Prováděcí smlouva č. PPR-2499-9/ČJ-2022-990656

k Rámcové dohodě č.j PPR-17787-13/ČJ-2021-990656

Smluvní strany:

Česká republika – Ministerstvo vnitra

Sídlo:	Nad Štolou 936/3, PSČ 170 34, Praha
IČ:	00007064
DIČ:	CZ00007064
Zastoupená:	plk. Mgr. Pavlem Osvaldem, ředitelem Ředitelství pro podporu výkonu služby Policejního prezidia České republiky
Bankovní spojení:	Česká národní banka, Praha 1 č.ú. 5504881/0710
Korespondenční adresa:	Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, poštovní schránka 62/ ŘPVS, 170 89 Praha 7

(dále jen „Objednatel“)

a

TAKTIK, s.r.o.

Sídlo:	Eberlova 1472/9, 155 00, Praha 5
IČ:	285 22 869
DIČ:	CZ28522869
Zastoupená:	[redacted] jednatelem
Bankovní spojení:	Komerční banka a.s. č.ú. 115-2635940257/0100
Korespondenční adresa:	Kubrův dvůr, Červeňanského 2825/11, 155 00, Praha 5

(dále jen „Dodavatel“)

(společně dále také jen „Smluvní strany“, nebo jednotlivě „Smluvní strana“)

uzavřely tuto Prováděcí smlouvu (dále jen „Prováděcí smlouva“) k Rámcové dohodě PPR-17787-13/ČJ-2021-990656 ze dne 22.11.2021 (dále jen „Rámcová dohoda“) v souladu s ustanoveními zákona č. 89/2012 Sb., občanský zákoník, (dále jen „občanský zákoník“) a zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ) k veřejné zakázce s názvem Dodávka, implementace a technická podpora NG Firewallů ČJ-2021-990656

1. PŘEDMĚT SMLOUVY

1.1. Předmětem této Prováděcí smlouvy je závazek Dodavatele poskytnout Objednateli plnění v souladu se specifikací uvedenou v Příloze č. 1 této Prováděcí smlouvy (dále též jen „Plnění“).
Jmenovitě jde o dodávku a implementaci 4 ks NG FW a 1ks SW pro správu FW včetně jednoleté podpory (Plnění A specifikované v Příloze č. 1) a konfigurační a konzultační práce v rozsahu max. 20 MD (Plnění C specifikované v Příloze č. 1).

1.2. Objednatel se zavazuje řádně dodané Plnění převzít a zaplatit za něj dohodnutou cenu, a to způsobem definovaným v této Prováděcí smlouvě a v Rámcové dohodě.

2. CENA

2.1. Celková cena za Plnění dle této Prováděcí smlouvy činí 16 676 000,- Kč bez DPH. Cena za jednotlivé položky Plnění je uvedena v Příloze č. 2 této Prováděcí smlouvy.

2.2. V případě Plnění C je Dodavatel oprávněn vystavit fakturu za poskytnuté dílčí plnění, a to vždy za uplynulé kalendářní čtvrtletí, na základě dílčího akceptačního protokolu.

3. TERMÍN PLNĚNÍ A MÍSTO PLNĚNÍ

3.1. Prováděcí smlouva bude uzavřena na dobu jednoho (1) roku ode dne účinnosti této smlouvy.

3.2. **Plnění A** (tj. A.1 a A.2): bude realizováno do 16 týdnů ode dne účinnosti prováděcí smlouvy. Technická podpora NG Firewallů bude zahájena ode dne podepsání akceptačního protokolu oběma smluvními stranami, a to na dobu 12 měsíců.

Plnění C bude zahájeno nejdéle do 5 dnů ode dne uvedeného v dílčí objednávce, pokud nebude v objednávce stanoveno jinak.

3.3. Místem plnění je Bubenečská 20, Praha 6, Dejvice a Strojnická 27, Praha 7, Holešovice

3.4. Adresa Objednatele pro doručení daňového dokladu je Policejní prezidium ČR, Ředitelství pro podporu výkonu služby, Strojnická 27, poštovní schránka 62/ŘPVS, 170 89 Praha 7

4. OSTATNÍ UJEDNÁNÍ

4.1. Veškerá ujednání této Prováděcí smlouvy navazují na Rámcovou dohodu a podmínkami uvedenými v Rámcové dohodě se řídí, tj. práva a povinnosti či skutečnosti neupravené v této Prováděcí smlouvě se řídí ustanoveními Rámcové dohody.

4.2. Tato Prováděcí smlouva nabývá účinnosti dnem uveřejnění v registru smluv dle zákona č.340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv).

4.3. Tato Smlouva je podepsána oběma Smluvními stranami elektronickým podpisem.

4.4. Nedílnou součástí této Smlouvy jsou následující přílohy:
Příloha č. 1 – „Specifikace předmětu plnění“
Příloha č. 2 – „Rozpočet ceny“

V Praze dne …….

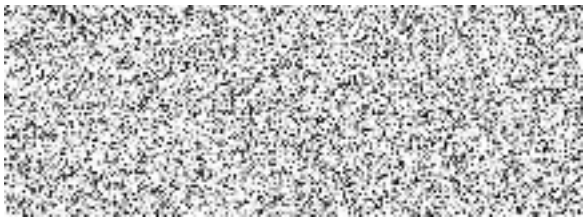
Objednatel:

……..
Ministerstvo vnitra – Česká republika

Zástupce: plk. Mgr. Pavel Osvald
ředitel Ředitelství pro podporu výkonu služby
Policejního prezidia České republiky

V Praze dne …….

Dodavatel:



TAKTIK, s.r.o.

Zástupce [redacted]ednatel

Specifikace předmětu plnění

Plnění A:

Předmětem dodávky plnění A (tedy plnění A1 a A2) dle Prováděcí smlouvy je:

Plnění A.1:

- Dodání 4 ks NG Firewallů (2 HA instalace do 2 lokalit), které **splňují požadavky uvedené v následující tabulce.** Dodaná zařízení budou nová, která nebyla dříve dodána jinému koncovému uživateli.

Plnění A.2.:

- Dodání potřebného 1 ks SW pro správu Firewallů, které **splňuje požadavky uvedené v následujících tabulkách.**

Společné pro plnění A.1 a A.2:

- Implementace, jejímž výstupem je analýza nasazení a oživení a nastavení zařízení a SW pro jeho správu dle této analýzy tak, že **plní požadované funkce dle požadavků v zadávací dokumentaci.**
- Technická podpora pro NG Firewally a SW pro správu na období 12 měsíců.

Specifikace NG Firewallu (Plnění A.1):

Požadovaná funkcionalita/vlastnost	**Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)**	**Doplní Účastník dle nabízeného zařízení**
Typ zařízení	Bezpečnostní zařízení typu Next-generation firewall (dále jen „NGFW“) musí být jako celek složen z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS, AV, Anti-Spyware, databází pro URL kategorizaci, sandbox definic apod.	Palo Alto Networks PA-5250 včetně předplatných Threat Prevention, Wildfire, DNS a URL filtering vč. centrální správy (Palo Alto Networks Panorama) ve formě virtuálního stroje pro VMware
Počet zařízení	Počet odpovídající zajištění HA řešení vždy v rámci jedné lokality a v rámci dvou lokalit (celkem pro 2 lokality), min. 4 zařízení	2 ks PA-5250 v každé lokalitě (4ks celkem)
Formát zařízení	HW appliance do racku, rozměrově kompatibilní s 19“ rozvaděčem, max. 3U	Výška zařízení 3U
HW appliance musí obsahovat 2 nezávislé redundantní zdroje AC 230V s podporou hotswap	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
Počet 10GbE SFP+ portů pro data	Min. 16, včetně osazení 10GE SFP+ moduly	16ks 10GbE portů osazených SFP+ moduly
Počet 40GbE/100GbE QSFP28 portů pro data	Min. 4, včetně osazení moduly 2x40GE LR4 QSFP+ 10 km a 2x100GE LR4 QSFP28 10 km	4ks 40G/100G QSFP28 portů osazených moduly 2x40GE LR4 QSFP+ 10 km a 2x100GE LR4 QSFP28 10 km
Počet portů pro management min 1GbE	Min. 1	2x 10/100/1000 Mbit
Dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	Ano
Počet portů pro zapojení HA	Min. 2	3 porty pro HA
Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění	ANO	Ano
Všechny parametry propustnosti musí dodavatel uvádět pro multiprotokolový datový provoz (Mix různých aplikací a protokolů)	ANO	Ano
Propustnost	Min. 35 Gbps	37,3 Gbps
Propustnost při plné aplikační kontrole a zapnutí všech dostupných signatur IPS, AV a logování	Min. 22 Gbps	23 Gbps
Maximální počet souběžných spojení	Min. 8 000 000	8 000 000
Počet nových spojení za sekundu	Min. 380 000	392 000
Funkce režimu HA v módu Active-Active složeného alespoň ze dvou zařízení	ANO	Ano
Funkce režimu HA v módu Active-Pasive složeného alespoň ze dvou zařízení	ANO	Ano
V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes NGFW	ANO	Ano
Funkce režimu HA clusteringu, využitelného pro případné dodatečné zvýšení propustnosti i v geograficky oddělených lokalitách	ANO	Ano
Funkce provedení HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy	ANO	Ano
Součástí dodávky musí být potřebná kabeláž pro konfiguraci HA v maximálním podporovaném režimu (metalické propojení min. CAT6 nebo optické propojení včetně modulů v maximální dostupné rychlosti)	ANO	Ano
Plná podpora IPv4 i IPv6	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
Požadována možnost zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	Ano
Funkce překladů adres typu Static NAT, Dynamic NAT, PAT, NAT64, NPTv6	ANO	Ano
Funkce směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBR (Policy Based Routing)	ANO	Ano
PBR (Policy Based Routing) musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel.	ANO	Ano
Funkce sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou pomocí protokolu 802.3ad (LACP)	ANO	Ano
Funkce VLAN (802.1Q)	ANO, min. 4094 VLAN	Ano, 4094 VLAN
Podpora virtuálních kontextů	Min. 25 (Pokud se licencuje na počet, min. 25 musí být součástí nabídky).	Ano, podpora až 125 virtuálních kontextů. 25 virtuálních kontextů je součástí nabídky.
Funkce VPN typu site-to-site pomocí protokolu IPSec a Remote Access VPN pomocí protokolu IPSec nebo SSL (TLS, DTLS) bez licenčního omezení počtů tunelů nebo současně připojených uživatelů	ANO	Ano
Propustnost VPN	Min. 16 Gbps	19 Gbps
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování	ANO	Ano
GUI musí obsahovat offline kontextovou nápovědu.	ANO	Ano
Jednotlivé HW appliance musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu a čtení logových záznamů bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování	ANO	Ano
Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro čtení a konfiguraci všech nastavení, týkajících se bezpečnostních a dalších pravidel i rozhraní a směrování	ANO	Ano
Jednotlivé HW appliance musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash disku	ANO	Ano
Funkce autentizace a autorizace administrátorů pomocí protokolů LDAP, Radius, TACACS+, Kerberos a osobním certifikátem	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	Ano
NGWF musí podporovat nativní nástroj pro odchycení provozu	ANO	Ano
Podpora správy NGFW z administrátorských stanic s OS Windows a macOS	ANO	Ano
Management NGFW musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	Ano
Součástí dodávky musí být nástroj, určený pro analýzu a zjednodušení převodu L3/L4 pravidel na pravidla L7. Tento nástroj nemusí být součástí NGFW	ANO	Ano
NGFW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	Ano
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	Ano
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	Ano
Funkce identifikace aplikací napříč všemi porty/protokoly	ANO	Ano
Funkce identifikace aplikací na nestandardních portech	ANO	Ano
Identifikace aplikace musí probíhat přímo ve NGFW	ANO	Ano
Funkce detekce a zabránění aplikaci měnit porty, tzv. port-hopping	ANO	Ano
Funkce řízení neznámého provozu	ANO	Ano
Funkce tvorby uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	Ano
Funkce vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	Ano
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	Ano
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	Ano
Možnost automatického přesunu uživatele do jiné skupiny na základě bezpečnostního incidentu vztahujícímu se k danému uživateli, bez nutnosti manuální intervence	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontrolér	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
Funkce získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno přes webový formulář – Captive Portal	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno z VPN agenta	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno z NAC zařízení (přes XML nebo API)	ANO	Ano
Funkce získávání vazby IP adresa-uživatelské jméno z X-Forwarded-For (XFF) hlaviček	ANO	Ano
Funkce kontroly klientských stanic v pravidelných intervalech přes Windows Management Instrumentation (WMI) nebo NetBIOS aby zjistil, jestli je vazba IP adresa-uživatelské jméno pořád platná	ANO	Ano
Funkce dešifrování odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	Ano
Funkce dešifrování příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	Ano
Funkce dešifrování Secure Shell (SSH proxy) a kontroly tunelované aplikace	ANO	Ano
Dešifrovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	ANO	Ano
Funkce dešifrování za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	Ano
Funkce dešifrování protokolu TLS verze 1.3	ANO	Ano
Funkce přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následně přepošle čistě přefiltrovaná data zpět do NGFW (tzv. decryption broker)	ANO	Ano
Funkce přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu	ANO	Ano
Funkce umožňující odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem HTTP, HTTPS, SMTP, SMTPS, IMAP, IMAPS, FTP a SMB	ANO	Ano
Sandbox systém musí být od stejného výrobce jako je NGFW, ale nemusí být HW součástí NGFW	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý	ANO	Ano
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze, pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	ANO	Ano
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C	ANO	Ano
Sandbox musí podporovat analýzu vzorku na operačním systému instalovaném přímo na hardwaru, tzn. ne ve virtuálním prostředí	ANO	Ano
Sandbox musí podporovat operační systémy Windows, Linux, MacOS a Android	ANO	Ano
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní FW	ANO	Ano
Aktualizace zero-day signatur musí být instalována do FW v reálnem čase čili s nulovou prodlevou	ANO	Ano
Funkce detekce a zablokování stažení neznámého škodlivého souboru v reálném čase, bez toho, aby byl doručen na koncový bod	ANO	Ano
Funkce detekce neznámých vzorků přímo na firewallu bez nutnosti napojení na externí zařízení nebo službu	ANO	Ano
Funkce zavedení tzv. pozitivního bezpečnostního modelu – povolení pouze vybraných aplikací a zákaz všech ostatních aplikací, včetně neznámého provozu	ANO	Ano
NGFW musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	Ano
Funkce tvorby uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	Ano
NGFW musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	Ano
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích – SMTP, POP3, IMAP, HTTP, HTTPS, HTTP/2, FTP a SMB	ANO	Ano
Funkce tvorby uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	Ano
Funkce umožňující zablokování útoku využívajícího známá C&C centra i v případě, že	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
je provoz šifrován a není možné provádět SSL dekrypci		
NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; NGFW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	Ano
Funkce importu SNORT signatur	ANO	Ano
NGFW musí pro přístup ke kritickým aplikacím, poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci; tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla	ANO	Ano
Funkce umožňující zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných než povolených URL kategorií, pro zabránění phishingu	ANO	Ano
Funkce ochrany proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	Ano
Funkce analýzy DNS dotazu tzv. Sinkhole metoda, která na dotaz malware DNS URL vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane	ANO	Ano
NGFW musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase	ANO	Ano
NGFW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa a uživatelská identita	ANO	Ano
Funkce umožňující prioritizaci provozu a omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)	ANO	Ano
Funkce prioritizace provozu na základě DSCP	ANO	Ano
Funkce prioritizace provozu na základě Identifikované aplikace	ANO	Ano
NGFW musí obsahovat nativní podporu pro využívání databáze URL	ANO	Ano
URL databáze musí být od stejného výrobce jako je NGFW	ANO	Ano
Funkce umožňující použití URL kategorii v definici bezpečnostního pravidla	ANO	Ano
Funkce vytváření uživatelsky definovaných URL kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	Ano

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	ANO	Ano
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	Ano
Možnost požádat o rekategorizaci nevhodně zařazených URL přímo v grafickém rozhraní NGFW bez nutnosti kontaktování technické podpory	ANO	Ano
NGFW musí mít možnost rozšíření o funkcionalitu SD-WAN – detekce kvality WAN připojení s automatickou volbou nejlepšího WAN připojení pro vybrané aplikace	ANO	Ano
NGFW musí obsahovat lokální úložiště logů o velikosti minimálně 2 TB (RAID1)	ANO	Ano, 2TB HDD + 240GB SSD v RAID1 konfiguraci
NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	Ano
Funkce agregovaného zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL	ANO	Ano
Funkce přeposílání logů na zařízení třetích stran	ANO	Ano
Funkce umožňující výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	Ano
Přeposílané logy z NGFW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM např. Microfocus ArcSight, který zadavatel používá.	ANO	Ano
Funkce umožňující vytváření vlastních reportů přímo z grafického rozhraní FW	ANO	Ano
NGFW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	Ano

Specifikace SW pro správu NG Firewallů (Plnění A.2):

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality/vlastnosti (požadavek se vztahuje k 1 zařízení)	Doplní Účastník dle nabízeného zařízení
Řešení musí obsahovat virtuální platformu pro centrální správu všech dodaných firewallů do VMware ESXi prostředí	ANO	Ano
Součástí dodávky musí být licence pro centrální správu, tak aby bylo možné centrálně spravovat všechny dodané HW appliance včetně všech virtuálních kontextů	ANO	Ano
Centrální management musí podporovat sběr logových záznamů, analýzu logových záznamů, správu veškerých bezpečnostních a	ANO	Ano

síťových konfigurací, korelaci logových záznamů, analýzu hrozeb a korelaci hrozeb v jediné instanci		
Centrální management musí podporovat sběr 20 000 logových záznamů za vteřinu	ANO	Ano
Administrátor musí mít možnost úpravy veškeré síťové a bezpečnostní konfigurace přímo na grafickém rozhraní FW a zároveň přes grafické rozhraní centrálního managementu	ANO	Ano
Administrátor musí mít možnost importovat FW konfiguraci do centrálního managementu	ANO	Ano
Grafické rozhraní a způsob konfigurace na centrálním managementu se musí shodovat s grafickým rozhraním a způsobem konfigurace NGFW kvůli konzistenci a jednoduchosti přechodu mezi platformami	ANO	Ano

Součástí plnění A je:

Implementační projekt, který **plně pokrývá požadavky uvedené v zadávací dokumentaci**.

Dokumentace:

Dokumentace plně **pokryje všechny požadavky uvedené v zadávací dokumentaci**.

Ostatní požadavky – hodnocení rizik:

Na základě požadavku Zadavatele jsme učinili a předkládáme jako součást nabídky vlastní hodnocení rizik postupem dle VKB, resp. příloh č. 1, 2 a 3 VKB.

Katalogové č.	Popis nabízeného zařízení	Počet kusů	Úroveň rizika HW & SW celkem / Dopad x Hrozba x Zranitelnost	Dopad	Hrozba	Zranitelnost
PA-5250	NGFW Palo Alto Networks PA-5250	4	12	3	2	2
	Palo ALto Networks Panorama	1	12	3	2	2

Technická podpora:

Součástí dodávky Plnění A1 a Plnění A2 této Prováděcí smlouvy je technická podpora pro NG Firewally (Plnění A.1) a SW pro správu NG Firewallů (Plnění A2), a to na období 12 měsíců.

Součástí technické podpory musí být minimálně:

- Hlášení incidentů a závad, tak i veškeré činnosti spojené s jejich vyřízením, bude realizováno prostřednictvím ServiceDeskového nástroje Dodavatele, ze kterého bude Zadavateli poskytován na měsíční bázi export dat týkajících se zařízení Zadavatele (zejména popis zařízení, konfigurace zařízení, činnosti prováděny se zařízením).
- Přijímání incidentů a závad musí být umožněno v režimu 24x7.
- Odstranění závady nejdéle do 4 hodin od nahlášení incidentu nebo závady. V případě neodstranění závady do 4 hodin, bude účtována sankce ve výši 2 000,00 Kč za každou

započatou hodinu, resp. 10 000 Kč za každou započatou hodinu v případě, že není vždy alespoň jeden NG Firewall v rámci lokality plně funkční. V případě neodstranění závady do 24 hodin, bude účtována sankce ve výši 5 000,00 Kč za každý započatý den, resp. 100 000 Kč za každý započatý den v případě, že není vždy alespoň jeden NG Firewall v rámci lokality plně funkční. V případě nedostupnosti ServiceDeskového nástroje (resp. nemožnosti nahlášení závady ani náhradním předem dohodnutým způsobem) pro nahlášení závady bude účtována sankce ve výši 3 000,00 Kč za každou započatou hodinu.

- Technická podpora musí být zajištěna přímo od výrobce zařízení dle Plnění A.
- Technická podpora musí obsahovat právo instalovat nejnovější verze obsažených SW produktů (např. firmware) a právo instalovat nejnovější aktualizace pro zajištění funkcionalit (např. definic pro IPS, antivir, antimalware, atd) i právo zakládat servisní tikety u výrobce zařízení.
- Technická podpora musí být na veškerý dodaný HW a s tím související SW licence dle Plnění A.

Plnění C:

Předmětem dodávky Plnění C (nenárokové plnění) jsou volitelně objednatelné práce (formou MD) v celkovém počtu 20 MD.

Specifikace volitelných prací:

- Implementační a konfigurační práce.
- Tvorba návrhů architektury, konfigurací a způsobů zapojení zařízení definovaných v předmětu Plnění A (tj. Plnění A1 a A2) a s tím související síťové infrastruktury; způsobů integrace zařízení definovaných v předmětu Plnění A do infrastruktury Zadavatele;
- Tvorba a aktualizace dokumentací.
- Diagnostika, profylaxe, upgrade firmware zařízení definovaných v předmětu Plnění A.
- Podpora provozu zařízení definovaných v předmětu Plnění A neobsažená v Plnění B.
- Konzultační a školící práce související se zařízeními definovanými v předmětu Plnění A, a současně konzultační práce související s architekturou a provozem komunikační infrastruktury; zajištění certifikovaného proškolení pracovníků Zadavatele na zařízení dle Plnění A.

Zadavatel je oprávněn objednat libovolný rozsah činností v maximálním objemu **20 MD (tj. člověkodnů) po dobu 12 měsíců od účinnosti prováděcí smlouvy**. Minimální jednotka k objednání je 1/2 člověkohodina, tj. 1/16 člověkodne.

Dodavatel je povinen poskytnout požadované služby ve lhůtě do 5 pracovních dnů ode dne objednávky, pokud nebude v objednávce dohodnuta lhůta delší.

Nabídnutá cena musí obsahovat všechny náklady Dodavatele, včetně cestovného do místa instalace dodaných zařízení (Praha). V případě, že jsou objednány práce v prostorách Zadavatele v rozsahu kratším než 4h, je Dodavatel oprávněn zahrnout čas cesty v maximálním rozsahu 2x1 hodina do hodin vykázaných k fakturaci.

Příloha č. 2 - Specifikace ceny

Požadované plnění	Počet	Jednotka	Jednotková cena bez DPH	Cena celkem bez DPH	Cena celkem s DPH
Plnění A.1 - Firewally včetně implementace a jednoleté technické podpory	4	ks	4 058 000,00 Kč	16 232 000,00 Kč	19 640 720,00 Kč
Plnění A.2 - SW pro správu Firewallů včetně implementace a jednoleté technické podpory	1	ks	264 000,00 Kč	264 000,00 Kč	319 440,00 Kč
Plnění C - Práce na objednávku	20	MD	9 000,00 Kč	180 000,00 Kč	217 800,00 Kč
Celkem				16 676 000,00 Kč	20 177 960,00 Kč