Specifické požadavky

Veřejná zakázka malého rozsahu na dodávky:
„Dodávka internetové konektivity, včetně zabezpečení na dobu 48 měsíců“

1. POPIS STÁVAJÍCÍHO STAVU ZADAVATELE

Zadavatel v současné době disponuje Router MikroTik Cloud Core CCR1036-12G-4S, který slouží jako firewall.

Z městem řízených organizací dochází k připojení pomocí trvalých VPN a využívání Informačního systému Vera a telefonní ústředny. V organizacích jsou routery Miktotik.

2. POŽADAVKY NA DODAVATELE

2.1. TECHNICKÁ SPECIFIKACE PŘEDMĚTU PLNĚNÍ

Předmětem plnění veřejné zakázky je zajištění konektivity a dodávka nového (nepoužitého, nerepasovaného) NGFW, případně je připuštěna SW appliance v datovém, centru Dodavatele.

Ochrana koncových stanic musí výkonově pokrýt až 300 koncových zařízení s plným nasazením UTM[1] funkcionalit.

Účastník je povinen s dodávkou doložit, že dodaná zařízení:

- pochází z autorizovaného prodejního kanálu výrobce
- má záruku výrobce po celou dobu kontraktu (výměna HW[2] v rámci RMA[3] do NBD[4])
- splňuje podmínky servisní podpory výrobce
- obsahuje software výrobce s platnou licencí UTM po celou dobu kontraktu
- splňuje podmínky předpisů EU ohledně paralelního importu

Všechna nabízená zařízení a software musí být určeny pro český trh.

Realizace zahrnuje dodávku komponent, montáž, instalaci a konfiguraci zařízení dle požadavků a nároků prostředí zadavatele.

2.2. PŘIPOJENÍ EXTERNÍCH ORGANIZACÍ

Řešení musí mít možnost připojit externí organizace přes internet pomocí VPN tunelu – na druhé straně jsou organizace vybaveny HW Mikrotik. Cílová zařízení v koncové lokalitě nesmí vyžadovat žádnou další licenci.

1 Reklamačního řízení
2 Hardware
3 Return Merchandise Authorization - je označení pro součást reklamačního procesu
4 Next Business Day

2.3. DOSTUPNOST A SPOLEHLIVOST SLUŽBY – SLA

U služby je standardně garantována minimální dostupnost 99,8 %. Výpočet dostupnosti je vztažen na dobu jednoho měsíce přepočítaného na 720 hodin (24 hodin × 30 dnů). Do doby dostupnosti nejsou započítávány pravidelné servisní odstávky služeb. Výpočet použitý pro stanovení dostupnosti je následující:

$$A = \frac{ATS - MW - DT}{AST - MW} * 100$$

Kde vzorec pro výpočet obsahuje následující hodnoty

Hodnota	Popis
A	Dostupnost (Availability)
AST	Celková odsouhlasená provozní doba za sledované období (měsíc) (Approved Service Time)
MW	Celková odsouhlasená doba pracovních odstávek ve sledovaném období (měsíc) (Maintenance Window)
DT	Celková doba neplánovaných odstávek ve sledovaném období (měsíc) (Downtime)

Dodavatel se zavazuje odstranit vady, v součinnosti se Zadavatelem, v níže uvedených termínech:

- **Kritický problém**

  problém bránící provozu kritických zdokumentovaných funkcí s vysokou četností nebo dlouhou dobou trvání – do 2 hodin.

- **Závažný problém**

  problém soustavně bránící provozu nekritických zdokumentovaných funkcí, nebo občasně ovlivňuje zdokumentované funkce, nebo kritický problém, pro který bylo poskytnuto dočasné řešení – do 4 hodin.

- **Nezávažný problém**

  problém, který má nějaký vliv na správu nekritické operace či jiné sekundární funkce, nebo závažný problém, pro který bylo poskytnuto dočasné řešení – do 12 hodin.

Nemůže-li Zadavatel využívat službu pro poruchu služby zaviněnou Dodavatelem, je oprávněn požadovat vrácení poměrné části měsíční ceny za nedostupnost služby dle níže uvedené tabulky, pokud dostupnost služeb ve sledovaném období klesla pod garantovanou hodnotu.

2.3.1.1. Sankce za nedodržení SLA

Dostupnost za měsíc	Maximální délka nedostupnosti	Sleva z měsíčního paušálu
99,80%	1,4 hodiny	0%
99,50%	3,6 hodiny	5 %
99,00%	7,2 hodiny	10 %
98,00%	14,4 hodiny	25 %
97,00%	21,6 hodiny	40 %
95,00%	36 hodin	75 %
menší než 95,0%	větší než 36 hod	100 %

Jiná náhrada (např. náhrada škody a ušlého zisku) bude řešena samostatně dle platných znění Obchodního a Občanského zákoníku.

O případné vrácení příslušné částky bude Zadavatel písemně žádat na adrese Dodavatele.

2.3.1.2. Garance kvality služby (SLA):

Dodavatel 1x měsíčně vyhodnocuje dodržení garantovaných parametrů. Report o hodnotách dosažených v uplynulém měsíci poskytne Zadavateli nejpozději do 10. pracovního dne následujícího měsíce. Při nesplnění garantovaných ukazatelů dodavatel automaticky sníží měsíční cenu za pronájem služby na následující období (tj. v následujícím kalendářním měsíci) o poměrnou část, závislou na míře překročení garantovaných parametrů.

2.4. PŘIPOJENÍ VPN KLIENTA

Řešení musí mít možnost připojení softwarového klienta instalovaného do zařízení uživatele (stolní PC, Notebook, nebo mobilní zařízení s operačním systémem MS Windows, macOS, Android nebo iOS) přes internet pomocí VPN tunelu. Cílová zařízení nesmí vyžadovat žádnou další licenci.

2.5. ZÁKLADNÍ FUNKCE FIREWALLU

Úkolem poptávané dodávky je ochrana a případná filtrace dat na internetovém připojení Zadavatele dle definované bezpečnostní politiky. Ochrana musí obsahovat i aplikační zabezpečení v podobě:

2.5.1. Ochranu před útoky firewall:

Stavový firewall na síťové vrstvě (L3). V jeho nastavení musí být možné vybírat, které protokoly (TCP, UDP, ICMP apod.), na kterých portech a na kterých dotčených IP adresách a v jakém směru (příchozí, odchozí) se uplatní definované akce (základní akce ACCEPT, DENY a dále monitoring, traffic shaping, apod.)

2.5.2. Ochrana před útoky IPS[5]

IPS je systém pro prevenci narušení. NGFW musí sledovat pomocí IPS senzorů síťový provoz na výskyt definovaných anomálií a signatur útoků. Anomálií je to, když případný útočník používá síťovou komunikaci jako zbraň. Typicky se jedná o zahlcující (flood) komunikace, jejichž cílem je odepření koncové služby (DoS – Denail of Service). IPS není ochranou proti distribuované variantě (DDoS). Druhým typem obrany bude obrana založená na signaturách. Každý útok je charakterizován specifickou sekvencí v komunikaci, kterou lze odhalit a na základě toho blokovat daný provoz. Tento typ se bude používat pro ochranu systémů, na které není aplikován (případně dostupný) softwarový patch, který danou zranitelnost řeší (zero day útoky apod.).

2.5.3. Ochranu nevyžádanými maily (antispam)

Antispam bude službou, která bude sloužit pro detekci nevyžádané pošty. Kromě vlastní antispamové funkcionality musí nabízet také karanténu pro zachycené zprávy (pro eliminaci tzv. false positive).

2.5.4. Ochranu antimalware a antivir

Antivirová funkcionalita bude prohledávat komunikaci na výskyt malwarových sekvencí v rozličných druzích komunikace: HTTP, FTP, IMAP, POP3, SMTP a NNTP, včetně šifrovaných variant. Provádět sken na výskyt virů také souborové archivy (ZIP, RAR …) včetně několinásobně zanořených archivů (ZIP v ZIPu). Musí pracovat se všemi druhy malware, tedy nejen viry, ale také trojskými koni, spyware, síťovými červy apod. Pro detekci musí využívat neustále aktualizovanou databázi signatur.

2.5.5. Obsahovou filtraci webu (webfiltering/content filtering/URL filtrace)

Webová filtrace musí být nedílnou součástí NGFW. Její aplikace bude jednak pro zajištění bezpečnosti (návštěvy nebezpečných stránek), ale stejně tak musí poskytnout možnost filtrace stránek s nevhodným pracovním obsahem a bude potom nástrojem na zvýšení produktivity, či „zrychlení“ linky díky odstranění nežádoucí komunikace.

Tři hlavní části webového filtru musí být následující:

- obsahový filtr (Web Content Filter)
- URL Filter
- Služba Web Filtering,

Dojde k maximální kontrole nad tím, co je možné na internetu navštěvovat a kým. Obsahový filtr bude hledat definovaná slova (specifikovaná divokými znaky či regulárními výrazy), URL filtr musí používat databázi vyjmenovaných domén a služba Web Filtering definovat kategorie a do těchto kategorií řadit jednotlivé domény na denní bázi.

[5] Intrusion Protection System

2.5.6. Řízení aplikací (application control)

Jedná se o řízení síťových aplikací. Díky spojení s Applicaton Control, NGFW musí rozeznat na základě parametrů síťové aplikace, které budou řazeny do kategorií. Tyto kategorie budou například Hry (Games), Botnet, P2P apod. Na základě identifikace aplikace se budou provádět různé akce (obdoba funkcionality u web filteringu).

2.5.7. Ochranu před únikem interních dat (DLP)

DLP zabrání odesílání citlivých informací Zadavatele mimo společnost a tím úniku důvěrných informací. Musí umožnit kontrolu odchozích i příchozích dokumentů na základě různých parametrů (obsah dokumentu, vodotisk, jméno souboru, specifický otisk – fingerprint apod.). Na základě shody s kontrolou bude možné provést řadu akcí (nic, blokování, karanténa, logování). DLP se uplatí na e-mailovou, http, ftp a IM komunikaci. Kromě standardní DLP funkcionality, bude možné DLP využít také v režimu archivace, kdy bude možné zaznamenávat aktivitu daných souborů.

2.5.8. VPN (IPSec i SSL, klientská i site-to-site)

Služba NGFW Dedicated musí umožnit vytváření virtuálních privátních sítí (VPN) na bázi protokolu SSL a TLS. Vyžaduje se podpora různých verzí těchto protokolů. VPN sítě musí být možné vytvářet v několika formách, tzv. bezklientské či pouze webové formě – pro vybrané protokoly (HTTP, CIFS, FTP apod.) musí být vytvořen zabezpečený webový portál na který budou tyto služby publikovány, aby přistupující uživatel nepotřeboval instalaci žádného VPN klienta. K přístupu stačí pouze webový prohlížeč podporující SSL a TLS.

2.5.9. Reporting

Na základě definovaných pravidel musí být vytvářen komplexní report v několika formátech (PDF, HTML apod.), který bude možné zasílat emailem, případně si ho ze zařízení stahovat. Parametrizovatelný report v podobě grafů a tabulek musí dát přehled využití služeb (např. četnost virů, provoz, uživatelé, blokované stránky apod.) za definované období.

2.5.10. Antispam

Doplňková služba, která využívá prvky Dodavatele pro detekci nevyžádané pošty. Službu je možné implementovat také samostatně bez nutnosti ostatních komponent NGFW.

2.5.11. Součástí služby bude dále

2.5.11.1. Svěřená správa

- Plně v režii Dodavatele

  Konfigurační a konzultační podpora, kdy Zadavatel nebude mít administrátorské oprávnění ke správě bezpečnostní platformy „Virtuální domény“, ale veškeré konfigurační zásahy provede na základě požadavků Zadavatele vyškolený personál Dodavatele. Časová kapacita podpory se stanoví individuálně, dle požadavku Zadavatele. V ceně nabídky je vždy 1. hod./měs.

- Rozdělení části správy mezi Zadavatele a Dodavatele

  „Virtuální domény“ (či obdobný nástroj) se použije k rozdělení Firewallu na dvě nebo více virtuálních jednotek, které musí fungovat nezávisle. Virtuální domény bude poskytovat samostatné zásady zabezpečení a v režimu NAT zcela samostatné konfigurace pro směrování a služby VPN pro každou připojenou síť.

  Nejčastěji se použije správa s rozdělenou úlohou, přičemž jedna doména bude sloužit pro management a správu Firewallu a druhá doména pro bezpečnost, WiFi, LAN, DMZ apod.

2.6. POŽADOVANÁ FUNKCIONALITA / VLASTNOST NA NGFW

Zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené níže:

- Firewall Throughput (1518 byte UDP) ..... 10 Gbps
- IPsec VPN Throughput (512 byte) ..... 6 Gbps
- New Sessions/Sec 40 000
- SSL VPN Throughput ..... 900 Mbps
- Concurrent SSL VPN Users..... min. 180
- Application Control Throughput ..... 1,5 Gbps
- Interface.....min. 8x GE RJ45
- Rack provedení 1U, nebo umístění na poličku (součástí řešení), přípustná je i SW appliance v datovém, centru Dodavatele (další případný HW musí být součástí dodávky).
- Podpora L2 (transparentního) módu s podporou NAT a PAT
- Podpora L3 (routovaného) módu s podporou NAT a PAT
- Podpora Policy based Routing
- Funkce pro kontrolu DLP
- Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v internetu
- Možnost rozšíření o funkce IPS
- Možnost rozšíření o funkce URL filtrace
- Možnost řízení rychlosti datových toků na úrovni pravidel FW
- Možnost rozšíření o funkce antimalware filtrace

2.7. PRIMÁRNÍ KONEKTIVITA

Předávací rozhraní internetové služby bude metalické rozhraní Ethernet 1000 BaseT. Zadavatel předpokládá možnost využití odpovídajících vnitřních rozvodů v rámci objektu, možnost umístění potřebných technologických prvků a jejich napájení AC 230 V.

Konektivita musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Linka	symetrická	ano
Rychlost	200 Mb/s bez agregace	ano
Počet veřejných IP adres	16	ano
NAT – lokálních IP adres na veřejné	Ano	ano
sekundární DNS	Ano	ano
Možnost změnit parametry (šířka pásma, jiná varianta) v průběhu provozu služby	Ano	ano
Koncové zařízení (internetová konektivita bude ukončena přímo na firewallu)	NGFW	ano

2.8. MOBILNÍ ZÁLOŽNÍ PŘIPOJENÍ

Musí umožnit vytvoření záložního spojení s využitím technologie mobilní sítě operátora dle volby Dodavatele. Součástí této služby musí být i potřebný HW. Musí se jednat o nezávislé zálohování přípojky jinou technologií, s nižší přenosovou rychlostí. Přepojení na záložní spoj se musí dít automaticky v případě výpadku primárního spoje. A naopak v případě dostupnosti primárního spoje se automaticky přepojí na primár. Veřejné IP adresy se musí (bez zásahu Zadavatele, či Dodavatele) přeroutovat z primárního spoje na záložní a naopak. IP adresy musí být zachovány.

Mobilní záložní připojení musí umožnit download připojení rychlostí obvyklou na mobilní LTE či 5G, bez rychlostního a datového omezení.

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Doplní Uchazeč dle nabízeného zařízení
HW	Ano	ano
V případě výpadku primárního spoje dojde automaticky k přepojení na záložní a naopak	Ano	ano
Zachování IP adres na primárním a záložním spoji	Ano	ano
Technologie LTE, 5G	Ano	ano

2.9. SERVICE DESK

Zadavatel požaduje proaktivní dohled sítě – Service Desk. V případě problému musí dojít k automatickému založení poruchového hlášení při výpadku, aby byla minimalizována doba pro opravu poruchy.

Service Desk pracoviště pro řešení incidentů bude umístěno u Dodavatele. Doba dostupnosti musí být 24x7

Požadovaná funkcionalita/vlastnost	Způsob splnění požadované funkcionality / vlastnosti	Doplní Uchazeč dle nabízeného zařízení
Správa NGFW v rozsahu 1 hodiny měsíčně v ceně služby	Ano	ano
Doba pracoviště Servis Desku 24/7	Ano	ano
Reakční doba na přijetí požadavku	1 hodina	ano
Proaktivní Service Desk (zahájení práce na opravě bez nutnosti nahlášení poruchy uživatelem)	24/7	ano

3. IMPLEMENTACE

Zadavatel požaduje provedení implementaci zařízení, software a dalších služeb, která zahrnuje:

- Kompletní nahrazení současného firewallu města Rýmařova (tak, aby je bylo možno odpojit/odstranit ze sítě).
- Dodavatel provede kompletní implementaci zařízení a software za asistence zaměstnanců města Rýmařov nebo přes vzdálený přístup.
- Součástí implementace bude potřebné zaškolení, u Zadavatele, v rozsahu max 1 hod. tak, aby byli zaměstnanci Zadavatele schopni zadat potřebné úkoly, nastavit VPN atd.
- Implementace spočívá zejména v:
  - analýze stávajícího stavu
  - instalaci, zapojení a kompletní konfiguraci všech hardwarových a softwarových komponent, jež jsou předmětem této veřejné zakázky
  - migraci, popř. úpravě stávajících pravidel ze stávající infrastruktury do nové (Zadavatel požaduje převod všech pravidel do nového řešení NGFW).
- Dodavatel po úspěšném zprovoznění všech součástí dodávky vypracuje a dodá objednateli v písemné podobě základní technickou dokumentaci (ve formátu MS Office 2013 a vyšší), která musí minimálně obsahovat kompletní popis konfigurace a nastavení jednotlivých částí dodávky.

  Technická dokumentace se po předání Zadavateli stává jeho majetkem a může s ní nakládat dle svých potřeb.

4. OSTATNÍ POŽADAVKY NA PŘEDMĚT VEŘEJNÉ ZAKÁZKY

Celé řešení bude dodáno formou služby na 48 měsíců s paušální měsíční platbou. Řešení se bude sestávat z následujícího:

4.1. POŽADAVKY NA PROVOZ

- veškeré požadované funkcionality v technické specifikaci musí být licencovány na dobu 48 měsíců
- správu dodaného řešení v rozsahu min 1 hodiny měsíčně
- odbornou spolupráci při rozvoji, kontrole a testování bezpečnosti
- rozdělení správy mezi Zadavatele a Provozovatele (dvě virtuální domény)

David Janoušek
Digitálně podepsal David Janoušek
Datum: 2023.08.23 09:46:32 +02'00'