**Specifikace předmětu plnění**

1. **Předmět plnění**

Předmětem plnění veřejné zakázky je dodávka a odborná implementace vysoce dostupného pokročilého aplikačního firewallu pro ochranu publikovaných technologií a služeb Technologického centra Karlovarského kraje (dále jen TCKK).

1. **Popis současného stavu**
	1. Popis lokalit

TCKK je rozmístěno ve 2 datových centrech (lokalitách) v areálu Krajského úřadu Karlovarského kraje. V těchto lokalitách bude probíhat poskytování poptávaných služeb

* 1. Popis stávajícího HW prostředí
	+ TCKK je technicky i provozně navrženo, vybudováno a provozováno pro poskytování vysoce dostupných infrastrukturních ICT služeb Krajskému úřadu a jeho zřizovaným organizacím. Technologické centrum je napojeno na RKI – WAN na bázi optických vláken propojující významné úřady v kraji (vesměs obce s rozšířenou působností) a některé zřizované organizace kraje. Přenosové kapacity RKI páteřních spojů je 1 Gb/s.
	+ TCKK je tvořeno dvěma rovnocennými datovými centry, pouze zálohovací technologie jsou soustředěny v jedné lokalitě.
	+ Serverová infrastruktura je tvořena dvěma Blade šasi HP c7000 osazených blade servery Gen7 – Gen10, v současné době probíhá konsolidace hardware – vyřazovaní starších serverů z produkčního provozu s cílovým stavem 11 ks blade serverů. Šasi jsou vybavena redundantními 8Gb FC SAN přepínači, redundantními 1 GbE passtrought moduly a redundantními Virtual Connect Flex 10Gb moduly. 8 fyzických serverů je virtualizováno technologiemi VMware vSphere 7 Enterprise. Všechny servery využívají k ukládání dat replikované datové úložiště Dell Unity.
	+ Datové úložiště se skládá z 2x Dell Unity 300 rozmístěné rovnoměrně do obou lokalit. Disková pole jsou doplněna odpovídající SAN FC 8 Gb infrastrukturou sestavenou z FC přepínačů Brocade. Délka optických tras mezi lokalitami je cca 300 metrů. Celková disková kapacita činí: 91,5 TB.
	+ V budově A Krajského úřadu je umístěn řídící a úložný server HP DL380 G8 zálohovacího systému Veeam Backup a Recovery Enterprise. Pro dlouhodobé ukládání záloh slouží pásková knihovna HPE MSL3040.
	+ Síťová vrstva TC je redundantní a využívá síťové prvky Juniper EX4500, EX4200 (síťové přepínače) a Checkpoint (firewally) a je také virtualizována. Síťové přepínače EX4500 a EX4200 jsou nakonfigurovány jako tzv. virtuální šasi a propojeny 10 Gbps spoji v rámci lokalit i mezi lokalitymi. TC je do RKI připojeno prostřednictvím redundantních centrálních prvků HP A7506.
	+ Inspekci a řízení internetového provozu zajišťuje perimetrový firewall Checkpoint, který slouží i pro publikaci některých služeb TCKK bez pokročilých ochran a autentizačních mechanismů.
	+ Publikace většiny služeb TCKK do Internetu a RKI je prováděno prostřednictvím Forefront TMG 2010 a virtuální instance Citrix Netscaler (služby Citrix XenApp). Oby tyto systémy budou v rámci této zakázky nahrazeny.
	+ Distribuční a přístupová vrstva síťové infrastruktury využívá síťové prvky Juniper, pro bezdrátovou komunikaci jsou využívány prvky Extreme.
	+ Obě lokality jsou vybaveny motorgenerátory, překlenutí doby jejich náběhu a krátkodobých výpadků zajištují UPS EATON 9355.
	+ Datová centra jsou dále vybavena klimatizacemi, zhášecím systémem, IP kamerami a Rack management systémem (dále RMS) s kouřovými, pohybovým a vlhkostními čidly s možností zasílání varování přes SMS.
	1. Popis stávajícího SW prostředí
	+ Systémové služby jsou provozovány na platformě Microsoft, jde zejména o následující systémy:
		- Microsoft Windows Server Datacenter a Standard
		- Microsoft SQL Standard
		- Microsoft Exchange Standard
		- Microsoft 365
	+ Verze systémů Microsoft jsou průběžně aktualizovány v konzervativním režimu, tj. jsou udržovány cca. 1-2 verze za aktuální verzí.
	+ Pro doručování aplikací uživatelům jsou využívány technologie Microsoft Remote Desktop Service (v rámci LAN úřadu) a Citrix XenApp (v rámci WAN-RKI, např. pro příspěvkové organitaze)
	+ Primární adresářovou službou je Active Directory provozovaná na redundantních replikovaných řadičích, které zajištují také služby DNS a DHCP.
	+ K ukládání sdílených souborů je kromě prostředků Windows serveru využívána NAS funkcionalita diskového pole Dell Unity.
	+ Virtualizační platformou TCKK je Vmware vSphere Enterprise 7 řízená jedním vCentrem. Jsou implementovány a využívány pokročilé funkce vSphere – High availability, Dynamic Resource Scheduler, vMotion, virtuální switche apod.
	1. Popis dokumentace
* K provozování a řízení rozvoje TCKK je využívána a udržována Provozní dokumentace. Jednotlivé dokumenty Provozní dokumentace jsou uloženy na řízeném úložišti.
* Provozní dokumentace popisuje aktuální nastavení technologií, hardwarových a softwarových systémů TCKK. Softwarové systémy jsou popsány v rozsahu infrastrukturních služeb (AD, DNS, DHCP apod.), SQL a Exchange.
* K provozování a řízení rozvoje RKI je využívána a udržována Provozní dokumentace. Jednotlivé dokumenty provozní dokumentace jsou uložen na řízeném úložišti, odlišném od úložiště Provozní dokumentace TCKK
* Společným dokumentem TCKK, LAN a RKI je IP plán. Jde o určující dokument pro přidělování a využívání IP adres v TCKK a RKI včetně napojených organizací. Aktuálnost a konzistenci IP plánu zajišťují pracovníci KÚKK.
* Základní dokumenty jsou doplňovány dalšími dokumenty charakteru Provozní dokumentace k systémům a aplikacím provozovaným v TCKK a k systémům a aplikacím organizací napojených na RKI. Struktura a rozsah těchto dokumentů není jednotný.
* Citlivé údaje (přístupové účty apod.) jsou součástí Bezpečnostní dokumentace a jsou uloženy odděleně od Provozních dokumentací
* Relevantní část dokumentace bude Dodavateli zpřístupněna až po podpisu Smlouvy k této zakázce ve formátech MS Office (xls, doc) nebo PDF.
* Dodavatel je povinen zajistit nezbytné doplnění dokumentace TCK reflektující provedené změny v průběhy poskytování služeb
	1. Popis způsobu řešení incidentů
* Zadavatel pro řešení incidentů a podporu uživatelů používá interní HelpDesk vytvořený na zakázku.
* Incidenty a požadavky uživatelů se řeší formou ticketů v systému HeldpDesk, uživatelé tak mají přehled o stavu řešení jejich požadavků. Zadavatel také zajišťuje podporu 1. úrovně a většinu běžných problémů jsou schopni vyřešit interní pracovníci Zadavatele.
* Incidenty a požadavky, které nevyřeší interní HelpDesk budou předávány do helpdeskového systému dodavatele provozní podpory. Hlášení incidentů a požadavků bude prováděno telefonicky, emailem nebo přímo zadáním ticketu/požadavku do helpdeskového systému dodavatele.
	1. Popis servisních oken
* TCKK nemá pevně definovaná pravidelná servisní okna. Aplikace aktualizací a oprav virtuálních serverů provádějí zaměstnanci KÚKK dle potřeby a s přihlédnutím k minimalizaci omezení uživatelů.
1. **Požadavky na technické řešení**
	1. Základní požadavky na technické řešení
* Cílem projektu je zvýšení úrovně zabezpečení publikovaných aplikací a digitálních služeb TCKK implementací samostatného aplikačního firewallu nezávislého na perimetrovém firewallu. Aplikační firewall umožní využívat pokročilé a moderní způsoby ochrany webových i specifických aplikací a systémů včetně autentizace (a autorizace) uživatelů před přístupem k aplikaci či systému. Aplikační firewall bude umožňovat napojení na systémy typu SIEM (Security Information and Event Management) pro správu logů a kybernetických událostí či incidentů.
* Je požadováno řešení zachovávající a rozvíjející současné softwarové platformy Vmware a Microsoft pro zachování kompatibility se stávajícími systémy a výukovými a provozními aplikacemi. Přechod na jinou platformu by způsobil uživatelské a provozní potíže.
* Pokud dodavatel vyžaduje využití konkrétních softwarových produktů a jím zvolený přístup k realizaci zadání je na takových konkrétních řešeních závislý, musí jejich pořízení zahrnout ve své nabídce v potřebném rozsahu a v rámci nabídnuté ceny.
* Pokud dodavatelem nabízené řešení vyžaduje komponenty či služby neobsažené v požadavcích zadání, zahrne dodavatel do své ceny všechny náklady na jejich pořízení, instalaci, konfiguraci a další služby potřebné pro uvedení do provozu, přičemž nesmí překročit předpokládanou hodnotu zakázky.
* Zadavatel z důvodů co nejjednodušší a jednotné správy a minimalizace provozních nákladů vyžaduje využití stávajících prostředků a používaných technologií. V případě, že dodavatel vyžaduje ve svém řešení stejné nebo podobné funkce, jaké poskytují stávající prostředky a technologie, je povinen využít nebo vhodným způsobem rozšířit stávající prostředky.
* Veškeré produkty, které dodavatel dodává v rámci plnění zadavateli, musí splňovat následující podmínky:
1. jsou nové, byly oprávněně uvedeny na trh v EU nebo pochází z autorizovaného prodejního kanálu výrobce,
2. mají plnou záruku od výrobce,
3. mohou být podporovány výrobcem a mohou být součástí servisního a podpůrného programu výrobce,
4. obsahují všechny nezbytné licence na používání příslušného softwaru,
5. jsou v databázi výrobce uvedeny jako prodaná kupujícímu,
6. jsou určeny pro provoz v České republice.
* Zadavatel si vyhrazuje právo na zjištění původu výrobků při jejich předávání, a to dle příslušných sériových čísel a právo podpisu akceptačního protokolu, osvědčujícího převzetí dodávky, až po ověření původu výrobku.
* Veškerá dokumentace vytvořená v rámci realizace veřejné zakázky, musí být zhotovena výhradně v českém jazyce, bude dodána v elektronické formě ve standardních formátech (např. MS Office, Open Office, PDF) používaných zadavatelem. Struktura i forma dokumentace musí být před předáním předána ke kontrole a výslovně schválena zadavatelem.
	1. Specifické požadavky na technické řešení
* Je požadováno softwarové řešení ve formě tzv. virtuálních appliance poskytovaných přímo výrobcem řešení a určených pro virtualizační platformu Vmware vSphere
* Řešení musí být implementováno jako vysoce dostupné s minimálně 2 uzly schopnými samostatné funkčnosti, s centrální správou a jednotnou (synchronizovanou) konfigurací.
	1. Popis povinných parametrů dodávaného řešení
* V dále uvedených tabulkách jsou uvedeny povinné parametry nabízeného řešení. Dodavatel musí všechny parametry splnit, v případě nesplnění požadavku zadavatele bude nabídka dodavatele vyřazena a dodavatel bude následně vyloučen z účasti v zadávacím řízení.
* V relevantním pravém sloupci tabulky dodavatel doplní, jaké zboží konkrétně nabízí. Dodavatel ve své nabídce popíše způsob naplnění každého povinného parametru včetně značkové specifikace nabízených dodávek. Popis způsobu naplnění každého povinného parametru bude konkrétní, úplný a musí výslovně prokazovat (nepostačuje pouze potvrzení či zkopírování požadavku Zadavatele), že nabízené řešení jednoznačně splňuje všechny aspekty povinného parametru. K tomu může účastník využít odkazy na přílohy nabídky (technické listy, manuály apod.), které mohou být i anglickém jazyce. V případě nesplnění požadovaného způsobu prokázání plnění povinných parametrů bude účastník vyloučen z účasti ve výběrovém řízení na danou VZ.
* Dodavatel může nabídnout řešení a zboží s lepšími parametry (v případě, že lze objektivně stanovit, že se jedná o parametry lepší), nikoliv s parametry horšími (či horší kvality), než požaduje zadavatel v zadávacích podmínkách. Zadavatel připouští i jiná kvalitativně a technicky obdobná řešení za podmínky, že nesmí dojít ke zhoršení požadovaných parametrů.
* Tabulka povinných parametrů

| **Popis povinného parametru** | **Podrobný popis nabízeného řešení - plnění povinného parametru** |
| --- | --- |
| *Výkonnostní parametry jsou požadovány pro 1 uzel vysoce dostupného řešení* |
| Pokročilý, ICSA certifikovaný web aplikační firewall |   |
| Virutální appliance pro Vmware vSphere |   |
| Datová propustnost alespoň 200 Mbps či více na L4 a L7  |   |
| Minimální propustnost HTTP požadavků: 40k za sekundu |   |
| Minimální pocet novych L4 spojeni: 20k za sekundu |   |
| Počet současných L4 spojení: min 1M |   |
| Počet SSL transakcí za sekundu min. 900 při použití 2K klíče  |   |
| Počet SSL transakcí za sekundu min. 4k při použití ECC klíče |   |
| Počet současných SSL spojení min. 200k |   |
| Propustnost SSL spojení (bulk Encryption) RSA/ECC min. 170 Mbps  |   |
| Plnohodnotná proxy architektura |   |
| Integrovaný NAT/SNAT/PAT |   |
| Integrovaná IPv6, IPv4/IPv6 gateway |   |
| Integrovaná podpora IPSEC IKE v2 |   |
| Redundance dvou a více uzlů v režimech Active-Active/Active-Standby/N+1 s možností automatické i manuální synchronizacie konfigurace |   |
| Integrovaná podpora heterogenního clusteru (různé virtuální edice nebo kombinace virtuální edice a hw/cloud platformy) |   |
| Integrované IP směrování |   |
| Správa přes GUI a plnohodnotné CLI (SSH přístup s možností ověření uživatele heslem a certifikátem/klíčem) s ověřováním uživatelů a oprávnění proti externím službám (min. RADIUS/TACACS+, LDAP, AD) |   |
| Integrovaný skriptovací nebo obdobný nástroj pro tvorbu vlastních funkcí – možnost plnohodnotné manipulace a správy veškerého aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz |   |
| Integrovaná podpora Javacript / ECMAScript k úpravě a správě provozu |   |
| Integrované RBAC (Role-based access control) – správa na bázi uživatelských rolí |   |
| Integrované filtrování paketů |   |
| QoS – markování, rate – limiting |   |
| TCP optimalizace síťových flows např. při přístupu k aplikaci z mobilu pomocí výrobcem dodaných, nebo vlastních profilů |   |
| Ukončení šifrovaného provozu SSL TLS 1.2 TLS 1.3 |   |
| Dvoucestná SSL autentizace – serverový, klientský certifikát |   |
| Podpora SSL certifikátů s elektronickým podpisem dle standardu SHA-2 s podporou TLS |   |
| Podpora ECC a RSA certifikátů |   |
| Podpora šifrovacích algoritmů, minimálně : AES 256, SHA256, RSA klíče min. o velikosti 4k |   |
| Validace intermediate certifikátu |   |
| Práce s CRL a jeho automatická obnova |   |
| Podpora vysokorychlostního granulárního logování / logování per aplikace na externí logovací systém  |   |
| Možnost odeslání elektronické zprávy (e-mail) určené osobě při vzniku sledované události. |   |
| Podpora otevřeného API pro konfiguraci a automatizaci pro nástroje třetích stran |   |
| Podpora SW utilit na troubleshooting např. tcpdump |   |
| Podpora různých typů balančních metod (minimálně):- kruhová metoda, včetně varianty s vážením- podle aktuálního počtu navázaných spojení- podle URL a cookie- podle vah skupiny serverů |   |
| Zajištění “session persistence” na základě IP adresy, HTTP cookie, HTTP host |   |
| Podpora různých typů health monitoringu – ICMP, HTTP/HTTPS, ICMP, TCP/UDP port. |   |
| Monitorování stavu a zátěže zdrojů/serverů:- průběžné monitorování cílových serverů i všech souvisejících aplikačních komponent- možnost kombinace (AND/M of N) více metod (např., ICMP, HTTP, TCP port)- možnost definování intervalu pro monitorování (samostatný interval pro oba stavy UP/DOWN) |   |
| Podpora modifikace provozu- vložení/přepsání cookie- vložení/přepsání http hlavičky - modifikace URL- možnost vložit zdrojovou IP do L7 hlavičky (XFF)- modifikace http/html obsahu |   |
| Použití existující aplikační cookie k zajištění persistence spojení na server |   |
| Možnost směrovat požadavky z určitého subnetu jen na určité servery |   |
| Podpora cachování a komprese HTTP pro každou službu samostatně |   |
| Podpora HTTP/2 směrem k uživateli i k serveru |   |
| SSL Session a SSL Connection mirroring napříč více uzly |   |
| Podpora monitoringu o počtu připojených spojení, stavu poskytovaných služeb a připojených systémů |   |
| Podpora monitoringu per specifická služba |   |
| Podpora logování per aplikace na syslog server |   |
| [Zajištění ochrany proti TOP 10 zranitelnostem dle metodiky OWASP dle https://owasp.org/www-project-top-ten/včetně podpory pro AJAX/JSON XML/SOAP](https://owasp.org/www-project-top-ten/) |   |
| Negativním i positivní bezpečnostní model (aplikačního firewallu) |   |
| Integrovaný XML firewall |   |
| Logování přístupů k webovým službám |   |
| Aplikační firewall pro protokol SMTP |   |
| Konfigurace s využitím učícího se módu |   |
| Automatické nahrávání a aplikování nových signatur od výrobce |   |
| Automatická korelace zranitelností do jednoho incidentu |   |
| Možnost vynucení vytvoření hierarchie bezpečnostních politik - nadřízené a podřízené politiky. |   |
| Validace aplikačních flow pro webové aplikace |   |
| Validace přihlašovacích parametrů |   |
| Ochrana přihlašovací stránky proti brutforce attack |   |
| Ochrana vstupních polí jméno/heslo šifrováním na straně klienta bez nutnosti zásahu do aplikace  |   |
| Podpora CAPTCHA  |   |
| Inteligentní detekce aktivity klávesnice a myši (rozlišení člověk/robot) |   |
| Možnost integrace s externími skenery zranitelností webových aplikací pro automatickou tvorbu/úpravu bezpečnostních politik, např. Cenzic Hailstorm, WhiteHat Sentinel, IBM Rational AppScan, QualysGuard Web Application Scanning. Nabízené řešení musí podporovat alespoň 1 z uvedených skenerů. |   |
| Podpora integrace s externímSIEM  |   |
| Ochrana proti Session Highjackingu jednoznačnou identifikace prohlížeče uživatele. V případě vyhodnocení rizika vynucení provedení definované akce dle vlastností prohlížeče (“challenge”). |   |
| Podpora standardu PCI DSS 3.2 a možnost vytváření PCI reportů  |   |
| Podpora maskování/odstranění citlivých informací jako např. čísla kreditních karet apod., včetně možnosti použití vlastních regulárních výrazů/filtrů. |   |
| Filtrování WebSocket provozu |   |
| Podpora externí antivirové kontroly pomocí ICAP |   |
| DoS a DDoS detekce a ochrana na L7 |   |
| Ochrana proti DDoS detekcí stresu chráněné aplikace – zpoždění odpovědi a následné omezení počtu požadavků, Captcha, TCP reset a podobně |   |
| Detekce legitimního provozu na silně vytížených URL, odlišení od DoS nebo DDoS útoku a tím zamezení blokování legitimních uživatelů.  |   |
| Automatické nebo ruční „blacklistování“ IP adres, které se opakovaně snaží překonat zabezpečení ochranu a/nebo mají vysokou mírou nežádoucího provozu |   |
| Podpora nastavení specifických bezpečnostních politik podle IP adresy, doménového jména a URI |   |
| Podpora viditelnosti a reportingu pro jednotlivé http request/response |   |
| Podpora geolokace včetně monosti blokování útočníků podle geolokace |   |
| Automatické odlišení platných uživatelů od botnetů  |   |
| Možnost definovat bezpečnostní politiku na základě kategorie Botu |   |
| Ochrana proti automatizovanému provozu/útokům (botnetům) pomocí signatur i aktivním odlišením prohlížeče od botu (např. pomocí tzv. „challenge“ - akcí pro identifikaci uživatel x bot), pokud umí bot simulovat chování skutečného prohlížeče. Zablokování komunikace bota na aplikační server. |   |
| Průběžná analýza stresu aplikace, analýza nestandardního chování tzv. behaviorální analýzy a vylaďování ochrany aplikace za pomocí uplatňování dynamických signatur. WAF mapuje a zaznamenává standardní chování uživatelů vrámci aplikace. V případě zjištění odchylky se dynamicky vygeneruje signatura založená na těchto odchylkách, která jednoznačně identifikuje zdroje škodlivého provozu, který může být zablokován nebo zpomalen. |   |
| Ochrana proti Credential Stuffingu - rozšíření ochrany proti bruteforce útokům - rozpoznání, že zadávaná uživatelská jména a hesla jsou součástí známých databází kompromitovaných identit. Zablokování detekovaných požadavků nebo notifikace administrátora. Databáze porovnávaných identit musí být uložena v hashované podobě.  |   |
| Ochrana proti útoku typu Session Highjacking jednoznačnou identifikací prohlížeče uživatele (tzv „fingerprintu“ webového prohlížeče). |   |
| Ochrana dat a přihlašovacích údajů proti malware během zadávání do citlivých polí formuláře na webové aplikaci šifrováním dat na aplikační vrstvě na straně klienta s následnou dekrypcí výhradně aplikačním firewallem |   |
| Podpora využití CI/CD pipeline pro nasazování security politik na webových aplikacích  |  |
| Podpora importu souboru Swagger pro definici security politiky pro ochranu API  |  |
| Podpora importu souborů OpenAPI 3.0 za účelem vytvoření komplexní politiky |  |
| Podpora mikroslužeb v politikách |  |
| Podpora integrace s komunikačními nástroji (min. Slack a MS Teams) pro hlášení stavu systému a logování  |  |
| **Řízení uživatelských přístupů k publikovaným službám** |
| Napojení na externí AAA-servery |   |
| Ověřování uživatelů min. prostřednictvím metod HTTTP basic, HTML form, Certificate, OCSP, CRLDP, Radius, LDAP, Active Directory, NTLM v1/v2, Kerberos, SAML, RSA SerurID, OAM, Tacacs+, místní databáze |   |
| Podpora pro přihlášování k webovým aplikacím pomocí externích serverům  |   |
| Jednorázové heslo - OTP (generování a ověření) |   |
| Podpora CAPTCHA  |   |
| Podpora Google recaptcha v2 |   |
| Přidělování přístupů uživatelů podle metadat v Radius, LDAP a Active Directory |   |
| Modifikace SAML atributů |   |
| Podpora SAML 2.0 a OAuth |   |
| SAML 2.0 a OAuth: |   |
| Nativní schopnost plnit roli SP SP (poskytovatel služeb) a IdP (poskytovatel identit) |   |
| SSO (single-sign-on) prostřednictvím HTML basic, HTML form, NTLM v1/V, Kerberos, SAML |   |
| Cachování uživatelských identit a SSO proxy |   |
| Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS) |   |
| Podpora pro Kerberos ticketing |   |
| PCoIP proxy |   |
| RDP proxy |   |
| Citrix ICA/HDX proxy |   |
| Patching/rewriting (publikování Web aplikací z interní sítě do intranetu/extranet/internetu) pro HTML, JavaScript, CSS, Flash a Java |   |
| Jednotný Webový portál |   |
| Uživatelský aplikační portál se seznamem aplikací podle přístupových práv  |   |
| Podpora L7 ACL (http) |   |
| Dynamický import ACL z AD  |   |
| Dynamická kontrola přístupů |   |
| Network SSL/DTLS VPN |   |
| Samostatný SSL VPN tunel pro každou přístupnou aplikaci |   |
| Možnost „client less“ přístupu  |   |
| Podpora klientských operačních systémů Windows, MAC, Linux, iOS, Android |   |
| Kontrola stavu koncových bodů jako podímka připojení |   |
| Grafický editor pro správu řízení uživatelských přístupů  |   |
| Podpora Microsoft ActiveSync a Outlook Anywhere s client-side NTLM  |   |
| Step-up autentizace |   |
| Podpora forward proxy chaining |   |
| Podpora ADFS proxy a ADFS-PIP protokolu |   |
| Připojení až 500 uživatelů současně. Požadováni jsou konkurenční uživatelé, nikoli pojmenovaní.  |   |

1. **Implementační služby**
	1. V rámci implementace předmětu plnění dodavatel realizuje následující služby, které jsou zahrnuté v ceně dodávky:
2. Zpracování detailního finálního popisu cílového stavu a postupu implementace (včetně plánovaných změn v konfiguraci současné infrastruktury, zejména síťové) a provedení související nezbytné analýzy současného stavu. Výstupem bude prováděcí dokumentace, podle které bude dodavatel řešení implementovat. Prováděcí dokumentace musí být před zahájením implementace výslovně schválena zadavatelem. Prováděcí dokumentace musí respektovat a využívat osvědčené praktiky (tzv. Best Practice) a doporučení výrobců nabízených technologií.
3. Dodávka a implementace předmětu plnění podle schválené prováděcí dokumentace včetně technické podpory a provedení potřebných změn na stávajících systémech.
4. Rozsah implementace musí zahrnout publikaci min. 10 služeb různého charakteru (publikované aplikace (Microsoft RDP, Citrix XenApp), webové aplikace, Microsoft Exchange, VPN apod.) včetně autentizace.
5. Zajištění projektového vedení realizace předmětu plnění.
6. Zpracování provozní dokumentace v rozsahu detailního popisu skutečného provedení popisu činností běžné údržby a činností pro spolehlivé zajištění provozu. Popis činností běžné údržby bude pokrývat minimálně následující oblasti:
* Kontrola a aktualizace firmware a bezpečnostních signatur/aktualizací
* Kontrola systémových a bezpečnostních logů
* Správa požadavků na technickou podporu
1. Zpracování popisu cílového stavu bude zahrnovat analýzu pravidel a nastavení stávajících systémů Checkpoint, Forefront TMG a Netscaler návrh jejich optimalizace a migrace do nového systému.
2. Pro zpracování popisu cílového stavu bude dodavatel organizovat a vést strukturované workshopy a konzultace za účelem vypracování optimálního návrhu řešení na základě požadavků zadavatele.
3. Zpracování materiálů pro školení a provedení školení v rozsahu minimálně 6 hodin dle požadavků (5).
4. Zajištění zkušebního provozu infrastruktury v délce minimálně 2 týdnů včetně technické podpory specialistů na dané zařízení/službu s dostupností specialisty maximálně do 2 hodin od nahlášení požadavku v pracovní den v době od 8h do 17h.
5. Provedení akceptačních testů dle požadavků (7)
6. Předání do plného provozu.
	1. Činnost omezující práci uživatelů musí být prováděny mimo běžnou pracovní dobu úřadu, tj. mimo pracovní dny 7 – 15 hod.
	2. Zadavatel dále požaduje provést minimálně výše implementační práce na dodaných komponentech a případně dalších zařízeních. Dodavatel je dále povinen zahrnout do nabídky veškeré další činnosti a prostředky, které jsou nezbytné pro provedení díla v rozsahu doporučeném výrobci a dle tzv. nejlepších praktik, i v případě, že nejsou explicitně uvedeny, ale jsou pro realizaci předmětu plnění podstatné.
	3. Harmonogram realizace.
7. Dodavatelzajistí projektové vedení po celou dobu realizace zakázky projektovým manažerem. Zadavatel vyžaduje dodržení následujícího harmonogramu plnění – zde jsou uvedeny maximální možné lhůty pro jednotlivé kritické milníky. Údaj D značí datum účinnosti smlouvy. Čísla značí počet kalendářních dnů.

|  |  |  |  |
| --- | --- | --- | --- |
| **Č.** | **Etapa projektu – činnost** | **Zahájení etapy** | **Ukončení etapy** |
| 1 | Předimplementační analýza, zpracování Cílového stavu a zhotovení Prováděcí dokumentace včetně vypořádání připomínek a akceptace Zadavatelem | D | D+45 |
| 2 | Dodávky a implementace | D+45 | D+100 |
| 3 | Školení administrátorů | D+80 | D+110 |
| 4 | Zkušební provoz | D+90 | D+100 |
| 5 | Akceptační testy | D+100 | D+110 |
| 6 | Zahájení plného provozu | D+110 |  - |

1. Dodavatel může dle svého uvážení výše uvedené maximální lhůty trvání zkrátit při dodržení všech částí předmětu plnění a bez snížení kvality dodávaných služeb.
2. Maximální lhůty trvání nesmí Dodavatel při tvorbě detailního harmonogramu prodloužit.
3. Dodavatel uvede potřebnou součinnost Zadavatele pro splnění harmonogramu plnění ve své nabídce.
4. **Požadavky na školení.**
5. Dodavatel zajistí pro školení pracovníků Zadavatele – administrátorů na zařízení a systémy, dodávané v rámci této veřejné zakázky, a to v rozsahu předávané provozní dokumentace. Školení dále zajistí seznámení administrátorů Zadavatele se všemi podstatnými částmi díla v rozsahu potřebném pro provoz, údržbu a identifikaci nestandardních stavů systému a jejich příčin.
6. Školení bude probíhat v sídle Zadavatele, přípustná je forma telekonference.
7. Předpokládá se účast max. 5 administrátorů.
8. **Požadavky na testovací prostředí.**
* Zadavatel nedisponuje testovacím prostředím.
* Vyžaduje-li Dodavatel pro realizaci zakázky testovací prostředí, zahrne do nabídky náklady na jeho vybudování a požadovanou součinnost Zadavatele.
1. **Obecné požadavky na provedení akceptačních testů a přechod do ostrého provozu**
2. Dodavatel navrhne způsob a provedení akceptačních testů. Součástí akceptačních testů musí být pro každou komoditu minimálně:
3. Prokázání kompletnosti dodávky a splnění povinných parametrů a požadavků.
4. Prokázání funkčnosti migrovaných systémů.
5. Prokázání vysoké dostupnosti u řešení, která jsou takto koncipována.
6. Prokázání přiměřených odezev systému při náročnějších operacích.
7. Prokázání aktivací aktivačními klíči či jinými prostředky, je-li aktivace potřebná.
8. Pro každý systém či modul navrhne Dodavatel vhodné doplňující testy a kritéria, kterými bude prokázána bezproblémová funkčnost, bezpečnost a odpovídající výkon a stabilita dodaného řešení.
9. O provedení akceptace a jejím výsledku musí být vyhotoven písemný protokol.
10. Přechodem do ostrého provozu se rozumí okamžik úspěšné akceptace díla včetně vypořádání všech vad a nedodělků.
11. **Požadavky Zadavatele na zajištění provozu**
12. Součástí dodávky bude poskytnutí maintenance, tj. přímého přístupu k podpoře výrobce řešení a nároku na nové verze software/firmware (včetně hlavních) a nároku na bezpečnostní či funkční aktualizace (signatury, definice, sestavy apod.) na dobu 36 měsíců.
13. Zadavatel požaduje poskytnutí záruky 120 dnů.
14. Pro hlášení servisních požadavků zajistí Dodavatel Zadavateli přístup ke svému helpdeskovému systém s on-line přístupem pro kompletní správu požadavků včetně uchování historie požadavků a jejich řešení. Detailní popis helpdeskového systému a jeho obsluhy musí být součástí nabídky. Provozní doba helpdeskového systému musí být minimálně v době 7-17 hod. v pracovních dnech, po dobu 36 měsíců.