problém/incident: do 4 hodín, Next Business Day	Do 4 hod. NBD	Áno
Maximálna doba nástupu na odstránenie všetkých HW a SW porúch od ich nahlásenia: 8 hodín, Next Business Day.	8 hod.	Áno
Plánovaná údržba: max. 24 hodín / rok	Max.24 hod./rok	Áno
Nepretržitý monitoring a dohľad nad poskytovanými službami v režime 24/7/365	24/7/365	Áno
Zákaznícky helpdesk + portál na nahlasovanie incidentov a problémov. Riešenie incidentov a problémov prostredníctvom servisných ticketov	Áno	Áno