Příloha č. 1 – Formulář nabídky

Sekce I – Identifikační údaje

|  |
| --- |
| Identifikace veřejné zakázky |
| Next Generation FireWall  pro zadání veřejné zakázky na dodávky  v otevřeném řízení  v nadlimitním režimu |

|  |  |
| --- | --- |
| Identifikace účastníka zadávacího řízení | |
| Název / Obchodní firma / Jméno: |  |
| Odkaz na obchodní rejstřík či jinou obdobnou evidenci: |  |
| IČO (je-li přiděleno): |  |
| Adresa sídla: |  |
| Osoba oprávněná jednat za účastníka zadávacího řízení: |  |
| e-mail: |  |
| ID datové schránky: |  |
| Kontaktní osoba pro tuto veřejnou zakázku: |  |
| e-mail: |  |

Sekce II - Specifikace předmětu plnění

Předmětem plnění veřejné zakázky jsou **4 kusy „Firewall nové generace“**, jehož parametry, požadavky na obecné funkce, požadavky na management funkce, požadavky na síťové funkce a požadavky na bezpečnostní funkce jsou uvedeny níže. Účastník nabídne pouze zařízení, které splňuje všechny požadované parametry a uvedené požadavky na funkce. Přičemž u požadavků na funkce účastník explicitně uvede, že nabízené zařízení požadavek splňuje, kde je to relevantní, bude specifikováno, jakým způsobem je požadavek splněn.

|  |  |
| --- | --- |
| **FireWall nové generace – výkonnové parametry** | **Požadované hodnoty parametrů** |
| min. propustnost firewall (IPv4, udp provoz paket o velikosti 512 B) | 163 Gbps |
| max. vložené zpoždění firewallu | 4 μs |
| min. počet nových spojení za sekundu | 720 000 |
| min. počet současně navázaných TCP spojení | 16 000 000 |
| min. propustnost fuknce IPSEC VPN (při použití AES256, SHA256) | 55 Gbps |
| min. propustnost funkce SSL VPN | 10 Gbps |
| min. propustnost funkce SSL inspekce | 16 Gbps |
| min. propustnost funkce IPS (Intrusion Protection Systém, enterprise mix) | 26 Gbps |
| min. propustnost funkce NGFW (stavový firewall + IPS, rozpoznávání aplikací na L7) | 22 Gbps |
| min. propustnost ochrany proti hrozbám (stavový firewall + IPS, rozpoznávání aplikací na L7, ochrana proti škodlivému kódu) | 20 Gbps |
| min. propustnost funkce klasifikace aplikací na L7 (pro protokol http) | 74 Gbps |
| min. počet metalických sítových rozhraní GE RJ45 | 16 |
| min. počet optických sítových rozhraní GE SFP | 8 |
| min. počet optických sítových rozhraní 25GE SFP28 | 4 |
| min. počet optických sítových rozhraní 10GE SFP+ | 4 |
| konzolový port (sériová linka) | 1 |
| USB port (bootstrap konfigurace, připojení externího LTE modemu) | 1 |
| min. počet virtuálních kontextů | 10 |
| provedení | Rack mount 1RU, HW appliance |
| redundantní napájení (min 2 vestavěné zdroje 230 V) | ano |

|  |  |
| --- | --- |
| **Požadavky na obecné funkce** | **splňuje** |
| Konsolidované bezpečnostní řešení obecně značené jako firewall nové generace (next generation firewall, NGFW) |  |
| Grafické konfigurační rozhraní (např. webový prohlížeč) a příkazový řádek bez omezení na počet administrátorů |  |
| Podpora virtuálních kontextů v požadovaném počtu, kontexty mohou nezávisle pracovat v NAT/router nebo transparentním režimu, je možné vytvářet virtuální propoje mezi jednotlivými virtuálními kontexty bez nutnosti použití fyzického propoje |  |
| Podpora stavového firewallingu pro IPv4 i IPv6, podpora nat 64/46, plnohodnotná podpora IPv6 |  |
| Nasazení NGFW ve všech z následujících režimů (kombinace možné pomocí použití různých režimů pro různé virtuální kontexty): L2 bridge režim (inline), virtual wire (L2), L3 router/NAT režim (inline), explicitní proxy (inline/out of path), transparentní proxy (inline), reverzní proxy s loadbalancingem a healtcheck funkcí pro fyzické servery |  |
| Plnohodnotná správy z lokálního management rozhraní celého HA clusteru (správa celého clusteru probíhá z jednoho místa, konfigurace se automaticky sdílí), podpora možnosti centrální správy |  |
| Obousměrná integrace (min. ve smyslu sdílení informací o odhalených hrozbách a provozně/telemetrický informací) nabízeného NGFW s dalšími instalovanými bezpečnostní prvky (nástroj pro sběr a vyhodnocování logů, nástroj pro centrální správu) |  |
| Podpora řežimu nasazení v režimu WCCP (WCCP v2) |  |
| Podpora konfiguračních PAC souborů pro režim nasazení explicitní proxy |  |
| Podpora ICAP rozhraní pro obousměrnou integraci s externími inspekčními servery dle RFC 3507 |  |
| Podpora tunelování provozu pomocí technologie GRE |  |
| Podopra automaticky aktivovaného bypass režimu v případě přetížení systému a jeho inspekčních funkcí |  |
|  |  |
| **Požadavky na management funkce** | **splňuje** |
| Možnost využít stávající centrální management řešení pro hardwarové appliance i virtuální kontexty, případně dodání nového centrálního mangementu pro 2 hardwarové appliance a 20 virtuálních kontextů |  |
| Podpora centálního sběru logů o kapacitě 1GB dat/den s možností licenčního rozšíření |  |
|  |  |
| **Požadavky na sítové funkce** | **splňuje** |
| Podpora VLAN dle IEE 802.1Q |  |
| Podpora agregovaných interface (LACP) IEE802.3ad |  |
| Podpora redundatních rozhraní |  |
| Podpora looback rozhraní |  |
| Možnost vytvořit switch nad několika fyzickými porty |  |
| Možnost práce se zónamy (logická skupina sítových rozhraní zastoupená objektem v konfiguraci) |  |
| Podpra vytvoření tzv. wire pair pro L2 transparetní inspekci |  |
| Podpora VXLAN (enkapsulace L2 sítových rámců do L3 IP paketů za účelem transportu do vzdáléné sítě) |  |
| Podpora dynamických směrovacích protokolů min v rozsahu: RIP, OSPF, BGP, IS-IS; podpora BFD |  |
| Podpora LLDP |  |
| Podpra funkce SD-WAN minimálně v rozsahu: režim vytvoření overlay a underlay virtuálních sítových rozhraní zahrnující fyzické propoje, IPSEC tunely či jiná rozhraní s možností definice pravidel pro řízení směrování, strategie využívání jednotlivých linek současně a monitorování stavu jednotlivých linek |  |
| SD-WAN pravidla musí jako rozhodovací kritérium brát v potaz uživatele, zdroj komunikace, cíl komunikace, stav undrlay/overlay linky, definovanou šířku pásma a prioritu komunikace |  |
| SD-WAN funkce proměřuje stav jednotlivých overlay a underlay link z koncového bodu (pobočkový NGFW), podpora pasivního měření (dle stavu komunikace) aktivní měření (min. ping, tcp-echo, udp-echo, http, twamp, dns, tcp-connect); možnost konfigurace přechodu z pasivního měření na aktivní v případě chybějící komunikace |  |
| Podpora výpočtu MOS (Mean Opinion Score) a jeho logování do prvozního logu |  |
| Funkce SD-Wan podporuje minimálně tyto strategie: manuální nastavení, strategie linky s nejvyšší kvalitou spojení, strategie linky s nejnížší cenou spojení, strategie maximalizace šířky pásma |  |
| Funkce SD-WAN podporuje automatické proměřování šířky pásma u připojení s dynamickými parametry |  |
| Možnost využívat SDN konketory pro SD-WAN pravidla |  |
| Podpora funkce vzdáleného připojení uživatelů v režimu ZTNA (zero trust network access), moderní náhrada klasické VPN |  |
| Ověřování identity uživatelů (možnost napojení na MS Active Directory, LDAP, Radius, Kerberos), práce s identitou uživatele v bezpečnostní politice firewallu v režimu tzv. Single Sign On |  |
| Podpora lokální databáze a vzdálené databáze (radius, ldap, tacacs+, saml, kerberos) pro ověřování uživatelů |  |
| Ověřování uživatelů pomocí SSO funkcionality pomocí Radius Single Sign On a AD pollingu |  |
| Funkce QoS a traffic shaping min. ve variantě policing a queuing, aplikace politiky globálně nebo pomocí pravidel, podpora DSCP v pravidlech |  |
| Podpora funkcí VPN brány ‐ IPSec VPN (dle platných standardů pro možnost propojení se zařízeními třetích stran); -  SSL VPN pro klientský přístup s tunelovacím režimem včetně klienta pro osobní počítače i mobilní platformy, portálový režim pro bezklientský přístup; ZTNA pro vzdálené bezpečné připojení klientů realizované v moderní podobě vzdáleného přístupu |  |
| Podpora funkce SSL inspekce (MITM) včetně podpory TLS 1.3 |  |
| Integrovaná funkce load balancingu (reverzní proxy) s podporou základní algorimtů pro rozklad zátěže (round robing, váhování, nejkratší odezva, nejmenší počet aktivních spojení) s detekcí stavu reálných serverů na pozadí, podpora funkce ssl offloading a ssl inspekce pro rozkládaný provoz |  |

|  |  |
| --- | --- |
|  |  |
| **Požadavky na bezpečnostní funkce** | **splňuje** |
| Antivirový engine musí být vybaven lokální databází vzorků škodlivého kódu a AI/ML enginem pro identifikaci podezřelých či neznámých vzorků |  |
| Funkce ochrany před škodlivým kódem s databází vzorků škodlivého kódu pravidelně aktualizovanou výrobcem, podpora rozpoznávání škodlivého kódu určeného pro mobilní zařízení (tzv. mobile malware), detekce komunikace do sítí typu botnet (minimálně na základě IP adres a domén), podpora ochrany před rychle se šířícími kampaněmi škodlivého kódu (tzv. virus outbreak), podpora sanitarizace aktivního obsahu běžných kancelářských dokumentů (odstranění např. skriptů či maker z dokumentu, extrakce obsahu dokumentu do neškodné podoby); podpora napojení na sandboxovací funkce včetně funkce akceptace lokálních signaturových databází generovaných sandboxem, vše bez nutnosti instalace pluginů do prohlížeče. Sandboxovací funkce musí být součástí nabídky (možno jako službu výrobce poskytovanou z cloud prostředí). |  |
| Funkce rozpoznávání populárních sítových aplikací na základě jejich charakteristiky provozu na aplikační vrstvě, podpora min. 5000 aplikací, pravidelná aktualizace signatur aplikací výrobcem, aplikace rozděleny do přehledných kategorií, možnost vytvářet signatury pro vlastní aplikace |  |
| Možnost definice zakázaných slov pro vyhledávání na internetu |  |
| Funkce kategorizace multimediálního videoobsahu dle channel ID, možnost blokovat, monitorovat či povolit daný druh video obsahu. |  |
| Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze, vynikající pokrytí českého internetu; požadované akce – povolení stránky, logování stránky, brouzdání s proklikem, nutnost autentizace uživatele pro určitou kategorii, možnost definice časových kvót pro uživatele a kategorie webu |  |
| Funkce ochrany před sítovými útoky (IPS) s výrobcem aktualizovanou databází, přednastavenými profily, možností definovat různé profily na různý druh komunikace, možnost vytvářet vlastní signatury, integrovaný anomální filtr a mechanismus kontroly validity vybraných protokolů |  |
| Možnost blokovat sítový provoz na základě URL, kategorie webové stránky, IP adresy (rozsahu), GeoIP databáze, data a času |  |
| Podpora dvoufaktorové autentizace pomocí HW nebo mobilních OTP tokenů pro uživatele i administrátory |  |
| Analýza a zabezpeční DNS dotazů (ochrana před DNS posoningem), filtrování DNS dotazů na základě kategorizace |  |
| Možnost filtrovat Java applety, ActiveX prvky, Cookie soubory ve webovém provozu |  |
| Integrovaná funkce filtrování přenášených souborů pro protokoly CIFS, FTP, HTTP, IMAP, MAPI, POP3, SMTP a SSH; možnost konfigurace různého chování pro příchozí a odchozí směr, možnost práce s heslem chráněnými soubory, možnost logovat a blokovat provoz |  |
| Integrovaný web aplikační firewall pro ochranu publikovaných webových služeb proti sítovým útokům, možnost konfigurace ochrany proti útokům typu SQL injection, generické techniky, trojské koně, únik informací, známé zranitelnosti). |  |
| Ochrana VoIP komunikace min. pro protokoly SIP a SCCP s podporou NAT46 a NAT64 SIP ALG, inspekce SIP komunikace, SIP pinholes, SIP over TLS, kontrola MSRP provozu |  |
| Obousměrná (výrobcem podporovaná) intergrace s nabízenou WAF platformou. Včetně vizualizace stavu WAF v konfiguračním rozhraní NGFW |  |
| Obousměrná integrace s nabízenou platformou pro ochranu pracovních stanic (EPP), propojení formou konektoru, propojení musí být podporováno výrobcem, možnost sdílení konfiguračních objektů a provozních informací |  |

Sekce III – Prohlášení o nabídkové ceně

Prohlašuji, že nabízená zařízení odpovídají požadovaným parametrům uvedeným ve Formuláři nabídky v sekci II tohoto Formuláře nabídky a že nabídková cena je konečná zahrnující veškeré náklady na kompletní a kvalitní realizaci předmětu plnění veřejné zakázky včetně montáže, zapojení, konfigurace, migrace pravidel a demontáž původních zařízení a včetně požadovaného režimu záručního servisu po dobu 5 let a dalších souvisejících výkonů, které nejsou v nabídce výslovně uvedeny. Dále jsou v ceně zahrnuty náklady na odvoz nepotřebného obalového materiálu.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Specifikace nabízeného zařízení | | | | Výrobce |
|  | | | |  |
| **Počet kusů: 4** | | | | |
|  | | | | |
|  |  | Cena za 4 ks | DPH | Cena s DPH |
| **Nabídková cena** | |  |  |  |

…………………………………….………………………………………………………………

Podpis osoby oprávněné jednat za účastníka zadávacího řízení