Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **7.6. 2021** do odvolání.

1. Obsah Služby

Služba Managed Firewall spočívá v pronájmu výkonného bezpečnostního zařízení typu UTM od špičkového výrobce z oblasti síťové bezpečnosti, zajišťujícího služby firewallu, intrusion prevention systému (IPS), filtrace webového obsahu, antiviru, antispamu, antispyware, kontroly provozu a řízení IM/P2P aplikací, která zabraňuje narušení bezpečnosti kombinovanými útoky nebo neautorizovaným užíváním. Řešení je doplněno plným outsourcingem veškerých služeb konfigurace a správy tohoto zařízení. Managed Firewall může být nasazen v kombinaci se službami propojení poboček (VPN) a / nebo připojení k internetu a může také vhodně doplnit stávající firewall, který nedisponuje aplikačními ochranami, případně nemá integrovanou antivirovou či antispyware ochranu.

Základní princip Služby spočívá typicky v dodávce bezpečnostního řešení na rozhraní internetové přípojky a privátní sítě Smluvní partnera (LAN či VPN) – dle povahy služeb může být Zařízení (firewall) umístěno v datovém centru Poskytovatele, či přímo u Smluvního partnera. Veškerá firemní komunikace Smluvního partnera procházející Zařízením Poskytovatele je tímto zařízením kontrolována. Služba tak zajišťuje ochranu systémů Smluvního partnera a dodržování definovaných bezpečnostních politik. Zařízení a software jsou ve vlastnictví Poskytovatele a/nebo výrobce, včetně správy a konfigurace. Veškeré aktualizace operačního systému a modulů Zařízení, bezpečnostní patche (záplaty) vydané výrobcem a případné doplňkové služby jsou prováděny v komplexním outsourcingu prostřednictvím specialistů Poskytovatele, kteří mají v oblasti bezpečnosti dlouholeté zkušenosti.

Na straně Smluvního partnera se jedná pouze o definování bezpečnostní politiky uživatelů a jejich uživatelských práv (přístup do sítě Internet a využívání služeb jednotlivých aplikací), včetně možností pokročilé autentizace. Mezi klíčové výhody patří vysoká dostupnost Služby, což ve svém důsledku znamená, že zařízení bude v případě výpadku nebo poruchy nahrazeno tak, aby došlo k minimálnímu omezení provozu na straně Smluvního partnera. Náhrada je provedena bezplatně a zařízení je dodáno v požadované konfiguraci dle aktuálního funkčního nastavení tak, aby mohlo okamžitě po nasazení plnit bezpečnostní požadavky Smluvního partnera a nedošlo k jeho ohrožení.

Součástí Služby je i pravidelné hodnocení výkonnosti zařízení, které je na žádost Smluvního partnera možno provádět v pravidelných intervalech. V případě, že v průběhu poskytování Služby vzrostou potřeby nebo požadavky Smluvního partnera nad úroveň dodaného řešení, dojde k vyhodnocení požadavků na služby a na výkonnost zařízení a Smluvnímu partnerovi je nabídnuto výkonnější řešení.

2. Charakteristika Služby

2.1. Standardní funkce Služby/Zařízení poskytovaných pro Službu

2.1.1. UTM firewally (Unified Threat Management)

UTM firewally poskytované v rámci Služby disponují vynikajícími bezpečnostními a výkonovými parametry. Pro dosažení vysoké míry bezpečnosti bez negativního dopadu na datovou propustnost, jsou v zařízeních použity vysoce výkonné specifické procesory pro skenování aplikační vrstvy TCP/IP protokolu.

2.1.2. IDS / IPS (Intrusion Detection and Prevention Systém)

IDS podává varování vycházející z aktualizované databáze více než 1000 známých charakteristik útoků. IPS zastavuje útoky, které obcházejí běžné host-based antivirové systémy, přičemž reaguje v reálném čase na rychle se šířící útoky. Výrobce Zařízení v rámci své celosvětová sítě sleduje nové internetové hrozby a jejich „signatury“ (vzorky chování) v cca hodinových intervalech dodává do Zařízení na hranici sítě. Systém také podporuje metody založené na učení se a heuristice, což přidává cenné rozpoznávací schopnosti ve srovnání s prostým porovnáváním obsahu se známými šiframi.

2.1.3. Inspekce šifrovaného provozu

Zařízení umožňuje kontrolovat jak nešifrovaný webový provoz (protokol http), tak dnes i stále běžnější provoz šifrovaný (protokol https). Inspekce šifrovaného provozu probíhá ve 2 variantách.

Běžná inspekce nedešifruje vlastní provoz a hodnotí pouze vzorec (tzv. pattern) komunikace a dle známých vzorců útoků je schopna odhalit hrozící nebezpečí.
Hloubková inspekce, která díky architektuře a výkonnosti zařízení, významně nesnižuje výkon zařízení (propustnost), dešifruje vlastní provoz a provádí tak inspekci přímo kontrolou procházejících dat, stejně jako v případě nešifrovaného provozu. Zapnutí hloubkové inspekce se děje na žádost Smluvního partnera, zejména uvedením v konfiguračním formuláři, a vyžaduje na straně Smluvního partnera zajištění instalace bezpečnostních certifikátů na jeho koncových stanicích.

2.1.4. Archivace logů

Z provozovaného zařízení jsou archivovány veškeré logy (záznamy). Tyto logy jsou určeny pro provozní účely a jsou archivovány po potřebnou dobu (obvykle 1 kalendářní týden).

2.2. Doplňkové funkce

Základem Služby Managed Firewall je vlastní Firewall s aktivovaným IPS. Mimo funkcionalit, uvedených výše, které jsou základem Služby, zahrnuje Služba Managed Firewall další možnosti ve formě doplňkových funkcí. Tyto jsou také součástí Služby Managed Firewall a aktivují se na žádost Smluvního partnera dle požadavků uvedených zejména v konfiguračním formuláři.

2.2.1. Antivir a Antispam

Antivirus Gateway
Odhaluje a odstraňuje viry, červy a spyware v reálném čase. Prohlíží přílohy příchozích a odchozích emailů (SMTP, POP3, IMAP) a veškerý provoz přes FTP a HTTP včetně webových e-mailů, to vše bez snížení výkonu. Antivirová gateway zastavuje viry a červy dříve, než mohou vniknout do vnitřní sítě Smluvního partnera. Výrobce zařízení nabízí nepřetržité aktualizace antivirových signatur v reálném čase s využitím celosvětové aktualizační sítě.

Antispam
Antispam udržuje seznamy zakázaných (black list) a povolených (white list) domén, IP adres a e-mailových adres, které mohou být spravovány a aktualizovány podle potřeb Smluvního partnera. Obsahová filtrace koordinuje činnost s URL filtrací Služby - jde o techniku otisků vyhledávající specifické URL či jiné objekty jako například obrázky obsažené ve zprávách a porovnává je s otisky dříve identifikovanými jako původci spamu. Tento inovativní způsob tak umožňuje velice efektivní boj s obrázkovým a pdf spamem, se kterým má většina antispamových řešení potíže díky nemožnosti číst a následně zpracovávat text v obrázku.

2.2.2. Webový filtr (web filtering)

Webfiltering testuje veškerý webový obsah na výskyt známých nežádoucích URL, blokuje nevhodný obsah a nebezpečné Java aplety, cookies, Active X skripty před jejich vstupem do sítě. Web filterng kategorizuje více než 50 milionů domén a přes dvě miliardy webových stránek tak, aby ochránil Smluvního partnera před nežádoucími stránkami. Filtrování webových stránek spolupracuje dynamicky se systémy, které poskytují automatické aktualizace kategorizovaných stránek, které jsou dle obsahu členěny do více než 70 kategorií. Služby jsou také uživatelsky přizpůsobitelné, aby umožnily Smluvnímu partnerovi přidat jednotlivé URL individuální/skupinové určení rozsahu přístupu (kategorizaci určuje výrobce Zařízení) pro zabránění přístupu k dalším nežádoucím stránkám. Filtrace obsahu webu zaručuje firmám zlepšenou produktivitu práce a dodržování interních pravidel, které jsou v rozporu např. s firemní etikou.

2.2.3. Aplikační kontrola a P2P provoz (application control + P2P)

Profilování provozu pomáhá Smluvnímu partnerovi optimalizovat a efektivně řídit datový tok pro maximální využití přenosových kapacit při dodržení garancí propustnosti, nízké čekací doby a potřebné šířky pásma pro kritické podnikové služby. Umožňuje kontrolovat (úplná blokace nebo vymezení maximální šířky pásma) využívání sítí pro sdílení dat (jako jsou kazaa, gnutella, eDonkey, BitTorrent, WinNY, apod). Tyto protokoly typicky navazují obrovské množství spojení, díky kterým jsou schopny vytížit (nebo i zahltit) přípojku do internetu na úkor pro společnost důležitějších protokolů a kritických podnikových služeb. Tyto sítě jsou navíc velkým zdrojem nelegálního obsahu a škodlivého software. Aplication control – kontrola obsahu dat přenášených z internetových stránek, typicky slouží pro odfiltrování (nebo omezení) datových přenosů různých aplikací (streamované video, audio, datová úložiště, herní portály) ze stránek typu rapidshare, youtube, online radia atd.

2.2.4. Reporting

V pravidelných intervalech (1x za kalendářní týden nebo 1x za kalendářní měsíc) bude formou e-mailu s přílohou ve formátu PDF zasílán na adresu Smluvního partnera uvedenou ve Specifikaci služby ucelený report v podobě grafů a tabulek, který bude popisovat využití definovaných parametrů Služby (četnost virů, provozních špiček, největších zdrojů SPAMu nebo vlastního internetového provozu) za sledované období. Jednotlivé možnosti a obsah reportu jsou dány strukturou nastavených doplňkových funkcí.

2.2.5. VPN koncentrátor (SSL)

VPN koncentrátor zajišťuje jednotlivým uživatelům vzdálený přístup do sítě Smluvního partnera přes technologie VPN. Pro službu je možno využít klientský VPN software přímo na koncových stanicích, nebo může být služba v tzv. portálovém módu, to znamená, že se připojený počítač nestává prvkem vzdálené sítě. Toto má své výhody i nevýhody – nedojde k infiltraci vzdálené sítě z potenciálně nebezpečného počítače mimo dosah správců sítě, nebude však možné vyměňovat data z připojeného počítače s ostatními síťovými zařízeními – sdílené disky, tiskárny.

Funkce VPN koncentrátoru (SSL) je Poskytovatelem podporována výhradně na straně koncentrátoru (firewallu), na straně koncové stanice (počítače apod.) Smluvního partnera je tato funkcionalita standardně poskytována bez podpory. Podporu na straně koncové stanice je možné zajistit na základě objednání Smluvního partnera formou zákaznického řešení Poskytovatele.

3. Zpoplatnění Služby

Cena služby je určena následujícími dokumenty:

1. Specifikace služby
2. Smlouva
3. Ceník služby Managed Firewall

V případě rozporu konkrétních ustanovení jednotlivých dokumentů mají přednost ustanovení výše uvedeného dokumentu.

3.1. Měsíční poskytování (provoz) Služby obsahuje:

- Pronájem veškerého zařízení (hardware), zajištění softwarových licencí pro provoz Služby
- Správu Služby a zajištění její trvalé funkčnosti dle definovaných garantovaných parametrů
- Technickou podporu a konfiguraci Služby v rozsahu 1 hodiny/kalendářní měsíc (technickou podporou se rozumí především vzdálené úpravy konfigurace Služby dle požadavků Smluvního partnera) - větší objem technické podpory a vyšší limity garantovaných parametrů je možné dokoupit prostřednictvím příplatku za vyšší třídu garantovaných parametrů (Premium, Nonstop).
- Upgrade firmwaru a softwaru Zařízení, kontrola licenční politiky výrobce (zajištění potřebných licenčních update)
- Provozní, servisní a administrativní náklady Služby (včetně softwarových upgradů databáze antiviru, antispamu a antispyware, bezpečnostní záplaty a upgrade software, kontrola licenční politiky výrobce (hlídání expirace licencí a update software)
- Havarijní zásah v případě poruchy Zařízení (dle zvolené technické podpory),
- Vytvoření a uchování zálohy poslední změny konfigurace.

Vyhodnocení a nasazení bezpečnostních záplat (patchů) je plně v kompetenci Poskytovatele služby, pokud není ve Specifikaci služby explicitně uvedeno jinak. Poskytovatel je oprávněn testovat úroveň bezpečnostního řešení (vulnerability scan) dle doporučení daných výrobcem, nezávislými autoritami v oblasti síťové bezpečnosti a vlastními interními pravidly (formou best practice).

3.2. Měsíční poskytování (provoz) Služby neobsahuje:

- Technickou podporu vyžádanou Smluvním partnerem, která přesáhne časový objem obsažený ve standardní Službě (dle zvolené varianty)
- Havarijní zásah, pokud závada či nefunkčnost Zařízení byla způsobena Smluvním partnerem, uživatelem, třetí osobu, apod. – tzn. z příčin, které neleží na straně Poskytovatele.

4. Minimální doba užívaní Služby

Minimální doba užívání Služby Managed Firewall je stanovena na 12, 24 nebo 36 měsíců dle požadavku Smluvního partnera, není-li výslovně dohodnuta mezi Poskytovatelem a Smluvním partnerem jiná doba ve Smlouvě/Specifikaci služby.

5. Nabídka Služeb

5.1. Model Služby

Služba Managed Firewall umožňuje dva modely poskytování Služby:

a) Dedikovaný (vyhrazený) Managed Firewall – Zařízení je vyhrazeno pouze pro jednoho konkrétního Smluvního partnera
b) Sdílený Managed Firewall – Zařízení je využíváno větším počtem zákazníků, kteří jsou technologií výrobce od sebe bezpečně odděleni

Dedikovaný model
V případě dedikovaného modelu je Smluvnímu partneru vyhrazeno konkrétní Zařízení. Toto Zařízení může být umístěno buď v lokalitě (např. datovém centru) Smluvního partnera nebo v Datovém centru poskytovatele – viz kapitola Umístění Služby. V případě Dedikovaného modelu je pro Smluvního partnera určeno vždy 1 konkrétní Zařízení bez zálohování. Smluvní partner si v rámci Dedikovaného modelu může zvolit řešení typu Cluster, kde jsou pro Službu použita Zařízení dvě ve shodné konfiguraci a tedy redundantní.

Sdílený model
Sdílený model Služby je poskytován na „clusterové“ (zálohované) platformě, která díky tomuto řešení dosahuje větších dostupností Služby. U sdíleného modelu je automaticky řešena redundance konektivních služeb mezi clusterovou platformou a páteřní sítí Poskytovatele. Sdílenou variantu Služby je možné považovat za ekvivalent clustrového provedení dedikovaného řešení, avšak s tím rozdílem, že v rámci sdílené varianty Služby je fyzická infrastruktura sdílena větším počtem uživatelů. Každý virtuální kontext (vyhrazený pro Službu jednoho zákazníka) je striktně oddělený s plnou možností individualizace z pohledu správy a nastavení služeb. Sdílený model Služby lze poskytnout pouze v kombinaci s konektivními službami Poskytovatele.

Zvláštním řešením sdíleného modelu je poskytování Služby ze dvou geograficky oddělených datových center Poskytovatele. Tento model se nazývá GeoCluster a zajišťuje tak ze své technologické podstaty maximální možnou míru redundance a tím i dostupnosti Služby.

U sdílené varianty nelze využít doplňkový model DMZ. Pokud je požadována volba doplňkového modulu DMZ, je potřeba zvolit z nabídky Dedikovaných variant, případně využít službu Multiple IP VPN.

5.2. Umístění Služby

Při poskytování Služby v Dedikovaném modelu může být Zařízení (firewall) umístěno v prostorách Smluvního partnera (např. prostory Smluvního partnera, Datové centrum Smluvního partnera, prostor v Datovém centru libovolného poskytovatele pronajatý Smluvním partnerem či jiné odpovídající umístění). V případě umístění dedikovaného Zařízení v prostorách Smluvního partnera budou veškeré náklady spojené s fyzickým umístěním Zařízení – např. elektrické napájení, chlazení prostor a zařízení, připojení do sítě Poskytovatele – hrazeny přímo Smluvním partnerem
. Při umístění dedikovaného zařízení v Datovém centru Poskytovatele jsou náklady na umístění zařízení (viz výše) hrazeny Poskytovatelem a jsou promítnuty do ceny Služby.

Volba umístění závisí na přání Smluvního partnera nebo může být determinována konkrétní topologií a parametry vlastního řešení.

Při poskytování Služby ve Sdíleném modelu je zařízení (firewall) umístěno vždy v Datovém centru/Datových centrech Poskytovatele a náklady na jeho fyzické umístění tak vždy hradí Poskytovatel.

5.3. Varianty služby

Služba je v Dedikovaném i Sdíleném modelu poskytována ve čtyřech výkonnostních variantách – Basic, Normal, Profi a Exclusive (řešení typu GeoCluster je poskytováno pouze ve variantách Normal, Profi a Exclusive).

Doporučené parametry jednotlivých nabízených variant Služby jsou následující:

Varianta Služby	Maximální propustnost při plné inspekci a zapnutí všech funkcí zařízení	Nejvyšší počet současně pracujících koncových uživatelů
Basic	250 Mb/s	25
Normal	500 Mb/s	40
Profi	660 Mb/s	80
Exclusive	1 000 Mb/s	120

6. Zřízení a poskytování (provoz) Služby

Zařízení jsou ve vlastnictví Poskytovatele, Poskytovatel k nim zajišťuje nezbytný software. V rámci poskytování Služby je zahrnuta správa a konfigurace příslušného Zařízení a software. Veškeré aktualizace operačního systému a modulů zařízení, bezpečnostní patche (záplaty) vydané výrobcem a další služby jsou prováděny prostřednictvím specialistů Poskytovatele. Na straně Smluvního partnera je nutné definování bezpečnostní politiky, oprávněných uživatelů a jejich uživatelských práv.

6.1 Lhůta pro zřízení Služby

Standardní lhůta pro zřízení Služby činí obvykle **15** pracovních dní ode dne podpisu Smlouvy (Specifikace služby) Poskytovatelem a Smluvním partnerem. Tato lhůta neplatí v případě, kdy je společně se Službou Managed Firewall zřizována i jiná služba Poskytovatele a zřízení těchto služeb je navzájem provázáno. Nezbytnou podmínkou pro dodržení sjednaného termínu Služby je poskytnutí nezbytné součinnosti ze strany Smluvního partnera a rovněž i existence (zprovoznění) konektivních služeb, k nimž je tato Služba Managed Firewall zřizována.

6.2 Zřízení Služby obsahuje:

Dodávku a zapojení Zařízení v datovém centru Poskytovatele či u Smluvního partnera, nastavení výchozí konfigurace Zařízení a doplňkových funkcí dle Specifikace služby Managed Firewall a konfiguračního formuláře v rozsahu standardní instalace, uvedení do provozu, provedení testů a předání Služby Smluvnímu partnerovi.
Zřízení zahrnuje:

- Konfiguraci síťových rozhraní Zařízení
- Konfiguraci routingu (statický/dynamický) Zařízení
- Konfiguraci DNS serverů Zařízení
- Konfiguraci firewall pravidel
- Vytvoření zálohy základní konfigurace
- Oznámení o předání Služby Smluvnímu partnerovi

Celkový rozsah zřízení standardní Služby je limitován časovým objemem 4 hodin .

Zřízení Služby obsahuje i poinstalační podporu, kterou se rozumí technická podpora Poskytovatele v objemu 2 hodin, která je Smluvnímu partnerovi k dispozici po dobu prvního měsíce provozu Služby k odladění konfigurace dle jeho specifických potřeb.

Zřízení Služby nezahrnuje žádné práce na místních rozvodech ani konfiguraci LAN sítě Smluvního partnera. Doporučena je účast správce sítě v době instalace Služby.
Součástí zřízení Služby není žádný audit stávajícího zabezpečení a definice bezpečnostních pravidel pro Smluvního partnera.
Zřízení Služby neobsahuje, vzhledem k charakteru Služby, kdy se o její provoz plně stará Poskytovatel, žádné školení Smluvního partnera, resp. jeho uživatelů.

6.3 Předání Služby po jejím zřízení (zprovoznění)

Služba je zřízena a předána Smluvnímu partnerovi do provozu následně po nastavení výchozí konfigurace Zařízení dle konfiguračního formuláře, uvedení do provozu, provedení testů a předání Předávacího protokolu Služby, který je zaslán na kontaktní osobu Smluvního partnera.

Následně má Smluvní partner lhůtu 2 pracovních dnů na odzkoušení funkčnosti, konfigurace nastavení parametrů, porovnání souladu Služby s parametry dle konfiguračního formuláře a potvrzení převzetí Služby v souladu s dále uvedeným.

V uvedené lhůtě je Smluvní partner povinen potvrdit Poskytovateli písemně (formou e-mailu) převzetí Služby dle příslušné Specifikace služby, resp. může uplatnit připomínky nebo reklamovat funkčnost a parametry Služby, jinak se má za to, že uplynutím lhůty dvou celých pracovních dnů se Služba považuje za řádně předanou v souladu s příslušnou Specifikací služby. Okamžikem doručení potvrzení převzetí Služby ze strany Smluvního partnera Poskytovateli bez výhrad, resp. marným uplynutím uvedené lhůty, je Služba považována za řádně zřízenou ve smyslu příslušné Specifikace služby ze strany Poskytovatele vůči Smluvnímu partnerovi. Pro vyladění konfigurace Služby pro specifické potřeby Smluvního partnera je určena především poinstalační podpora v objemu 2 hodin v prvním měsíci poskytování Služby.

7. Technická podpora Služby

Poskytovatel poskytuje Smluvnímu partnerovi následující varianty technické podpory Služby. Varianta Standard je součástí standardní Služby a je již zahrnuta i v základní Cenové nabídce služby. Varianty technické podpory Premium a Nonstop jsou Smluvnímu partnerovi k dispozici za příplatek stanovený v platném Ceníku služby Managed Firewall, popř. sjednaný výslovně Smluvními stranami ve Smlouvě/Specifikaci služby.

Technická podpora	Standard	Premium	Nonstop
Zákaznická a technická podpora vzdáleně	24 x 7	24 x 7	24 x 7
Rozsah TP podpory/kalendářní měsíc (úpravy, nastavení, rekonfigurace, řešení uživatelských problémů)	1 hodina	2 hodiny	4 hodiny

Výluky z SLA a obecné podmínky SLA a odpovědnosti Poskytovatele za zřízení a poskytování Služby jsou stanoveny v platném dokumentu Popis služby SLA v jeho článku „Výluky z SLA“ a článku „Závěrečná ustanovení“, které se uplatní i na zřízení a poskytování Služby Managed Firewall, resp. zde definované SLA Služby Managed Firewall.

8. Podmínky poskytnutí Zařízení do užívání

Součástí Služby je poskytnutí Zařízení (nebo vyhrazení zařízení či části sdíleného zařízení) včetně jeho příslušenství nezbytného pro řádné poskytnutí Služby (účel poskytnutí zařízení), a to po dobu užívání Služby na základě příslušné Specifikace služby. Specifikace zařízení je stanovena ve Smlouvě / předávacím protokolu Služby.
Součástí Zařízení je i příslušný software, k němuž jsou Smluvnímu partnerovi zajištěna dočasná užívací práva po dobu trvání užívání Služby na základě příslušné Specifikace služby. Zařízení zůstává po celou dobu poskytování Služby ve vlastnictví Poskytovatele. Smluvní partner není oprávněn se zařízením, jakkoliv disponovat (např. provádět zásahy na zařízení nebo zařízení přesouvat), ani jej jakkoliv zcizit. Smluvní partner není oprávněn dát Zařízení do užívání třetí osobě bez předchozího písemného souhlasu Poskytovatele. Smluvní partner není oprávněn použít Zařízení k jinému účelu než k účelu zřízení a poskytování Služby dle Smlouvy. Smluvní partner je oprávněn užívat Zařízení výhradně pouze se Službou a v případě Dedikovaného modelu pouze v lokalitě Smluvního partnera uvedené ve Smlouvě. S ohledem na to, že se jedná o managed Službu, tak Smluvní partner není oprávněn sám nebo prostřednictvím třetí osoby jakýmkoliv způsobem měnit jakékoliv parametry Služby, zejména však není oprávněn nijak zasahovat do poskytnutého Zařízení včetně software a/nebo jeho nastavení. Zásahy do Zařízení včetně software a/nebo jeho nastavení je oprávněn provádět výlučně Poskytovatel, resp. jeho subdodavatel. Poskytovatel nenese jakoukoliv odpovědnost za vady v poskytování Služby (včetně jakékoliv další újmy tím způsobené) způsobené v důsledku jakýchkoliv zásahů

do Zařízení včetně software a/nebo jeho nastavení. Porušení povinnosti dle předchozích vět Smluvním partnerem se považuje za podstatné porušení povinnosti dle Smlouvy.
Smluvní partner je povinen užívat Zařízení jako řádný hospodář ke sjednanému účelu a v souladu s tímto Popisem služby a Smlouvou, dbát o jeho dobrý stav a zabránit jeho poškození. Smluvní partner je povinen upozornit Poskytovatele na všechna zjištěná nebezpečí a závady, která mohou vést ke vzniku škod na Zařízení. Smluvní partner je povinen oznámit Poskytovateli bez zbytečného odkladu potřeby oprav Zařízení, které má provést Poskytovatel.
V případě Dedikovaného modelu je Smluvní partner povinen počínat si tak, aby nedošlo k poškození, zničení nebo ztrátě zařízení. Smluvní partner je zejména povinen dodržovat podmínky stanovené v návodu k obsluze Zařízení, v tomto Popisu služby, ve Smlouvě, popř. jiné oprávněné pokyny Poskytovatele, resp. jeho subdodavatele či výrobce. Smluvní partner je povinen nahradit Poskytovateli v plné výši škodu, která mu vznikne v důsledku poškození, ztráty či odcizení Zařízení včetně software a příslušenství, a to bez ohledu na zavinění, zejména uhradit Poskytovateli veškeré náklady spojené s opravou Zařízení (včetně přepravních nákladů a jiných nákladů s tím spojených) a/nebo náhradu škody za ztracené, odcizené či neopravitelné Zařízení.
V případě Dedikovaného modelu se v případě ukončení poskytování Služby Smluvní partner zavazuje umožnit deinstalaci Zařízení a poskytnout k tomu potřebnou součinnost, a to nejpozději do 5 pracovních dnů ode dne ukončení poskytování Služby. Zařízení je povinen předat ve stavu, v jakém jej převzal, s přihlédnutím k běžnému opotřebení. Pro případ prodlení s umožněním deinstalace Zařízení dle předchozích vět je Smluvní partner povinen uhradit Poskytovateli smluvní pokutu ve výši 1/30 ceny Služby včetně DPH za každý i započatý den prodlení a dále náhradu škody přesahující smluvní pokutu.
Servisní podporu Zařízení bude po dobu trvání Smlouvy, resp. poskytování Služby, zajišťovat Poskytovatel sám nebo prostřednictvím subdodavatele, a to v souladu s podmínkami dále uvedenými nebo podmínkami uvedenými v Popisu služby SLA. Smluvní partner není oprávněn zajišťovat servisní podporu Zařízení, zejména odstraňování vad Zařízení, sám či pomocí třetí osoby odlišné od Poskytovatele, resp. jeho subdodavatele či výrobce.

9. Podmínky poskytnutí součinnosti Smluvním partnerem a technické předpoklady pro Zřízení a poskytování Služby na straně Smluvního partnera

Včasné / řádné zřízení a poskytování Služby závisí i na včasném a úplném poskytnutí součinnosti ze strany Smluvního partnera, a proto je Smluvní partner povinen pro včasné/řádné zřízení, změnu a poskytování Služby zajistit zejména následující činnosti:

- zajištění součinnosti osob znalých prostředí Smluvního partnera v rozsahu nezbytném pro správné iniciální nastavení a následné řádné a plynulé poskytování Služby (zejména v případě Dedikovaného modelu);
- poskytnutí Poskytovatelem požadovaných informací a dokumentace;
- zajištění přístupu Poskytovatele, resp. jeho subdodavatele, do prostor Smluvního partnera, ve kterých je umístěno zařízení (v případě Dedikovaného modelu);
- umožnění vzdáleného připojení k Zařízení poskytnutémuo v rámci Služby.

V případě Dedikovaného modelu je Smluvní partner povinen zajistit a udržovat následující podmínky pro umístění Zařízení:

- čisté neprašné prostředí
- nepřerušené napájení: střídavé napětí 220 V – 230V / 50Hz – 60Hz
- provozní teplota / vlhkost: 0°C – 40°C bez kondenzující vlhkosti
- na Zařízení není dovoleno pokládat žádné předměty, ani ho nijak zakrývat.
- se Zařízením není dovoleno nijak manipulovat, vyjma pokynů daných prostřednictvím Zákaznického centra, Oddělení Technické podpory nebo Dohledového centra služeb Poskytovatele.

Poskytovatel neodpovídá za prodlení se splněním svých povinností či újmu způsobenou nedostatkem součinnosti či nezajištěním podmínek pro zřízení a poskytování Služby, ke kterým je Smluvní partner povinen dle tohoto Popisu služby a/nebo Smlouvy, nebo které je povinen objektivně poskytnout/zajistit.

10. Změny nastavení parametrů a konfigurace Služby

Iniciální nastavení Služby Smluvní partner určí v konfiguračním formuláři, který je jedním ze základních předpokladů pro zřízení Služby.
Následnou změnu parametrů nebo konfigurace Služby (dále jen „Změna nastavení Služby“) Smluvní partner objednává u Poskytovatele:

a) V případě Změny nastavení Služby ovlivňující cenu Služby prostřednictvím změnové Specifikace služby
b) V ostatních případech Smluvní partner o změnu telefonicky či e-mailem požádá „Oddělení péče o zákazníky“,
c) Změna varianty Služby (Basic, Normal, Profi nebo Exclusive) je pro účely Smlouvy považována za ukončení původní Služby (ukončení původní Specifikace služby) a zřízení nové Služby dle nové Specifikace služby, popř. změnové Specifikace služby.
   Změny nastavení Služby jsou prováděny v rámci hodin sjednané Technické podpory Služby. Pokud je rozsah a pracnost Změny nastavení služby náročnější než příslušný rozsah hodin technické podpory sjednaný v rámci Služby, mohou být tyto změny zpoplatněny dle platného Ceníku služby Managed Firewall. Požadavek na Změnu nastavení Služby muže podat jen oprávněný zástupce Smluvního partnera. Žádné změny nelze provádět v době 5 a méně pracovních dní před dohodnutým termínem zřízení Služby.

11. Reklamace Služby, řešení odstranění výpadku (Poruchy) Služby

„Oddělení péče o zákazníky“ je dostupné 24 hodin denně, 365 dní v roce a hovory jsou vyřizovány nepřetržitě. Pro urychlení odstranění Poruchy/vyřízení reklamace Služby Poskytovatel požaduje, aby jej Smluvní partner kontaktoval již při prvních známkách závady. Hlášení Poruchy/vyřízení reklamace Služby je povinen Smluvní partner provést telefonicky na pracoviště „Oddělení péče o zákazníky“ Poskytovatele. Kontakt je specifikován ve Smlouvě.
Informace Smluvního partnera (hlášení) o závadě/reklamaci Služby musí obsahovat zejména:

- identifikace Smluvního partnera (název, IČO, číslo Smluvního partnera nebo číslo smlouvy mezi Poskytovatelem a Smluvním partnerem)
- identifikace místa Poruchy (adresa místa koncového bodu služby / lokalita Smluvního partnera, nebo místa Poruchy)
- popis Poruchy/reklamace
- datum a čas vzniku Poruchy
- jméno a příjmení osoby jednající jménem Smluvního partnera a jeho telefonické spojení.

„Oddělení péče o zákazníky“ podnikne potřebné kroky k odstranění Poruchy/vyřízení reklamace. Smluvnímu partnerovi bude přiděleno číslo závady, které bude používat při následných kontaktech, aby bylo možno správně sledovat postup opravy.

V rámci analýzy a následného odstranění vady Služby je Smluvní partner povinen poskytnout nutnou poskytovateli součinnost, zejména však:

- Odpojení Zařízení od napájení a následné připojení zařízení k napájení;
- Reset Zařízení pomocí tlačítka;
- Test funkčnosti internetového připojení s odpojeným Zařízením;
- Zajistit přístup Poskytovatele, resp. jeho subdodavatele, do prostor, ve kterých se nachází Zařízení včetně příslušenství.

Pokud nelze Poruchu Služby odstranit zásahem „na dálku“ s pomocí obsluhy Smluvního partnera, pověřené pracoviště Poskytovatele zorganizuje k opravě Poruchy servisní zásah, který provádí servisní skupina na základě příkazu. Výjezd technika v případě závady způsobené Smluvním partnerem je zpoplatněn dle platného Ceníku služby Managed Firewall. Za Poruchu způsobenou Smluvním partnerem je považován i tzv. marný výjezd technika (Porucha neexistuje nebo je Smluvním partnerem znemožněno provést potřebné práce k odstranění Poruchy v dohodnutém termínu, či neposkytnutí příslušné součinnosti ze strany Smluvního partnera při odstranění vady Služby nebo Poruchu prokazatelně zavinil Smluvní partner).

12. Poskytování Služby zahájené před 7.6.2021

Tato část uvádí pouze odchylky oproti výše uvedenému Popisu služby, a to pro Službu Managed Firewall zřízenou (a zároveň nezměněnou Změnovou Specifikací služby) přede dnem 7.6.2021

1. Charakteristika Služby

1.1 Standardní varianty Služby - Firewall + Intrusion prevention (IPS)

UTM firewally (Unified Threat Management)

UTM firewally nabízejí nedostižné bezpečnostní a výkonové parametry ve všech svých produktech. Pro dosažení vysoké míry bezpečnosti bez negativního dopadu na datovou propustnost, vyvinul Fortinet vysoce výkonný ASIC procesor pro skenování aplikační vrstvy TCP/IP protokolu – FortiASIC. Dalším patentem je Content Pattern Recognition Language (CPRL), který urychluje neustále se opakující operace užívané při analýze obsahu dat. Tato technologie je mnohem pokročilejší než hloubková kontrola paketů, kterou používá mnoho konkurenčních firewallů. Díky výhodě sdílení informací mezi bezpečnostními prvky je možné zabránit útokům, které nejsou založeny na signaturách a jsou dosud neznámé.

Intrusion Detection and Prevention System

Podává varování vycházející z přizpůsobitelné databáze více než 1300 známých šifer útoků. IPS zastavuje útoky, které obcházejí běžné host-based antivirové systémy, přičemž reaguje v reálném čase na rychle se šířící útoky. Celosvětová síť těchto zařízení nabízí Smluvním partnerům signatury šifer virů a útoků v reálném čase. Díky celosvětové aktualizační síti zastavuje IPS modul většinu ničivých útoků na hranici sítě bez ohledu na to, zda se jedná o síť klasickou, bezdrátovou nebo pobočku připojenou k síti. FortiASIC také podporuje metody založené na učení a heuristice, což přidává cenné rozpoznávací schopnosti ve srovnání s prostým porovnáváním obsahu se známými šiframi.

1.2 Doplňkové služby

Základem Služby je Firewall + Intrusion prevention systém (IPS), k tomuto základu je možné zvolit libovolné doplňující sady Služeb:

1.2.1 Antivir + Antispam

Antivirus Gateway

Odhaluje a odstraňuje viry, červy a spyware v reálném čase. Prohlíží přílohy příchozích a odchozích emailů (SMTP, POP3, IMAP) a veškerý provoz přes FTP a HTTP včetně webových e-mailů, to vše bez snížení výkonu. Antivirové gateway zastavují viry a červy dříve, než mohou vniknout dovnitř sítě. Celosvětový antivirový personál těchto zařízení nabízí Smluvním partnerům nepřetržité aktualizace antivirových signatur v reálném čase s využitím celosvětové aktualizační sítě FDN (FortiGuard Distribution Network).

Antispam

Antispam udržuje seznamy zakázaných (black list) a povolených (white list) domén, IP adres a e-mailových adres, které mohou být spravovány a aktualizovány podle potřeb společnosti. Obsahová filtrace koordinuje činnost s URL filtrací Služby FortiGuard - jde o techniku otisků vyhledávající specifické URL či jiné objekty jako například obrázky obsažené ve zprávách a porovnává je s otisky dříve identifikovanými jako původci spamu. Tento inovativní způsob tak umožňuje velice efektivní boj s obrázkovým a pdf-kovým spamem, se kterým má naprostá většina antispamových řešení potíže díky nemožnosti číst a následně zpracovávat text v obrázku.

1.2.2. Web Filtering

Webfiltering testuje veškerý webový obsah na výskyt známých nežádoucích URL, blokuje nevhodný obsah a nebezpečné Java aplety, cookies, Active X skripty před jejich vstupem do sítě. Web filterng kategorizuje více než 50 milionů domén a přes dvě miliardy webových stránek tak, aby ochránil Smluvního partnera před nežádoucími stránkami. Filtrování webových stránek spolupracuje dynamicky se systémy, které poskytují automatické aktualizace kategorizovaných stránek, které jsou dle obsahu členěny ve více než 70 kategoriích. Služby jsou také uživatelsky přizpůsobitelné, aby umožnily podnikové síti přidat další URL pro zabránění přístupu k dalším nežádoucím stránkám. Filtrace obsahu webu zaručuje podnikům zlepšenou produktivitu práce a dodržování regulací ve výchovných institucích znepřístupněním stránek, které jsou v rozporu s firemní etikou.

1.2.3 Reporting

V pravidelných intervalech bude formou e-mailu s přílohou ve formátu PDF zasílán ucelený report v podobě grafů a tabulek, který bude popisovat využití definovaných parametrů služeb (četnost virů, top provoz, top users, top spam apod.) za sledované období. Jednotlivé možnosti reportingu jsou dány i strukturou objednaných doplňkových modulů.

1.2.4 Ochrana úniku dat (DLP; Data-Leak Protection)

DLP zabrání odesílaní citlivých dokumentů Smluvního partnera mimo společnost a tím úniku důvěrných informací. Umožňuje kontrolu odchozích i příchozích dokumentů čitelných v plain-textu (dokumenty: *.txt, *.doc, *.rtf, apod.) na přítomnost definovaných (zakázaných) slov. V případě, že dokument definovaná slova obsahuje, DLP zabrání jeho odeslání. Kontrolu je možné provádět nad protokoly SMTP, FTP, HTTP.

1.2.5 Aplication control a P2P

Profilování provozu pomáhá Smluvnímu partnerovi optimalizovat a efektivně řídit datový tok pro maximální využití přenosových kapacit při dodržení garancí propustnosti, nízké čekací doby a potřebné šířky pásma pro kritické podnikové služby. Umožňuje kontrolovat (úplná blokace, nebo vymezení maximální šířky pásma) využívání sítí pro sdílení dat (jako jsou kazaa, gnutella, eDonkey, BitTorrent, WinNY, apod). Tyto protokoly typicky navazují obrovské množství spojení, díky kterým dokáží vytížit a přetížit přípojku do internetu na úkor pro společnost důležitějších protokolů a kritických podnikových služeb. Tyto sítě jsou navíc velkým zdrojem nelegálního obsahu a škodlivého software. Aplication control – kontrola obsahu dat přenášených z internetových stránek, typicky slouží pro odfiltrování datových přenosů rozličných aplikací (streamované video, audio, datová úložiště, herní portály) ze stránek typu rapidshare, youtube, online radia atd.

1.2.6 VPN koncentrátor (SSL)

VPN koncentrátor zajišťuje jednotlivým uživatelům vzdálený přístup do firemní sítě přes technologie VPN. Jedná se o alternativu k VPN přístupu založenému na protokolu IPSec, oproti kterému má mnohem vyšší prostupnost filtrovaným prostředím různých zdrojů internetové konektivity, kdy IPSec tunel nemusí být

možné navázat. Typicky se jedná o připojení přes veřejné hotspoty, v hotelech, internetových kavárnách a dalších sítích využívajících vícenásobný překlad adres a případné restrikce portů a protokolů. Služba běží v tzv. portálovém módu, to znamená, že na rozdíl od IPSec VPN se připojený počítač nestává prvkem vzdálené sítě. Toto má své výhody i nevýhody – nedojde k infiltraci vzdálené sítě z potenciálně nebezpečného počítače mimo dosah správců sítě, nebude však možné vyměňovat data z připojeného počítače s ostatními síťovými zařízeními – sdílené disky, tiskárny.

2. Zpoplatnění Služby

Služba je zpoplatněna:

- Smlouva/Specifikace služby
- Ceníkem služby Managed Firewall;
- Případně Ceníkem nadřazené hlavní konektivní služby (IP VPN, Profesionální Internet, housing apod.)

3. Zřízení a poskytování (provoz) Služby

3.1 Model Služby

V rámci řešení Služby Managed Firewall jsou uvažovány dva modely (profily): Dedikované (vyhrazené) Managed Firewall firewally pro jednotlivé uživatele anebo sdílené Managed Firewall firewally využívané větším počtem uživatelů. U sdílené varianty nelze využít možnosti volitelného setu DMZ. Pokud preferujete volbu tohoto doplňkového modulu, je potřeba zvolit z nabídky dedikovaných firewallů, případně využít Služby Multiple IP VPN.

Sdílený model Služby je možné nabídnout pouze v případě umístění firewallu v datacentru Poskytovatele – Nagano v Praze. Pokud je přístup k Internetu v jiné lokalitě (např. jiné datové centrum Poskytovatele, datové centrum Smluvního uživatele, datové centrum jiného subjektu či centrální pobočka Smluvního partnera), je nezbytné zvolit dedikovanou variantu Služby (zejména u Služby Profesionální internet). Sdílený model Služby lze poskytnout pouze s konektivními Službami od Poskytovatele.

Sdílená varianta (profil) Služby je poskytována na „clusterové“ platformě, která díky tomuto řešení dociluje významně větších dostupností Služby. Z pohledu konektivních služeb je u sdíleného řešení automaticky řešená redundance i konektivních služeb až do páteřní sítě poskytovatele služeb (ať už se jedná o službu Profesionální Internet nebo službu IP VPN). Sdílenou variantu Služby je možné považovat za ekvivalent clustrového provedení dedikovaného řešení, avšak s tím rozdílem že, v rámci sdílené varianty Služby je fyzická infrastruktura sdílena větším počtem uživatelů. Každý virtuální kontext je však plně oddělený s plnou možností individualizace z pohledu správy a nastavení služeb.

Doporučené parametry u jednotlivých nabízených variant Služeb:

Označení	Velikost zákazníka		Použití - účel						Vysoká dostupnost	
HTTP : HTTPS			Perimetrvý firewall		Perimetrový + Interní (segmentační) firewall					
50 : 50	Uživatelé	Nová spojení	WAN - Internet	Vzdálený přístup	WAN - Internet	LAN - routing	Vzdálený přístup	Segmenty sítě		
	počet	**počet za sek.**	**Internet IPS, AC, WF, Antivir**	**SSL VPN**	**Internet IPS, AC, WF, Antivir**	**L4 + IPS**	**SSL VPN**	**počet VLAN**	**HA**	**LACP**
MF Normal	45	80	80 Mbit/s	50	50 Mbit/s	150 Mbit/s	50	10	ANO	NE
MF Profi	50	80	100 Mbit/s	150	60 Mbit/s	200 Mbit/s	150	15	ANO	ANO
MF Exklusive	200	200	350 Mbit/s	250	250 Mbit/s	400 Mbit/s	250	25	ANO	ANO

3.2 Zřízení a poskytování (provoz) Služby Managed Firewall

Zařízení a software jsou ve vlastnictví Poskytovatele (resp. subdodavatele). V rámci poskytování Služby je zahrnuta správa a konfigurace příslušného zařízení a software. Veškeré aktualizace operačního systému a modulů zařízení, bezpečnostní patche (záplaty) vydané výrobcem a další služby jsou prováděny v komplexním outsourcingu prostřednictvím specialistů Poskytovatele, kteří mají v oblasti bezpečnosti dlouholeté zkušenosti. Na straně Smluvního partnera jde tedy pouze o definování bezpečnostní politiky, uživatelů a jejich uživatelských práv.

3.2.1 Zřízení standardní Služby obsahuje Firewall +IDS:

Dodávku a zapojení zařízení v datovém centru Poskytovatele či u Smluvního partnera, nastavení výchozí konfigurace zařízení dle Specifikace služby Managed Firewall v rozsahu standardní instalace, uvedení do provozu, provedení testů a předání Služby Smluvnímu partnerovi.

- Konfigurace síťových rozhraní
- Konfigurace routingu (statický/dynamický)
- Konfigurace DNS serverů
- Konfigurace firewall pravidel
- Vytvoření zálohy základní konfigurace
- Oznámení o předání Služby Smluvnímu partnerovi

Celkový rozsah zřízení standardní Služby je limitován časovým objemem 3 hodiny.

Zřízení standardní Služby obsahuje i poinstalační podporu, kterou se rozumí technická podpora v objemu 2 hodin, která je Smluvnímu partnerovi k dispozici po dobu prvního měsíce provozu Služby k odladění konfigurace dle jeho specifických potřeb.

Zřízení Služby nezahrnuje žádné práce na místních rozvodech ani konfiguraci LAN sítě Smluvního partnera. Doporučena je účast správce sítě v době instalace Služby. Součástí zřízení Služby není žádný audit stávajícího zabezpečení a definice bezpečnostních pravidel pro Smluvního partnera. Součástí zřízení Služby není školení Smluvního partnera, resp. uživatelů.

3.2.2 Měsíční poskytování (provoz) standardní Služby obsahuje Firewall + IDS:

- Dodávku a pronájem veškerého zařízení (hardware), pronájem softwarových licencí pro provoz Služby
- Správu Služby a zajištění její trvalé funkčnosti dle definovaných garantovaných parametrů
- Technickou podporu a konfiguraci Služby v rozsahu 1 hodiny/kalendářní měsíc (technickou podporou se rozumí především vzdálené úpravy konfigurace Služby dle požadavků Smluvního partnera) - větší objem technické podpory a vyšší limity garantovaných parametrů je možné dokoupit prostřednictvím příplatku za vyšší třídu garantovaných parametrů (Premium, Nonstop).
- Havarijní zásah v případě poruchy zařízení (dle zvolené technické podpory),
- Upgrade firmwaru a softwaru zařízení, kontrola licenční politiky výrobce,
- Hodnocení výkonnosti systému,
- Vytvoření a uchování zálohy poslední změny konfigurace.

3.2.3 Zřízení každé jednotlivé doplňkové Služby obsahuje:

Nastavení výchozí konfigurace zařízení dle Specifikace služby v rozsahu standardního zřízení doplňkové Služby, uvedení do provozu, provedení testů, předání Služby Smluvnímu partnerovi. Předpokládaný rozsah prací na zřízení doplňkové Služby do 2 hodin/jedna doplňková Služba.

3.2.4 Měsíční poskytování (provoz) doplňkové Služby obsahuje:

- Provozní, servisní a administrativní náklady Služby (včetně softwarových upgradů DB antiviru, antispamu, antispyware atd., bezpečnostní patche a upgrade software, kontrola licenční politiky výrobce apod. pro jednotlivé doplňkové Služby)
- Zálohování konfigurace doplňkové Služby

3.2.5 Měsíční poskytování (provoz) standardní i doplňkové Služby neobsahuje:

- Technickou podporu vyžádanou Smluvním partnerem, která přesáhne časový objem obsažený ve standardní Službě (dle zvolené varianty)
- Instalace nezahrnuje žádné práce na místních rozvodech ani konfiguraci LAN sítě Smluvního partnera. Doporučena je Smluvního partnera správce sítě v době instalace Služby.
- Havarijní zásah, pokud závada či nefunkčnost zařízení byla způsobena Smluvním partnerem, uživatelem, třetí osobu, apod. – tzn. z příčin, které neleží na straně Poskytovatele.

4. Varianty garantovaných parametrů Služby a rozsah technické podpory

Garantované parametry Služby jsou nabízeny ve 3 variantách. Parametry varianty Standard jsou součástí standardní Služby, parametry Premium a Nonstop jsou k dispozici na základě požadavku Smluvního partnera za příplatek stanovený v platném Ceníku služby Managed Firewall, popř. stanovený výslovně smluvními stranami ve Smlouvě/Specifikaci služby. U této služby jsou sledovány a vyhodnocovány garantované parametry Služby: Reakční doba a Maximální doba odstranění výpadku Služby. Více ke garantovaným parametrům Služby včetně smluvní sankce za porušení SLA je stanoveno v platném Popisu služby SLA.

Varianty garantovaných parametrů Služby
Poskytovatel poskytuje Smluvnímu partnerovi následující garantované parametry Služby (konkrétní sjednaná varianta garantovaných parametrů Služby je sjednána ve Smlouvě/Specifikaci služby, a pokud výslovně není sjednána, tak se má za to, že se jedná o variantu Standard):

Garantované parametry Služby	Standard	Premium	Nonstop
Reakční doba započetí řešení odstranění výpadku Služby. V pracovní době (tzn. v pracovní dny od 8:00 do 18:00)/mimo pracovní dobu (tzn. mimo pracovní dny a v pracovní dny od 18:00 do 8:00)*	max. do 3 h/ max. do 6h*	max. do 2h / max. do 5h*	max. do 1h / max. do 4h*
Maximální doba odstranění výpadku Služby – pro dedikovanou/sdílenou variantu Služby, kdy jsou zařízení umístěná v datových centrech Poskytovatele v Praze	max. do 18 h/ max. do 9 h	max. do 12 h/ max. do 6h	max. do 9 h/ max. do 6h
Maximální doba odstranění výpadku Služby – pro dedikovanou/sdílenou variantu Služby, kdy jsou zařízení umístěná kdekoliv v ČR (mimo datová centra Poskytovatele v Praze)	max. do 24 h	max. do 18 h	max. do 12 h
Zákaznická a technická podpora Služby na místě	max. do 24 h	max. do 18 h	max. do 12 h
Sdílená varianta Služby má definovaný čas pro plánovanou údržbu	max. do 2h/měsíc	max. do 2h/měsíc	max. do 2h/měsíc

Veškeré zde uvedené lhůty počínají běžet okamžikem doručení příslušného požadavku (na odstranění výpadku Služby nebo na zákaznickou a technickou podporu Služby na místě) sjednaným způsobem Poskytovateli ze strany Smluvního partnera.

V případě nedodržení kteréhokoliv sjednaného garantovaného parametru Služby ze strany Poskytovatele v důsledku jeho zavinění, je Smluvní partner oprávněn požadovat po Poskytovateli smluvní sankci ve výši 200,- Kč za každou hodinu prodlení u jednotlivého nedodrženého garantovaného parametru Služby. Souhrn všech smluvních sankcí za veškerá nedodržení kterýchkoli garantovaných parametrů Služby v jednom zúčtovacím období může činit maximálně výši sjednané pravidelné měsíční ceny za poskytování (provoz) sjednané varianty Služby. Tato smluvní sankce je Smluvnímu partnerovi poskytována formou slevy z vyúčtované pravidelné měsíční ceny Služby po doručení příslušného požadavku Smluvního partnera. O tuto smluvní sankci je Smluvní partner povinen písemně požádat Poskytovatele nejpozději do 2 měsíců od ukončení příslušného zúčtovacího období, za které má nárok na tuto smluvní sankci, jinak jeho právo na tuto smluvní sankci zaniká.

Technická podpora Služby

Poskytovatel poskytuje Smluvnímu partnerovi následující varianty technické podpory Služby. Varianta Standard je součástí standardní Služby a je již zahrnuta i v základní Cenové nabídce služby. Varianty technické podpory Premium a Nonstop jsou Smluvnímu partnerovi k dispozici za příplatek stanovený v platném Ceníku služby Managed Firewall, popř. stanovený výslovně smluvními stranami ve Smlouvě/Specifikaci služby.

Technická podpora	Standard	Premium	Nonstop
Zákaznická a technická podpora vzdáleně	24 x 7	24 x 7	24 x 7
Rozsah TP podpory/kalendářní měsíc (úpravy, nastavení, rekonfigurace, řešení uživatelských problémů)	1 hodina	2 hodiny	4 hodiny

5. Technické údaje Služby Managed Firewall

Služba Managed Firewall může být nedílnou součástí služeb propojení poboček a připojení k Internetu (VPN) a může také vhodně doplnit Váš stávající firewall, který nedisponuje aplikačními ochranami, případně nemá integrovanou antivirovou či antispyware ochranu pro http či smtp.

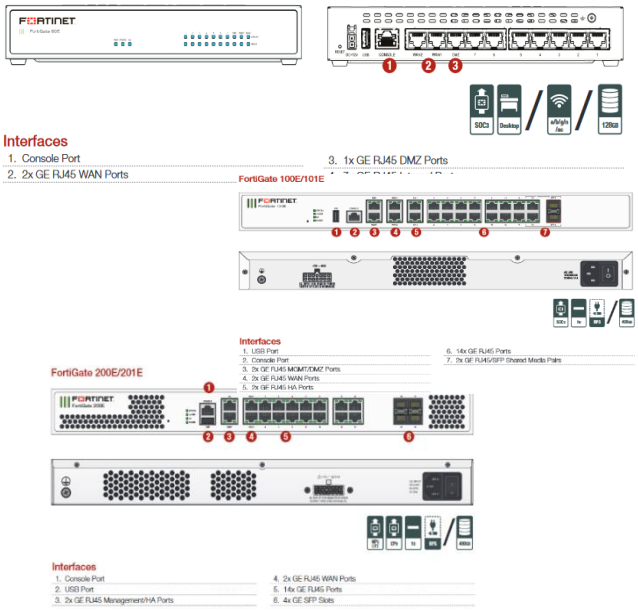
6. Změna varianty Služby

Změna varianty Služby (standardní, nestandardní, Normal, Profi, Exclusive) je pro účely smlouvy považovaná za ukončení původní Služby (ukončení původní Specifikace služby) a zřízení nové Služby dle nové Specifikace služby, popř. změnové Specifikace služby.

Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **7.6. 2021** do odvolání.

Technické prostředky, na kterých je Služba realizována:

Name (Fortigate)	60E	100E	200E
platform	SOC	SOC	CPU + ASIC
wan ports	2	2	2
HA ports		2	1
switch ports	7	14	14
SFP ports		2 shared	4 shared
LACP (802.3ad)	NO	YES	YES
Concurrent session (TCP)	1.3 M	2 M	2 M
New Sessions/Second (TCP)	30 K	30 K	135 K
S2S IPsec VPN Tunnels	200	2 K	2 K
RA IPsec VPN Tunnels	500	2 K	5 K
Concurrent SSL-VPN Users ***	100	300	300
FW throughput	3 Gb	4.4 Gb	20 Gb
Ipsec VPN throughput *	2 Gb	4 Gb	9 Gb
SSL VPN throughput	150 Mb	250 Mb	900 Mb
IPS performance	350 Mb	500 Mb	2.2 Gb
APP Control	550 Mb	800 Mb	3.5 Gb
NGFW	250 Mb	360 Mb	1.8 Gb
Threat protection	180 Mb	250 Mb	1.2 Gb
SSL Inspection (se zap. IPS)	340 Mb	350 Mb	1 Gb
VDOM (Default/Max)	10/10	10/10	10/10
Build in FAN	NO	YES	YES

FortiGate/FortiWiFi 60E/61E