Technická specifikace pro projekt „Rozvoj konsolidované IT infrastruktury Policie ČR – ZÁLOŽNÍ CENTRUM“

Policie České republiky provozuje roztříštěnou strukturu infrastrukturní platformy a zdroje pro jednotlivé informační systémy. Tyto informační systémy jsou provozovány na různých platformách hardwarových (různé typy serverů) i softwarových (operační a databázové systémy). Jejich správa je složitá na počet specialistů obslužného personálu a finančně nákladná na zajištění provozu.

K zajištění redukce nákladů na provoz IT infrastruktury se Policie ČR rozhodla konsolidovat provozované informační systémy tak, aby byly odstraněny výše uvedené nedostatky a zároveň byla poskytnuta potřebná flexibilitu při přidělování infrastrukturních zdrojů. Budoucím cílem je stav, kde je koncovým uživatelům poskytována služba infrastrukturních zdrojů a to v měřitelné kvalitě. Prvním krokem pro naplnění budoucího cíle je zajištění robustní infrastrukturní platformy, včetně potřebného SW, což pokrývá předmět této veřejné zakázky.

Z důvodu zajištění vysoké dostupnosti dat provozuje PČR dvě datová centra v geograficky oddělených lokalitách, která jsou funkčně rovnocenná a vzájemně se zálohují.

Projekt „Rozvoj konsolidované IT infrastruktury PČR – ZÁLOŽNÍ CENTRUM“ řeší obnovu části IT infrastruktury v záložní lokalitě a přímo navazuje na projekt připravovaný v rámci Programu švýcarsko-české spolupráce s názvem „Rozvoj konsolidované IT infrastruktury PČR“.

Součástí nabídky uchazeče musí být integrace do SAN infrastruktury bez nutností odpojení zařízení (tzv. HA režim) a taktéž možný upgrade komponent (firmware upgrade). Vzhledem k tomu, že se jedná pouze o doplnění a rozšíření již stávající konsolidované ITC infrastruktury, požadujeme, aby dodavatel plně akceptoval požadavky na již vytvořenou konsolidovanou infrastrukturu a navrhované komponenty byly plně kompatibilní s touto nově budovanou konsolidovanou infrastrukturou. V této souvislosti zadavatel požaduje potvrzení výrobce zařízení pro LAN sítě, že uchazeč je oprávněn instalovat, servisovat a upgradovat zařízení, která souvisí s instalací sítě LAN. Jmenovitě pro sítě SAN i LAN se jedná o zařízení HP 3PAR V800, HP 6600-24G-4XG, HP 7506, HP F1000-EI, HP Blade System C7000, HP Blade Server 460c G6 a G7. Zadavatel dále požaduje prohlášení dodavatele, že nabízené komponenty jsou plně kompatibilní se zařízeními uvedenými v předchozí větě.

Základní bloky projektu – veřejné zakázky

Seznam podle položek technické specifikace veřejné zakázky:

Číslo položky	Název položky	Počet jednotek
Blok 1	**Dodávka HW produktů**	
1.1	Kabinet pro umístění HW komponent (rack)	1 ks
1.2	Serverová police pro blade servery (blade šasi)	1 ks
1.3	Sestava – aplikační blade server x86	4 ks
1.4	Sestava – aplikační blade server x86 s rozšířenou RAM	2 ks
1.5	Sestava – databázový blade server UNIX	2 ks
1.6	Specializované řešení ochrany proti bezpečnostním rizikům a zranitelnostem systémů a aplikací - Systém NG-IPS	1 ks
1.7	Rozšíření diskového pole 3Par	1 ks
Blok 2	**Dodávka SW produktů**	
2.1	Virtualizační SW	12 ks
2.2	SW pro správu HW a poskytování infrastruktury jako služby	1 set
2.3	Ostatní software	Soubor licencí
Blok 3	**Integrační a konzultační služby**	
3.1	Vypracování návrhu architektury a fungování vysoké dostupnosti mezi oběma datovými centry v oblasti konsolidované infrastruktury dle této zakázky a předcházející etapy v primárním centru.	
3.2	Implementační a konfigurační práce spojené s vybudováním konsolidované infrastruktury a začleněním do stávající infrastruktury PČR	

Technická specifikace jednotlivých bloků řešení – veřejné zakázky

Blok 1 Dodávka HW produktů

1.1 Kabinet pro umístění HW komponent (rack)		**1 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Výška	42 U	
Značka – typ	-	
Hloubka	dostatečná pro všechny dodávané komponenty, min. 80 cm	

Provedení	dveře vpředu i vzadu s horizontálním provětráváním	
Příslušenství	racková KVM konzole (max 1U, 17´´monitor, klávesnice, polohovací zařízení)	
	Boční panely	
	2 x PDU (min 40A) pro redundantní připojení zdrojů šasi ke dvěma nezávislým vstupům	
Záruka	min. 3 roky na všechny komponenty s odezvou 4h v místě plnění, pokrytí 24 x 7;	

1.2 Serverová police pro blade servery (blade šasi)		**1 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Provedení	Rackové a 100% kompatibilní s dále specifikovanými blade servery uvedenými pod číslem 1.3 Sestava-aplikační blade server x 86, 1.4 Sestava - aplikační blade server x 86 s rozšířenou RAM a 1.5 Sestava-databázový blade server UNIX. Umožňující společnou instalaci všech dále poptávaných i již provozovaných serverů, tak aby byly zapojeny redundantně všechny LAN i FC porty	
Hloubka vnitřní	min. 14 aktivních pozic pro blade servery poloviční výšky. Aktivní pozice znamená, že při vložení dalšího serveru nebude třeba nic přikupovat a server bude fungovat. Požadavek možno splnit instalací 2 blade šasi.	
Napájení	Hot-plug zdroje pro zajištění redundantního provozu plně osazeného šasí	
Ventilátory	Hot-plug ventilátory pro zajištění redundantního provozu plně osazeného šasí	
Management	redundantní	
LAN konektivita	2 x 10Gb Ethernet modul umožňující HW rozdělení serverových síťových	

	karet, a to každé minimálně na 4 samostatné prezentované serverům, Každý Ethernet modul bude osazen 4 x 1Gb RJ45 a 2 x 10Gb SFP+ modulem	
FC konektivita	2 x Storage Area Network 8 Gb/s interconnect modul (8 externích portů včetně short wave 8Gb SFP, počet interních portů musí odpovídat počtu serverů osaditelných do blade šasi, webové rozhraní pro správu, licence pro všechny porty)	
Vzdálená správa	pomocí LAN (možnost vypnout napájení, 128bitové šifrování, monitorování stavu HW bez nainstalovaného OS) možnost nastavení a ovládání více serverových polic z jednoho místa monitoring a reporting informací o provozní teplotě a příkonu každého serveru nebo police v reálném čase vestavěný display pro snadnou obsluhu integrovaný a jednotný přístup k management procesorům všech serverů v polici single sign-on přístup ke všem zařízením v polici. asset management všech zařízení v rámci police	
Instalace	HW instalace, kompletní zprovoznění a oživení	
Záruka	min. 3 roky na všechny komponenty • zásah do 4 hodin v místě plnění • pokrytí 24 x 7 • pravidelná kontrola stavu HW • vyhotovení reportů o incidentech • podpora při nasazování nových verzí FW a SW • pravidelné konzultace s technickým zástupcem výrobce	

1.3 Sestava – aplikační blade server x86		**4 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Požadavky na CPU dle testů SPEC CPU2006		
SPECint_2006	**min. 43,2**	
SPECfp_2006	**min. 71,2**	
SPECint_rate 2006	**min. 436**	
SPECfp_rate 2006	**min. 357**	
Značka – typ serveru	-	
Provedení	do požadovaného blade šasi	
Procesor	-	
	Min. počet – 2	
Paměť	96 GB RAM DDR3 1333MHz	
Interní úložiště	min. 2 GB USB flash nebo SD karta pro instalaci hypervizoru	
Řadič	HW RAID 0,1; 512 GB Cache	
Síťový adaptér	2 x 10 Gb/s TCP/IP Offload Engine; každý s možností rozdělení na úrovni HW až na 4 virtuální adaptéry	
FC rozhranní	Dvouportový Fibre Channel 8Gb adaptér, SW pro redundantní připojení serveru s MS Windows 2008/2003 k dodávanému diskovému poli	
Monitoring HW	Integrovaný přímo v HW komponentách bez nutnosti instalace agentů do operačního systému	
Vzdálená správa	pomocí LAN (grafická konzole i bez nainstalovaného OS, možnost vypnout napájení, reset systému, klávesnice, myš, 128bitové šifrování, monitorování stavu HW bez nainstalovaného OS SW pro vzdálenou správu musí umožňovat: centralizovanou vzdálenou správu HW a shromažďování informací o konfiguraci a stavu jednotlivých HW komponent serverů (včetně ukládání	

	těchto informací do databáze k dalšímu využití), detekci a zasílání zpráv (minimálně pomocí protokolu SNMP) o chybových stavech	
Kompatibilita	Microsoft Windows 2008/2012, Red Hat EL4, SuSe Linux, VMWare ESX 4.x, 5.x	
Instalace	HW instalace, kompletní zprovoznění a oživení	
Záruka	min. 3 roky na všechny komponenty • zásah do 4 hodin v místě plnění • pokrytí 24 x 7 • pravidelná kontrola stavu HW • vyhotovení report ů o incidentech • podpora při nasazování nových verzí FW a SW • pravidelné konzultace s technickým zástupcem výrobce	

1.4 Sestava – aplikační blade server x86 s rozšířenou RAM		**2 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Požadavky na CPU dle testů SPEC CPU2006		
SPECint_2006	**min. 43,2**	
SPECfp_2006	**min. 71,2**	
SPECint_rate 2006	**min. 436**	
SPECfp_rate 2006	**min. 357**	
Značka – typ serveru	-	
Provedení	do požadovaného blade šasi	
Procesor	-	
	Min. počet – 2	
Paměť	128 GB RAM DDR3 1333MHz	
Interní úložiště	min. 2 GB USB flash nebo SD karta pro instalaci hypervizoru	
Řadič	HW RAID 0,1; 512 GB Cache	

Síťový adaptér	2 x 10 Gb/s TCP/IP Offload Engine; každý s možností rozdělení na úrovni HW až na 4 virtuální adaptéry	
FC rozhranní	Dvouportový Fibre Channel 8Gb adaptér, SW pro redundantní připojení serveru s MS Windows 2008/2003 k dodávanému diskovému poli	
Monitoring HW	Integrovaný přímo v HW komponentách bez nutnosti instalace agentů do operačního systému	
Vzdálená správa	pomocí LAN (grafická konzole i bez nainstalovaného OS, možnost vypnout napájení, reset systému, klávesnice, myš, 128bitové šifrování, monitorování stavu HW bez nainstalovaného OS SW pro vzdálenou správu musí umožňovat: - centralizovanou vzdálenou správu HW a shromažďování informací o konfiguraci a stavu jednotlivých HW komponent serverů (včetně ukládání těchto informací do databáze k dalšímu využití), - detekci a zasílání zpráv (minimálně pomocí protokolu SNMP) o chybových stavech	
Kompatibilita	Microsoft Windows 2008/2012, Red Hat EL4, SuSe Linux, VMWare ESX 4.x, 5.x	
Instalace	HW instalace, kompletní zprovoznění a oživení	
Záruka	min. 3 roky na všechny komponenty • zásah do 4 hodin v místě plnění • pokrytí 24 x 7 • ponechání vadných disků u zadavatele • pravidelná kontrola stavu HW • vyhotovení report ů o incidentech • podpora při nasazování nových verzí FW a SW • pravidelná konzultace s technickým zástupcem výrobce	

1.5 Sestava – databázový blade server UNIX		**2 ks**
Položka	Požadováno	
Značka – typ serveru	-	
Provedení	do požadovaného blade šasi	
Procesor	64 Bit RISC/EPIC Processor min. 8 jader (2 GHz)	
	Počet osaditelných CPU: min. 2 ks	
Paměť	48 GB RAM DDR3 1333MHz	
Interní úložiště	2x 146GB 6G SAS 15krpm	
Řadič	HW RAID 0,1; 512 GB Cache	
Síťový adaptér	4 x 10 Gb/s TCP/IP Offload Engine; každý s možností rozdělení na úrovni HW až na 4 virtuální adaptéry	
FC rozhraní	Dvouportový Fibre Channel 8Gb adaptér, SW pro redundantní připojení serveru k dodávanému diskovému poli	
Vzdálená správa	pomocí LAN (grafická konzole i bez nainstalovaného OS, možnost vypnout napájení, reset systému, klávesnice, myš, 128bitové šifrování, monitorování stavu HW bez nainstalovaného OS SW pro vzdálenou správu musí umožňovat: centralizovanou vzdálenou správu HW a shromažďování informací o konfiguraci a stavu jednotlivých HW komponent serverů (včetně ukládání těchto informací do databáze k dalšímu využití), detekci a zasílání zpráv (minimálně pomocí protokolu SNMP) o chybových stavech	
OS	UNIX včetně clusterových licencí kompatibilních s používaným HP-UX SW	
Virtualizace	V rámci fyzického serveru systém umožní provozování virtuálních serverů, každý s vlastní instancí OS, host name a IP adresou. Virtualizační technologie musí být uznaná jako	

	„hard partitioning“ pro produkty Oracle	
Instalace	HW instalace, kompletní zprovoznění a oživení	
Záruka	min. 3 roky na všechny komponenty • zásah do 4 hodin v místě plnění • pokrytí 24 x 7 • pravidelná kontrola stavu HW • vyhotovení report ů o incidentech • podpora při nasazování nových verzí FW a SW • pravidelné konzultace s technickým zástupcem výrobce	

1.6 Specializované řešení ochrany proti bezpečnostním rizikům a zranitelnostem systémů a aplikací - systém NG-IPS

Pro ucelení systému zabezpečení perimetru a demilitarizované zóny a vybraných virtuálních sítí je nutné nasadit in-line NG-IPS na datové linky. NG-IPS musí za minimálního přidaného zpoždění provádět inspekci komunikace a automaticky blokovat závadný síťový provoz. To vše za poskytování přehledných informací bezpečnostním analytikům správy počítačové sítě a reportování do nadřízené SIEM aplikace.

Hlavních požadované služby od systému NG-IPS:

1. ***Standardní set funkcí IPS první generace*** – poskytovat transparentní ochranu proti zranitelnostem a exploitům se začleněním inspekce na cestě komunikace (in-line).
2. ***Znalost a viditelnost do aplikace*** – schopnost identifikovat nepřátelské aplikace a prosazovat bezpečnostní politiky na aplikační vrstvě nezávisle na použitém portu či protokolu.
3. ***Kontextové povědomí –*** schopnost zahrnout do rozhodování o blokování informace z vnějších zdrojů a aplikovat rozhodnutí s přihlédnutím ke geografické lokaci partnera síťové transakce, jeho reputaci a možným informacím z adresářových služeb.
4. ***Povědomí o obsahu*** – schopnost kontrolovat a třídit příchozí a odchozí soubory, příkazy a celkově rozumět obsahu s hyperlinkovou strukturou.
5. ***Připravenost na vývoj v bezpečnostní oblasti*** – podporovat možnosti upgrade na nové technologie, které se budou zabývat příštími hrozbami.

Obecné parametry a vlastnosti požadované od NG-IPS řešení

- Ochrana proti bezpečnostním rizikům a zranitelnostem systémů a aplikací

- Ochrana před DoS a DDoS
- Rovnocenná podpora IPv4 a IPv6
- Ochrana reputační službou (Rep DV) s geografickým systémem rozpoznání zdroje
- Široká a přesná bezpečnost s limitováním falešných poplachů
- Integrace funkcí Next-Gen Firewallů – rozpoznávání a viditelnost do aplikací
- Podpora inspekce v heterogenním prostředí bez ohledu na výrobce síťové infrastruktury
- Podpora inspekce ve virtualizovaném prostředí
- Možnost řešení s vysokou dostupností pro zamezení výpadku sítě
- Škálovatelný výkon a minimální přidané zpoždění
- Intuitivní ovládání - snadné k naučení a spolehlivé k využívání
- Dohledová konzole pro řízení NG-IPS v redundantním řešení nebo pro virtuální prostředí vSphere
- Technická podpora 24*7*365 v základu po dobu 3 let

Popis požadavků pro systém NG-IPS s výkonem minimálně 700Mbit/s:

Systém NG-IPS		**1 ks**
Požadovaná funkcionalita	Specifikace požadavku	**Nabízená hodnota uchazečem**
Agregovaná propustnost NG-IPS při plném zatížení se všemi zapnutými filtry ověřená nezávislou testovací organizací ICSA Labs, Tolly Group nebo NSS	min. 700 Mbit/s	
Minimální celkový počet segmentů pro in-line inspekci (může být kombinace 10/100/1000 Base-T a SFP)	10 x 1GE segmenty	
Zařízení musí podporovat typy SFP portů bez nutnosti externích převodníků	1000 Based UTP SFP	
	1000 Based-SX SFP	
	1000 Based-LX/LH SFP	
Maximální zpoždění NG-IPS při plném zatížení se všemi zapnutými filtry, ověřeno nezávislou testovací organizací ICSA Labs, Tolly Group nebo NSS	< 80 mikrosekund	
Počet inspektovaných spojení v reálném čase	min. 6 000 000	
Množství nově otvíraných spojení za sekundu, inspektovaných na NG-IPS	min. 110 000 spojení/s	
Podpora SYN-Proxy	min. 300 000 spojení/s	
Požadovaná inspekce transportních systémů	VLAN 802.1Q, VLAN QinQ 802.1ad, GRE, MPLS, IPv4, IPv6	
Redundantní Hot-Swap napajecí zdroj v základu	PODPORUJE	

Vysoká dostupnost v režimu	Active-Active	
	Active-Passive	
Podpora L2 Fallback v případě interní chyby software, nebo zahlcení systému	PODPORUJE	
Podpora Zero Power High Availability (ZPHA) pro optické i metalické porty	PODPORUJE	
Součástí dodávky je řešení pro ZPHA metalické porty – 5 segmentů	PODPORUJE	
Podpora asymetrického provozu (zařízení nemusí v rámci inspekčního segmentu vidět do obou směrů TCP spojení - typicky u Link Agregace) a podpora asymetrické inspekce (rozdílná konfigurace NG-IPS bezpečnostního profilu pro rozdílný směr v rámci inspekčního segmentu)	PODPORUJE	
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne neefektivní filtr, který může způsobit zahlcení systému	PODPORUJE	
Podpora Hitless upgrade Operačního systému NG-IPS bez nutnosti plánování odstávky systému, podpora Hitless reboot.	PODPORUJE	
NG-IPS musí obsahovat filtry/signatury popisující	exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií	
Podpora automatické aktualizace filtrů/signatur a databáze IPv4, IPv6 a DNS jmen systémů na internetu s poškozenou reputací Automatická aktualizace musí být prováděna minimálně 2x týdně.	PODPORUJE	
Databáze IPv4, IPv6 a DNS jmen musí umožňovat třídění podle země původu IP adresy, potencionální nebezpečnosti a typu zjištěné nebezpečnosti	PODPORUJE	
Podpora aplikace pro psaní zákaznických filtrů	PODPORUJE	
Podpora importu komunitních filtrů/signatur Snort	PODPORUJE	
Minimální set požadovaných akcí NG-IPS po zásahu filtru: Block (Drop Packet), Block (TCP Reset), Permit, Trust, Notify, Trace (Packet Capture), Rate Limit and Quarantine	PODPORUJE	

Podpora translace 802.1Q VLAN ID v rámci bezpečnostního segmentu, pro inspekci na vnitřních VLAN bez potřeby zapojovat zařízení do všech fyzických cest kde je požadována inspekce provozu.	PODPORUJE	
NG-IPS musí umět detekovat a blokovat útoky průzkumných aktivit	PODPORUJE	
NG-IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na NG-IPS	PODPORUJE	
NG-IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host“ jako je spyware, phishing nebo Botnet C&C	PODPORUJE	
NG-IPS musí umět rozpoznávat provoz na základě Geo-lokace a umět blokovat nebo aplikovat rozdílné bezpečnostní sety na provoz dle detekce geografického původu zdrojové IP adresy	PODPORUJE	
Možnost omezování a řízení šířky pásma pro streamovaná multimedia a P2P sítě	PODPORUJE	
NG-IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii	PODPORUJE	
NG-IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	PODPORUJE	
Podpora SNMPv3, privátní MIB, Syslog-NG, SNMP Trap	PODPORUJE	
NG-IPS musí být spravovatelné z nabízeného centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole), ale v případě jeho výpadku musí umožnit konfigurační změny i bez dohledového nástroje prostřednictvím webového/SSL rozhraní NG-IPS	PODPORUJE	

Popis požadavků pro řídicí systém (dohledovou konzoli) pro dodané NG-IPS:

Požadováno	Nabízená hodnota uchazečem
Centrální dohledová konzole musí být schopna spravovat více NG-IPS – minimálně 10	
Centrální dohledová konzole musí mít možnost obsluhy z operačních systémů Linux, Microsoft a Mac-OS	
Centrální dohledová konzole musí být v redundantním provedení s plnou odolností proti výpadku libovolné komponenty nebo musí být ve virtuálním provedení pro prostřední VMWARE vSphere	
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	
Centrální dohledová konzole musí být schopna udržovat a spravovat Operační systém NG-IPS	
Centrální dohledová konzole musí podporovat minimálně 100 milionů záznamů v Event logu.	
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu pro kategorie All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report	
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, XML apod.	
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních profilů pro uživatele a skupiny uživatelů.	
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro dohledání uživatelů v Event logu.	
Centrální dohledová konzole musí podporovat Syslog NG (syslog na TCP, včetně podpory šifrování)	

1.7 Rozšíření kapacity stávajícího diskového pole a povýšení funkcionality

Z důvodu maximálního využití stávající technologie, tedy i využití investovaných prostředků, požadujeme jako datový prostor pro požadované řešení využít stávající pole HP 3PAR T800. V rámci tohoto projektu požadujeme jak kapacitní upgrade tohoto pole, tedy navýšení hrubé kapacity pole, tak funkční upgrade, tedy dodání příslušných licencí

Rozšíření kapacity stávajícího diskového pole a povýšení funkcionality		**1 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Provedení	Diskové magazíny (HDD) do stávajícího diskového pole HP 3PAR T800 včetně SW	

	licence pro správu požadované kapacity	
Diskový prostor č.1 - kapacita	Požadováno 4,8 TB hrubé kapacity	
Diskový prostor č.1 - parametry HDD	300 GB FC 15k	
Diskový prostor č.2 - kapacita	Požadováno 16 TB hrubé kapacity	
Diskový prostor č.2 - parametry HDD	1 TB SATA 7,2k	
Povýšení funkcionality – požadované licence	SW HP 3PAR RemoteCopy licence pro dodávanou kapacitu SW pro integraci s vSphere a Vcenter serverem	
Instalace	HW instalace, kompletní zprovoznění a oživení	
Záruka	min. 3 roky na všechny komponenty se službou zajišťující: - Závazek vyřešení hardwarového problému do šesti hodin - Okamžitou odezvu/zásah pro kritické problémy - Vyhrazené náhradní díly - Přidělený tým zákaznické podpory - Přiděleného manažera podpory - Přiděleného HW a SW specialistu - Plán technické podpory - Technické ověření vysoké dostupnosti diskového pole - Aktualizace storage Micro-code - Elektronickou podporu - Aktualizaci softwaru - Kontrolu provozních podmínek dodavatel nepožaduje vrácení vadných HDD	

Blok 2 - Dodávka SW produktů

2.1 Virtualizační SW		**12 ks**
Položka	**Požadováno**	**Nabízená hodnota uchazečem**
Provedení	software – licence na CPU	
Parametry	funkce automatického vyvažování výkonnosti mezi fyzickými servery. Přesun virtuálních serverů za běhu podle jejich vytížení a výkonnostní potřeby HW. Automatický náběh virtuálních serverů v případě výpadku fyzického serveru	
	Implementovaná správa virtualizačního systému z jednoho centra, zařazení do stávající správy virtualizačního řešení, která je realizována produktem VMware vCenter Server.	
	funkce vyšší dostupnosti - virtuální server může mít spuštěnu záložní kopii na dalším HW serveru. V případě havárie primárního HW serveru dojde k automatické bezvýpadkové aktivaci záložní kopie	
	funkcionalita virtuálního distribuovaného switche	
Instalace	SW instalace, kompletní zprovoznění a konfigurace	
Záruka	min. 1 rok SW podpora produktu	

2.2 SW pro správu HW a poskytování infrastruktury jako služby		**1 set**
Položka	Požadováno	**Nabízená hodnota uchazečem**
Provedení	Software	
Parametry, funkce a vlastnosti softwaru	Správa nejen samotného šasi, jeho zdrojů, popř. ventilátorů, ale i všech ostatních instalovaných prvků – serverů, ethernet i FC switchů	

	integrovaná podpora pro správu a dohled virtuálních serverů instalovaných na platformě VMware vSphere (včetně integrace s vCenter) a MS Hyper-V (včetně integrace s MS SCVMM)	
	ukládání informací do lokálně umístěné db MS SQL (samotná db bude na SQL serveru v lokalitě, ne na lokálních discích serveru, kde bude instalován sw pro vzdálenou správu)	
	možnost instalovat instanci serveru do každého datového centra a jednoho serveru, co by řídícího	
	možnost instalace v HA režimu	
	řízení přístupových práv k centrální části SW a k management nástrojům pomocí účtů Active Directory domény	
	jediné plně grafické rozhraní pro správu všech instalovaných komponent (servery, switche, zdroje, ventilátory) včetně možnosti přechodu do plně grafické konzole jednotlivých serverů	
	Vytváření a uchovávání definic „logických serverů“, které pak bude možno spustit ve virtuálním prostředí nebo na fyzickém serveru. Tyto definice logických serverů pak musí být přenositelné z jednoho fyzického serveru na druhý tak, aby šla jednoduše přesunout zátěž na server s jinou HW konfiguraci	
	SW musí zajistit tzv. drag&drop správu „logických serverových profilů“ a jejich přenesení na jakýkoliv fyzický nebo virtuální server bez dopadu na nastavení LAN a SAN infrastruktury mimo serverovou polici (tj. beze změn na top of rack prvcích nebo patřeních prvcích)	
	logický serverový profil musí minimálně řešit definici MAC a WWN pro servery (tzv. virtualizaci LAN a SAN rozhraní), připojení k stávající LAN (stačí definice VLAN a port mirroring) a SAN (včetně FC boot parametrů) infrastruktuře	
	Zobrazení a aktivní správa virtuálních a fyzických serverů z jediné konzole, stejně jako správu uložených definice logického serverového profilu	

	Podpora vytváření „seznamu IT zdrojů“ na úrovni fyzických i virtuálních serverů, fyzických i virtuálních datových úložišť (storage), síťových zdrojů (např. VLAN), image OS/aplikace.	
	Vytváření standardních předpřipravených instalací, které jsou přístupné přes samoobslužný portál jako automatické instalace. umožnuje distribuované nasazení	
	SW musí umožnit standardizaci IT na úrovni „vzorů“ využívajících prvků propagovaných v „seznamu IT zdrojů“	
	Definování vzorů v integrovaném grafickém prostředí a automatické vytvoření scriptů k zavádění těchto vzorů	
	Možnost přiřazení účetní/finanční hodnoty pro jednotlivé „vzory“, resp. pro jednotlivé „IT zdroje“ využité v daném „vzoru“	
	Rozhraní umožňující integraci do stávajících nástrojů a procesů, např. řízení změn, servisní katalog	
	Možnost jednoduchého DR řešení pro fyzické i virtuální servery mezi dvěma lokalitami pro nekritické procesy bez využití clusterových služeb	
	integrace s softwarem HP System Insight Manager používaným nyní pro HW dohled x86 infrastruktury	
Instalace a doplňkové služby	SW instalace, kompletní zprovoznění a konfigurace včetně těchto služeb: • předinstalační příprava a konzultace, kontrola prostředí, příprava konfigurace • kompletní instalace HW a kompletní instalace SW pro správu • zahrnutí do sw pro vzdálenou správu stávajcího prostředí x86 serverů • integrace stávající blade infrastruktury HP c7000 a BL460 do nabízeného SW pro vzdálenou správu • firmwarové upgrady HW • komplexní systémová kontrola pro SW min. jednou ročně • pravidelná proaktivní kontrola kompatibility prostředí (proaktivní notifikace nových, testovaných firmwarů a ovladačů) • konfigurace a customizaci	

	celého řešení	
Záruka	min. 3 roky na všechny komponenty se službou zajišťující: • Podpora Software - okamžitá odezva pro kritické závady, ve všech ostatních případech odezva 2 hodiny, • Přidělený tým zákaznické podpory (přidělený manažer podpory, přidělený HW specialista, přidělený SW specialista), • Pravidelné plánování podpory a činností dle evidence v technickém plánu, • Provozní porady čtvrtletně, • Report přehled aktivit technické podpory čtvrtletně, • Prověření stavu systému (pro servery) ročně, • Analýza operačního systému a správa opravných modulů čtvrtletně, • Elektronická podpora, ucelený zdroj elektronických informací, nástrojů a služeb i nástroje samoobslužné podpory, fóra a také přístup k nejúplnější více-dodavatelské, multi-platformní databázi IT informací, • Zrychlené eskalační procesy a elevace problémů, • Vyhrazené náhradní díly, • Flexibilní nahlášení závady (telefonicky, e-mail, web), • Zaškolení obsluhy pro základní správu pořízeného SW • Asistence při vytváření plánu pro budoucí pokročilá školení	

2.3 Ostatní SW		**Soubor licencí**
položka	Požadováno	
Provedení	software – licence, poslední aktuální revize k datu soutěže	
Parametry	9x Microsoft SQLSvrEntCore OLP 2 Lic NL Gov CoreLic Qlfd (2core licence)	
	6 x Microsoft OS Windows Server (každá licence musí obsahovat neomezený počet virtuálních licencí)	

	2 x licence pro web SW Microsoft SharePoint Server Enterprise Edition	
Instalace	SW instalace, kompletní zprovoznění a konfigurace	

Blok 3 Integrační a konzultační služby

Zadavatel dále požaduje, aby součástí dodávky byly i související služby, které povedou k naplnění cílů uvedených na úvod technické specifikace, konkrétně se jedná o:

3.1 Vypracování návrhu architektury a fungování vysoké dostupnosti mezi oběma datovými centry v oblasti konsolidované infrastruktury dle této zakázky a předcházející etapy v primárním centru

- Vypracování návrhu architektury konsolidované infrastruktury v záložním datovém centru, včetně detailního technického projektu řešení v záložní lokalitě
- Vypracování návrhu architektury a fungování vysoké dostupnosti mezi oběma datovými centry v oblasti konsolidované infrastruktury dle této zakázky a předcházející etapy v primárním centru.

3.2 Implementační a konfigurační práce spojené s vybudováním konsolidované infrastruktury a začleněním do stávající infrastruktury PČR

- Vypracování detailního technického projektu pro řešení specializované ochrany proti útokům
- Technický projekt začlenění dodaných komponent do ICT prostředí Policie ČR
- Fyzická instalace dodaných komponent do prostředí záložního centra (případně i primárního centra na základě schválného návrhu architektury a technického projektu)
- Oživení dodaných komponent
- Instalace SW
- Konfigurace komponent (HW, SW) dle technického projektu
- Nastavení prostředí v primární i záložní lokalitě pro vytvoření vysoké dostupnosti
- Integrace se stávajícím prostředím ICT Policie ČR (zejména oblast zálohování, dohledů infrastruktury)
- Provedení testů definovaných v technické projektu
- Dokumentace prostředí