# TECHNICKÉ POŽADAVKY NA POPTÁVANOU TECHNOLOGII

Technické požadavky jsou koncipovány **ve smyslu minimálních technických požadavků** z pohledu jejich technického hodnocení. Dodavatel může ve své odpovědi na tuto VZ použít jiné technologické řešení, ale v rámci své odpovědi je případnou neshodu s **minimálními technickými požadavky** (dále také jako „Technické požadavky“)je povinen jasně označit a dále uvést:

* Technické důvody, proč identifikoval neshodu s Technickými požadavky.
* Technické důvody, které ho vedou k volbě jiného/alternativního řešení.
* Technické opatření a doporučení zadavateli, které budou, nebo mohou mít vliv na zadavatelem realizovaná řešení v rámci jím realizované infrastrukturní sítě.

Zadavatel si vyhrazuje právo vyloučit takového dodavatele, který ať již záměrně, nebo jen náhodou ze své nabídky vypustí, opomene uvést, nebude technicky komentovat, nebo neoznačí neshodu s Technickými požadavky, a to byť jen u jediného požadovaného parametru VZ. Dodavatel musí ve své odpovědi aplikovat sloupce A a B a to včetně čísla ID požadavku. Neshoda odpovědi dodavatele s realitou v rámci testování nabízených zařízení je pro zadavatele bezpodmínečným důvodem pro vyloučení dodatele z VZ.

# HW parametry FW typu NG (Next generation)

Jsou poptávány 2 ks zařízení splňující Technické požadavky pro v tomto bodu uvedené parametry:

1. pro inspekci sítového provozu typu Next Generation.
2. Provedení jako HW appliance určená do low-latency prostředí jako interní segmentační firewall.
3. Zadavatel nepřipouští v rámci tohoto bodu nabídku SW appliance do virtualizovaného prostředí, jenž není součástí dodavatelem nabízeného celkového řešení.

**HW požadavky:**

| **ID požadavku** | **Popis požadavku** |
| --- | --- |
| FW\_HW\_01 | Počet síťových rozhraní copper/RJ45 10/100/1000 min. 8, každý zvlášť konfigurovatelný |
| FW\_HW\_02 | Počet síťových rozhraní SFP min. 8, každý zvlášť konfigurovatelný |
| FW\_HW\_03 | Rozšiřitelnost: V rámci síťových rozhraní SFP+ - min. 2x |
| FW\_HW\_04 | Konzolový a management port |
| FW\_HW\_05 | Nízká latence firewallu (výrobce kvalifikuje nabízený produkt jako low-latency firewall; očekávaná hodnota je v řádu jednotek mikro sekund) |

**Výkonnostní parametry:**

| **ID požadavku** | **Popis požadavku** |
| --- | --- |
| FW\_P\_01 | Počet současných TCP spojení stavového firewallu min. 8 M |
| FW\_P\_02 | Počet nových spojení za sekundu min. 250 000 |
| FW\_P\_03 | Propustnost firewallu (UDP provoz, pakety o velikosti 512 B) min 30 Gbps |
| FW\_P\_04 | Propustnost IPSEC VPN (AES256) min. 20 Gbps |
| FW\_P\_05 | Propustnost SSL VPN min. 4 Gbps |
| FW\_P\_06 | Propustnost IPS/IDS (http/enterprise traffic mix) min. 10 Gbps / 5 Gbps |
| FW\_P\_07 | Propustnost NGFW (min. firewall, IPS, L7 analýza aplikací) min. 4 Gbps (enterprise traffic mix) |
| FW\_P\_08 | Propustnost všech funkcí ochrany proti hrozbám (min. firewall, IPS, L7 analýza aplikací, antivirus, url/web filtering, zero day) min. 4.5 Gbps (enterprise traffic mix) |
| FW\_P\_09 | Propustnost funkce SSL inspekce min. 5 Gbps |
| FW\_P\_10 | Dodavatel se zavazuje demonstrovat dosažení vybraných výkonových parametrů při reálném měření v prostředí zákazníka. Pro tyto účely dodavatel zapůjčí generátor provozu. |

**Požadované funkce (integrovaná funkce nebo modul) – Typu NG:**

|  |  |
| --- | --- |
| **ID požadavku** | **Popis požadavku** |
| FW\_F\_01 | Podpora funkce vysoké dostupnosti (HA/clustering) v režimu active/active a active/passive |
| FW\_F\_02 | Podpora virtualizace (min. 6 virtuálních kontextů) na úrovni HA/cluster |
| FW\_F\_03 | Integrovaná podpora jednorázových hesel (OTP), generátor OTP jako aplikace pro MT iOS, Android, OS Windows; zasílání OTP jako SMS (SMS brána musí být součástí nabídky a dodávky) |
| FW\_F\_04 | Režim nasazení L2 a L3 (transparentní režim, nat/router režim) |
| FW\_F\_05 | Funkce stavového firewallu s podporou multicast |
| FW\_F\_06 | Funkce SSL VPN (portálový režim, tunelový režim), |
| FW\_F\_07 | Funkce IPSEC VPN (IKE, manual key, certifikát, gateway to gateway, hub and spoke, internet browsing konfigurace, podpora vice tunelů – redundantní VPN s podporou dynamického routování) |
| FW\_F\_08 | Funkce rozpoznávání identity uživatele (single sign on) v prostředí MS AD |
| FW\_F\_09 | Funkce antivirové kontroly provozu pro vybrané protokoly s možností sanitarizace aktivního obsahu kancelářských souborů (odstranění možného škodlivého kódu z dokumentů), podporou detekce Botnet IP/domén, detekce malware pro mobilní platformy, podpora kontroly souborů a odkazů technikou sandboxing (on prem nebo cloud); všechny databáze udržovány a aktualizovány výrobcem. |
| FW\_F\_10 | Funkce filtrování nevyžádané elektronické pošty s výrobcem udržovanou a aktualizovanou databází |
| FW\_F\_11 | Funkce ochrany před únikem citlivých dat ze sítě (DLP) |
| FW\_F\_12 | Funkce kategorizace webových stránek s bezvadným pokrytím českého internetu s databází udržovanou a aktualizovanou výrobcem |
| FW\_F\_13 | Funkce ochrany před sítovými útoky (IPS) s databází udržovanou a aktualizovanou výrobcem včetně možnosti vytvářet vlastní signatury |
| FW\_F\_14 | Funkce analýzy/rozpoznávání aplikací na L7 s podporou min. 2500 aplikací |
| FW\_F\_15 | Funkce SSL inspekce s možností vyjmutí určitých kategorií webových stránek |
| FW\_F\_16 | Integrovaná funkce explicitní proxy |
| FW\_F\_17 | Funkce zabezpečení a řízení práce s cloudovými aplikacemi (Dropbox, Google drive, …) možnost řízení, zabezpečení a auditování aktivit uživatelů přistupujících k cloudovým službám (přes portál propojení přes API k dané cloudové službě (Dodavatel popíše tuto funkcionalitu v separátní části nabídky.). |
| FW\_F\_18 | Funkce auditu nastavení instalované báze bezpečnostních zařízení – firewall sám vyhodnotí konfiguraci a upozorní na možné chyby, nabídne nápravu (Dodavatel popíše tuto funkcionalitu v separátní části nabídky.). |
| FW\_F\_19 | Funkce SD-WAN softwarově definovaná WAN konektivita, kombinace a skládání více aktivních konektivit |
| FW\_F\_20 | Funkce automatizace – firewall sám umí na základě detekce určité události spustit sérii nápravných kroků např. k mitigaci vzniklé hrozby (Dodavatel popíše tuto funkcionalitu v separátní části nabídky.). |
| FW\_F\_21 | Funkce propojení firewallu s dalšími bezpečnostními komponentami v síti (další firewall, emailová brána, web aplikační firewall, sw-klient) za účelem lepší vizualizace, sdílení informací o hrozbách, snazší konfigurace a centrálního řízení (Dodavatel popíše tuto funkcionalitu v separátní části nabídky). |

# Log management pro FW

Je poptáván systém pro ukládání a korelaci logů v síti zadavatele.

1. Systém musí být plně kompatibilní s dodávanými zařízeními (firewally, sandbox,…), musí podporovat analýzu logů nad provozem.
2. Součástí nabídky a dodávky musí být technická podpora VM/HW appliance a všechny potřebné aktualizace a předplatné služeb na 5 let.
3. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny a splňovat Technické požadavky pro v tomto bodu uvedené parametry:

| **ID požadavku** | **Popis požadavku** |
| --- | --- |
| FW\_LOG\_01 | Musí se jednat o virtuální appliance s podporou VMware, KVM a Hyper-V nebo HW appliance |
| FW\_LOG\_02 | Kapacita úložiště logů minimálně 2TB a minimální limit pro množství přijatých logů za jeden den 6 GB |
| FW\_LOG\_03 | Možnost škálovatelného navýšení kapacity úložiště na základě licence |
| FW\_LOG\_04 | Musí se jednat o centrální logovací prvek pro všechny firewally |
| FW\_LOG\_05 | Musí být zajištěna obousměrná komunikace mezi logujícím zařízením (např. firewall) a log management nástrojem. |
| FW\_LOG\_06 | Všechna logující zařízení musí být podporována výrobcem log management nástroje (včetně technické podpory pro případ řešení potíží) |
| FW\_LOG\_07 | Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení) |
| FW\_LOG\_08 | Vizualizace provozu nad všemi firewall |
| FW\_LOG\_09 | Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy |
| FW\_LOG\_10 | Realtime a historický náhled do logů |
| FW\_LOG\_11 | Samostatná sekce týkající se hrozeb v síti |
| FW\_LOG\_12 | Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF |
| FW\_LOG\_13 | Automatické generování reportů v pravidelných intervalech |
| FW\_LOG\_14 | Předefinované vzory pro reporty na nejčastější použití |
| FW\_LOG\_15 | Možnost vytváření vlastních reportů na základě konkrétních parametrů |
| FW\_LOG\_16 | Podpora prohlížení statistických údajů nad logy |
| FW\_LOG\_17 | Upozorňování na důležité informace z logů – emailem a snmp trapy |
| FW\_LOG\_18 | Integrovaný nástroj pro práci s incident - Event Management |
| FW\_LOG\_19 | Možnost propojení se systémem SIEM třetích stran. |
| FW\_LOG\_20 | Fulltext prohledávaní logů, včetně technologií indexace pro účinné a rychlé prohledávání logů/záznamů v milionech |

# Parametry managementu pro dodávané FW

Je poptáván systém pro **Centrální správu firewallů** v síti Zadavatele. Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat centrální dohled nad IPsec VPN a splňovat Technické požadavky pro v tomto bodu uvedené parametry:

| **ID požadavku** | **Popis požadavku** |
| --- | --- |
| FW\_MAN\_01 | Musí se jednat o virtuální appliance s podporou VMware, KVM a Hyper-V nebo HW appliance |
| FW\_MAN\_02 | Množství spravovaných zařízení/virtuálních kontextů musí být minimálně 200 |
| FW\_MAN\_03 | Možnost škálovatelného navýšení množství spravovaných zařízení na základě licence |
| FW\_MAN\_04 | Musí se jedna o centrální management pro všechny UTM firewally |
| FW\_MAN\_05 | Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení) – multitenantnost |
| FW\_MAN\_06 | Možnost nastavení centrálních policy pro všechny zařízení |
| FW\_MAN\_07 | Podpora RESTfulAPI pro integraci se již aktivními systémy zadavatele |
| FW\_MAN\_08 | Možnost vytváření skupin zařízení na základě jejich geografické polohy nebo logického členění |
| FW\_MAN\_09 | Podpora vytváření vzorů konfigurací pro nově instalovaná zařízení |
| FW\_MAN\_10 | Možnost vytváření a aplikace konfiguračních skriptů pro spravované firewally |
| FW\_MAN\_11 | Revize konfigurací spravovaných firewallů, jestli nejsou pravidla duplikována |
| FW\_MAN\_12 | Ukládání konfiguračních revizí a porovnávání změn mezi nimi |
| FW\_MAN\_13 | Podpora SNMP, logování na SYSLOG server |
| FW\_MAN\_14 | Podpora centrálního upgradu firmwaru spravovaných firewallů |
| FW\_MAN\_15 | Podpora správy licencí spravovaných firewallů |
| FW\_MAN\_16 | Podpora stahování signatur přes centrální management pro spravovaná zařízení |
| FW\_MAN\_17 | Podpora centrální konfigurace a monitoring VPN sítě |
| FW\_MAN\_18 | U monitoringu IPsec VPN možnost manuálního shození a nahození tunelu |
| FW\_MAN\_19 | Možnost správy administrátorských účtů na základě profilů, kde dle přiřazeného profilu bude mít daný administrátor oprávnění vidět nebo spravovat zařízení v různých administrativních kontextech |
| FW\_MAN\_20 | Možnost nastavení módu, kdy bude hlavní administrátor schvalovat změny v konfiguraci firewallů ještě před tím, než se aplikují |
| FW\_MAN\_21 | Podpora vzdáleného ověření administrátorů přes RADIUS a LDAP |
| FW\_MAN\_22 | Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů |
| FW\_MAN\_23 | Konzistentní modifikace politiky více administrátory najednou, konzistence politik na základě uzamykání pravidel, politik a objektů |
| FW\_MAN\_24 | Hit count statistiky pro jednotlivá pravidla za účelem optimalizace bezpečnostní politiky |
| FW\_MAN\_25 | Integrovaný monitoring musí poskytovat grafické rozhraní pro sledování parametrů v reálnem čase (využití paměti, CPU, počet navázaných spojení, počet nově otevřených spojení za sekundu, propustnost atd.). |
| FW\_MAN\_26 | Bezpečnostní audit, provedení bezpečnostních testů správného nastavení fw, upozornění na správný firmware, vypršení licencí atd., nepoužívaných pravidel, správného nastavení interních segmentačního fw, endpoint compliance, soulad s bezpečnostními practices. |
| FW\_MAN\_27 | Podpora revizí bezpečnostních politik, jejich verzování |
| FW\_MAN\_28 | Podpora auditních informací u změn bezpečnostní politiky (kdo provedl změnu) |

# Řešení SANDBOX – SANDBOX, hostované v infrastruktuře Metropolnet a.s.

Je poptáváno řešení ochrany před zero-day škodlivým kódem, viry a malware (založeném na principu tzv. sandbox) ve formě HW appliance (pokud je k dispozici) nebo VM appliance (pokud je k dispozici, v případě VM musí být součástí ceny i doporučené provozní HW/SW vybavení)

1. Dodávané řešení musí být plně integrováno s dodávaným firewallem za podmínky plné technické podpory výrobce (pro případ řešení potíží).
2. Plnou integrací se rozumí nativní integrace, umožňující obousměrnou komunikaci mezi firewallem/AS&AV (antispam/antivir) řešením a platformou sandbox (předávání souborů pro kontrolu, předávání detailních informací o kontrole zpět na firewall).
3. Součástí nabídky a dodávky musí být podpora výrobce a předplatné pro veškeré požadované funkce na dobu 5-ti let.
4. Navržené řešení VM Sandbox hostované v síti Metropolnet a.s. musí splňovat Technické požadavky pro v tomto bodu uvedené parametry:

**Hardwarové parametry:**

| **Id požadavku** | **Popis požadavku** |
| --- | --- |
| SAND\_I\_VM\_01 | Požadujeme řešení ve formě HW nebo VM appliance. Řešení musí umožňovat paralelní běh až 8 virtuálních operačních systémů. |
| SAND\_I\_VM\_02 | Součástí dodávky musí být licence na min. 4 virtuální systémy typu MS Windows (např. 7/8/10) |
| SAND\_I\_VM\_03 | Vše musí být součástí jedné HW nebo VM appliance. |
| SAND\_I\_VM\_04 | Požadujeme plnohodnotnou, výrobcem podporovanou a obousměrnou integraci s nabízeným modelem firewall a dalších bezpečnostních appliance. Dále musí být dostupná možnost integrace s interními systémy pomocí API. |
| SAND\_I\_VM\_05 | Sandbox musí být nakonfigurován tak, aby nekomunikoval přímo do internetu. Dodavatel navrhne způsob a možnosti managementu SANDBOX platformy v tomto scénáři – např. tím, že Výrobcem navržené řešení bude doplněno o management platformu, která bude instalovaná v samostatné DMZ s povoleným přístupem do internetu a se kterou bude SANDBOX komunikovat. Výjimkou je komunikace virtuálních strojů do internetu, která bude vedena samostatným fyzickým portem a samostatným internetovým připojením. |
| SAND\_I\_VM\_06 | U sandbox platformy nepožadujeme dodání vysoce dostupného řešení (HA), nicméně dodaná platforma musí tuto funkcionalitu podporovat s ohledem na možný další rozvoj sítě (včetně zvýšení výkonnosti formou active-active HA). To vše ale pouze za předpokladu, že zapojení do síťové infratruktury, s ohledem na požadované funkce, nevyžaduje nasazení tzv. v “inline režimu” a případný výpadek sandbox platformy neohrozí produkční komunikaci (komunikace uživatel do internetu, přístup uživatel do vnitřní sítě, emailová komunikace atd.). V opačném případě požadujeme dodání platformy sandbox ve vysoce dostupné HW konfiguraci, s požadovanou výkonností zajištěnou i při výpadku jednoho z uzlů sandbox clusteru. |
| SAND\_I\_VM\_07 | Oddělená konektivita pro systémovou/management komunikaci a pro komunikaci virtuálních strojů do internetu |
| SAND\_I\_VM\_08 | Podpora hypervisorů v případě VM appliance: VMWARE, KVM |

**Požadované funkce:**

| **Id požadavku** | **Popis požadavku** |
| --- | --- |
| SAND\_I\_F\_01 | Řešení musí poskytovat vícevrstvou ochranu před škodlivým kódem. Vícevrstvou ochranou je myšlena kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandbox (spuštění v reálném operačním systému). Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat. |
| SAND\_I\_F\_02 | Všechny prvky ochrany musí být poskytovány lokálně, nikoliv jako cloud služba. |
| SAND\_I\_F\_03 | Požadujeme následující podporované operační systémy: Windows XP, Windows 7, Windows 8.1, Windows 10, Android, MAC OS |
| SAND\_I\_F\_04 | Volitelně: Podpora zákaznické konfigurace Windows VM (zákazník si může připravit specifickou konfiguraci OS, využívanou jako standard v prostředí zákazníka). |
| SAND\_I\_F\_05 | Požadujeme ochranu proti zjištění běhu v sandbox prostředí (anti evasion techniky) |
| SAND\_I\_F\_06 | Požadujeme detekce komunikace s C&C centry |
| SAND\_I\_F\_07 | Požadujeme Podpora detekce přístupu na kompromitované URL |
| SAND\_I\_F\_08 | Požadujeme funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture, a v případě projevu malware v GUI také screenshoty) |
| SAND\_I\_F\_09 | Požadujeme podporu kontroly minimálně následujících typů souborů: spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. JPEG, QuickTime, MP3; archívy (ZIP/RAR/7ZIP/TNEF), asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm |
| SAND\_I\_F\_10 | Podpora reportování ve standardních formátech (HTML, CSV, PDF, XML, …) |
| SAND\_I\_F\_11 | Požadujeme automatická aktualizace signaturových databází. |
| SAND\_I\_F\_12 | Požadujeme automatické aktualizace VM zveřejněných výrobcem |

# Požadavky na Mailovou bránu

Je poptávána bezpečná e-mailová brána, jež bude implementována v transparentním módu jako sekundární ochranný prostředek a bude sloužit zejména jako sonda pro ochranu a nativní integraci s řešením Sandbox.

Navržené řešení na Bezpečnou mailovou bránu pro klienty sítě Metropolnet a.s. musí splňovat Technické požadavky pro v tomto bodě uvedené parametry.

*Pozn.: Pokud výrobce ve svém řešení bezpečnou bránu nenabízí, tak tuto skutečnost musí dodavatel jasně označit a uvést důvody (zejména bezpečnostní apod.), které ho k tomu vedou.*

**Obecné parametry SW:**

|  |  |
| --- | --- |
| **ID požadavku** | **Popis požadavku** |
| MA\_GE\_01 | Musí se jednat o virtuální appliance s podporou VMware, KVM a Hyper-V nebo HW appliance. Z důvodu výkonu nesmí být součástí dodávaných FW typu NG. |

**Výkonnostní parametry:**

| **ID požadavku** | **Popis požadavku** |
| --- | --- |
| MA\_PE\_01 | Směrování pošty – min. 30 000 zpráv (zpráv/hodinu, 100kb prům. velikost zprávy) |
| MA\_PE\_02 | Antispamová ochrana – min. 28 000 zpráv (zpráv/hodinu, 100kb prům. velikost) |
| MA\_PE\_03 | Antispamová a antivirová ochrana – min. 25 000 zpráv (zpráv/hodinu, 100kb prům. velikost) |
| MA\_PE\_04 | Podpora počtu provozovaných domén – alespoň 10 |

**Požadované funkce:**

|  |  |
| --- | --- |
| **ID požadavku** | **Popis požadavku** |
| MA\_FU\_01 | Možnost nasazení v režimu MTA a/nebo v transparentním režimu |
| MA\_FU\_02 | Možnost nasazení v režimu vysoké dostupnosti (včetně sdílené fronty) |
| MA\_FU\_03 | Plná podpora antivirové kontroly – AV kontrola musí být plně integrována s platformou Sandbox (viz níže), umožňující pokročilou ochranu před pokročilými typy hrozeb včetně tzv. zero-day útoků. Tato integrace musí být v režimu pozdržení emailu ve frontě až do konce analýzy na sandboxu. Je požadovaná integrace na úrovni sdílení signatur dynamicky vytvářených na platformě sandbox.  |
| MA\_FU\_04 | Kompletní nabídka antispamové funkcí; systém by měl podporovat minimálně následující AS funkce: |
| MA\_FU\_05 | * Kontrola na úrovni spojení, hlaviček i těla zprávy
 |
| MA\_FU\_06 | * Kontrola proti databázi známých SPAM zpráv, s neustálým přístupem k plně aktualizované DB
 |
| MA\_FU\_07 | * Kontrola proti reputační databázi odesílajících poštovních serverů
 |
| MA\_FU\_08 | * Velkou výhodou je i funkce lokální, dynamicky udržované reputační databáze komunikujících poštovních serverů a klientů
 |
| MA\_FU\_09 | * Behaviorální a heuristická analýza
 |
| MA\_FU\_10 | * Podpora tzv. Bayesova filtru
 |
| MA\_FU\_11 | * Analýza obrázků a pdf
 |
| MA\_FU\_12 | * Kategorizace URL obsažených v emailu
 |
| MA\_FU\_13 | * Podpora tzv. greylistingu
 |
| MA\_FU\_14 | * Podpora integrace s tzv. blacklisty třetích stran
 |
| MA\_FU\_15 | * Možnost nastavení citlivosti (váhy) Antispam policy
 |
| MA\_FU\_16 | * Centrální White/Black listy pro domény/maily/mailservery + uživatelské White/Black listy minimálně pro odesílatele
 |
| MA\_FU\_17 | * Možnost vytváření pravidel pro email gateway až na úroveň jednotlivých email účtů
 |
| MA\_FU\_18 | Podpora funkce DMARC |
| MA\_FU\_19 | Podpora IPv4 i IPv6 |
| MA\_FU\_20 | Podpora VLAN |
| MA\_FU\_21 | Možnost konfigurovat akci na základě detekovaného SPAMu: |
| MA\_FU\_22 | * Přidání tagu
 |
| MA\_FU\_23 | * Přidání hlavičky
 |
| MA\_FU\_24 | * Předání emailu na jiný poštovni server
 |
| MA\_FU\_25 | * Odmítnutí (reject)
 |
| MA\_FU\_26 | * Zahození (discard)
 |
| MA\_FU\_27 | * Uložení do karantény
 |
| MA\_FU\_28 | * Přepsání adresy příjemce
 |
| MA\_FU\_29 | Podpora karantény: |
| MA\_FU\_30 | * Včetně webového uživatelského přístupu do karantény
 |
| MA\_FU\_31 | * Uživatelská možnost zobrazení obsahu a hlaviček mailů v karanténě před uvolněním z karantény (pokud možno přímým odkazem u každého mailu z denního reportu).
 |
| MA\_FU\_32 | Plnohodnotná integrace s LOG manažerem a SIEM platformou (bude předmětem jiné VZ a oznámena Uchazeči před započetím projektu) a dále |
| MA\_FU\_33 | * uživatelská spam karanténa (lokalizace do ČEŠTINY) + přihlášení doménovým uživatelem (řešení SSO s AD)
 |
| MA\_FU\_34 | * možnost zasílání denních souhrnů ze spam karantény uživatelům s možností uvolnění jednotlivých mailů z karantény (lokalizace do ČEŠTINY)
 |
| MA\_FU\_35 | * možnost zobrazení minimálně hlaviček veškerých mailů v karanténě pro administrátora s možnost uvolnění mailů z karantény administrátorem
 |
| MA\_FU\_36 | * pro administrátora možnost zobrazení podrobného trasování příchozích i odchozích mailů s důvody odmítnutí mailů a zařazení do karantény
 |
| MA\_FU\_37 | Plnohodnotná integrace se síťovým dohledem GNU SW např. Zabbix, Nedi, Nagios (podpora SNMP (v2c, v3) včetně dostupnosti MIB souboru dodávaného výrobcem)  |

# OSTATNÍ POŽADAVKY ZADAVATELE

## Fakturační a dodací podmínky

Požadavky na dodavatele jsou následující:

1. Po podpisu smlouvy budou na etapy vystaveny objednávky (na každou etapu zvlášť):
	1. Etapa I.: Dodání HW zařízení
	2. Etapa II.: Implementace a zaškolení a nasazení do provozu
2. Dodávka bude rozdělena na 2 etapy:
* Dodávka v rámci Etapy I. bude dodána do sídla zadavatele najednou v termínu do 4 týdnů po přijetí objednávky Dodavatelem.
* Dodávka v rámci Etapy II. bude dodána do sídla zadavatele v období do 8 týdnů po skončení etapy I.
* O přesných datech a časech dodání bude dodavatel zadavatele informovat minimálně 5 pracovních dní před uskutečněním dodávky.
* O předání budou sepsány předávací protokoly, potvrzené osobou pověřenou zadavatelem pro tuto zakázku, obsahující podrobný seznam dodaných produktů (včetně sériových a jiných čísel) a místo dodání. Sériová čísla musí být viditelná na obalu bez nutnosti otevírat balení.
* Náklady na dodání na uvedená místa dodání, včetně nákladů na pojištění a vystavení dokumentů potřebných pro doručení na místa dodání jsou hrazeny dodavatelem.
1. Faktury budou vystaveny dodavatelem až po dodání všech produktů v rámci každé etapy na určená místa dodání a potvrzení všech předávacích protokolů:
* K fakturám budou přiloženy předávací protokoly.
* Faktury musí být vystaveny přímo dodavatelem.
* Faktury budou vystaveny zvlášť pro každou etapu se splatností 30 dní od úplného dodání zařízení v rámci etapy.
1. V databázi výrobce musí být zadavatel veden jako první uživatel zboží. Zadavatel požaduje originální a nová zařízení. Dodavatel je povinen doložit potvrzení od výrobce o určení dodávaného HW pro evropský trh a zadavatele (včetně sériových čísel dodávaných zařízení), pokud ho o to Zadavatel při dodání zařízení požádá.
2. U každého dodávaného zařízení Účastník uvede v nabídce jeho přesnou specifikaci, obchodní název, výrobce a identifikátor zboží (*part number*).

## Minimální požadavky na Záruční servis

Dodavatel musí zajistit minimálně následující podmínky záručního servisu:

1. Záruční doba bude činit minimálně 60 měsíců pro každý dodaný produkt a začne běžet dnem podpisu Předávacího protokolu – tj. po dodání všech zařízení příslušné etapy.
2. Účastník nabídne zadavateli možnost objednat v rámci Záručního servisu SLA služby po dobu 5 let, a to pro každou Etapu, nebo Typ zařízení (Log management pro FW, Nástroj pro centrální správu FW, Sandbox a Mailová brána) nezávisle. Je požadováno SLA a to: 8 x 5 x NBD s odezvou do 8 hodin při plnění v sídle zadavatele, a to při platnosti všech bodů tohoto odstavce.
3. Účastník poskytne Zadavateli po dobu trvání záručního servisu všechny relevantní verze SW nabízené výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad.
4. Dodavatel se zavazuje informovat zadavatele o nových verzích SW a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který zadavatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení. Dodavatel se zavazuje získat potřebné SW produkty legálním způsobem za podmínek stanovených výrobcem zařízení.
5. Dodavatel je povinen zajistit zadavateli přistup k dokumentaci výrobce zařízení a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
6. Zadavatel musí mít možnost se sám zaregistrovat na stránkách výrobce a musí mít možnost samostatného stahování nových verzí SW a registrace k odběru automatických e-mailových zpráv týkajících se dodávaných zařízení a upozorňující na tyto skutečnosti:
	1. bezpečnostní incidenty, které vyžadují od zadavatele povýšení operačního systému/firmware či aplikování změny konfigurace či opravy (záplaty),
	2. konec prodeje či podpory,
	3. nové verze operačního systému/firmware,
	4. známé chyby operačního systému/firmware.
7. Servisní zásahy v rámci záruky budou přednostně prováděny v místě plnění. Závada, jejíž odstranění z jakýchkoliv důvodů nebude na místě možné, nebo vhodné, bude řešena výměnným způsobem. Veškerá manipulace s opravovanou komponentou bude protokolárně zaznamenána. V případě, že oprava vadné komponenty nebude možná, bude předmětná komponenta nahrazena novou stejných nebo lepších parametrů, na níž bude možno provozovat stejný SW jako na původní.
8. Záruční podmínky budou jasně definovány v rámci Servisní smlouvy, jejíž textaci, Sankční a škodní podmínky navrhne dodavatel v rámci nabídky. Oboustranně odsouhlasené podmínky Servisní smlouvy jsou podmínkou pro uzavření Smlouvy o dílo mezi vítězným dodavatelem a zadavatelem.

## Testování nabízených zařízení Firewall

Zadavatel si vyhrazuje právo otestování shody udávaných parametrů propustnosti jednotlivých bezpečnostních funkcí s reálným měřením/chováním zařízení v testovacím prostředí. S ohledem na požadavky zadávací dokumentace mohou být/budou testovány zejména tyto funkce:

1. Test kapacity firewallu (UDP PPS test, test propustnosti UDP/512 1518 B)
2. Test počtu konkurenčních spojení (TCP)
3. Test počtu nově navazovaných spojení
4. Test propustnosti NGFW

Dodavatel se podáním nabídky zavazuje k bezplatnému zapůjčení testovací platformy, včetně generátoru požadovaných zátěží, pro provedení výše požadovaných testů. Testovací platforma musí odpovídat dodavatelem nabízeným platformám definovaným v (Log management pro FW, Nástroj pro centrální správu FW, Sandbox a Mailová brána).

V případě, že zadavatel při testech zjistí, že zařízení nesplňují požadované parametry, bude toto zadavatelem hodnoceno jako nesplnění zadávacích podmínek a účastník bude vyloučen z výběrového řízení pro nesplnění zadávacích podmínek.

Dodavatel se podáním nabídky zavazuje k dodání MIB k dodaným firewallům, ze které bude možné vyčítat minimálně následující parametry:

1. Vytížení procesoru (včetně jednotlivých jader), paměti a jednotlivých interface.
2. Počet celkových navázaných spojení, a průměrnou dobu potřebnou k navázání spojení.
3. Stavy hlavních systémových front.

V případě, že zadavatel v době záruky (60 měsíců) na základě provozních charakteristik, provozních obalových křivek nebo ad hoc testů pomocí testovací platformy, nezávislé na dodavateli zjistí, že libovolné zařízení nesplňuje požadované parametry, je dodavatel povinen zařízení nahradit vyšším modelem splňujícím požadované parametry na své náklady, a to včetně subskripcí analogicky k původně dodanému zařízení. Dále je povinen provést bezplatnou implementaci tohoto náhradního řešení, a to dle harmonogramu stanoveném zadavatelem.

Náhradní řešení bude vyhodnoceno a akceptováno zadavatelem, a to na základě Akceptační procedury, která bude provedena shodně jako akceptační procedura původní dodávky. Akceptovaná dodávka bude do 5 dní bezplatně převedena do majetku zadavatele.

Tyto případy nezbaví dodavatele povinnosti zaplatit smluvní pokuty a náhradu škody dle podmínek Smlouvy o dílo uzavřené na základě této veřejné zakázky.