TECHNICKÁ SPECIFIKACE

pro zakázku na dodávku s názvem

„IT infrastruktura města Vyškov“ dílčí část 2: „Bezpečnost“

V tabulce níže jsou uvedeny požadované technické parametry pro řešení bezpečnosti infrastruktury v podobě rozšíření stávající licence Netscaler, nasazení síťové sondy vč. kolektoru a modulu pro vyhodnocení dat, dále řešení bezpečnosti na koncových zařízeních. Parametry jsou definovány jako minimální. Zadavatel požaduje, aby nabízená technologie splňovala požadavky uvedené v tabulce.

Do prázdné kolonky účastník doplní:

- v případě vyčíslitelného parametru: konkrétní číselnou hodnotu (odpovídající požadovanému minimu)
- v případě nevyčíslitelného parametru: ANO/NE v závislosti na tom, zda jeho nabízené zařízení požadavek splňuje/nesplňuje.

V případě, že nabídka účastníka nebude splňovat požadované parametry (tj. v případě vyčíslitelného parametru nabídka nesplní požadovanou hodnotu a v případě nevyčíslitelného parametru bude u požadavku uvedeno NE) bude nabídka takového účastníka vyloučena z výběrového řízení.

MINIMÁLNÍ TECHNICKÉ PARAMETRY				
Jsou-li v ZD (zadávací dokumentaci) nebo jejích přílohách uvedeny konkrétní obchodní názvy, jedná se pouze o vymezení požadovaného standardu a zadavatel umožňuje i jiné technicky a kvalitativně srovnatelné řešení. Zadavatel nepřipouští variantní řešení a nabídky obsahující plnění nad rámec požadavků v ZD. Jakákoli nesplněná podmínka zadání je považována za nesplnění zadání a je důvodem k vyřazení účastníka.				
Požadavek	**Parametr**	**Jednotky**	**Vepište číselnou hodnotu, příp. ANO/NE**	**Vepište název a typ produktu**
Rozšíření Netscaler, 1 ks				
Základní vlastnosti	Bezpečný přístup k aplikacím (web aplikační firewall - WAF) a balancování provozu aplikací (loudbalancing - LB) v prostředí Citrix	ANO		
	Zvýšení výkonu a dostupnosti provozovaných aplikací a dat	ANO		
	Bezpečný vzdálený přístup k aplikacím z jakéhokoli typu zařízení	ANO		
	Kompatibilita se stávající licencí Citrix NetScaler Gateway Enterprise VPX	ANO		
	Minimální rychlost přístupu 25 Mbps s	ANO		

	možností upgrade na vyšší rychlost			
	Nástroje pro uživatelsky přívětivou administraci a přehlednost architektury aplikací	ANO		
	Reverzní proxy s pokročilými autentifikačními schopnostmi	ANO		
Bezpečnost aplikací	L4 DoS defenses	ANO		
	L7 DoS defenses	ANO		
	L7 rewrite and responder	ANO		
	MultiFactor authentication	ANO		
SSL akcelerace	Serverové certifikáty instalované již na LB zařízení, LB bude vykonávat funkci SSL šifrování a odebere část zátěže aplikačního WWW serveru	ANO		
Inteligentní komprese dat	Snížení objemu přenášených dat na základě vlastností typických aplikačních protokolů a klientů, komprese nevyžadující instalaci doplňkových produktů na koncové zařízení uživatele	ANO		
Dočasné ukládání dat (caching)	Podpora LB pro ukládání často se opakujících dat do interní paměti pro zvýšení výkonnosti aplikace	ANO		
Další požadovaná funkcionalita	Podpora LDAP, NTLM, Radius, TACACS+	ANO		
	Možnost řízení spojení a LB procesu na základě obsahu komunikace na L3 až L7 vrstvě	ANO		
	Možnost zpracovat libovolný síťový protokol (založený na IP)	ANO		
	Možnost změny obsahu přenášených dat až na L7 vrstvě	ANO		
	Možnost filtrování provozu na úrovni packetů	ANO		
	Možnost filtrování provozu podle obsahu na L7 vrstvě	ANO		
	Reporting událostí	ANO		
	Možnost logovat na externí Syslog server	ANO		
	Podpora uživatelských rolí	ANO		
	Programovatelný frontend na úrovni HTML, který umožňuje vytvoření vlastní přihlašovací stránky	ANO		
	Monitorování cílových serverů a na nich provozovaných služeb prostřednictvím: ICMP, HTTP, HTTPS, TCP, UDP, SNMP	ANO		

	Možnost zaznamenávat statistiky provozu HTTP a vytvářet exportovatelné výstupy včetně grafu, přes jednotlivé služby	ANO		
	Možnost zachytit uživatelský HTTP provoz (response/request)	ANO		
	Plná podpora Ipv6, Ipv6/Ipv4 gateway	ANO		
	Podpora standardu SHA-2 , TLS 1.1 i TLS 1.2	ANO		
	Podpora SNMP v1, v2, v3	ANO		
Maintenance	Technická podpora výrobce a nárok na nové verze přímo od výrobce min. po dobu 5 let	ANO		
	Dostupnost bezpečnostních aktualizací po dobu 5 let	ANO		
Síťová sonda a kolektor, 1 ks				
Požadované parametry	HW zařízení do RACK 19 palců, výšky 1U	ANO		
	Výkonná autonomní NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd sonda	ANO		
	Podpora pro 2 x 10/100/1000 Mb Ethernet, výkon na 1 port min. 1,45 Mp/s	ANO		
	Zpracování dat bez ztráty paketů	ANO		
	Podpora pro IPv4, IPv6, MAC, VLAN a MPLS	ANO		
	HTTP, DNS a VoIP analýza, detekce aplikací (NBAR2)	ANO		
	Monitorování výkonových parametrů sítě (RTT, SRT, retransmise, out-of-order pakety, delay a jitter)	ANO		
	Identifikace zařízení, operačního systému, verze internetového prohlížeče	ANO		
	Min 2 monitorovací porty v jednom zařízení	ANO		
	Jednoduchá správa přes webové rozhraní	ANO		
	Reportování a alertování událostí do: E-mail, SMS, Syslog, SNMP, spuštění záchytu paketů, spuštění skriptu	ANO		
	Výkon analytického modulu dimenzován na velikost sítě min 5000 IP adres	ANO		
	Podpora LDAP, audit změn konfigurace	ANO		
	Detekce VoIP/SIP anomálií	ANO		
	Integrovaný kolektor pro zobrazení a analýzu dat s výkonem min. 50 000 toků/s a úložnou kapacitu min 500 GB	ANO		
	Popora pro výkonové parametry sítě (NPM, AVC ART)	ANO		

	Statistiky zobrazovány ve formě grafů a tabulek s možností volby různých perspektiv	ANO		
	Podpora konceptu BYOD (bring-your-own-device) a identifikace zařízení včetně operačního systému	ANO		
	Automatická detekce zdrojů dat	ANO		
	RESTful API pro automatizované získávání a zpracování flow statistik v systémech třetích stran	ANO		
	Plně kompatibilní s NetFlow kolektory třetích stran	ANO		
Maintenance	Technická podpora výrobce min. po dobu 5 let	ANO		
Detekce síťových anomálií a bezpečnostních incident, 1 ks				
Požadované parametry	Port scan (horizontal, vertical, tcp, udp, icmp, …)	ANO		
	Detekce hádání hesel http/s, ssh, rdp, mailové služby, detekce DoS a DDoS, IP spoofing, duplikace/změna IP nebo MAC	ANO		
	Úniky dat (anomální přenosy dat), datové tunely (například přenos http protokolu maskovaného v DNS protokolu)	ANO		
	Detekce nestandartní komunikace (P2P sítě, botnety, malware, …)	ANO		
	Detekce na základě aktuálních blacklistů a Threat Intelligence databáze	ANO		
	Možnost exportu informací o detekci minimálně formou emailu a syslog CEF formátu	ANO		
Zaznamenávání plného obsahu provozu, 1 ks				
Požadované parametry	Možnost zaznamenávání komunikace na úrovni plného obsahu paketů na základě uživatelem definovaného filtru	ANO		