Objednávka Objednatele č.	
Objednávka Poskytovatele č.	**5**
Objednatel	**Poskytovatel**
MĚSTSKÁ ČÁST PRAHA 14	**HLAVNÍ MĚSTO PRAHA**
se sídlem: Bratří Venclíků 1073/8, 198 21 Praha 9	se sídlem: Mariánské náměstí 2/2, 110 00 Praha 1
IČO: 00231312	IČO: 00064581
DIČ: CZ00231312	DIČ: CZ00064581
Uzavřeno v souladu s podmínkami a na základě:	Smlouvy o poskytování IT služby číslo INO/40/05/003802/2022 uzavřené dne 22. 12. 2022
Předmět Objednávky:	Bezpečné připojení MČ o detailní specifikace dodávky je dle přílohy č. 1 této objednávky – Katalogový list „Bezpečné připojení MČ“ o technická realizace implementace bude popsána ve fázi I – Implementační plán, jehož schválení je podmínkou realizace fáze II
Výše spoluúčasti Objednatele:	0%
Cena (jednorázová):	0,- Kč – bezúplatně
Cena (měsíčně):	0,- Kč - bezúplatně
Uzavřeno na dobu:	51 měsíců T0 = podpis objednávky T1 = T0 + 2m = příprava implementačního plánu T2 = T1 + 1m = akceptace implementačního plánu T3 = T2 + 48 m = instalace a zahájení podpory M&S HW
Další informace:	Akceptace předmětu Objednávky bude probíhat ve dvou fázích: 1. Implementační plán o oprávněná osoba za MČ zadá požadavek na implementační plán o řešitel na službě jim stanoví konkrétní termín realizace dle harmonogramu o tiket bude následně v SD uzavřen s výsledem analýzy tzn., **lze / nelze** 2. Dodávka a instalace HW o dodávka HW a instalace dle schváleného Implementačního plánu 3. Zahájení provozu – akceptace objednávky – aktivace M&S HW

Příloha 1: KATALOGOVÝ LIST – Bezpečné připojení MČ

příloha 2: technická specifikace

Místo:

Datum:

Za Objednatele:

Ing. Martin Dušek

Digitálně podepsal Ing. Martin Dušek
Datum: 2023.09.28 19:15:42 +02'00'

_____

Jméno a příjmení: Ing. Martin Dušek

Funkce: vedoucí odboru informačních a komunikačních technologií ÚMČ Praha 14

Poskytovatel akceptuje tuto Objednávku v plném rozsahu a bez výhrad.

Místo:

Datum:

Za Poskytovatele:

_____

Jméno a příjmení: Mgr. Jiří Károly

Funkce: ředitel OIC MHMP

Příloha č.1 Objednávky: Katalogový list – Bezpečné připojení MČ

Zkratka / pojem	Popis			
Služba	**Bezpečné přípojení MČ (Firewall sítě MePNet)**			
Krátký popis	Služba bezpečné připojení MČ prostřednictvím „Firewall" (FW) do sítě MepNet, zajišťuje dodávku FW, jeho implementaci a konfiguraci. FW spravovaný přes centrální management konzoli slouží MČ jako koncový hraniční bod do sítě MePNet a do Internetu.			
Provozní doba	24 x 7			
Cena služby	0% spoluúčast MČ			
Zodpovědná osoba za KL na MČ	Pozice	Oddělení / odbor	Osoba	Kontakt
	referent	odbor informačních a komunikačních technologií	Miroslav Palounek	[redacted]
Zodpovědná osoba za KL na MHMP	technický garant služby	Odbor OIC MHMP	Vlastimil Matějek	

1. Popis dodávky a implementace

Služba bezpečné připojení MČ do sítě MePNet zajišťuje dodávku, instalaci a konfiguraci firewallu (FW). Tento centrálně konfigurovaný FW slouží jako koncový hraniční bod pro sít MePNet a hraniční bod MČ do Internetu. Předpokladem či podmínkou bezpečného připojení MČ, je odběr služby MePNet (tzv. připojení do městské sítě) a zajištění provozní podpory certifikovaným technikem. Související podmínky konfigurace:

- FW je spravován z centrálního management nástroje běžícího v DC MHMP. FW může obsluhovat několik (1-3) virtuálních instancí na jednom fyzickém zařízení (HW). FW vždy obsahuje instanci (root VDOM), která slouží jako hraniční bod do sítě MePNet. Zbylé VDOM mohou být využity MČ pro její účely (Interní a Externí firewall).
- MČ se zavazuje pro připojení k MePNet síti dodržovat pravidla stanovená globálním správcem MePNet. VDOM root obsahuje globální pravidla spravovaná MHMP (Správcem MePNet), zbylé VDOM (pokud jsou použita) jsou pod správou MČ. Každá MČ má přístup jen ke správě svého svěřeného FW.

Součásti služby bezpečné připojení MČ jsou typické zabezpečovací funkce firewallu a sítí. Příkladem je používání „black/white list", filtrování paketů, ochrana proti spoofing, DDoS, atd.

Objednateli je Služba poskytnuta na základě schváleného požadavku a za podmínek uvedených v tomto katalogovém listu.

2. Komponenty služby

Dodávka Služby bezpečného připojení se skládá z následujících dílčích služeb:

- Dodávka 1 ks FW – Fortinet FG-601F - detailní popis dodaného HW je v příloze tohoto KL.
- Zajištění implementace FW jako hraničního bodu.
- Konfigurace a správa bezpečnostních politik během migrace.
- Správa bezpečnostních politik root VDOM.
- Zajištění podpory výrobce na období 4 let.

Služba, případně její součásti, jsou poskytovány nepřetržitě v režimu 7x24. Provozní požadavky spojené s M&S FW lze realizovat na základě formálního požadavku prostřednictvím Service Desku MHMP tak, aby byla vedená zde potřebná evidence.

3. Činnosti zajišťované poskytovatelem služby

V následující tabulce jsou uvedeny činnosti zajišťované poskytovatelem Služby:

Název	Popis
Dodávka FW	○ Realizace Služby (zřízení, změna, zrušení) na základě schválených požadavků. ○ Návrh preventivních opatření s cílem předejít bezpečnostní události. ○ Zajištění podpory výrobce, založení požadavku na výrobce, komunikace s výrobcem.
Řešení incidentů a požadavků na výrobce FW	○ Řešení poruch, zajištění servisu, zajištění potřebných eskalací incidentu. ○ Řešení požadavků, případně zajištění potřebných eskalací požadavků.

4. Technické předpoklady na straně MČ

Pro realizaci Služby je nutné na straně Objednatele splnit následující technické předpoklady:

- Zajištění odpovídajících podmínek pro umístění FW v serverovně.
- Zajištění součinnosti při implementaci FW.
- Připojení a využívání služeb MHMP prostřednictvím sítě MepNet.
- Zajištění provozní podpory certifikovaným technikem Fortinet na úrovni alespoň NSE4 v případě, že budou využívány jiné VDOM než root.

5. Parametry dodávky Bezpečné připojení MČ

Poskytovaná služba a spravované funkce či parametry služby Bezpečné připojení MČ jsou shrnuté v této části obecného katalogového listu. Detailní a vybrané technické parametry poskytované služby budou definovány v rámci implementační analýzy dle konkrétního Objednatele (danou MČ).

Technické parametry služby

Služba bezpečné připojení MČ je nadstavba služby MePNet pro MČ s cílem maximálně zabezpečit provoz metropolitní sítě, včetně MČ. Služba poskytuje funkce firewallu a bezpečnostní politiky sítě MePNetu. Typické funkce a technické parametry, které jsou v rámci root VDOM standardizované a které lze dle dohody přizpůsobit pro potřeby MČ, jsou vyjmenované níže:

- Uživatelská firewallovací pravidla (whitelist/blacklist).
- Poskytnutí služby záložního DNS serveru pro reverzní DNS záznamy.
- Zabezpečení interní komunikace v rámci MePNet proti odposlechu.
- Zabezpečení interní komunikace v rámci MePNet proti spoofingu.
- Ochrana interní sítě MČ proti cíleným útokům z Internetu a od ostatních účastníků MePNet.
- Ochrana interní sítě MČ proti malware z Internetu a od ostatních účastníků MePNet.
- Ochrana technologií IPS (Intrusion Prevention System) z Internetu a od ostatních účastníků MePNet.
- Ochrana technologií antibot z Internetu a od ostatních účastníků MePNet.
- Ochrana technologií antivirus z Internetu a od ostatních účastníků MePNet.
- Ochrana uživatelů pomocí pokročilých bezpečnostních funkcionalit URL filtering.
- Ochrana uživatelů pomocí pokročilých bezpečnostních funkcionalit Application Control.

V ostatních VDOM jsou výše zmíněné technické parametry plně pod správou MČ.

Zajištění implementace FW jako hraničního bodu

Dodávka zařízení FW na klíč.

Zajištění podpory výrobce a poskytovatele

Poskytovatel zajistí poskytnutí opravného patche, aktualizace SW nebo service packu. Technická podpora je služba poskytovaná výrobcem, resp. poskytovatelem.

6. SLA/M&S parametry služby

Dodaný FW je krytý službou FortiCare Premium, která je zaměřena na zařízení, jež vyžadují podporu 24x7x365 s hodinovou odpovědí na kritické problémy a odpověď následující pracovní den pro problémy nekritické.
Podmínky pro M&S jsou uvedeny na webu výrobce:
https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

7. Postup objednání a zrušení služby

Objednání a zřízení služby

Objednání služby provede oprávněná osoba (viz. Příloha 1. Smlouvy) zadáním požadavku Servis desku MHMP. V rámci zadaného požadavku oprávněný uživatel specifikuje požadované parametry služby.
V případě schválení požadavku Poskytovatelem služby, je tento požadavek realizován dle parametrů odsouhlasených v předmětném požadavku.
O realizaci požadavku je oprávněná osoba informována prostřednictvím Service Desk MHMP.

Změna služby

Změnu služby provede oprávněný uživatel prostřednictvím zadání požadavku s identifikací, že se jedná o službu dle tohoto KL přes Service Desk MHMP a s uvedením konkrétních informací o požadované změně již poskytované služby. V případě schválení změny již poskytované služby Poskytovatelem, je změna realizována dle parametrů dohodnutých v předmětném požadavku.
O realizaci úpravy již poskytované služby je oprávněný uživatel informován prostřednictvím Service Desk MHMP.

Zrušení služby

Zrušení služby provede oprávněný uživatel prostřednictvím požadavku s identifikací, že se jedná o službu dle tohoto KL přes Service Desk MHMP. Požadavek je následně předán Poskytovateli služby. V případě schválení zrušení již poskytované služby Poskytovatelem, je změna realizována dle parametrů dohodnutých v předmětném požadavku.
O realizaci požadavku je oprávněný uživatel informován prostřednictvím Service Desk MHMP.

** změny parametrů služby, které můžou mít dopad na cenu / provoz musí být předem schválené formálním postupem. V takovém případě, kde lze předpokládat změnou i finanční dopad, se zahájí proces schvalování, který spočívá v projednání a konsensu Řídícího výboru, který návrh postoupí ke schválení Řídící radě. Tento postup je v souladu s odstavcem 3.3, z „Celoměstská koncepce rozvoje informačních systémů pro potřeby hl. m. Prahy a městských částí na období do roku 2025, Společně řízená informatika ve správě města".*

Příloha č.2 Objednávky: Technická specifikace

Funkcionality
1) Bezpečnostní funkcionality
○ stavový
firewall ○ IPS
○ aplikační kontrola: ▪ detekce a řízení síťových aplikací. Minimální počet rozpoznávaných aplikací: 2000
○ URL filtrace - automatické řízení web přístupů zaměstnanců
○ filtrování internetového spojení (URL, IM, P2P, RAT, Anonymizers, …)
○ detekce a řízení datových souborů na základě obsahu
○ antivirus a ochrana před spyware a červy na úrovni brány včetně schopnosti skenovat e-mail (SMTP), FTP a webové (HTTP, HTTPSs) přenosy v reálném čase a zjišťovat potenciální hrozby skryté uvnitř legitimního provozu
○ anti-bot ochrana
○ HTTPs inspekce: ▪ ochrana proti SNI spoofing v rámci HTTPs kontroly
○ zero-day ochrana s podporou souborových typů minimálně: ▪ Microsoft Office soubory ▪ Portable document format (PDF) ▪ Adobe Flash soubory ▪ Portable executable soubory (včetně MSI souborů) ▪ Archive (RAR, 7-Zip, Zip) ▪ Java Archive soubory (JAR) ▪ MacOS X soubory ▪ ISO soubory
○ emulace neznámých hrozeb (zero-day sandboxing)
○ podpora explicitní nebo transparentní HTTP/HTTPs proxy
○ VPN ▪ uživatelská - bezpečný flexibilní vzdálený přístup pomocí IPSec a SSL a SSL portál (tj. clientless) ▪ s2s (IPsec) s podporou níže uvedených enc a vyšších ▪ P1 IKE, AES-256, SHA256, DH 14 (3072-bits)
2) Služba vlastní certifikační autority pro vydávání PKI certifikátů pro uživatele (pro VPN).
3) Možnost přiřazení více veřejných IP adres na WAN rozhraní bez nutnosti policy routing.
4) Podpora policy based routingu.
5) Centrální správa/management, jednoduché centrální zálohování a obnova systému (nejen částí, ale celé konfigurace). Je nutné doplnit licenci pro veškerá dodaná zařízení se zohledněním počtu zakoupených licencí pro virtuální FW v režimu vysoké dostupnosti.
6) NGFW platforma ve formě samostatné hardware appliance.
7) Interní HDD (SSD), min 200 GB, pro logování v případě výpadku spojení na centrální SIEM log servery.
8) Podpora režimů Active-Active/Active-Standby s automatickou synchronizací spojení.

Sizing

1) Instalace do standardního 19" RACK, výška maximálně 3U.
2) Out of band management pro vzdálenou správu a konzolový port RJ45.
3) Redundantní napájení zařízení.
4) Počet požadovaných fyzických metalických síťových rozhraní, min. 8x 100/1000baseT.
5) Počet požadovaných fyzických 10Gb SFP+ rozhraní - min. 2x 10GE SFP+.
6) Propustnost NGFW (Firewall, IPS, Aplikační kontrola), minimálně 4 Gbps.
7) IPSec VPN, průchodnost VPN 4 Gbps s AES256-SHA256.
8) Propustnost Threat ochrana (Firewall, IPS/IDS, Aplikační kontrola, Antivir, URL filtering, Zero day), minimálně 4 Gbps (metrika Enterprise Mix). 9) Počet nových spojení za vteřinu (CPS) minimálně 150.000.
10) Počet současných spojení, min. 7.000.000.
11) SSL inspekce.
12) Propustnost Firewall pro malé pakety (576 byte) min. 10 Gbps.
13) Počet požadovaných virtuálních instancí firewallu, min. 4.

Dodaný model Fortigate600f:

https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/fortigate-600f-series.pdf