

## 1 Předmět plnění veřejné zakázky

Předmětem plnění veřejné zakázky je dodávka technologie reverzní proxy a aplikačního firewallu pro ochranu aplikací provozovaných v síti Zadavatele, implementace a konfigurace dodané technologie a odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Zadavatele (pokud hovoří tato Technická specifikace o zadavateli je jím objednatel dle smlouvy, již je přílohou). Nedílnou součástí plnění je také technická podpora dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Zadavatele.

Tato veřejná zakázka bude obsahovat následující poptávané oblasti:

- Dodávka technologií a subskripcí
- Implementační práce
- Odborné školení správy a údržby dodaných technologií
- Post-implementační a technická podpora
- Konzultační služby na vyžádání.

## 2 Požadavky na plnění

Plnění Veřejné zakázky se musí skládat alespoň z níže uvedených částí:

1. Dodávka HW včetně subskripcí pro funkcionality reverzní proxy a web aplikačního firewall
2. Implementace obou funkcionalit v prostředí Zadavatele
3. Migrace služeb ze stávajícího řešení
4. Odborné školení
5. Post-implementační a technická podpora
6. Konzultační služby na vyžádání.

### 2.1 Dodávka dvou HW zařízení

V oblasti dodávky dvou HW zařízení včetně subskripcí nebo potřebných licencí na 36 měsíců definuje Zadavatel následující požadavky pro každé z nich:

Požadovaná funkcionality/vlastnost
<b>Platforma</b>
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelérátoru a webového aplikačního firewallu.
Každé zařízení podporuje připojení 4 x 10/1 Gbps metalické RJ45 porty a alespoň 4x 25/10 Gbps optické SFP+ porty.
Datová propustnost zařízení alespoň 23 Gbps či více na L4 a 15 Gbps či více na L7
Minimální propustnost HTTP požadavků: 1.5 mil. za sekundu
Minimální propustnost L7 požadavků: 800 tis. za sekundu
Počet současných L4 spojení: 17 mil.
Offload – HW komprese – propustnost min. 10 Gbps

SSL akcelerace v HW
Počet SSL transakcí za sekundu min. 10 tis. (při použití 2K klíče)
Počet SSL transakcí za sekundu min. 8000 (při použití ECDSA P-256 klíče)
Celkový šifrovací výkon 8 Gbps
Nezávislé rozhraní pro management
Redundantní napájení
K dispozici jako autonomní box nebo ve formě šasi
Management: sériový port, GUI, příkazový řádek, iLO
<b>Operační systém</b>
Full-Proxy architektura (plné oddělení klientského a serverového spojení)
Podpora IPv4
Plná podpora IPv6, IPv4/IPv6 gateway
Podpora externích šifrovacích karet pro SSL (HSM)
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)
Podpora Spanning Tree Protokolu (STP)
Možnost přidat vlastní funkce pomocí skriptování
Podpora HTTP/2
Podpora IPSec IKEv2
Podpora konfigurace a správu zařízení přes REST API
Podpora SNMP (v1/v2c/v3)
Možnost aktivovat následující funkce na jedné HW platformě: <ul style="list-style-type: none"> <li>- L4-7 loadbalancing</li> <li>- ICSA certifikovaný Web aplikační firewall</li> <li>- Autorizace a autentizace aplikací, SSL VPN</li> </ul>
Možnost dodatečně aktivovat další funkcionality zakoupením licencí <ul style="list-style-type: none"> <li>- ICSA certifikovaný síťový firewall</li> </ul>
DNS služby a DNS firewall
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu
Podpora Active-Active a Active-Pasive módu
Možnost vytvoření HA clusteru mezi Virtuální a Hardware platformou
<b>Web aplikační Firewall</b>
Integrace s nástrojem na detekci zranitelností webových aplikací
Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10
Možnost doprogramovat si filtrovací pravidla pro aplikace

Automatická korelace zranitelností do jednoho bezpečnostního incidentu
Ochrana AJAX a JSON aplikací
Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)
Podpora Captcha metody
Automatické odlišení skutečných uživatelů od robotů
Integrovaný XML firewall
Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění...
Automatické nahrávání a aplikování nových signatur
Podpora pozitivního a negativního bezpečnostního modelu
Blokování útočníků na základě geolokace
Podpora ICAP pro antivirovou kontrolu – pro HTTP, SOAP a SMTP
Ochrana SMTP a FTP na aplikační úrovni
Podpora SSL (šifrování a dešifrování)
Podpora různých typů reportů – PCI, geolokační reporty
Podpora standardů PCI DSS, HIPAA, Basel II a SOX
Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Oracle Applications, Wordpress a Microsoft SharePoint
Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)
Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů: <ul style="list-style-type: none"><li>• Cenzic Hailstorm</li><li>• WhiteHat Sentinel</li><li>• IBM Rational AppScan</li></ul>
QualysGuard Web Application Scanning
Podpora aplikačního firewallu ve virtuálních kontextech
Podpora aplikačního firewallu v cloudu
Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu
Ochrana proti Session Hijacking pomocí Browser Fingerprintingu
Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávací URL apod.)
Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace

Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI
Podpora a filtrování WebSocket provozu
Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice
Možnost ochrany proti Credential Stuffing útokům
Možnost doplnění modulu pro přístup k online databázi nejnovějších útoků
Rozpoznání zdrojů Phishingu, Anonymních Proxy a spojení na Command and Control centra Botnetů
Schopnost detekovat probíhající útok konkrétní útočné skupiny s cílem zneužít známé zranitelnosti CVE, aktualizace definicí těchto útoků a vytvoření signatur ve WAF v reálném čase.
<b>Řízení provozu</b>
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API
Podpora REST API
Povolení/zakázání ICMP a ARP pro VIP
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení
Podpora alespoň pro 19 metod rozvažování zátěže
Podpora filtrace paketů
Podpora ToS, QoS (marking/preservation/mimic)
Podpora SNMP (v1/v2c/v3)
Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí
Podpora SSL certifikátů podepsaných SHA-2 algoritmem
Podpora práce s 4096-bit klíči
Současná podpora ECC a RSA certifikátu
Podpora Camellia šifer SSL
Podpora pro TLS 1.2
Podpora ECC a DH šifer v HW
Podpora SSL Forward proxy
Stavové filtrované paketů (ACL)
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb
Podpora monitorování služeb na základě výkonu konkrétních hostů
TCP optimalizace síťových toků
Komprese a cachování specifických služeb
Podpora zrcadlení SSL relací a SSL spojení v HA clusteru

Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)
--

## 2.2 Implementace a integrace

V oblasti implementace a integrace funkcionalit dodávaného řešení jsou definovány následující činnosti, resp. požadavky:

Oblast	Činnost
Dodávka zařízení	Zadavatel požaduje dodávku všech zařízení do lokality Pod Tábořem 369/8A, 190 00 Praha 9
Síťová konfigurace	<ul style="list-style-type: none"> <li>- IP adresace</li> <li>Linková agregace</li> </ul>
Základní konfigurace	<ul style="list-style-type: none"> <li>- Ověření zařízení na absenci HW vad</li> <li>- Registrace zařízení</li> <li>- Instalace výrobcem doporučené verze operačního systému <ul style="list-style-type: none"> <li>o Konfigurace základních parametrů (management rozhraní, hostname, DNS, NTP, administrátorské přístupy, napojení na centrální uživatelský systém (LDAP/RADIUS), odesílání událostí do externího zařízení).</li> </ul> </li> </ul>
Konfigurace clusteru	Vytvoření clusteru z dodaných zařízení
Přenos objektů a politik	Příprava a konfigurace 100 site – 80 site dodá dodavatel, 20 site bude realizováno v rámci Hands-on-školení

## 2.3 Odborné školení

V oblasti odborného školení je požadován následující rozsah školení:

Typ školení	Popis
Hands-On školení	Dodavatel provádí implementaci a integraci definovanou v kapitole 2.2 této Technické specifikace ve formě slovního průvodce, kdy veškeré činnosti provádí zástupce Zadavatele. Jednotlivé kroky implementace jsou zástupci Zadavatele podrobně popsány tak, aby došlo k ideální konfiguraci pro dané prostředí Zadavatele. Hands-On školení bude v rozsahu 20 site (očekávaná doba školení je 10MD). Školení bude realizováno minimálně pro 5 zástupců Zadavatele.

## 2.4 Post-implementační a technická podpora

V oblasti post-implementační a technické podpory jsou definovány následující požadavky:

Oblast	Požadavky
Oficiální podpora výrobce	<p>Dodavatel zajistí oficiální podporu výrobce po dobu 36 měsíců od dodávky technologií a licencí dle 2.1 této Technické specifikace, která zahrnuje minimálně:</p> <ul style="list-style-type: none"> <li>• Režim podpory 24x7x4 (24 hodin denně, reakční doba 4 hodiny).</li> <li>• Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu</li> </ul>

Podpora dodavatele	Dodavatel zajistí podporu po dobu 34 měsíců od ukončení odborného školení dle 2.3 této Technické specifikace. Podpora je požadována v režimu A4 dle Zvláštních obchodních podmínek pro zakázky v oblasti ICT.
--------------------	---

## 2.5 Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

Oblast	Požadavky
Konfigurační konzultace	Dodavatel zajistí certifikovaného odborníka v oblasti dodané technologie, který Zadavateli umožní konzultovat konfigurační parametry dodaného řešení.  Předpokládaný počet MD k čerpání za dobu trvání smlouvy: 50
Implementační činnosti	Dodavatel zajistí certifikovaného odborníka v oblasti dodané technologie, který pro Zadavatele realizuje konfigurační práce na dodaném řešení.  Předpokládaný počet MD k čerpání za dobu trvání smlouvy: 50
Analytická konzultace	Dodavatel zajistí certifikovaného odborníka v oblasti vyšetřování kybernetických událostí v rámci dodané technologie pro konzultace bezpečnostních nálezů identifikovaných dodaným řešením.  Předpokládaný počet MD k čerpání za dobu trvání smlouvy: 20

## 3 Fáze dodávky a akceptační milníky

Plnění musí být dodáno ve fázích dle harmonogramu. Každá Fáze (tj. každý řádek harmonogramu) musí být Zadavatelem separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. Zadavatel akceptuje výstupy dané Fáze, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je dodavatel povinen napravit nedostatky plnění.