Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

1 Obsah Služby

Managed Firewall alias Komplexní bezpečnost formou služby
Množství různých ohrožení datových sítí, souborů a identity je dnes nepřeberné. Viry, spyware, spamy, podvodné e-maily, škůdci online, hackeři, zloději identity a narušitelé bezdrátových sítí, to vše představuje ohrožení bezpečnosti pro Vás a Vaši firmu. Poskytovatel nabízí mimořádnou příležitost, jak jednoduše zajistit potřebnou ochranu pro Vaši síť na velmi vysoké úrovni – pomocí Služby **Managed Firewall.** Služba Managed Firewall je koncipovaná jako doplňková služba ke Službám VPN, Profesionální internet apod.

Managed Firewall spočívá v pronájmu špičkového bezpečnostního zařízení společnosti Fortinet (Fortigate), zajišťující služby firewallu, intrusion prevention systému (IPS), filtrace webového obsahu, antiviru, antispamu, antispyware, kontroly provozu a řízení IM/P2P, která zabraňuje narušení bezpečnosti kombinovanými útoky nebo neautorizovaným užíváním. Řešení je doplněno plným outsourcingem veškerých služeb správy. 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.
Podoba komplexní bezpečnosti jako služby přináší výrazné úspory oproti jednorázové investici do celého řešení a přitom nezvyšuje bezpečnostní rizika.

Základní princip Služby spočívá v dodávce špičkového bezpečnostního řešení na rozhraní internetové přípojky a privátní sítě Smluvní partnera (LAN či VPN – dle povahy služeb může být firewall umístěn v datovém centru Poskytovatele, či přímo u Smluvního partnera). Veškerá firemní komunikace Smluvního partnera prochází firewallem Poskytovatele, který zajišťuje ochranu systémů Smluvního partnera a dodržování definovaných bezpečnostních politik. Zařízení a software jsou ve vlastnictví Poskytovatele, včetně správy a konfigurace. 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 (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 tak, aby mohlo okamžitě plnit bezpečnostní požadavky Smluvního partnera a nedošlo k jeho ohrožení.

V případě, že v průběhu poskytování Služby vzrostou potřeby nebo požadavky Smluvního partnera nad úroveň dodaného řešení, dochází ke zhodnocení požadavků a výkonnosti zařízení a Smluvnímu partnerovi je nabídnuto jiné, vhodnější řešení. Součástí Služby je i pravidelné hodnocení a konzultace výkonnosti zařízení, které je na žádost Smluvního partnera možno provádět v pravidelných tříměsíčních intervalech.

2 Charakteristika Služby

2.1 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.

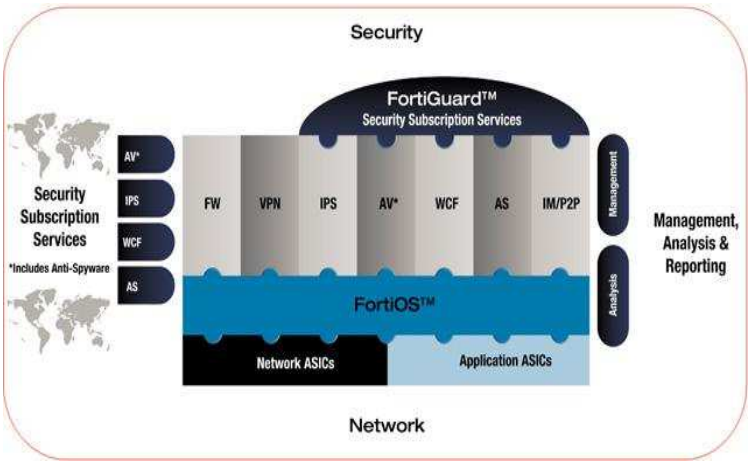
2.2 Doplňkové služby

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

2.2.1 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).



Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

1) U sdílené varianty bohužel nelze využít možnosti volitelného setu Antivir + Antispam (AV+AS). Pokud preferujete volbu tohoto doplňkového modulu je potřeba zvolit z nabídky dedikovaných firewallů.

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.

2.2.2. 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.

2.2.3 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.

2.2.4 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.

2.2.5 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.

2.2.6 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.

2.2.7 Test zranitelnosti (Vulnerability scan)

Umožňuje jednorázově zkontrolovat systémy zapojené v datové síti pro odhalení jejich zranitelností. Týká se zejména operačních systému (Windows, Linux i MacOS.), aplikačních a databázových serverů, odhalení backdooru, provozu P2P sítí, červů, DNS zranitelností, DOS zranitelností apod. Výstupem je PDF dokument, popisující nalezené zranitelnosti, míru jejich závažnosti, možnosti zneužití a informace pro správce sítě, jak tyto zranitelnosti odstranit, či jak zneužití těchto zranitelností zabránit.

3 Klíčové výhody Služby:

- Firewall je poskytován jako služba a je v plné správě odborníků Poskytovatele.
- Nulové investice na pořízení – měsíční poplatky za Službu jsou přímé provozní náklady, žádné náklady na hardware, jeho údržbu a upgrade, žádné náklady na software správu dalšího systému, úspora nákladů na řešení výpadků komunikace a dalších následků ataků hackerů, úspora provozních výdajů na bezpečnost (cena za poskytované služby je výrazně nižší než cena nutná na přímé pořízení a správu s využitím zkušeného specialisty), žádné riziko špatné nebo nedokončené implementace.
- Kompletní outsourcing umožňuje IT týmu Smluvního partnera věnovat se plně problematice vlastní práce, nikoliv se zatěžovat problematikou hrozeb Internetu, patchování, licencování a servisních smluv.
- Aktualizace software, upgrade hardware, sledování bezpečnostní problematiky, školený a zkušený personál.
- Jednoduché nasazení – síť Smluvního partnera může být chráněna během několika dnů.
- Garance kvality, komplexní zabezpečení – firewall, IPS, antivirová + antispam + antispyware ochrana, filtrování webového obsahu a vzdálený přístup „mobilních“ VPN klientů.
- Certifikace Common Criteria EAL4+, 8 certifikací ICSA Labs.
- Ochrání Vaši síť i celou VPN, navíc optimalizuje náklady na kapacitu připojení.
- Maximální spolehlivost a dostupnost poskytovaných služeb.
- Změny konfigurace firewallu - podle potřeb Smluvního partnera.
- Vysoká úroveň technické podpory – garance výměny zřízení v případě jeho výpadku.
- Dle povahy služby možnost hostování firewallu v prostorách datového centra Poskytovatele, které splňuje nejpřísnější kvalitativní limity datových center

Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

4 Klíčové funkce Služby:

- Zabezpečení vnitřní sítě Smluvního partnera na úrovni aplikačních kontrol komunikace (vyšší stupeň ochrany než běžná kontrola poskytovaná na opensourcových nebo i komerčních paketových firewallech).
- Umožňuje zabezpečený vzdálený přístup mobilních klientů do vnitřní sítě.
- Ochrana interního mailserveru a DNS díky jejich proxy funkcím přímo na firewallu.
- Antivirová, antispyware a antispamová ochrana pro http, smtp, pop3, IMAP, FTP...
- Kontrola odchozího web přístupu s IM a P2P blokováním.
- Detekce provozních anomálií, IPS/IDS, vyřazení DoS aj.
- Integrace efektivní filtrace webového obsahu.

Ke Službě Managed Firewall je možné objednat konektivní služby, které je možné realizovat protokolem IPv6 (standardně však IPv4). Konektivní služby s protokolem IPv6 jsou realizovány jako doplňkové služby, nejsou však podporované na všech přístupových technologiích a ani nejsou plně kompatibilní se všemi Službami uvedenými v tomto Popisu služby. Podmínkou pro zřízení Služby je kladný technický průzkum.

5 Zpoplatnění Služby

Služba je zpoplatněna:

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

V případě rozporu konkrétních ustanovení jednotlivých dokumentů mají postupně přednost ustanovení tam uvedená podle výše uvedeného pořadí.

6 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.

7 Minimální doba užívaní Služby

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

Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

8 Zřízení a poskytování (provoz) Služby

8.1 Model Služby

V rámci řešení Služby Managed Firewall jsou uvažovány dva modely: Dedikované (vyhrazené) Managed Firewall firewally pro jednotlivé uživatele anebo sdílené Managed Firewall firewally využívané větším počtem uživatelů. U sdílené varianty bohužel nelze využít možnosti volitelného setu Antivir + Antispam (AV+AS). Pokud preferujete volbu tohoto doplňkového modulu je potřeba zvolit z nabídky dedikovaných firewallů.
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 musí se zvolit varianta Služby s umístěním u Smluvního partnera (zejména u Služby Profesionální internet).

Doporučené parametry u jednotlivých nabízených variant Služeb:

Typ serveru	Propustnost linky	Počet sessions	Počet VPN tunelů	Propustnost AV+AS	Propustnost IPS	Propustnost VPN
Dedikovaná Služba Managed Firewall – Basic	100 Mbps	80 tis	50	20 Mbps	70 Mbps	30 Mbps
Dedikovaná Služba Managed Firewall – Normal	150 Mpbs	100 tis	60	30 Mbps	100 Mbps	100 Mbps
Dedikovaná Služba Managed Firewall – Profi	300 Mbps	1 mil.	300	80 Mbps	150 Mbps	300 Mbps
Dedikovaná Služba Managed Firewall – Exklusive	1,5 Gbps	1 mil.	300	300 Mbps	400 Mbps	400 Mbps
Sdílená Služba Managed Firewall	200 Mbps	80 tis	50	N/A	80 Mbps	100 Mbps

8.2 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.

8.2.1 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, testy a předání.

- 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. Smluvních partnerů.

8.2.2 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.

8.2.3 Zřízení každé jednotlivé doplňkové Služby obsahuje:

Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

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

8.2.4 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

8.2.5 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.

8.3 Předání Služby po jejím zřízení (zprovoznění)

Služba je zřízena a předána Smluvnímu partnerovi do provozu následně po nastavení výchozí konfigurace zařízení dle Specifikace služby, uvedení do provozu, testy a předání Předávacího protokolu Služby, který je zaslán na kontaktní osobu Smluvního partnera.

Následně má Smluvní partner Služby ze strany Poskytovatele na odzkoušení funkčnosti, konfigurace nastavení parametrů, porovnání souladu Služby s parametry uvedenými v příslušné Specifikaci služby 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 uvedené lhůty, tzn. dvou (2) 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 připomínek a reklamací, 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.

9 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.

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 zařízení umístěná v datových centrech Poskytovatele v Praze	max. do 18 h	max. do 12 h	max. do 9 h
Maximální doba odstranění výpadku Služby – pro zařízení umístěná kdekoliv v ČR	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

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 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.

Popis Služby Managed Firewall

Tento Popis služby je platný pro **službu Managed Firewall** objednané (pro Specifikace služby Managed Firewall uzavřené) v období od **25. 2. 2015** do odvolání.

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

10 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.

Technické prostředky, na kterých je Služba realizována:

FortiGate-80D Features

Maximum Firewall Throughput (1518 byte UDP packets) 1300 Mbps
Maximum Firewall Throughput (512 byte UDP packets) 950 Mbps
Maximum Antivirus Throughput 250 Mbps
Maximum IPS Throughput 80000 Mbps
Maximum Concurrent Sessions TCP 1.5M
Network Interfaces 4x GE RJ45
3G WAN Connectivity via USB

FortiGate-100D Features

Maximum Firewall Throughpu (1518/512/64 byte UDP pakets): 2500/1000/200 Mbps
Maximum IPSec VPN Throughput 300 Mbps
Maximum Antivirus Throughput 300 Mbps
Maximum Concurrent Sessions 3 Mil.
Network Interfaces: 2 x WAN, 1 x DMZ, 1 x MGMT, 2 x HA, 16 x INTERNAL ports, 2x SFP shared media with RJ45, all are 10/100/1000 ports

FortiGate-240D Features

Firewall Throughput (Max, 512B/1518B UDP) 4 Gbps
Firewall Throughput (Max, 64B UDP) 4 Gbps
Antivirus Throughput (Max, 32KB HTTP) 600 Mbps
IPSec Throughput 512 Byte Packet: 1.3 Gbps
Maximum Concurrent Sessions: 3.2 Million
Network Interfaces 52x 10/100/1000 RJ45 LAN, 2x 10/100/1000 RJ45 WAN, 4x SFP

11 Změny nastavení parametrů a konfigurace Služby

Změnu parametrů nebo konfigurace Služby Smluvní partner objednává u Poskytovatele prostřednictvím příslušné změnové Specifikace služby, případně přes „Oddělení péče o zákazníky“. Změny jsou prováděny v rámci hodin sjednané technické podpory Služby. Pokud je rozsah a pracnost změny požadovaných parametrů náročnější než příslušný rozsah hodin technické podpory sjednaný v rámci Služby, jsou tyto změny zpoplatněny dle platného Ceníku služby Managed Firewall. Požadavek na změnu muže podat jen oprávněný zástupce Smluvního partnera. Žádné změny nelze provádět v době 5 a méně pracovních dní před dohodnutým termínem zřízení Služby.

12 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.

13 Reklamace Služby, řešení odstranění výpadku (závady) Služby

„Oddělení péče o zákazníky“ je dostupné 24 hodin denně, 365 dní v roce a hovory jsou vyřizovány nepřetržitě. Pro urychlení odstranění závady/reklamace Služby Poskytovatel požaduje, aby jej Smluvní partner kontaktoval již při prvních známkách závady. Hlášení závady/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 závady (adresa místa koncového bodu služby / lokalita Smluvního partnera, nebo místa závady)
- popis závady/reklamace
- datum a čas vzniku závady
- jméno a příjmení osoby jednající jménem Smluvního partnera a jeho telefonické spojení

„Oddělení péče o zákazníky“ podnikne potřebné kroky k odstranění závady/reklamace. Smluvnímu partnerovi bude přiděleno číslo závady, které bude používat při následných kontaktech, aby bylo možno správně sledovat postup opravy.
Pokud nelze závadu Služby odstranit zásahem „na dálku“ s pomocí obsluhy Smluvního partnera, pověřené pracoviště Poskytovatele zorganizuje k opravě závady 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 závadu 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, neposkytnutí příslušné součinnosti nebo poruchu prokazatelně zavinil Smluvní partner).