PŘÍLOHA Č. 1

Technická specifikace

„DODÁVKA A IMPLEMENTACE APLIKAČNÍHO ZABEZPEČENÍ PROVOZOVANÝCH SLUŽEB A APLIKACÍ“

(i) Specifikace plnění

(ii)

Předmětem plnění je dodávka, implementace a podpora provozu technologie, která zajistí kontinuitu, vysokou dostupnost a zejména efektivní bezpečnost provozovaných služeb a aplikací a to jak veřejně dostupných, tak ryze interních. Cílem je významné zvýšení úrovně komplexní bezpečnosti a odolnosti proti kybernetickým hrozbám. Možnost rychlé a včasné reakce na auditní nálezy, výsledky penetračních testů a zajištění shody s legislativou. Technologie musí být schopna rychle (řád hodin, max. jednotky dní) reagovat na nově publikované zranitelnosti a to s ohledem na provozované systémy a také podpůrný software, který je využíván pro běh služeb. Technologie musí efektivně chránit systémy minimálně proti OWASP TOP 10 útokům a musí být schopna ochránit systémy před útoky typu DoS a to i v distribuovaných variantách.

1) Dodávka technologie
2) Implementační práce
3) Podpora výrobce - Podpora výrobce na 3 roky
4) Servisní podpora - Servisní podpora spojená s provozem technologie na 3 roky

Dodávka technologie

Technologie	množství
Technologie HW, včetně licencí, v konfiguraci 2+2	4
Redundantní napájení	4
Duální konektivita SFP 8x 1Gps	8

Technické požadavky na jednotlivý dodávaný box

Technologie musí být schopna rychle (řád hodin, max. jednotky dní) reagovat na nově publikované zranitelnosti a to s ohledem na provozované systémy a také podpůrný software, který je využíván pro běh služeb. Technologie musí efektivně chránit systémy minimálně proti OWASP TOP 10 útokům a musí být schopna ochránit systémy před útoky typu DoS a to i v distribuovaných variantách. Detailní seznam požadavků je v následující tabulce:

Tabulka požadavků na dodávaný box:

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Splňuje Ano/Ne	Nabízená hodnota (Popis)
Provedení	Mamostatná skříň s možností montáže do RACK, maximální výška 1U min. 4 x 1Gbps Ethernet interface, s možností dalšího rozšíření min. o 2 x 10 Gbps interface	ANO	4x1Gbps per box 2x10Gbps per box 1U
Napájení	Možnost rozšíření na dva redundantní zdroje napájení.	ANO	1+1 zdroje
Management	Lokální management - sériová linka Vzdálený management – dedikovaný management interface (GUI, příkazová řádka) Lights-out management - nezávislý servisní procesor umožňující provádění veškerých administrátorských operací (včetně zastavení bootovacího procesu) vzdáleně po síti ethernet	ANO	Serial console Web GUI + SSH cli AOM
Propustnost	Propustnost min. 10/10Gbps (L4/L7)	ANO	L4/L7
Požadavky za sekundu L7 (1-1)	Minimálně 60k	ANO	70k
Množství paralelně zpracovávaných požadavků L4	Přes 10M	ANO	14M
Izolace síťového provozu	Úplné oddělení síťové komunikace. Schopnost vytváření izolovaných a na sobě nezávislých síťových segmentů (IP adresy, routovací tabulky, ...) za účelem úplného oddělení síťového provozu pro různé zóny. (virtuální routery)	ANO	Routing Domains Je možno implementovat virtuálně oddělené síťě s různými DGWs.
Možnost manipulace s provozem na úrovni http protokolu	Vkládání/mazání/úpravy stávajících nebo požadovaných http hlaviček, manipulace s http payloadem, možnost začištění provozu (rewriting obsahu), možnost volby záložního nebo záložních serverů v případě výpadku serverů primárních, možnost odpovídat klientovi přímo z technologie bez nutnosti implementace „maintenance" serverů.	ANO	Pfofily + možnost naprosté customizace pomocí TCL jazyka.
Webový aplikační firewall	Ochrana proti útokům na HTTP/HTTPs zejména: • OWASP TOP 10 včetně podpory pro AJAX/JSON/XML • DoS a DDoS	ANO	Veškeré požadavky technologie splňuje + mnohem více.

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Splňuje Ano/Ne	Nabízená hodnota (Popis)
	• BruteForce Zajištění čistoty protokolů HTTP, FTP a SMTP Integrovaný XML firewall (SOAP, web services). Zakončení uživatelských SSL spojení Podpora prevence úniku citlivých dat (response filtering). Možnost provozu v aktivním i pasivním módu. Možnost konfigurace za využití učícího se módu. Možnost testovat jednotlivá bezpečnostní pravidla v non-blokovacím režimu při zachování funkčnosti stávající bezpečnostní politiky WAF. Možnost vytvářet on-demand bezpečnostní politiky pro konkrétní aplikace nezávisle na dalších politikách. Možnost rychle reagovat na nově vznikající kybernetické hrozby. Možnost logovat na externí Syslog server. Podpora ICAP protokolu. Možnost vytvářet vlastní odpovědi při zablokování požadavku (blocking page) nezávisle pro jednotlivé typy narušení.		
SSL VPN přístup (optional)	Vzdálený SSL VPN přístup (client i clientless mód) pro minimálně 500 současně připojených uživatelů - možnost dalšího rozšíření (2000+). Plnohodnotný VPN přístup pro klienty OS Windows, Linux, Android, iOS, popřípadě další. Kontrolovat / řídit úroveň zabezpečení klientských stanic včetně kontroly aktivních (bezpečnostních) programů a jejich stavu (např. lokální antivirus, antimalware, personální firewall apod.), min. požadované verze OS (servis pack) apod. Spolupráce s více autorizačními servery - Active directory, podpora protokolu LDAP. Podpora pro protokoly Kerberos, NTLM, NTLM2, Radius, TACAS+, OCSP, Basic access authentication/form autentizace	ANO	Veškeré požadavky technologie splňuje + mnohem více.
Migrace ze stávajícího prostředí	Je požadováno zajištění úplné migrace všech funkcionalit ze stávající technologie	ANO	Po vytvoření mapy sptávajících služeb a plánu migrace je možné zmigrovat na nabízenou

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Splňuje Ano/Ne	Nabízená hodnota (Popis)
			technologii téměř cokoliv.
Podpora pro publikace aplikací	Přímá podpora aplikací Outlook Web Access, Outlook Anywhere a Exchange ActiveSync.	ANO	Technologie nabízí šablony pro konfiguraci nejrozšířenějších typů služeb a aplikací, mezi které MS Exchange, včetně souvisejících služeb, patří.
Monitoring	Monitorování cílových serverů a na nich provozovaných služeb prostřednictvím: ICMP, HTTP, HTTPS, TCP, SNMP	ANO	Technologie umožňuje naprostou volnost při tvorbě monitorů dostupnosti (interní předpřipravené s možností modifikace vs. externí – jakýkoliv skript).
Reporting	Možnost zaznamenávat statistiky provozu http/xml a vytvářet exportovatelné výstupy včetně grafu, přes jednotlivé služby. Možnost zachytit veškerý uživatelský http/xml provoz (response/request) Možnost posílání logu na externí úložiště minimálně ve formátu syslog	ANO	Reportovat je možné to, co je požadováno. Musí se ovšem vzít v potaz, že technologie není primárně určena pro skladování logů.
Vysoká dostupnost	Je vyžadován provoz zajišťující vysokou dostupnost služby spojením dvou a více zařízení v režimu active/passive	ANO	HA na úrovni datacentra. Možnost provozu active-active i active-passive.
Cache a compression	Možnost cachování a komprese http provozu (minimálně 4 Gbps) dle standardů http protokolu	ANO	Compression 5Gbps Caching podporován

Parametr	Požadovaná hodnota (pro jedno fyzické zařízení)	Splňuje Ano/Ne	Nabízená hodnota (Popis)
IPv6	Plná podpora IPv6, IPv6/IPv4 gateway.	ANO	Plná podpora pro IPv4 i IPv6
SSL	Je vyžadováno zpracování SSL komunikace na HW úrovni (šifrovací karta). Min. 4000 SSL transakcí za sekundu (2K RSA klíče) Min. 400k SSL konkurenčních spojení Zařízení garantuje propustnost šifrovaného provozu min. 6 Gbps Podpora standardu SHA-2 , TLS 2	ANO	4300 TPS (Transactions per Second) 2k RSA keys Propustnost šifrovaného provozu (bulk encryption) 8Gbps
Napojení na systémy třetích stran	Podpora SNMP v1, v2, v3 Možnost odesílání logu na externí logovací systém.	ANO	SNMP v1, v2 a v3 je podporováno, remote logging taktéž.

Požadavky na celkové řešení

Řešení musí splňovat požadavky vysoké dostupnosti (pro dvě datová centra). Celkové řešení (2+2 zařízení pro 2 datová centra) musí splňovat následující požadavky:

Požadavky na celkové řešení:

Parametr	Požadovaná hodnota (pro celek – 4 zařízení)	Splňuje Ano/Ne
Sdílená konfigurace	Pro všechny členy clusteru musí existovat jedno místo pro tvorbu konfigurace a to jak pro loadbalancing tak pro bezpečnostní politiky webového aplikačního firewallu.	ANO
Automatické zálohování konfigurací	Schopnost automatické tvorby záloh, možnost jejich šifrování a možnost automatizovaného odlévání záloh na zálohovací zařízení.	ANO
Manuální nebo automatická synchronizace konfigurace	Schopnostt libovolně měnit konfigurační objekty, aniž by docházelo k automatické synchronizaci.	ANO
Možnosti provozu HA	Možnost různé kombinace aktivních a pasivních boxů. Varianty - 2 aktivní a 2 pasivní jednotky a 4 aktivní jednotky	ANO
Manuální volba aktivního člena	Schopnost manuální volby aktivního člena nebo členů clusteru / HA řešení	ANO
Mirroring uživatelského provozu	Schopnost mirrorovat uživatelský provoz z aktivních na neaktivní členy clusteru / HA řešení, zajištění maximální možné míry bezvýpadkového provozu v prostředí HA aplikací.	ANO
Možnost oddělit konfigurační objekty	Možnost oddělit jednotlivé konfigurační objekty a logické celky a možnost řídit přístupy k takto odděleným objektům (multitenancy).	ANO
Autentizace	Schopnost provádět autentizaci proti lokální DB nebo proti vzdálenému autentizačnímu serveru (LDAP, RADIUS, TACACS)	ANO
Možnost agregace linek	Schopnost připojit jednotlivá zařízení pomocí agregace linek (LACP)	ANO
Izolace síťového provozu	Úplné oddělení síťové komunikace. Možnost vytváření izolovaných a na sobě nezávislých síťových segmentů za účelem úplného oddělení síťového provozu pro různé zóny. (virtuální routery)	ANO
Implementace a verzování bezpečnostníc h politik WAF	Podpora pro verzování a aktivace nebo deaktivace bezpečnostních politik z jednoho místa (gui). Možnost implementace aplikačně specifických bezpečnostních politik.	ANO

Parametr	Požadovaná hodnota (pro celek – 4 zařízení)	Splňuje Ano/Ne
Implementace vázaných bezpečnostníc h politik pro WAF	Podpora možnosti implementovat bezpečnostní politiky, a parametry politik, vázaných na konkrétní URI.	ANO
Podpora transparentníh o režimu WAF	Podpora pro transparentní režim provozu, bez vlivu na běh aplikace.	ANO
Podpora učícího se režimu WAF	Možnost zapnout režim učení.	ANO
Vypnutí a zapnutí jednotlivých částí politiky WAF	Možnost libovolně zapínat a vypínat jednotlivé ochranné prvky, součásti bezpečnostních politik pro jednotlivé aplikace a služby.	ANO
Podpora IP geolokačních a IP reputačních služeb	Možnost budoucí implementace ochrany přístupů souvisejících s geolokační DB a IP reputačními službami.	ANO
Definice aplikačně specifických hlášení	V případě zaznamenání incidentu, je požadována možnost definovat odpovědi systému pro klienta v rámci jednotlivých aplikací (design, uživatelsky srozumitelné hlášení).	ANO
Monitoring	V případě nedostupnosti služby automaticky vyřadit nedostupný server a směrovat na další servery, v případě celkové nedostupnosti možnost generovat uživatelsky srozumitelná hlášení.	ANO
Reporting	Monitorovací a reportovací nástroje pro auditing zařízení a pro zaznamenané incidenty.	ANO

Další požadované klíčové vlastnosti řešení:

- Dostatečný výkonnostní a licenční prostor pro pokrytí a zabezpečení dalších aplikací a služeb
- Možnost pokrytí nově vznikajících aplikací

(iii) Požadavky na vykonání implementačních prací

Dodavatel provede úplnou implementaci dodaného řešení v HA architektuře 2+2 ve 2 datových centrech Magistrátu hl. m. Prahy, včetně úplné migrace nastavení ze stávajícího firewallového prostředí (technologie BIG-IP).
Požadujeme úplnou migraci služeb ze stávajícího řešení na nové řešení (cca 60+ služeb).
Dále požadujeme konfiguraci aplikačně specifických bezpečnostních politik, reflektujících OWASP top 10 a následující tabulku (40+ služeb + budoucí služby dle požadavků zadavatele). Zároveň je vyžadována následná podpora a správa při úpravě stávajících a tvorbě nových bezpečnostních politik.

Požadavky na implementovanou funkcionalitu řešení:

Ochrana	Poznámka	Splňuje Ano/Ne
Injection	Ochrana proti injection útokům na www aplikace a jejich formuláře (SQL, LDAP, XPath, NoSQL, příkazy OS, XML parsery, SMTP hlavičky, apod.).	ANO
Prolomení autentizace a ochrana systémů řízení přístupu	Ochrana proti útokům, které mají za cíl prolomení autentizačních mechanismů (brute force, slovníhové útoky) a podporu pro ochranu proti útokům souvisejících se systémem řízení přístupu k aplikacím a službám.	ANO
Ochrana proti úniku sensitivních dat	Požadujeme možnost filtrovat chybová hlášení aplikací a možnost konfiguračně upravit šifrování nebo tokenizování citlivých parametrů + možnost poskytovat informace tvůrcům aplikace za účelem dalšího zvyšování bezpečnosti.	ANO
Ochrana XML Externích Entit (XXE)	Ochrany XML procesorů a parserů také s ohledem na zpracování externích zdrojů.	ANO
Eliminace útoků souvisejících s chybnou konfigurací	Požadujeme možnost implementovat opatření, která budou schopna eliminovat projevy a důsledky útoků souvisejících s chybami v konfiguracích provozovaných systémů.	ANO
Cross-Site Scripting (XSS)	Ochrana proti útokům typu Cross-Site Scripting.	ANO
Ochrana proti známým zranitelnostem	Ochrana proti známým zranitelnostem a možnost aktualizace interních databází vzorků známých zranitelností.	ANO
Ochrana proti CSRF útokům	Ochrana proti útokům z rodiny Cross Site Request Forgery.	ANO
Ochrana proti útokům typu DoS a DDoS	Požadujeme možnost konfigurovat ochran souvisejících s přetěžováním aplikací a služeb a to i v distribuovaných variantách.	ANO
Ochrana proti web scraping metodám a podpora detekce robotů	Požadujeme možnost detekovat automatické procházení webů a zneužívání služeb. Dále je požadována možnost detekovat roboty a automaty a zamezit v jejich dalším přístupu ke službám, případně jinak omezit jejich aktivitu na chráněné službě nebo službách.	ANO
Virtual patching	Možnost rychlé (custom) implementace ochrany proti nově publikovaným zranitelnostem.	ANO
Ochrana parametrů aplikací	Požadujeme možnost manuální a automatické detekce a konfigurace jednotlivých parametrů http/s aplikací a služeb a ochranu dynamických parametrů generovaných aplikačními servery.	ANO

Ochrana	Poznámka	Splňuje Ano/Ne
Ochrana http hlaviček a cookies	Požadujeme možnost implementace mechanismů pro kontrolu a zabezpečení http hlaviček a možnost implementace ochrany/šifrování cookies.	ANO
Podpora pro vynucování standardů	Podpora pro vynucování komunikačních standardů (RFC) pro jednotlivé typy protokolů.	ANO
Ochrana na úrovni SSL	Požadujeme možnost zajištění bezpečného SSL provozu a podporu pro zajištění a udržení reputace služby (ssllabs).	ANO

Podpora výrobce celkem na 3 roky

- Upgrade, Update operačního systému a bezpečnostních DB
- Výměna vadného dílu next business day

(iv)

Servisní podpora spojená s provozem technologie

Servisní podpora spojená s provozem technologie na 3 roky v režimu 7x24.

Služba helpdesku

Příjem požadavků přes email, telefonní linku a webové rozhraní.

Řešení vad a incidentů

Kategorie vad

(v) **Vady kategorie A (kritická):**
Vady, které způsobují provozní problémy a neumožňují využívání systému firewallů k účelu, jemuž jsou určeny.

(vi) **Vady kategorie B (vysoká):**
Méně závažné vady a nedostatky, které funkčně nebo kapacitně omezují využívání systému firewallů k účelu, ke kterému jsou určeny.

(vii) **Vady kategorie C (střední a nízká):**
Vady a nedostatky, které neomezují využívání systému firewallů k účelu, ke kterému jsou určeny, ale nejsou v souladu se správnou funkcí systému.

Garance	Vada kategorie A (režim 24x7)	Vada kategorie B (režim 24x7)	Vada kategorie C (režim 24x7)
Potvrzení příjmu požadavku a oznámení jména řešitele zákazníkovi	Do 30 minut od okamžiku nahlášení vady.	Do 30 minut od okamžiku nahlášení vady.	Do 1 hodiny od okamžiku nahlášení vady.

Odstranění (fixace) závady.	Do 4 hodin od nahlášení závady.	Do 12 hodin od nahlášení závady.	Do 24 hodin od nahlášení vady. *Tento termín může být na základě dohody zákazníka s dodavatelem prodloužen.*

Vady mohou být nahlášené buď přes záznam v helpdesku poskytovatele, nebo hlášením z monitoringu proaktivně vedeného Poskytovatelem.

Změnové řízení

- Implementace nových služeb pro loadbalancing
- Implementace mechanismů upravujících aplikační provoz a pro vytváření aplikačně specifických „skriptů", které umožní manipulovat s provozem nebo provoz omezit
- Implementace nových bezpečnostních politik pro nové služby a aplikace
- Pokročilá konfigurace bezpečnostních politik, aktualizace politik a jejich řízená modifikace
- Pravidelný reporting pro odpovědné osoby

Ostatní servisní podpora

- Poskytování informací, také třetím stranám, s cílem
  - eliminace projevů útoku
  - podpora investigace
  - zvýšení celkové bezpečností provozované služby
- Zavedení ochrany v souvislosti např.
  - výsledky penetračních testů
  - auditních nálezů
  - nově publikovaných hrozeb