Príloha č. 1 súťažných podkladov Dodanie hardvéru Web Application Firewall a poskytnutie s tým spojených služieb

Podrobný opis predmetu zákazky

* + - 1. Predmetom zákazky sú nasledujúce tovary a služby:
  1. Dodanie hardvéru – zariadení Web Application Firewall s príslušenstvom. Podrobný opis a požadovaný počet zariadení je uvedený v bode 2.1 v tabuľke č. 1.
  2. Servisná podpora výrobcu Web Application Firewall a licencie pre zariadenia na obdobie šiestich rokov. Podrobný opis služby je uvedený v bode 2.2 v tabuľke č. 2.
  3. Poskytnutie implementácie Web Application Firewall (inštalácia, migrácia, integrácia a dodanie dokumentácie) pre dodané zariadenia. Podrobný opis implementácie je uvedený v bode 2.3 v tabuľke č. 3.
  4. Zriadenie a poskytovanie/prevádzka cloudovej služby. Podrobný opis služby je uvedený v bode 2.4 v tabuľke č. 4.
  5. Poskytovanie servisnej podpory uchádzača pre dodané zariadenia s príslušenstvom a správy pre cloudovú službu. Podrobný opis služby je uvedený v bode 2.5 v tabuľke č. 5.
  6. Poskytovanie konzultačných a implementačných služieb pre dodané zariadenia s príslušenstvom a cloudovú službu, uvedené v bode 2.6 v tabuľke č. 6.
  7. Verejný obstarávateľ požaduje dodanie tovaru a poskytovanie služieb v dvoch miestach plnenia:

hlavné technologické pracovisko (Národná banka Slovenska, ústredie, I. Karvaša 1, 81325 Bratislava); ďalej len „HTP“

záložné technologické pracovisko (Dátové centrum Datacube, Kopčianska 92/D, 851 01 Bratislava); ďalej len „ZTP“

* + - 1. Špecifikácia vecných požiadaviek na hardvér a prevádzku Web Application Firewall a poskytnutie s tým spojených služieb.
  1. **Vecné požiadavky na hardvér**

Verejný obstarávateľ požaduje dodanie hardvéru: zariadení a príslušenstva; (ďalej aj ako „nový HW“). Označenie, popis a požadovaný počet nového HW je uvedený v nasledujúcej tabuľke č. 1.

**Tabuľka č. 1** – Označenie, popis a požadovaný počet/hodnota

|  |  |  |
| --- | --- | --- |
| **Položka** | **Požadované**  **minimálne technické a funkčné parametre** | **Požadovaná hodnota** |
|  | | | |
| **Zariadenia** | | | |
| **1.** | **Web Aplication Firewall** | **3 ks** |
| **Technické parametre zariadení** | | | |
| 1.1 | Chassis Height (Rack Units) | 1U |
| 1.2 | 10G/1G RJ45 Ports | 4 ks |
| 1.3 | 25G/10G/1G SFP+/SFP28/SFP ports | 4 ks |
| 1.4 | Single DC Power Supply Capacity | 250 W |
| 1.5 | Redundantne AC Power | Áno |
| 1.6 | Number of Processors | 1x8-core |
| 1.7 | Memory | 32 GB |
| 1.8 | L4 Throughput | 20 Gbps |
| 1.9 | L4 HTTP Requests per Second | 850K |
| 1.10 | L4 Connections per Second | 170K |
| 1.11 | L4 Max Concurrent Connections (1) | 19M |
| 1.12 | L7 Throughput | 13 Gbps |
| 1.13 | L7 Connections per Second (1-1) | 70K |
| 1.14 | L7 Requests per Second (1-inf) | 200K |
| 1.15 | L7 Requests per Second (inf-inf) | 475K |
| 1.16 | Maximum SSL Concurrent Connections | 2M |
| **Požadované parametre APM** | | | |
| 1.17 | Max Concurrent SSL VPN Users | 150 |
| 1.18 | Max. Access Sessions | 5K |
| **Popis funkcionalít zariadení** | | | |
| **Loadbalancing** | | | |
| 1.19 | Podpora vlastných skriptov pre monitorovanie dostupnosti služieb | Áno |
| 1.20 | TCP optimalizácia pre každého pripojeného klienta nezávisle | Áno |
| 1.21 | Podpora kopresie a cache | Áno |
| 1.22 | SSL Session a SSL Connection mirroring cez viacero ADC zariadení | Áno |
| 1.23 | Dynamické ladenie a nastavovanie TCP parametrov | Áno |
| 1.24 | Schopnosť pripojenia sa na monitorovacie nástroje tretích strán cez otvorené API | Áno |
| 1.25 | Granulárne logovanie všetkých častí komunikácie per aplikácia | Áno |
| 1.26 | Schopnosť pracovať aj so 4k kľúčmi | Áno |
| 1.27 | Podpora viac ako 19 LB metód | Áno |
| 1.28 | Podpora filtrovania paketov | Áno |
| 1.29 | Podpora ToS, QoS (marking/preservation/mimic) | Áno |
| 1.30 | Ratio based load balancing s CARP persistenciou | Áno |
| 1.31 | Podpora pre dynamickú veľkosť záznamov TLS | Áno |
| 1.32 | TCP Nagle Auto mode | Áno |
| 1.33 | TCP Auto Buffer Tuning | Áno |
| 1.34 | Schopnosť skontrolovať pripravenosť systému prímať príkazy pomocou CLI/REST API | Áno |
| 1.35 | Schopnosť spustiť testovací monitor alebo probe z WEB UI | Áno |
| 1.36 | Podpora TLS Session Hash and Master Secret Extension (RFC 7627) | Áno |
| 1.37 | Podpora for MQTT Protocol | Áno |
| 1.38 | Podpora TLS1.3 | Áno |
| 1.39 | Podpora full proxy HTTP/2 | Áno |
| 1.40 | Vlastný skriptovací jazyk s podporou HTTP/2 | Áno |
| 1.41 | Schopnosť konvertovať HTTP/3 požiadavky od klientov na HTTP/2 a HTTP/1 na strane backendu | Áno |
| 1.42 | Podpora pre HTTP/3 | Áno |
| 1.43 | Podpora TLS1.3 | Áno |
| **Webový aplikačný firewall** | | | |
| 1.44 | Ochrana voči L7 útokom aplikáciách | Áno |
| 1.45 | Detekcia a mitigácia L7 DoS | Áno |
| 1.46 | Detekcia a mitigácia Brute force | Áno |
| 1.47 | Detekcia a mitigácia Heavy URL | Áno |
| 1.48 | Detekcia a mitigácia OWASP TOP 10 útokov | Áno |
| 1.49 | XML Firewall | Áno |
| 1.50 | Ochrana JSON a AJAX volaní | Áno |
| 1.51 | Zabezpečenie parametrov zmanipulovaných klientom | Áno |
| 1.52 | Validácia prihlasovacích údajov a aplikačného toku | Áno |
| 1.53 | Detekcia a mitigácia bot-ov a non-human aktivity vrátane tzv. Headless bot-ov | Áno |
| 1.54 | Ochrana pred únikom citlivých dát pomocou blokovania a maskovania informácií | Áno |
| 1.55 | Automatická korelácia viacerých útokov do jedného incidentu | Áno |
| 1.56 | Podpora pozitívnej a negatívnej bezpečnostnej politiky | Áno |
| 1.57 | Podpora detekcie a blokovania útočníkov na základe geolokačnej informácie | Áno |
| 1.58 | Podpora skenovania súborov pomocou ICAP | Áno |
| 1.59 | Ochrana SMTP a FTP protokolov na aplikačnej vrstve | Áno |
| 1.60 | Podpora PCI-DSS, HIPAA, SOX, Basel II | Áno |
| 1.61 | Preddefinovaná bezpečnostná politika pre Microsoft Outlook Web Access a Microsoft SharePoint | Áno |
| 1.62 | Možnosť aplikovania rozličnej bezpečnostnej politiky na IP adresu, doménové meno a URI | Áno |
| 1.63 | Možnosť importovať výsledky z penetračných testov web aplikácií | Áno |
| 1.64 | Podpora pre filtrovanie a vynucovanie politiky pre WebSocket komunikáciu | Áno |
| 1.65 | Blokovanie IP adries, ktoré opakovane porušujú bezpečnostnú politiku priamo v dedikovaných HW komponentoch | Áno |
| 1.66 | Podpora vytvárania unikátneho odtlačku zariadenia/klienta | Áno |
| 1.67 | Podpora vrstvených bezpečnostných politík | Áno |
| 1.68 | Podpora pre vynútenie globálnych bezpečnostných vlastností a nastavení cez všetky bezpečnostné politiky | Áno |
| 1.69 | Vyhodnotenie reputácie klienta pri automatickom budovaní bezpečnostnej politiky | Áno |
| 1.70 | Podpora pre SPA - Single Page Applications | Áno |
| 1.71 | Automatická detekcia typov back-end serverov | Áno |
| 1.72 | Podpora parsovania JSON parametrov | Áno |
| 1.73 | Automatické nastavenie parametrov pre L7 DDoS ochranu | Áno |
| 1.74 | Možnosť nevynucovať (iba sa učiť a budovať) bezpečnostnú politiku pre určité doménové mená | Áno |
| 1.75 | Možnosť deaktivovať konkrétne signatúry pre URL, HTTP hlavičku a parametre | Áno |
| 1.76 | Podpora nasadenia na SPAN/Mirror porte | Áno |
| 1.77 | Možnosť šifrovať senzitívne údaje na strane klienta bez nutnosti úpravy chránenej aplikácie | Áno |
| 1.78 | Detekcia automatickej modifikácie formulárových dát na strane klienta bez nutnosti úpravy chránenej aplikácie | Áno |
| 1.79 | Podpora aplikácií postavených na GraphQL | Áno |
| 1.80 | Možnosť mitigácie tzv. False-positives na základe offline ML modelu | Áno |
| 1.81 | Detekcia a mitigácia SSRF útokov | Áno |
| 1.82 | Možnosť exportovať a kompletnú WAF politiku v JSON formáte | Áno |
| 1.83 | Podpora OpenAPI serializáciu pre Array, Style, Explode a parametre Path | Áno |
| **APM** | | | |
| 1.84 | Podpora Radius autentifikacie | Áno |
| 1.85 | Podpora pre SSO Federačné služby cez viaceré domény | Áno |
| 1.86 | Podpora pre Kerberos ticketing | Áno |
| 1.87 | Podpora pre SAML 2.0 | Áno |
| 1.88 | SSL VPN Vzdialený prístup | Áno |
| 1.89 | Komplexné bezpečnostné a systémové kontroly na klientovi | Áno |
| 1.90 | Podpora pre aplikačné tunely | Áno |
| 1.91 | Pokročilý vizuálny editor na definovanie bezpečnostnej politiky (VPE) | Áno |
| 1.92 | Dynamická kontrola prístupu | Áno |
| 1.93 | Dynamické tzv. Webtopy na základe identity používateľa | Áno |
| 1.94 | Podpora URL filteringu | Áno |
| 1.95 | Prístup cez SSL Portal, Aplikačný tunel a sieťový prístup | Áno |
| 1.96 | Granulárne vynucovanie bezpečnostnej politiky | Áno |
| 1.97 | L7 prístupové politiky (ACL) | Áno |
| 1.98 | Chránená pracovná plocha | Áno |
| 1.99 | Podpora externej stránky pre logon | Áno |
| 1.100 | Široká podpora natívnych klientov na platformách (Win, Mac, Linux, iOS, Android) | Áno |
| 1.101 | Podporované autentifikačné metódy: form, certificate, Kerberos SSO, SecurID, basic, RSA token, smart card, N-factor | Áno |
| 1.102 | Podpora OAuth 2.0 | Áno |
| 1.103 | Podpora ADFS Proxy Integration Protocol (PIP) | Áno |
| 1.104 | Podpora JSON Web Token (JWT) s OAuth | Áno |
| 1.105 | Podpora importu Swagger files v prípade použitia API Protection | Áno |
| 1.106 | podpora pre Microsoft Conditional Access rules (Azure AD) | Áno |
| 1.107 | podpora Dynamic Split Tunneling (Zoom, Office 365) | Áno |
| 1.108 | Podpora pre OIDC protocol for Duo MFA | Áno |
| 1.109 | Podpora pre Microsoft Identity Platform 2.0 | Áno |
| **Príslušenstvo** | | | |
| Transceivers | | | |
| **2.** | **SFP+ 10Gbps** – transceivers do nového HW | **12 ks** |

* 1. **Vecné požiadavky na Servisnú podporu výrobcu Web Application Firewall a licencie**

Verejný obstarávateľ požaduje dodanie servisnej podpory výrobcu a všetkých potrebných licencií pre dodaný nový HW. Označenie, popis a požadovaný počet produktov je uvedený v nasledujúcej tabuľke č. 2.

**Tabuľka č. 2** Označenie a popis servisnej podpory výrobcu Web Application Firewall a licencií

|  |  |  |  |
| --- | --- | --- | --- |
| **Položka** | **Označenie** | **Popis** | **Počet** |
| **3.** | L1-L3 Podpora  výrobcu zariadení Web Application Firewall | L1-L3 Podpora  Prístup k technickej podpore je zabezpečený prostredníctvom telefonickej, emailovej alebo webovej platformy.  Zákaznícka podpora dostupná počas pracovných hodín 10 x 5 a poskytuje pomoc s problémami, konfiguráciou a prevádzkou.  Prístup pravidelným aktualizáciám softvéru a bezpečnostných záplat.  Prístup k technickej dokumentácii, príručkám a databázam znalostí. | pre 3 kusy zariadení s podporou výrobcu na 72 mesiacov |
| **4.** | NBD RMA  výrobcu zariadení Web Application Firewall | NBD RMA  Služba, ktorá zaručuje rýchlu a efektívnu výmenu hardvéru, alebo chybných komponentov v prípade poruchy nasledujúci pracovný deň. | pre 3 kusy zariadení s podporou výrobcu na 72 mesiacov |
| **5.** | Licencia WAF  výrobcu zariadení Web Application Firewall | Licencia WAF  Licencia poskytuje aktualizácie pre pokročilé zabezpečenie pre webové aplikácie a pomáha chrániť pred rôznymi hrozbami, ako sú útoky typu SQL injection, cross-site scripting (XSS) a iné formy kybernetických útokov. | pre 3 kusy zariadení s podporou výrobcu na 72 mesiacov |
| **6.** | Licencia pre Správu prístupu – APM  výrobcu zariadení Web Application Firewall | Licencia pre Správu prístupu  Ktorá umožňuje definovať politiky prístupu na základe rôznych faktorov, ako sú identita používateľa, umiestnenie, zariadenie a bezpečnostný stav.  Poskytuje funkciu SSO, ktorá používateľom umožňuje prihlásiť sa raz a získať prístup k viacerým aplikáciám bez nutnosti opätovného zadávania poverení.  Podporuje viacero autentifikačných metód, vrátane základnej autentifikácie, certifikátov, OTP (one-time password), a integrácie s RADIUS a LDAP.  Poskytuje funkcionalitu SSL VPN, ktorá zabezpečuje šifrovaný prístup k interným aplikáciám a zdrojom cez internet.  Záznam a analýza prístupových pokusov a autentifikačných aktivít, čo umožňuje sledovanie bezpečnostných incidentov a dodržiavanie predpisov.  Integrácia s rôznymi identifikačnými a autentifikačnými systémami, čím sa zabezpečuje bezproblémové riadenie prístupu. | pre 3 kusy zariadení s podporou výrobcu na 72 mesiacov |

* 1. **Vecné požiadavky na Implementáciu <7.>**

Verejný obstarávateľ požaduje k dodanému novému HW poskytnutie implementácie: inštaláciu, migráciu, integráciu nového HW a dodanie dokumentácie. Označenie, popis implementácie je uvedený v nasledujúcej tabuľke č. 3.

**Tabuľka č. 3** – Označenie a popis poskytnutia implementácie

|  |  |  |
| --- | --- | --- |
| **Položka** | **Označenie** | **Popis** |
| 7.1 | Inštalácia zariadení Web Application Firewall (nový HW) | Vybalenie, skompletizovanie, montáž do rackov verejného obstarávateľa, inicializácia HW vrátane updatu FW, vytvorenie HW klastra, základná konfigurácia po prvom štarte, pripojenie do internetovej DMZ LAN, likvidácia odpadu. |
| 7.2 | Migrácia konfigurácií zo súčasnej konfigurácie na nový HW - konfigurácií pre web aplikácie | Vytvorenie vysoko dostupného klastra v HTP z 2 kusov nového HW. 1 kus nového HW v ZTP. Migrácia celej konfigurácie (cca 60 webových aplikácií) zo súčasne prevádzkovaných WAF F5 BIP IP i2800 na nový HW. |
| 7.3 | Integrácia | Integrácia dodaného nového HW s existujúcim managementom **WAF BIG – IQ** prevádzkovaným verejným obstarávateľom |
| 7.4 | Dodávka dokumentácie | Dodanie dokumentácie k vykonaným implementačným (inštalačným, migračným a integračným) službám v rozsahu popisu riešenia a súpisu všetkých nastavení a konfigurácií vykonaných uchádzačom. |

* 1. **Vecné požiadavky na cloudovú službu**

Verejný obstarávateľ požaduje zriadenie a poskytovanie cloudovej služby. Označenie, popis a požadované trvanie sú uvedené v nasledujúcej tabuľke č. 4.

**Tabuľka č. 4** – Označenie a popis požadovanej cloudovej služby

|  |  |  |  |
| --- | --- | --- | --- |
| **Položka** | **Označenie** | **Popis** | **Trvanie** |
| **8.** | **Cloudová služba** s dostupnosťou služby 99,99 % | Zriadenie a zabezpečovanie vysokej dostupnosti dodaných Web Application Firewallov formou poskytovania dynamických DNS záznamov klientom pripájajúcim sa z prostredia Internetu. Sledovanie a vyhodnocovanie stavu dodaných Web Application Firewallov kontrolou dostupnosti HTTP/HTTPS služby na definovanom porte každých 10 sekúnd, alebo častejšie. Smerovanie klientov pomocou DNS na primárne pracovisko objednávateľa, pri výpadku zariadenia na primárnom pracovisku zabezpečiť automatické presmerovanie klientov na záložné pracovisko. Po opätovnom sprevádzkovaní zariadenia na primárnom pracovisku zabezpečiť automatické spätné presmerovanie klientov na primárne pracovisko (failover / failback). **Súčasne využívaná služba je založená na cloudovej službe MICROSOFT.** | 72 mesiacov |

Požadovaný spôsob fakturácie: štvrťročne po poskytnutí služby.

* 1. **Vecné požiadavky na servisnú podporu uchádzača <9.>**

Verejný obstarávateľ požaduje poskytovanie servisnej podpory pre Web Application Firewall a správu cloudovej služby. Označenie, popis a požadované trvanie poskytovania služieb sú uvedené v nasledujúcej tabuľke č. 5.

**Tabuľka č. 5** – Označenie, popis a požadované trvanie poskytovania servisnej podpory pre nový HW a správu cloudovej služby

|  |  |  |  |
| --- | --- | --- | --- |
| **Položka** | **Označenie** | **Popis** | **Trvanie** |
| 9.1 | Odstraňovanie HW a SW porúch | Odstránenie HW a SW porúch pre všetky dodané zariadenia a ich komponenty, nahlasovanie porúch v pracovnom čase (7.30 h až 16.30 h v pracovných dňoch v Slovenskej republike), odstránenie poruchy najneskôr nasledujúci pracovný deň od nahlásenia, v pracovnom čase. | 72 mesiacov |
| 9.2 | Profylaktika | Sledovanie vydávania nových verzií FW a SW pre všetky dodané zariadenia a ich komponenty, odporúčanie nasadzovania aktualizácií, nasadzovanie aktualizácií po vyžiadaní objednávateľom. | 72 mesiacov |
| 9.3 | Aktívny monitoring | Pravidelné vyhodnocovanie udalostí týkajúcich sa prevádzky samotných zariadení, ako i web aplikácií, minimálne na dennej báze. Predkladanie návrhov na úpravu bezpečnostných nastavení, resp. politík, ktoré budú eliminovať zistené riziká a nedostatky. | 72 mesiacov |
| 9.4 | Odstraňovanie prevádzkových incidentov | Riešenie incidentov a problémov súvisiacich s prevádzkou Web Application Firewallov a cloudovej služby, nahlasovanie incidentov v pracovnom čase, vyriešenie incidentu:  a) najneskôr do 4 hodín od nahlásenia v prípade, že v dôsledku incidentu či poruchy dôjde k úplnej nedostupnosti služby,  b) najneskôr nasledujúci pracovný deň od nahlásenia, v pracovnom čase, v prípade, že v dôsledku incidentu či poruchy dôjde k zníženiu kvality poskytovanej služby (napr. nárast web aplikačných odoziev), avšak bez dopadu na dostupnosť služby. | 72 mesiacov |

* 1. **Vecné požiadavky na poskytovanie konzultačných a implementačných služieb**

Verejný obstarávateľ požaduje poskytovanie konzultačných a implementačných služieb pre Web Application Firewall a cloudovú službu. Označenie, popis konzultačných a implementačných služieb je uvedený v nasledujúcej tabuľke č. 6.

**Tabuľka č. 6** – Označenie, popis a rozsah poskytovania konzultačných a implementačných služieb pre nový HW a cloudovú službu.

|  |  |  |  |
| --- | --- | --- | --- |
| **Položka** | **Označenie** | **Popis** | **Počet**  v osobohodinách |
| **10.** | Poskytovanie konzultačných a implementačných služieb | Poskytovanie konzultácií a dodatočných implementačných služieb pre predmet plnenia, a to najmä pre Web Application Firewally a cloudovú službu v rozsahu maximálne 800 osobohodín počas trvania platnosti tejto zmluvy. Súčasťou služby je aj úprava príslušnej dokumentácie zaznamenaním vykonaných implementačných zmien. Nahlasovanie požiadaviek na konzultačné alebo implementačné služby prebieha v pracovnom čase (7.30 h až 16.30 h v pracovných dňoch v Slovenskej republike), realizácia požiadavky najneskôr do 3 pracovných dní od nahlásenia, v pracovnom čase. | 800 |

* + - 1. Iné požiadavky verejného obstarávateľa
  1. Verejný obstarávateľ požaduje, aby uchádzač integroval zariadenia Web Application Firewall s príslušenstvom spolu s príslušnými licenciami do **existujúceho manažmentu WAF BIG – IQ** prevádzkovaného u verejného obstarávateľa.
  2. Verejný obstarávateľ požaduje, aby uchádzač v ponuke predložil úplnú technickú dokumentáciu ponúkaných zariadení Web Application Firewall a príslušenstva (dokumenty postačuje predložiť v elektronickej forme s vyznačením požiadavky verejného obstarávateľa), z ktorej bude možné posúdiť splnenie všetkých parametrov a technických požiadaviek požadovaných verejným obstarávateľom v časti 2.1 *Vecné požiadavky na hardvér* tejto prílohy súťažných podkladov. Verejný obstarávateľ akceptuje predloženie technickej dokumentácie v slovenskom, v českom alebo v anglickom jazyku. Odkazy na informačné zdroje na internete **nebude verejný obstarávateľ akceptovať**.
  3. Verejný obstarávateľ požaduje, aby uchádzač v ponuke predložil potvrdenie od výrobcu ponúkaných zariadení, že:

1. ponúkané zariadenia pochádzajú od autorizovaného distribútora z oficiálnej distribučnej siete výrobcu na území Európskeho hospodárskeho priestoru a
2. ponúkané zariadenia sú určené pre trh Európskeho hospodárskeho priestoru a budú mať plnú záruku a podporu výrobcu a
3. ponúkané zariadenia nemajú ukončenú životnosť (End of Life) alebo predaj (End of Sale), a že budú pod servisnou podporou výrobcu minimálne po dobu trvania zmluvy.