

Příloha č.1 Podrobná specifikace položek

Položka	Předmět	Ks	Cena za kus bez DPH	Předpokládaná cena bez DPH
1A	Web Application Firewall v HA, set dvou HW zařízení	1	3 600 000,00 Kč	3 600 000,00 Kč

!!!!UHAZEČE NEUVÁDÍ KONKRÉTNÍ ZAŘÍZENÍ, POUZE DOPLNÍ DO ZELENÝCH POLÍ TABULKY, ZDA ODPOVÍDÁ DANÉMU PARAMETRU (ANO/NE, PŘÍPADNĚ ČÁSTKU)!!!!

* Pokud předvíte dodávku s přílohou parametrů, napíšte "ANO". Pokud předvíte dodávku nepřesahující požadovaný parametr, napíšte "NE", účastník v takovém případě bude z výběrového řízení vyloučen.

* Zadávatel si vyhradzuje právo požadovat předložení technické specifikace od dodavatele, kdykoliv v průběhu veřejné zakázky

1A		Nabídková cena bez DPH za kus (Kč)	2 998 251,98 Kč
Web Application Firewall v HA, set dvou HW zařízení		Nabídková cena celkem bez DPH	2 998 251,98 Kč
Počet kusů (dodávaných setů)	1	DPH	629 632,92 Kč
		Nabídková cena celkem včetně DPH	3 627 884,90 Kč
Minimální konfigurace	Typ a počet dodávaných zařízení	Dodávka a instalace 2 kusů nových hardwarových zařízení WAF (web application firewall) v konfiguraci s vysokou dostupností umístěných ve dvou geografických lokalitách chránících webové aplikace zadavatele.	ANO
	Počet dodávaných identických HW boxů	2	ANO
	HW vlastnosti obou boxů (každého)	Zařízení pro RACK 19", napájení 230 V AC (zásuvka), redundantní napájení se dvěma zdroji vytížitelnými za provozu.	ANO
	HA, funkcionality	Vysoká dostupnost boxů v režimu Active-Active. Bezvytržný update/upgrade. WAF budou umístěné mezi Internetem a webovými servery zadavatele, budou skenovat veškerý přicházející webový provoz pro zablokování útoků. Možnost testovacího provozu nasazené aplikace v boxu či externím prostředí s exportem politik do dodáváného WAF řešení.	ANO
	Propustnost	Propustnost 2.5Gbps na box při funkcionalitě ochrany webových aplikací Počet chráněných backend serverů - min. 150 (fyzické i virtuální) Počet paralelních spojení 0.9M Počet HTTPS transakcí za sekundu 15 000k	ANO
	Připojení	Připojení každého boxu 2 x 10Gbit Plná podpora protokolu IPv4 Plná podpora protokolu IPv6 TLS/SSL Offloading (hardwarová akcelerace) Rozložení zábrže a content routing Podpora protokolů HTTP1.0, HTTP1.1, HTTP2.0, WebSockets Podpora IEEE 802.1q - VLAN Podpora NAT - DNAT Podpora LAG - Link bonding	ANO
	Ochrana webových aplikací, WAF podporuje	Ochrana OWASP TOP 10 Web Application Security Risk - https://owasp.org/www-project-top-ten/ Ochrana proti SQL injection Ochrana proti Cross Site Scripting Ochrana proti Cross Site Request Forgery Ochrana proti Session hijacking Geo-IP lokace a IP reputation Delektce/blokování známých hrozeb dle signatur File Upload Control Grammar per URL/parameter policies Rate Control	ANO
	Ochrana API webových aplikací	Ochrana proti OWASP Top 10 API Security Risk - https://owasp.org/API-Security/ API Security - JSON, XML	ANO
	BOT ochrana	Ochrana proti brute force útokům Možnost ochrany aplikací pomocí Captcha DDoS ochrana DDoS ochrana aplikací	ANO
	Ověřování	Zabezpečený přístup k aplikaci, ověření přes protokol SAM.2, OpenIDConnect, JWT.	ANO
	Logování	Lokální logování - systémové logy, firewall logy, audit logy, access logy Vzdálené logování - syslog Podpora SIEM/SOAR systémů	ANO
	Licence	Must pokrýt režim Active-Active, veškerou požadovanou funkcionalitu a min. požadovanou propustnost po celou dobu záruky Zařízení musí být schopné provozu i po vypršení záruky bez dodatečných licencí či subskripcí, min. do roku 2026. Po dobu záruky musí být pro boxy dostupná databáze zranitelnosti s možností automatického nahrazení a implementace.	ANO
	Instalace	Dodání a zprovoznění obou hardwarových web aplikacních firewallů pracujících v clustru s vysokou dostupností (HA) v režimu active-active. Zadavatel poskytne prvky s 10Gbit konektivitou v provedení LC-SMM. Dodavatel pro připojení do infrastruktury dodá boxy vybavené 10Gbit konektivitou osazenou SMMM moduly/kabely. Kabely pro připojení jsou součástí dodávky Pro management jsou k dispozici ETH porty. Každý z dodávaných boxů bude umístěn v jiné lokalitě. Zařízení budou umístěné ve dvou budovách - lokalitách České mládeže 8 a Pasteurova 1 v Uhř. Součástí dodávky je montáž v místě dodání, propoj se síťovými prvky zadavatele, konfigurace vč. HA podle best practices výrobce v režimu active-active. K dispozici jsou příslušné SM včetně mezi lokalitami v délce 800m, zakončení E2000.	ANO
	Implementace ochrany webů	Součástí implementace bude nastavení WAF, nasazení na testovací webové aplikace (dále jen WA) v počtu 3 ks: webový portál gpo.ujep.cz, skoleni.ujep.cz (Moodle), a vzorový Wordpress. Nastavení ochrany 4 produkčních webových aplikací vč. detailního doladění: - portal.ujep.cz, ins.ujep.cz, mensa.ujep.cz, www.ujep.cz. Pro systémy Moodle a Wordpress vypracovat postupy a šablony pro snadné následné zavádění. Vypracovat postupy a doporučení pro implementaci redakčních systémů Drupal a Joomla.	ANO
	Vypracování dokumentace, zavedení webové aplikace (WA) do WAF, předvedení funkcionality, informování o průběhu implementace, testy	V průběhu instalace bude vypracována dokumentace vč. zavedení WA. Pracovníci Centra informatiky UJEP - Oddělení počítačových sítí (OPS) budou informováni a detailně seznámeni s troky v průběhu instalace a konfigurace boxů a s vč. nastavení konektivit, vysoké dostupnosti, aktualizace FW/SW, nahrávání a konfigurace SSL certifikátů, konfigurace protokolů, nastavení ochrany proti útokům, GeoIP blokování, nastavení režimu provozu, zavedení do WAF testovacích a provozních WA které budou chráněny, konfigurace bezpečnostních politik pro jednotlivé WA, definice specifických pravidel pro ochrnu proti útokům, notifikace pro různé bezpečnostní incidenty, nastavení monitoringu výkonu, generace reportů, příprava pro integrace s SIEM, nastavení záloh konfigurace, OPS bude poučeno o budoucí správě a údržbě WAF. Bude prováděno testování funkčnosti dodáváného řešení, zejména vysoké dostupnosti jednotlivých WA, zda jsou správně chráněny WAF. Zda nedochází k nepřetržitým blokováním legálního provozu. Po nasazení do produkčního prostředí sledování výkonu a bezpečnostních incidentů. Ověření, že WAF účinně dektuje a blokuje reálné útoky, aťz by způsobovaly falešná pozitivní hlášení. Zejména zda systém účinně blokuje známé typy útoků jako: - SQL injection, XSS, CSRF, - atd.	ANO
	Postimplementační kontrola	Kontrola produkčního prostředí WAF, které bude provádět dodavatel v prvním roce po implementaci v intervalech po 3 měsících. Tedy počet revizí celkem: 4 v rozsahu min. 4 hodiny (každá revize). Revize budou zahrnovat i úpravy bezpečnostních politik, doporučení roz. změn nastavení systému dle aktuálních best practices.	ANO
Záruční doba, upgrade a update SW/FW	Min. 5 let dle smlouvy		ANO