

TECHNICKÁ SPECIFIKACE

Webový aplikační firewall

1) Virtualizační servery s příslušenstvím

Parametr	Minimální požadavek
Služby, funkce	Obousměrné reverzní proxy. Ukončování SSL komunikace. Validace protokolu HTTP dle RFC. Kontrola HTTP požadavků a obsahu přenášených dat, včetně XML a JSON. Zahajování relací a vynucování časového limitu. Vyvažování zátěže (Load Balancing - LB) na L7. LB persistence na základě source IP, URL, cookie, session ID. Ochrana aplikační logiky. (Pozitivní a negativní model aplikující politiky povolující nebo blokující HTTP/S komunikaci.) Předdefinované sady politik pro známé aplikace (Outlook, SharePoint) Detekce a blokáce aplikačních hrozeb na L7 na základě známých signatur. Detekce a blokáce hrozeb na L7 na základě anomálií a strojového učení. Detekce a blokáce automatizovaných klientů (robotických nástrojů). Detekce hrozeb využívající zranitelnosti aplikací dle OWASP Top 10. Detekce a ochrana před útoky hrubou silou (Brute Force). Detekce a ochrana před manipulacemi se soubory cookie. Detekce a ochrana před aplikačními útoky DoS a DDoS útoky na L7. Detekce škodlivého kódu (malware) antivirovou kontrola nahrávaných souborů. Ochrana před škodlivými weby na základě reputace. Ochrana před kompromitovanými přihlašovacími údaji uživatelů. Autentizace uživatelů (HTTP basic, SSL, LDAP, RADIUS, KERBEROS). Řízení přístupu uživatelů k webovým aplikacím (autorizace uživatelů). Sledování a hodnocení (reputace) uživatelů na základě reálného chování.
Provedení, způsob nasazení	Network-based WAF. Virtual appliance, podpora PLTF VMware, KVM a Hyper-V. Časově neomezená licence pro provoz všech požadovaných komponent a funkcí zařízení.
Rozšiřitelnost, škálovatelnost	Rozšíření na HA řešení typu active / active nebo cluster. Napojení na centrální log management systém.
Konektivita	Min. 8x virtual network interface (VIF)
Kapacita, výkon, parametry	Min. 1x vCPU. Propustnost WAF min 100 Mbps, Latence ≤ 5ms
Bezpečnostní parametry	Zabezpečené ukládání dat. Zabezpečený přístup (přes CLI nebo web GUI) ke správě zařízení. Web GUI v HTML5.
Výrobce	Služby reakce na incidenty (SIRT). Proces bezpečného vývoje aplikací (DevSecOps).

2) Stávající firewall

Požadujeme kompatibilitu se stávajícím zařízením Kerio Control (propojení)

3) Požadavky na instalaci a konfiguraci

Požadujeme instalaci a konfiguraci veškerých komponent v návaznosti na stávající infrastrukturu úřadu (tj. včetně dopravy, montáže, instalace a implementace do stávající IT infrastruktury) v sídle zadavatele. Součástí instalace musí být i zaškolení IT administrátorů minimálně v rozsahu nutném pro samostatnou administraci všech komponent dodávky. Administrací se rozumí zejména: konfigurace, monitoring činnosti, aktualizace, řešení problémů, zálohování konfigurace. Součástí dodávky bude i případný materiál nutný pro plnohodnotné zprovoznění a implementaci dodaného zařízení.

Součástí instalace bude testovací provoz pro ověření funkčnosti dodaného řešení.

4) Servisní podpora dodávky

Obecné požadavky na servisní podporu jsou uvedeny níže:

- Podpora a servis pro zakázku budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. 60 měsíců od předání díla).
- Bude zajištěna udržitelnost dodávky třetích stran, dodaných v rámci veřejné zakázky.
- Technická podpora a servis budou realizovány v místě zadavatele. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.
- Technická podpora bude zajišťována těmito způsoby:
 - Telefonicky prostřednictvím přiděleného tel. kontaktu.
 - Prostřednictvím servisního e-mailu.
 - Prostřednictvím elektronické oznamovací služby (tzv. helpdesku).
 - Prostřednictvím vzdáleného připojení na PC uživatele / server.
- Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.
- Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).

5) Splnění podmínek dodržení technických parametrů

Vítězný dodavatel (účastník) bude povinen před zahájení realizace plnění této veřejné zakázky, **předložit** zadavateli (kupujícímu) do max. 5 dnů od výzvy zadavatele (kupujícího) soupis konkrétních výrobků (produktů), které v rámci realizace zakázky dodá, a které **budou dodržovat veškeré technické parametry uvedené v technické specifikaci.**