



Časť B súťažných podkladov

Podrobný opis predmetu zákazky

Konsolidácia a migrácia WAF infraštruktúry a ďalších služieb

Súčasný stav:

Verejný obstarávateľ v rámci svojej IT infraštruktúry prevádzkuje v dvoch nezávislých datacentrách fyzické zariadenia na platforme F5, zabezpečujúcich služby WAF ASM (aplikačný firewall), LTM (load balancing) a (GTM DNS služby).

Sieťové integrácie s externým prostredím komunikujú cez existujúce zariadenia, následne je komunikácia zasielaná na LTM, ktorý zabezpečuje rozkladanie záťaže a komunikuje na cieľové servery v infraštruktúre. V súvislosti s postupným morálnym zastarávaním zariadení, ukončovaním termínov štandardnej podpory výrobcu, rastúcimi požiadavkami na výkon zariadení ako aj plánovaným prechodom z active/standby na novú active/active architektúru je zámerom verejného obstarávateľa realizovať konsolidáciu týchto systémov ako migráciu služieb na nové zariadenia spĺňajúce aktuálne funkčné a výkonnostné potreby verejného obstarávateľa.

Požadovaný stav:

Na zabezpečenie identifikovaných potrieb je predmetom tejto zákazky dodávka zariadení, licencií a služieb spĺňajúcich nasledovné požiadavky:

A. Funkčné požiadavky (Základné riešenie)

Požiadavka verejného obstarávateľa
Riešenie musí byť dodané vo forme min. dvoch fyzických zariadení (appliance) na zabezpečenie vysokej dostupnosti
Schopnosť ochrany pred útokmi na 7. vrstve RM OSI
Schopnosť detekcie a mitigácie DoS útokov na 7. vrstve RM OSI
Schopnosť detekcie a mitigácie aplikačných útokov typu brute force
Schopnosť detekcie a mitigácie útokov typu "Credential stuffing"
Schopnosť detekcie a mitigácie útokov typu "SSRF"
Schopnosť ochrany pred útokmi pre zneužitie relácie na základe kontroly Cookie vytvorenej na úrovni WAF
Schopnosť detekcie a mitigácie všetkých druhov útokov popísaných v metodike OWASP TOP 10
Schopnosť kontrolovať a validovať obsah dát vo formáte XML na základe vopred poskytnutého predpisu
Schopnosť ochrany API na základe vopred poskytnutého predpisu vo formáte OpenAPI 3.0
Schopnosť automatického sťahovania OpenAPI predpisov z externých zdrojov
Schopnosť kontrolovať a validovať obsah dát vo formáte JSON a na základe mechanizmu AJAX
Schopnosť používať mechanizmus "TLS fingerprinting"



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

2 z 7

Možnosť tvorby bezpečnostnej politiky prostredníctvom interaktívneho sprievodcu
Možnosť tvorby bezpečnostnej politiky pre API aplikácie na základe vopred definovaných šablón pokrývajúcich najčastejšie druhy ich nasadenia
Schopnosť automatickej detekcie a mitigácie prevádzky pochádzajúcej od automatizovaných programov (botov)
Schopnosť automatickej korelácie viacerých identifikovaných útokov do jedného bezpečnostného incidentu
Možnosť definovať bezpečnostnú politiku vo forme whitelist aj blacklist
Schopnosť identifikovať a blokovat' útočníkov na základe geolokácie
Schopnosť skenovať prenášané súbory prostredníctvom externého systému pomocou protokolu ICAP
Podpora spracovania protokolov SMTP a FTP na 7. vrstve RM OSI
Možnosť tvorby bezpečnostnej politiky pre aplikácie Microsoft Outlook Web Access, Lotus Domino Mail Server a Microsoft SharePoint na základe preddefinovanej šablóny prispôbenej pre danú aplikáciu
Schopnosť pre jednu aplikáciu definovať rôzne bezpečnostné politiky rozlíšené na základe IP adresy, domény alebo URI
Schopnosť spracovať výstup nástrojov na penetračné testovanie webových aplikácií pri tvorbe bezpečnostnej politiky
Schopnosť tvorby bezpečnostnej politiky pre protokol WebSocket
Schopnosť automatického blokovania útočníkov na základe prekročenia limitu prekročení bezpečnostnej politiky korelované na základe IP adresy
Schopnosť definovať globálne pravidlá pre bezpečnosť platné v každej bezpečnostnej politike
Možnosť ochrany "single page" webových aplikácií
Schopnosť automaticky identifikovať technológie použité na chránených backendových systémoch a aplikáciách
Schopnosť automatickej úpravy prahových hodnôt pre aktiváciu mitigácií DDoS útokov na 7. vrstve RM OSI
Schopnosť nevynucovať konkrétne ochranné signatúry na základe URL, HTTP hlavičiek alebo HTTP parametrov
Možnosť nasadenia v režime detekcie so zapojením prostredníctvom SPAN portu
Možnosť napojenia riešenia na centrálny systém umožňujúci zdieľanie učenia a konfigurácií medzi jednotlivými bezpečnostnými politikami
Schopnosť schovávať citlivé údaje pred správcom systému v GUI a v zobrazovaných záznamoch (data masking)
Možnosť detekcie a mitigácie cielených kampaní konkrétnych útočníkov na základe signatúr distribuovaných v reálnom čase



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

3 z 7

Možnosť zhodnotenia aktuálnej miery zabezpečenia v porovnaní s odporúčaniami z OWASP Top 10 (OWASP Top 10 Dashboard), vrátane schopnosti dávať odporúčania na úpravu konfigurácie
Schopnosť vynucovať bezpečnostnú politiku natívne aj pre protokol HTTP/2
Možnosť integrácie s CI/CD nástrojmi pre automatizované nasadzovanie bezpečnostnej politiky
Schopnosť detekcie a mitigácie úpravy dát na strane klienta
Schopnosť používať strojové učenie pre zamedzenie tvorby False-positive hlásení
Schopnosť fungovania v režime vysokej dostupnosti Active/Standby aj Active/Active
Riešenie musí obsahovať licenciu umožňujúcu prevádzkovať autoritatívny DNS server na zariadenia ktoré sú predmetom dodávky ako súčasť riešenia.
Riešenie musí byť schopné poskytovať služby rozkladania záťaže prostredníctvom protokolu DNS (GSLB)
Riešenie musí byť rozšíriteľné o funkcionality pokročilého rozkladania záťaže (Load Balancing), ako samostatnej doplnkovej funkcie/ licencie na zariadeniach ktoré sú predmetom dodávky ako súčasť riešenia.
Riešenie musí byť dodané v konfigurácii umožňujúcej vysokú dostupnosť
Súčasťou dodávky musí byť podpora výrobcu typu maintenance na všetok dodaný hardvér, softvér a licencie v trvaní na 24 mesiacov



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

4 z 7

B. Výkonnostné požiadavky (Základné riešenie)

Parameter	Minimálna požadovaná hodnota parametra
Počet appliance	2 pre zabezpečenie vysokej dostupnosti
L7 požiadaviek za sekundu	2.5M
L4 spojení za sekundu	1M
L4 HTTP dopytov za sekundu	18M
Maximálny počet súbežných L4 spojení	75M
Výkon hardvérového SSL/TLS offload-u	60K TPS (2K SSL TPS)
	30K TPS (ECDHE-ECDSA P-256 TPS)
	30K TPS (ECDHE P-256-RSA-2k TPS)
	35 Gbps hrubého šifrovacieho výkonu
Výkon kompresie v hardvéri	35 Gbps
DDoS ochrana v hardvéri mechanizmom SYN cookie	80M packetov za sekundu
Počet virtuálnych kontextov	8
Kapacita a druh diskového priestoru	1TB SSD
Počet manažmentových rozhraní	1x 1000BASE-T, 1xUSB 3.0, 1x serial console port RJ45
Počet dátových rozhraní typu 100/40 Gigabit fiber	2 x 100G/40G QSFP+/QSFP28
Počet dátových rozhraní typu 25/10 Gigabit fiber	8 x 25G/10G SFP28/SFP+
Montáž	montovateľné do štandardného serverového racku
Výška chassis v racku	1U



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

5 z 7

C. Požiadavky na doplnkové moduly

Požiadavka verejného obstarávateľa
Rozšírenie riešenia o LTM (Load Management) funkcionality prostredníctvom licencie nasadenej na zariadeniach ktoré sú predmetom dodávky ako súčasť riešenia,
Funkcionalita rozkladania záťaže musí podporovať aspoň nasledujúce algoritmy: round-robin, pevne stanovený pomer (ratio), najmenší počet spojení (least connections), najmenší počet relácií (least sessions)
Funkcionalita rozkladania záťaže musí podporovať smerovanie súvisiacich spojení na ten istý cieľový systém (session stickiness), a to na základe aspoň nasledujúcich algoritmov: cookie, zdrojová adresa, cieľová adresa, na základe skriptu
Funkcionalita rozkladania záťaže musí poskytovať možnosť riadiť činnosť rozkladania záťaže prostredníctvom skriptov.
Funkcionalita rozkladania záťaže musí poskytovať možnosť upravovať obsah dát prenášaných protokolom HTTP prostredníctvom skriptov.
Funkcionalita rozkladania záťaže musí byť schopná pracovať s aspoň nasledujúcimi protokolmi: HTTP, HTTP/2, QUIC, SMTP, SMTPS, IMAP, POP3, LDAP
Funkcionalita rozkladania záťaže musí poskytovať schopnosť určovať dostupnosť cieľového systému prostredníctvom testovacích dopytov používajúc aspoň nasledujúce algoritmy: HTTP, HTTPS, HTTP/2, DNS, FTP, SMB, LDAP, MySQL, PostgreSQL, MSSQL, SMTP, IMAP, POP3
Funkcionalita rozkladania záťaže musí poskytovať schopnosť určovať dostupnosť cieľového systému prostredníctvom výstupu externého skriptu spúšťaného na úrovni operačného systému zariadenia ktoré je dodávané ako súčasť riešenia.
Súčasťou dodávky musí byť podpora výrobcu typu maintenance na všetok dodaný hardvér, softvér a licencie v trvaní na 24 mesiacov resp. pokrývajúca rovnaké obdobie ako podpora základného riešenia



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

6 z 7

D. Požiadavky na dodávku služieb spojených s implementáciou základného riešenia

Verejný obstarávateľ požaduje dodávku nasledovných služieb ako súčasť predmetu zákazky:

Fáza	Popis činnosti
Analýza	Analýza súčasného stavu zapojenia infraštruktúry a prepojenia prvkov WAF a modulu GTM vzhľadom na WAN ako aj ostatné systémy v rámci datacenter.
Návrh riešenia	Príprava návrh spôsobu zapojenia novej infraštruktúry zariadení WAF a GTM. Popis migrácie z hľadiska postupu, zmien a funkčných testov a rizík, predloženie návrhu na schválenie.
Migrácia	Realizácia migrácie podľa návrhu schváleného obstarávateľom. Zahŕňa prípravné práce spočívajúce v konfigurácii nových zariadení, výmenu pôvodnej infraštruktúry za nové zariadenia v rámci dohodnutého údržbového okna a následne funkčné testy novej infraštruktúry.
Testovanie funkcionality	Zabezpečenie otestovanie end2end funkcionality pred spustením prevádzky nových F5 v 2 lokalitách v rámci Bratislavy minimálne v nasledujúcom rozsahu interných služieb: Integračný modul ESB: 67 služieb Informačný systém EOO: 18 služieb Informačný systém PTCA: 7 služieb Služby v rámci iných modulov IS obstarávateľa: 32 služieb Prepojenie na externé subjekty: Služby poskytované IS obstarávateľa: 12 služieb Služby konzumované IS obstarávateľa: 14 služieb
Troubleshooting	Zahŕňa všetky služby a prostriedky potrebné na odstraňovanie problémov priamo alebo nepriamo zapríčinených v dôsledku zmien v návrhu riešenia.
Dokumentácia	Poskytnutie projektovej dokumentácie vrátane zdokumentovania návrhu a migrácie, reportu o priebehu migrácie a dokumentácie výsledného stavu zapojenia infraštruktúry po ukončení migračnej a troubleshooting fáze projektu.
Projektový manažment	Služby riadenia projektu a projektového manažmentu



GENERÁLNA PROKURATÚRA SLOVENSKEJ REPUBLIKY

Štúrova 2, 812 85 Bratislava

Nadlimitná zákazka Konsolidácia a migrácia F5 WAF infraštruktúry a ďalších služieb

7 z 7

E. Požiadavky na dodávku služieb spojených s implementáciou doplnkových modulov

Fáza	Popis činnosti
Analýza	Analýza súčasného stavu zapojenia infraštruktúry a prepojenia prvkov LTM modulu vzhľadom na WAN ako aj ostatné systémy v rámci datacentier.
Návrh riešenia	Príprava návrh spôsobu zapojenia novej infraštruktúry zariadení LTM. Popis migrácie z hľadiska postupu, zmien a funkčných testov a rizík, predloženie návrhu na schválenie.
Migrácia	Realizácia migrácie podľa návrhu schváleného obstarávateľom. Zahŕňa prípravné práce spočívajúce v konfigurácii nových zariadení, výmenu pôvodnej infraštruktúry za nové zariadenia v rámci dohodnutého údržbového okna a následne funkčné testy novej infraštruktúry.
Troubleshooting	Zahŕňa všetky služby a prostriedky potrebné na odstraňovanie problémov priamo alebo nepriamo zapríčinených v dôsledku zmien v návrhu riešenia.
Dokumentácia	Poskytnutie projektovej dokumentácie vrátane zdokumentovania návrhu a migrácie, reportu o priebehu migrácie a dokumentácie výsledného stavu zapojenia infraštruktúry po ukončení migračnej a troubleshooting fáze projektu.
Projektový manažment	Služby riadenia projektu a projektového manažmentu