Príloha č. 1: Opis predmetu zákazky

Verejný obstarávateľ:
Národná agentúra pre sieťové a elektronické služby

Názov zákazky:
„Nákup LoadBalanceru s doplnkovými bezpečnostnými a firewall funkcionalitami - 13“

Predmet zákazky:
Nákup LoadBalanceru s doplnkovými bezpečnostnými a firewall funkcionalitami pre zabezpečenie ochrany aplikácií pred dátovými kybernetickými hrozbami. V počte 4ks HW zariadení, 4ks VE zariadení a centrálneho manažmentu týchto zariadení, so splnením min. technických parametrov uvedených podrobne v Popise a minimálnych požiadavkách verejného obstarávateľa vymedzených v Podrobnej technickej špecifikácii nižšie.
Nákup ďalšieho doplnkového materiálu podrobne definovaného nižšie, ako aj v excel prílohe, ktorá je neoddeliteľnou súčasťou tohto dokumentu.

Podrobná technická špecifikácia:

N°	Názov parametra	Popis a minimálne požiadavky obstarávateľa
1	Funkčný názov obstarávaného zariadenia	Lokálny dátový load balancer s doplnkovými bezpečnostnými a firewall funkcionalitami pre zabezpečenie ochrany aplikácií pred dátovými kybernetickými hrozbami.
2	Požadované umiestnenie a implementácia zriadenia	Dátové centrum obstarávateľa
3	Konštrukčné prevedenie HW zariadenia a vlastnosti virtuálnych zariadení	Multi tenantná HW platforma, ktorá umožní škálovať celkovú dátovú priepustnosť riešenia v prípade požiadaviek na nárast celkovej priepustnosti spracovania dát, alebo pri implementácii nových funkcionalít pre spracovanie dát. Samostatné hardware zariadenie o veľkosti 1U Rack Jednotiek, v počte procesorov 1x16-core a RAM pamäťou min 64GB, Diskom 480GB M.2 SSD Rack prevedenie, zariadenie osaditeľné do štandardného 19" racku VE platforma s celkovou priepustnosťou min 200 Mbps Centrálny management ako virtualizovaná platforma na centralizovanú správu a orchestráciu zariadení z predmetu zákazky a služieb, doručovanie aplikácií a bezpečnostných služieb
4	Požadované typy portov pre manažment a správu chassis zariadenia:	1 x 1000 Base-T management port 1 x serial console port 1 x USB 3.0 4 x 10G/1G RJ45 Porty 4 x 25G/10G/1G SFP+/SFP28/SFP porty
5	Napájanie zariadenia	Redundantné AC napájanie HW platformy Single DC Power Supply Capacity - 250W
6	Požadované základné aplikačné funkcionality pre 2ks HW zariadení	Lokálny dálový Load balancing, podporujúci funkcionality Intelligent load balancingu, Application health monitoring, Application connection state management, Dynamický routing (BGP, RIP, OSPF, ISIS, BFD), SDN services (VXLAN, NVGRE). Bezpečnostné cybersecurity funkcionality: L7 Aplikačný Firewall AWAF (Advance Web Aplication Firewall) s pridanou IP inteligence a Threat Campaigns ochranou a DNS funkcionalitou (GSLB, DNS, DNSSEC, Advance routing, unlimited RPS)

7	Požadované základné aplikačné funkcionality pre 2ks HW zariadení	Lokálny dálový Load balancing, podporujúci funkcionality Intelligent load balancingu, Application health monitoring, Application connection state management, Dynamický routing (BGP, RIP, OSPF, ISIS, BFD), SDN services (VXLAN, NVGRE). .
8	Požadované základné aplikačné funkcionality pre VE zariadenia	Lokálny dálový Load balancing, podporujúci funkcionality Intelligent load balancingu, Application health monitoring, Application connection state management, Dynamický routing (BGP, RIP, OSPF, ISIS, BFD), SDN services (VXLAN, NVGRE). Bezpečnostné cybersecurity funkcionality: L7 Aplikačný Firewall AWAF (Advance Web Aplication Firewall), Stavový Firewall FW (L4) s funkcionalitou Full proxy architektúry s pridanou funkciou rozkladania záťaže, s DNS funkcionalitou (GSLB, DNS, DNSSEC, Advance routing, unlimited RPS)
9	Požadované základné aplikačné funkcionality pre centrálny management	Centrálny management podporujúci centrálnu správu politík, analýzu aplikácií, podporu predlohy deklaratívnej konfigurácie, riadenie prístupových práv, Záloha a obnova konfiguračných súborov, automatická správa licencií spravovaných zariadení v HW a SW, vytváranie, konfigurácia, nasadzovanie, aktualizácia, oprava , správa certifikátov, Integrácia s Platformami na správu certifikátov tretích strán
10	Podpora vysokej dostupnosti implementovaného riešenia	Možnosť implementácie vysokej dostupnosti v režimoch A/A alebo A/S. Podpora funkčnej redundancie v režime N+1 a N+N.
11	Manažment a administrácia	Požadovaná podpora manažmentu a správy pomocou command-line interface (CLI), webUI a API rozhrania. Podpora štandardného webového prehliadača, HTTPS a SSH , SNMPv2c a SNMPv3, NTP, SYSLOG Podpora intagrácie s RADIUS, LDAP .
12	Minimálne požadované výkony a priepustnosti pre aplikačné spracovanie dátových tokov pre HW zariadenie	L4 priepustnost - min. 40 Gbps L4 HTTP Requests/s – 2,5M L4 connections/s - min. 500K L4 maximum concurent connection - min. 38M L7 priepustnost - min. 30Gbps L7 connections/s(1-1) - min. 200k L7 Request/s(1-inf) – min 600k L7 Requests/s(inf-inf) – min 1,3M SSL Max paralelných spojení min. 4,2 M SSL bulk throughput - min. 20Gbps Maximum SSL TPS (RSA 2K Keys) – 30k SSL/TLS Transakcií za sekundu (ECDSA P-256 Kľúče) - min. 14k SSL/TLS Transakcií za sekundu (ECDHE P-256-RSA-2K) - min. 14k
13	Minimálne požadované výkony a priepustnosti pre aplikačné spracovanie dátových tokov pre VE platformu	L4 priepustnost - min. 200 Mbps L4 HTTP Requests/s – 41K L4 connections/s - min. 25K L7 priepustnost - min. 200Mbps L7 connections/s(1-1) - min. 11k L7 Request/s(1-inf) – min 31k L7 Requests/s(inf-inf) – min 43K SSL Max paralelných spojení – 560K

14	Podpora funkcionalít pre load balancer	Podpora vlastných skriptov pre monitorovanie dostupnosti služieb TCP optimalizácia pre každého pripojeného klienta nezávisle Podpora kopresie a cache SSL Session a SSL Connection mirroring cez viacero ADC zariadení Dynamické ladenie a nastavovanie TCP parametrov Schopnosť pripojenia sa na monitorovacie nástroje tretích strán cez otvorené API Granulárne logovanie všetkých častí komunikácie per aplikácia Schopnosť pracovať aj so 4k kľúčmi Podpora viac ako 19 LB metód Podpora filtrovania paketov Podpora ToS, QoS (marking/preservation/mimic) Ratio based load balancing s CARP persistenciou Podpora pre dynamickú veľkosť záznamov TLS TCP Nagle Auto mode TCP Auto Buffer Tuning Schopnosť skontrolovať pripravenosť systému prímať príkazy pomocou CLI/REST API Schopnosť spustiť testovaci monitor alebo probe z WEB UI Podpora TLS Session Hash and Master Secret Extension (RFC 7627) Podpora for MQTT Protocol Podpora TLS1.3 Podpora full proxy HTTP/2 Vlastný skriptovací jazyk s podporou HTTP/2 Schopnosť konvertovať HTTP/3 požiadavky od klientov na HTTP/2 a HTTP/1 na strane backendu Podpora pre HTTP/3

15	Požiadavky na funkcionalitu - web aplication firewall	Ochrana voči L7 útokom aplikáciách Detekcia a mitigácia L7 DoS Detekcia a mitigácia Brute force Detekcia a mitigácia Heavy URL Detekcia a mitigácia OWASP TOP 10 útokov XML Firewall Ochrana JSON a AJAX volaní Zabezpečenie parametrov zmanipulovaných klientom Ochrana prihlasovacích stránok Detekcia a mitigácia bot-ov a non-human aktivity vrátane tzv. Headless bot-ov Ochrana pred únikom citlivých dát pomocou blokovania a maskovania informácií Autmatická korelácia viacerých útokov do jedného incidentu Podpora pozitívnej a negatívnej bezpečnostnej politiky Podpora detekcie a blokovania útočníkov na základe geolokačnej informácie Podpora skenovania súborov pomocou ICAP Ochrana SMTP a FTP protokolova na aplikačnej vrstve Podpora PCI-DSS, HIPAA, SOX, Basel II Preddefinovaná bezpečnostná politika pre Microsoft Outlook Web Access a Microsoft SharePoint Možnosť aplikovania rozličnej bezpečnostnej politiky na IP addresu, doménové meno a URI Možnosť importovať výsledky z penetračných testov web aplikácií Podpora pre filtrovanie a vynucovanie politiky pre WebSocket komunikáciu Blokovanie IP adries, ktoré opakovane porušujú bezpečnostnú politiku priamo v dedikovaných HW komponentoch Podpora vytvárania unikátneho odtlačku zariadenia/klienta Podpora vrstvených bezpečnostných politík
		Podpora pre vynútenie globálnych bezpečnostných vlastností a nastavení cez všetky bezpečnostné politiky Vyhodnotenie reputácie klienta pri automatickom budovani bezpečnostnej politiky Podpora pre SPA - Single Page Applications Automatická detekcia typov back-end serverov Podpora parsovania JSON parametrov Automatické nastavenie parametrov pre L7 DDoS ochranu Možnosť nevynucovať (iba sa učiť a budovať) bezpečnostnú politiku pre určité doménové mená Možnosť deaktivovať konkrétne signatúry pre URL, HTTP hlavičku a parametre Podpora nasadenia na SPAN/Mirror porte Moznosť šifrovať senzitívne údaje na strane klienta bez nutnosti úpravy chránenej aplikácie Detekcia automatickej modifikácie formulárových dát na strane klienta bez nutnosti úpravy chránenej aplikácie Podpora aplikácií postavených na GraphQL Možnosť mitigácie tzv. False-positives na základe offline ML modelu Detekcia a mitigácia SSRF útokov Možnosť exportovať a kompletnú WAF politiku v JSON formáte Podpora OpenAPI serializáciu pre Array, Style, Explode a parametre Path Aktualizovaná databáza škodlivých IP adries Aktualizované spravodajstvo o aktívnych útočných kampaniach Dekódovanie dátového obsahu pomocou Base64 Korelácia události na základe incident ID v logoch
16	Požadované Network Firewall funkcionality	Inšpekcia SSL Sessions Sieťová DDoS detekcia a ochrana SSH Proxy ochrana Detekcia a ochrana pred zneuťitím TCP portov Sieťový L3-L4 Firewall Network Behavioral DDoS Detekcia a ochrana DDoS ochrana s automatickým nastavením limitov per aplikáciu

17	Požiadavky na zabezpečenie DNS protokolu	DNS Firewall Inšpekcia a validácia DNS Protokolu ACL na základe typu záznamu DNS DNS load balancing ICSA Labs certifikácia Kompletné DNSSEC podpisovanie Centralizovaná DNSSEC key management DNSSEC podpora pre TLD DNSSEC validácia DNS DDoS Detekcia a mitigácia Mitigácia hrozieb pomocou blokovania škodlivých IP adries Hardened DNS kód (nie BIND server) Pokročilá DNS analytika a reporting Komplexné DNS služby (Authoritative DNS, DNS Caching, DNS Forwarding…) Podpora pre DNS cez HTTPS
18	Funkčné požiadavky na Autentifikáciu a Autorizáciu	Riešenie pre realizáciu vzdialeného prístupu a zabezpečenia prístupu k aplikáciam pomocou prístupových údajov Podpora minimálne pre AAA protokoly LDAP, RADIUS, TACACS, MS AD Podpora authentifikačných metód: Form, Certificate, Kerberos SSO, SecurID, Basic, RSA token, Smart card, N-factor, External API Možnosť konfigurácie jednotnej login stránky pre viacero aplikácií a následného SSO prístupu do týchto aplikácií Podpora pre externú login page Dynamické riadenie prístupu do aplikácií na základe informácie z AAA Možnosť definovať časti aplikácie a riadenie prístupu pomocou URL (L7 ACL) Podpora pre MS ADFS Proxy Integration Protocol (PIP) Podpora SAML 2.0 Podpora pre OAuth 2.0 Podpora pre JSON Web Token (JWT) with OAuth Podpora pre MFA (Multi Factor Authentication) Podpora pre dodatočné overenie pomocou MFA, napr. pri prístupe k senzitívnej časti aplikácie tzv. Step-up Authentication Podpora pre FIDO U2F via API (YubiKey) Podpora definovania rozhrani aplikácie (API) pomocou importovania OpenAPI súboru a následného aplikovania prístupovej politiky
19	Požiadavky na L3 funkcionalitu	Popdora Dynamic routing protocols BFD, BGP, IS-IS, OSPFv2, OSPFv3, RIPv1/RIPv2, RIPng
20	HW/VE záruka a servis dodaných komponentov	Záruka a servis na dodané HW/VE komponenty na dobu 5 **rokov** v rámci ceny za dodané riešenie. Zabezpečenie servisnej podpory v režime 24x7 na dobu 5 **rokov** v rámci ceny za dodané riešenie.
21	Minimálne požadovaná zostava dodaného riešenia:	**4ks** hardvérovej platformy so splnením min. technických parametrov uvedených vyššie **4ks** VE platformy so splnením min. technických parametrov uvedených vyššie **1ks** centrálneho managementu nad požadovanou zostavou
22	Doplnkový materiál	**8ks** SFP+ 10GBASE-SR Transceiver (Short Range, 300 m, Field Upgrade) kompatibilné s HW zostavou
23		**8ks** SFP+ SR Transceivery pre Cisco Nexus9k

Lehota dodania:
Najneskôr do 4 týždňov od nadobudnutia účinnosti Kúpnej zmluvy.

Komplexnosť:
Uchádzač je povinný predložiť ponuku na celý predmet zákazky, vrátane všetkých súvisiacich nákladov.