

ORIGINÁL / KOPIE

Nabídka služeb O2

O2 Internet Business

Datum: 4. 10. 2023

Pro zákazníka/zadavatele

Obec Kunčice pod Ondřejníkem

Obsah

Obsah	2
1. Identifikační údaje poskytovatele	3
2. Profil poskytovatele	4
3. Tým, který pracuje pro vás	5
4. Ochrana osobních údajů	6
5. Manažerské shrnutí	7
6. Popis nabízeného řešení O2 Internet Business	9
6.1 Služba O2 Internet Business	9
6.1.1 Volitelné doplňkové služby	9
6.1.2 Doplňkové služby pro zajištění bezpečnosti	12
6.1.3 Další doplňkové služby	13
6.1.4 Navazující služby vhodné k použití se službou O2 Internet Business	16
7. Cenová nabídka	18
8. Platební podmínky	18
9. Časový harmonogram zavedení služby	19
10. Servisní, záruční a provozní podmínky	19
11. Technické prostředky poskytovatele – páteřní síť	19
11.1.1 Konektivita	20
12. Popis zákaznického řešení NGFW	21
12.1 O2 Next Generation Firewall	21
12.2 Přehled variant NGFW Dedicated	24
12.2.1 Nabízené služby	24
12.3 Hlavní výhody služby	27
12.4 FortiGuard	28
13. Náklady na realizaci a provoz	29
13.1 Platební podmínky	29
14. Servisní, záruční a provozní podmínky	31
14.1 Zákaznická podpora – Service Desk	31

1. Identifikační údaje poskytovatele

Tato nabídka obsahuje návrh telekomunikačního / ICT řešení pro společnost **Obec Kunčice pod Ondřejníkem** (dále jen „zákazník“). Nabídku předkládá společnost O2 Czech Republic a.s. (dále jen „poskytovatel“).

Ve Zlíně dne 4. 10. 2023

Identifikační údaje poskytovatele:

Obchodní jméno: O2 Czech Republic a.s.
Sídlo firmy: Za Brumlovkou 266/2, 140 22 Praha 4
IČO: 60193336
DIČ: CZ60193336
Zapsaná: v obchodním rejstříku Městského soudu v Praze, oddíl B, vložka 2322
Generální ředitel: Ing. Jindřich Fremuth
Zákaznická linka: 800 111 777

Kontaktní osoba pověřená jednáním jménem poskytovatele:

Jméno a příjmení: Jiřina Pazderová
Telefon: +420
Mobil: +420 602 616 143
E-mail: jirina.pazderova@o2.cz

Zpracovatel nabídky:

Jméno a příjmení: Jiří Beňovský

Ochrana informací

Tento dokument i veškerý jeho obsah je předmětem obchodního tajemství společnosti O2 Czech Republic a.s. a nesmí být bez předchozího písemného souhlasu společnosti O2 Czech Republic a.s. zpřístupněn třetí osobě ani zveřejněn. Tento dokument není návrhem smlouvy. Společnost O2 Czech Republic a.s. poskytuje služby výhradně na základě písemně uzavřené smlouvy, která je řádně podepsaná a obsahuje všechny dohodnuté náležitosti a podmínky poskytování produktů a služeb.

2. Profil poskytovatele

O2 Czech Republic a.s.

O2 Czech Republic a.s. je předním integrovaným telekomunikačním operátorem na českém trhu. O2 je stabilním, spolehlivým a důvěryhodným partnerem, jehož vedoucí pozice na trhu umožňuje vytvářet nové příležitosti, sledovat nejnovější trendy v oblasti informačních a telekomunikačních služeb a neustále pracovat na rozvoji nových produktů a řešení.

V současnosti poskytuje O2 služby prostřednictvím více než sedmi miliónů mobilních a pevných linek s využitím nejrozsáhlejších fixních a mobilních sítí v ČR, včetně sítí 5. generace, což ze společnosti O2 činí současně jednoho z vedoucích poskytovatelů plně konvergentních služeb v Evropě.

O2 poskytuje profesionální služby v oblasti podnikové telefonie a multimédií a přední místo zaujímá rovněž v oblasti ICT služeb a Cloud Computingu. Kromě hostingů a řízených služeb, které poskytuje v nejmodernějších datových centrech více než patnáct let, nabízí řešení v oblasti networkingu, bezpečnosti sítí a připojení k internetu, telemetrie a komunikace mezi stroji a zařízeními (M2M). Je držitelem prestižních certifikací jako jsou Cisco Gold Integrator, VMware vCloud Powered, Microsoft Gold Partner & Service Provider a dalších.

Certifikace ISO

Společnost O2 Czech Republic a.s. je držitelem řady certifikátů spjatých s **integrovaným systémem řízení**, který má zaveden pro navrhování, projektování, vývoj, dodávání, prodej a servis komunikačních a informačních technologií, služeb a komplexních zákaznických řešení, včetně služeb systémové integrace, zřizování a provozování veřejných komunikačních sítí a měření jejich parametrů.

O2 je držitelem několika ocenění IMS, a to certifikátů pro:

- Systém managementu kvality dle **ISO 9001**
- Systém managementu ICT služeb dle **ISO 20000-1**
- Systém informační bezpečnosti dle **ISO 27001**, rozšířený o **ISO 27017** – bezpečnost cloudových služeb a **ISO 27018** – bezpečnost osobních údajů ve veřejném cloudu
- Systém BOZP dle **ISO 45001**
- Systém environmentálního managementu dle **ISO 14001**
- Systém hospodaření s energiemi dle **ISO 50001**
- Systém managementu kontinuity podnikání dle **ISO 22301**

Všechny výše uvedené mezinárodní certifikáty byly vydány certifikační společností TÜV SÜD, která je již od roku 1866 světovým lídrem v oblasti kvality, bezpečnosti a udržitelnosti. Certifikáty jsou veřejně dostupné na oficiálních stránkách společnosti O2 Czech Republic a.s., na žádost zákazníka je O2 připravena předložit jejich úředně ověřené kopie.

Politika EMS, etické zásady podnikání

Jedním ze strategických cílů společnosti O2 Czech Republic a.s. je neustálé zlepšování procesů ve vztahu k životnímu prostředí (politika EMS) a její prosazování je závazné pro všechny zaměstnance. O2 se dále zavázalo ke společensky a sociálně odpovědnému chování při všech svých činnostech. Etické zásady podnikání společnosti ho zavazují k dosahování a udržování nejvyšších standardů v chování vůči všem oprávněně zainteresovaným stranám.

3. Tým, který pracuje pro vás

Špičková kvalita služeb vyžaduje také perfektně fungující tým špičkových profesionálů. Poskládali jsme ho tak, abyste v každém ohledu dostávali jen to nejlepší.

Account manager sleduje nejnovější trendy v oboru a je vaším konzultantem v oblasti ICT a telekomunikací. Zajistí zpracování cenové nabídky přesně podle vašeho zadání, klidně i ve více variantách, abyste mohli posoudit, která verze je pro vás nejlepší. Pokud budete chtít představit vybrané řešení v rámci vaší společnosti, zařídí prohlídku našich odborných center s prezentací nabízených služeb. Security centrum, dohledové centrum nebo datové centrum? To vše je možné.

Spolu s Account managerem je vám k dispozici tým tvořený specialisty s příslušnou odborností.

Specialista podpory prodeje je pravou rukou Account managera, sdílí s ním stejné portfolio klientů a má k dispozici přístup ke všem potřebným interním systémům O2. Díky tomu zajistí rychlé zpracování vašich požadavků s potřebnou prioritou.

V případě designu technicky složitých či rozsáhlých řešení je podpůrný tým operativně doplňován specialisty z oddělení **Presales**. Každý z nich je úzce zaměřený na konkrétní oblasti služeb a disponuje expertní technickou znalostí, takže můžete počítat s individuálním řešením, šitým na míru vašemu firemnímu prostředí a provozu.

S vlastní implementací rozsáhlých či kritických řešení vám pomohou naši certifikovaní **Projektoví manažeři**. Celý proces je řízen dle standardu IPMA a garantuje vám dodání požadovaného plnění v dohodnutém kvalitativním, časovém a cenovém rámci.

V rámci každodenního provozu řídí vybrané služby a řešení **Servisní manažeři**. Díky nim se můžete spolehnout, že kromě hladkého provozu podloženého příslušnou provozní dokumentací od nás dostanete i doporučení pro případný další rozvoj, optimalizaci a konfigurační změny, a to v souladu se standardy ITIL.

Celou infrastrukturu pak nepřetržitě monitoruje nejmodernější **Zákaznické centrum provozu sítě**, které dohlíží na stav síťových prvků a služeb, analyzuje případné incidenty a sleduje jejich vyřešení.

Jsme partnerem klíčových výrobců a držiteli vysokých certifikací jako jsou Cisco Gold Integrator, VMware Solution Provider Enterprise, Microsoft Gold Partner a mnoha dalších a jsme plně kvalifikovaní prodávat, instalovat a podporovat jejich technologie. Jako jediný poskytovatel cloudových služeb v České republice jsme získali certifikát VMware Cloud Verified.

Jsme leaderem v oblasti managovaných ICT služeb, trvale investujeme do rozvoje služeb a inovací a nastavujeme standardy na trhu v České republice.

Naše týmy ale nezajišťují jen rozsáhlá či technicky složitá řešení. Najdete je za každou, i nejběžnější službou, bez níž si svůj pracovní či osobní život už ani neumíme představit, a pro jejichž objednání či konfiguraci není nezbytný kontakt s operátorem. K tomuto účelu máme k dispozici bezpečné internetové portály umožňující pohodlný nákup či servis koncového zařízení, základní nastavení tarifů i on-line přístup k informacím o vyúčtování a detailech jednotlivých služeb.

Značka O2 – to jsou špičkové technologie i služby... a také spokojení zákazníci. Jsme tu pro vás!

4. Ochrana osobních údajů

Zákazník se ve vztahu k osobním údajům předaným v rámci nabídky stává správcem těchto osobních údajů ve smyslu nařízení (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES („nařízení“) a je povinen plnit veškeré povinnosti, které správci osobních údajů ukládá toto nařízení a další platné právní předpisy pro ochranu osobních údajů.

5. Manažerské shrnutí

Požadavky na zákaznické řešení:

Zákazník požaduje nabídku garantovaného připojení do internetu s přístupovou rychlostí 100/20 Mb/s, O2 Internet Mobile Backup LTE v lokalitě: **Kunčice pod Ondřejníkem 569, 739 13 Kunčice pod Ondřejníkem,**

Zabezpečení sítě službou O2 Next Generation Firewall. Analýza, instalace a nastavení služby. Dohled a průběžná aktualizace.

Shrnutí nabídky:

Nabídka zahrnuje bezpečné připojení k internetu s následujícími parametry:

Profil:	Asymetrický
Přístupová rychlost:	100/20 Mb/s
Koncové zařízení v ceně služby:	Universal
Počet veřejných IP adres:	8
Garantovaná měsíční dostupnost (SLA):	99,7 %

Cenové shrnutí:

Jednorázové náklady:	1 Kč
Pravidelné měsíční platby:	
O2 Internet Business 24/2 Mbps	1900 Kč
Internet Mobile Backup 4/4 LTE	490 Kč
Doba realizace 1-2 týdny metalický spoj	

Poskytovatel nabízí službu O2 Next Generation Firewall Dedicated (dále jen O2 NGFW Dedicated) ve variantách Advanced a Premium Služba je postavená na technologiích od společnosti Fortinet.

Cenové shrnutí:

Zřizovací poplatek, Instalační cena	16 600 Kč
Měsíční cena za variantu Premium (IP SEC VPN)	2900 Kč/měs

Délka kontraktu:

Cenové podmínky pro kontrakt na: 24 měsíců.

Součinnost zákazníka:

Realizace řešení předpokládá možnost využití odpovídajících vnitřních rozvodů v rámci objektu, možnost umístění potřebných technologických prvků a jejich napájení AC 230V.

Platnost nabídky:

Tato nabídka je platná do 4. 11. 2023

6. Popis nabízeného řešení O2 Internet Business

Poskytovatel nabízí službu O2 Internet Business s přístupovou rychlostí 100/20 Mb/s.

6.1 Služba O2 Internet Business

Služba O2 Internet Business zajišťuje připojení LAN zákazníka k internetu s využitím dedikovaného optického, metalického nebo mikrovlnného spoje. Je standardně ukončena na metalickém rozhraní 100/1000 Base-T. Součástí služby je koncové zařízení (router) umístěné u zákazníka a dálkově monitorované poskytovatelem.

Základní parametry služby:

- Pro symetrické přípojky, rychlosti od 20 Mb/s do 10 Gb/s
- Pro asymetrické přípojky, rychlosti od 16/1 Mb/s do 100/20 Mb/s
- Plně garantovaný rychlostní profil bez agregace
- Přístupová technologie: optika, metalika, nebo mikrovlnný spoj TDMA (licencované nebo nelicencované pásmo), dle požadovaného rychlostního profilu a místních podmínek
- V ceně služby je:
 - 1+5 pevných IP adres, pro servery a zařízení zákazníka
 - NAT – překlad lokálních IP adres na veřejné
 - sekundární DNS
 - koncové zařízení s rozhraním 100/1000 BaseT v závislosti na požadované rychlosti (pokrytí WiFi je možné řešit objednáním profesionální služby O2 Managed WiFi Basic, nebo lze jednoduše doplnit koncové zařízení podporující WiFi)
- Součástí služby je technická podpora 24x7 a základní varianta služby eWatch (eWatch Basic), která obsahuje dashboard a přehled služeb a umožňuje zadávat poruchové lístky.

6.1.1 Volitelné doplňkové služby

Ke službě O2 Internet Business lze objednat řadu volitelných doplňkových služeb, které rozšiřují funkcionality služby, zvyšují spolehlivost služby, nebo poskytují informace pro správu a dohled služby.

6.1.1.1 Internet Mobile Backup

Služba Internet Mobile Backup umožňuje vytvoření záložního spojení s využitím technologie mobilní sítě O2. Součástí této doplňkové služby je potřebný HW. Jde o nezávislé zálohování přípojky jinou technologií, s nižší přenosovou rychlostí. Přepojení na záložní spoj se děje automaticky v případě výpadku primárního spoje. **Všechny IP adresy zákazníka jsou zachovány, přesměrování nastane do 100ms** (VPN se nerozpadá).

Internet Mobile Backup umožňuje download připojení rychlostí až 100 Mb/s. Rychlost závisí od aktuálního vytížení základnové stanice BTS a použitým koncovým zařízením.

6.1.1.2 Profesionální služba O2 Managed WiFi Basic

Profesionální služba O2 Managed WiFi Basic zahrnuje dodávku, montáž a konfiguraci WiFi přístupového bodu (Access Point, AP) v lokalitě zákazníka a zajištění provozu, řízení, správy a servisu. Používá se základní typ AP: Huawei AP 4050DE-M.

6.1.1.3 Pevné IP adresy

Možnost přidání dalších pevných IP adres k základním na základě požadavků zákazníka (forma zvýhodněného balíčku 8 IP adres).

6.1.1.4 SLA (Service Level Agreement – Garance kvality služby)

SLA garantuje zákazníkovi vysokou dostupnost, zkrácenou dobu oprav závady a definovanou komunikaci při provozních problémech služby.

Poskytovatel 1x měsíčně vyhodnocuje dodržení garantovaných parametrů. Report o hodnotách dosažených v uplynulém měsíci poskytne zákazníkovi do 6. pracovního dne následujícího měsíce v portálu eWatch.

Při nesplnění garantovaných ukazatelů poskytovatel automaticky snižuje měsíční cenu za pronájem služby na následující období (tj. v následujícím kalendářním měsíci) o poměrnou část, závislou na míře překročení garantovaných parametrů (neplatí pro SLA 0).

Následující tabulka ukazuje garantované parametry při určité úrovni SLA.

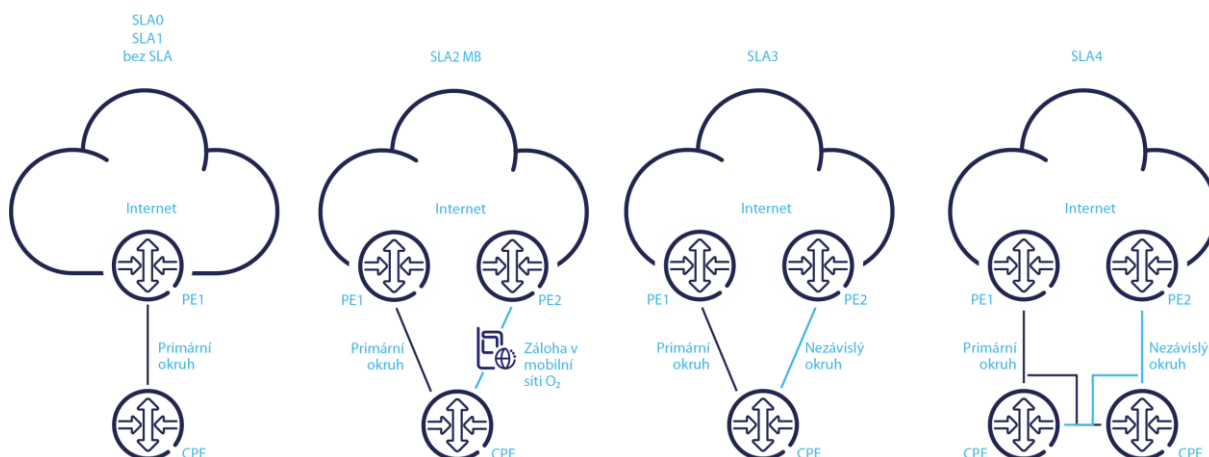
Tabulka 1 – Definice a garantované parametry SLA

Úroveň SLA		SLA 0	SLA 1	SLA 2 MB	SLA 3	SLA 4
Měsíční dostupnost služby	%	99,0	99,5	99,7	99,9	99,95
Odezva	Minuty	120	120	60	60	20
Max. délka závady	Hodin	12	12	6	4	4
Max. délka závady primární/záložní připojky	Hodin	-	-	-	48	48
Průběžné informace o závadě	Hodin	12	12	6	4	1
Záložní vedení		-	-	nezávislé *	nezávislé **	nezávislé***
Sleva za nedodržení parametrů		Ne	Ano	Ano	Ano	Ano

* SLA 2 MB – záložní linka na mobilní technologii bez garantovaných parametrů

** SLA 3 – záložní linka na dva různé páteřní boxy, směrovač je jen jeden – dále jako Backup pro SLA3

*** SLA 4 – záložní linka s vlastní trasou v celé délce na 2 různé páteřní boxy, navíc je ještě použito druhé CPE (směrovač) – dále jako Backup pro SLA4



Obrázek 1 – O2 Internet Business – SLA a backup

Dostupnost služby je poměr doby, kdy byla zákazníkovi služba dostupná bez funkčních závad z důvodů na straně poskytovatele, k délce celého sledovaného období. Vyjadřuje se v procentech. Nezahrnuje plánované a nahlášené výluky provozu (zkráceně PEW).

Odezva je doba mezi začátkem závady a informováním zákazníka o krocích vedoucích k jejímu odstranění a o předpokládané době jejího ukončení. Její délka je garantována úrovní služby SLA.

Maximální délka závady je doba potřebná na provedení servisního zásahu zaměřeného na odstranění příčiny závady. Do této doby se nezapočítávají prostoje způsobené nepřístupností zařízení zaviněná zákazníkem.

Začátek závady se pro určení doby trvání závady služby považuje čas jejího ohlášení, na kterém se operátor poskytovatele a kontaktní osoba zákazníka dohodnou při nahlásování závady – čas telefonátu nebo čas zadání požadavku v eWatch.

Ukončení závady. Závada je ukončena tehdy, když všechny parametry dané služby, na které byla identifikována závada, jsou lepší nebo shodné s technickými parametry, uvedenými v technické specifikaci dané služby.

Backup pro SLA2 MB

Garance kvality služby SLA2 je založena na využití záložního spoje na mobilní technologii (tj. také na jiných prostředcích poskytovatele). Záložní spoj zajišťuje vysokou dostupnost, ale má nižší kapacitu než primární spoj; jeho parametry nejsou garantované.

Backup pro SLA3 a SLA4 – záložní linka o stejné kapacitě

Garance kvality služby SLA3 a SLA4 je založena na využití plnohodnotné záložní linky na jiné technologii (tj. také na jiných prostředcích poskytovatele). Používá se taková záložní linka, aby byla zajištěna nejvyšší možná dostupnost; obvykle má stejnou kapacitu jako primární linka (podle technologických možností na konkrétním místě). Záložní linka je vedena jinou trasou než primární linka – je tedy plně redundantní, má i vlastní koncové zařízení v síti poskytovatele (PE). Přepojení na záložní linku se děje automaticky v případě výpadku primární linky. Všechny IP adresy zákazníka jsou zachovány, přesměrování nastane do 100ms, VPN se nerozpadá. U tohoto typu zálohy je také možná

garance hodnot ping/jitter. Tato doplňková služba se realizuje vždy individuálně jako zákaznické řešení na míru.

6.1.2 Doplňkové služby pro zajištění bezpečnosti

K datovým přípojkám je vhodné objednat službu na ochranu proti kybernetickým hrozbám a také proti tzv. DDoS útokům (Distributed Denial of Service) – službu **O2 Next Generation Firewall Dedicated a O2 AntiDDoS**.

6.1.2.1 O2 Next Generation Firewall Dedicated – on premise řešení

CPE ke službě O2 Internet Business umožňuje aktivaci špičkové ochrany formou dedikovaného O2 NGFW. Jedná se o bezpečnostní řešení na rozhraní Internetové přípojky a privátní sítě zákazníka (LAN či VPN). V ceně služby je implementace, aktualizace a know-how pro zajištění ochrany před kybernetickými hrozbami pomocí komplexního bezpečnostního řešení. Výhodou je funkčnost na lokálním CPE u zákazníka bez nutnosti zapojení dodatečného bezpečnostního zařízení.

Služba se nabízí ve 2 variantách:

- **O2 Next Generation Firewall Dedicated – ADVANCED**
 - Firewall
 - IPS (Intrusion Prevention System)
 - Antivirus a antimalware
 - Webfiltering
 - Application control
- **O2 Next Generation Firewall Dedicated – PREMIUM**

Varianta Premium umožňuje navíc oproti funkcím verze Advanced

 - Vzdálený přístup (VPN)
 - Reporting
 - DLP (Data Loss Prevention)

V rámci balíčku se službou O2 Internet Business je možné využít příznivější cenové nabídky, kterou si můžete dohodnout s Vaším obchodníkem. Službu je možné zřídit k vyzkoušení na období 1 měsíce zdarma (Trial).

Bezpečnostní Audit

Na CPE zařízení, které je dodávané ke službě O2 Internet Business, je možné aktivovat na 1 měsíc zdarma funkcionalitu Bezpečnostní Audit. Audit poskytuje podrobné informace o aktuálním stavu sítě zákazníka, které pokrývají klíčové oblasti bezpečnostních hrozeb, produktivity a výkonosti. Výstupem bezpečnostního auditu je detailní report, který zákazník může konzultovat s vyškoleným specialistou O2. Audit je určen pro potenciální zákazníky služby **O2 Next Generation Firewall Dedicated**.

6.1.2.2 O2 AntiDDoS

Při DDoS útoku se útočníci snaží zahltit síť, server nebo webové stránky zasláním obrovského množství požadavků (útoků), aby je znepřístupnili ostatním uživatelům. Služba O2 AntiDDoS dokáže tyto útoky detekovat, mitigovat (zmírňovat jejich dopad) a tím zabránit výrazným finančním škodám a poškození reputace společnosti.

O2 AntiDDoS je nabízen ve variantách:

- **O2 AntiDDoS Advanced** – Nejkomplexnější automatizované řešení, které se nastavuje konkrétně podle potřeb zákazníka. Mimo ochrany proti typickým volumetrickým útokům umí odvrátit i kombinované typy aplikačních útoků. Pomocí kombinace síťového řešení v datových centrech O2 a dodatečného on-premise zařízení v lokalitě zákazníka může zabránit útokům na záložní linky. Součástí služby je přístup do zákaznického portálu.
- **O2 AntiDDoS Standard** – Ideální varianta pro zákazníky, kteří vyžadují automatické odvracení volumetrických útoků v ceně služby a chtějí si nastavit vlastní politiku odvracení útoků. Součástí služby je přístup do zákaznického portálu.
- **O2 AntiDDoS Basic** – Cenově dostupná varianta s nízkým měsíčním paušálem a dodatečnou platbou za konkrétní odvrácený útok. Ideální varianta pro zákazníky, kteří chtějí vědět, jak často jsou na ně cíleny útoky a potřebují odvrátit nižší počty útoků ročně.

O2 má k dispozici nejnovější platformu s vysokou kapacitou pro odvracení různých druhů útoků. O2 tak umožní odvrátit i masivní DDoS útok. AntiDDoS platforma je umístěna v České republice v datových centrech O2. To umožňuje malé zpoždění při čištění provozu, což je důležité pro správné fungování kritických aplikací. Umístění dat a provozu v ČR má i legislativní výhody.

6.1.3 Další doplňkové služby

6.1.3.1 Managed WAN

Managed WAN je komplexní outsourcingová služba, která sestává z monitoringu, dohledu, správy, řízení, plánování a údržby všech komponent WAN sítě a přípojek do internetu.

V rámci služby Managed WAN zajistíme kompletní správu datové sítě a přípojek do internetu, včetně proaktivního řešení incidentů, konzultací ohledně rozvoje sítě a zpracování analýz pro přípravu implementace nových technologií (VoIP, bezpečnostní politika atd.). Pro zákazníka v rámci služby pracují špičkoví certifikovaní specialisté. Zákazník platí jen za dobu, po kterou tyto specialisty využívá, což výrazně snižuje jeho náklady na ICT.

Výhody služby Managed WAN:

- SLA (garantovaná úroveň služeb) – je možno zvolit globální SLA na celou síť nebo SLA pro každou lokalitu zvlášť.
- Proaktivní dohled sítě – Service Desk. Problémy na WAN síti jsou většinou vyřešeny dříve, než je způsoben skutečný výpadek služby. Automatické založení poruchového lístku při výpadku = zkrácení doby nezbytné pro opravy poruch -> zvýšení dostupnosti sítě.
- Jediný zástupce pro komunikaci – přiřazený Servisní Manager.

- Online monitoring sítě, eWatch – webová aplikace, která zákazníkovi umožní rychlý přístup k informacím o aktuálním stavu jeho sítě.
- Služba Managed WAN je škálovatelná – lze ji konfigurovat na míru, podle potřeb zákazníka.

Komponenty služby Managed WAN

- **Silver Service Desk**, pracoviště pro řešení incidentů, umístěné u poskytovatele. Doba dostupnosti Silver Service Desku může být 8x5, 12x7 nebo 24x7, podle požadavku zákazníka.
- **Servisní manager** – pro zákazníka je k dispozici jediná kontaktní osoba pro zajištění kvality služby – Servisní Manager, který má podrobnou znalost všech služeb, které zákazník sítě využívá a zajišťuje pravidelné osobní schůzky, reporting plnění SLA, řešení procesních nedostatků. Průběžně sleduje provozní statistiky a využití služeb a v případě potřeby navrhuje opravná opatření.
- **SLA Managed WAN** – poskytuje se v 5 úrovních: SLA 0 až SLA 4.

Služba Managed WAN je nabízena ve variantách:

- **Managed WAN Easy** – obsahuje: proaktivní dohled a správu linek, ServiceDesk “8x5”, SLA 1 (99,2 %) a eWatch portál
- **Managed WAN Silver Standard** – vhodné pro zákazníky od 1-50 linek, kteří chtějí individuální nastavení všech parametrů
- **Managed WAN Silver Complete** – vhodné pro zákazníky od 10 linek, kteří chtějí využít služeb dedikovaného servisního manažera
- **Managed WAN Gold Complete** – řešení pro největší zákazníky (od 30 linek) s možností alokace servisního manažera přímo na lokalitu k zákazníkovi

Služba Managed WAN přináší zákazníkovi efektivní správu datových linek, zvýšení dostupnosti primární konektivity, smluvní garance plnění SLA, proaktivní řízení a dohled nad celou WAN. Díky Managed WAN je správa linek flexibilnější a přehlednější. Veškeré provozní statistiky a stavy linek má zákazník k dispozici v portálu eWatch ve verzi Advanced.

6.1.3.2 eWatch

Zákaznický portál eWatch je určen hlavně pro dohled datových linek v reálném čase. Portál je komplexní – poskytuje veškeré informace a funkce potřebné pro správu datové sítě (WAN):

Verze Basic:

- Souhrn: základní obrazovka – dashboard se základním přehledem služeb a jejich stavu
- Služby: kompletní seznam sledovaných služeb zákazníka, základní údaje o stavu služeb
- TT: možnost založení „troubticketů“

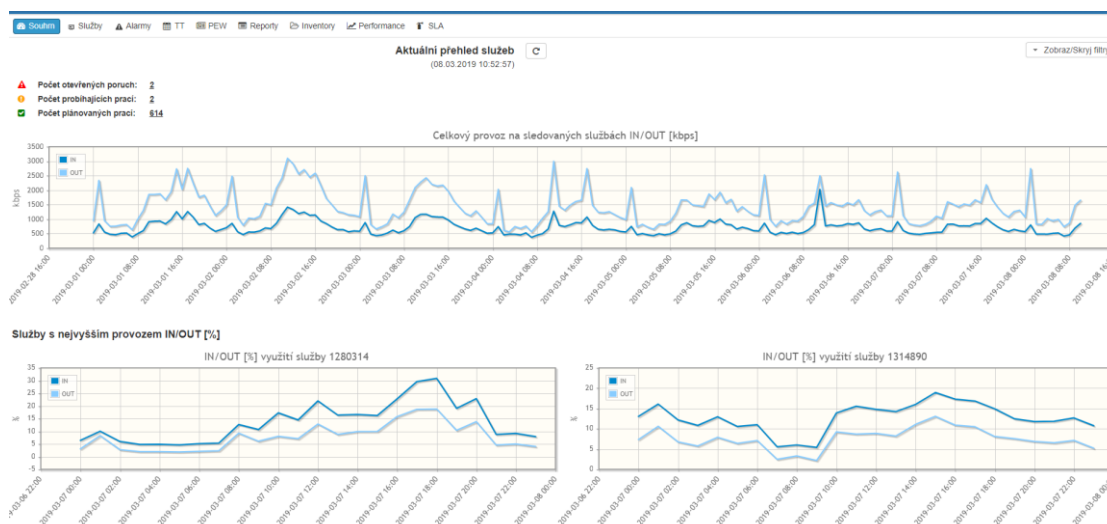
Verze Advanced (navíc oproti verzi Basic):

- TT: přehled založených „troubticketů“ a jejich aktuální stav
- Alarmy: přehled událostí, obvykle vyčítaných z routeru (down/up, kapacita, BGP)
- PEW: plánované výpadky, reálná doba nedostupnosti
- Inventory: informace o přístupových linkách, koncových zařízeních v síti zákazníka spravovaných O2

- Performance: přehled dostupnosti služeb, jejich vytížení a další provozní údaje
- SLA: vyhodnocení SLA na službách

Ukázkové video je k dispozici na adrese: <https://www.o2.cz/podnikatele-a-firmy/internet/ewatch>.

Pokud už zákazník má nějaké datové služby od O2, má už přístup k portálu zajištěn a může se rovnou přihlásit na adrese: <https://ewatch.o2.cz/apportal/login.jsf>

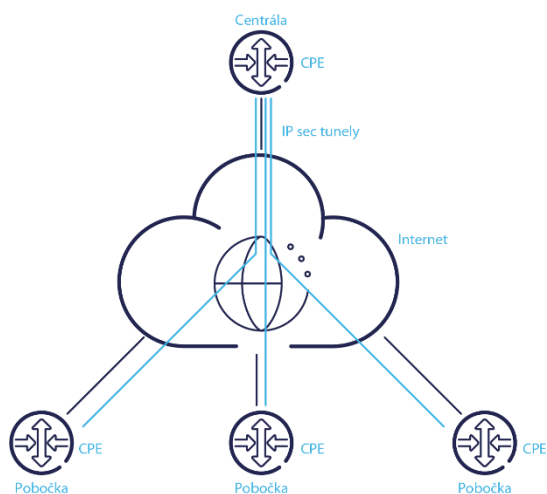


Obrázek 2 – Zákaznický portál eWatch pro monitorování stavu služeb

6.1.3.3 IP VPN

Doplňková služba IP VPN slouží k propojení lokalit a vytvoření podnikové privátní sítě (VPN). Přináší kvalitní a spolehlivé řešení za rozumnou cenu. Mezi lokalitami zákazníka se vytvoří tunelované šifrované propojení protokolem IP Sec. Jednotlivé lokality mohou kombinovat přístup do firemní VPN s přístupem do internet.

Služba neumožňuje řídit zpoždění a jeho rozptyl. Kapacita připojení do VPN je omezena na max. 10 Mb/s. Při požadavku na vyšší kapacitu doporučujeme přechod na MPLS VPN (služba IP Connect od O2), nebo můžeme dodat nadstandardní, výkonnější koncové zařízení.



Obrázek 3 – IP VPN

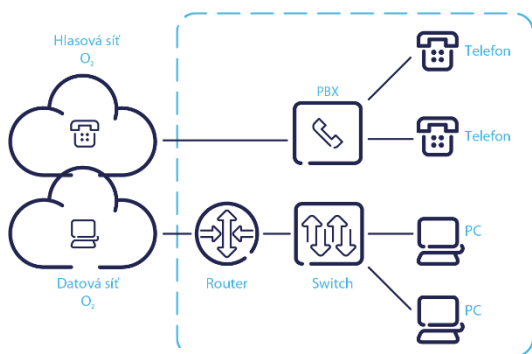
6.1.3.4 Notifikace o výpadcích

Tato služba umožňuje zákazníkovi, aby byl automaticky informován o stavu služby. Informování se provádí prostřednictvím notifikací. Ty mohou být buď zasílány prostřednictvím e-mailové zprávy (až 4 adresátům) nebo odesláním SMS zprávy (až na 2 telefonní čísla). Určení e-mailových adres a telefonních čísel je součástí objednávkové specifikace služby. Služba je vhodná pro zákazníky, kteří provozují kritické aplikace citlivé na poruchy počítačových sítí a kteří disponují vlastním útvarem správy počítačových sítí.

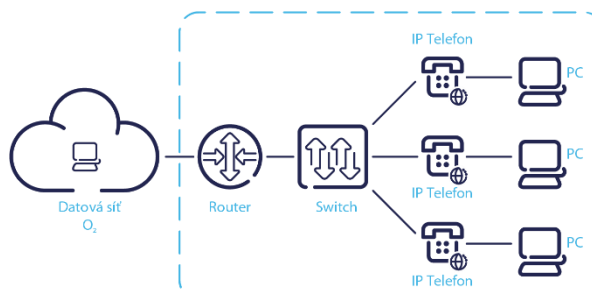
6.1.4 Navazující služby vhodné k použití se službou O2 Internet Business

6.1.4.1 VoIP Connect/IP Centrex – Digitální telefonní linka/ústředna

O2 Internet Business podporuje VoIP služby z portfolia O2. Nejpoužívanější je VoIP Connect (Digitální VoIP telefonní linka) a IP Centrex (virtuální ústředna s technologií VoIP). Výhodnou VoIP je možnost volání mezi pobočkami firmy zdarma, případně i levnější pro volání mimo firmu i do zahraničí. Pokud zákazník využije službu IP Centrex, nemusí investovat CAPEX do nákupu, správy a údržby pobočkových ústředí. Všechno dodáme na klíč podle potřeb zákazníka.



Obrázek 4 – Řešení s klasickou PBX



Obrázek 5 – Řešení se službou IP Centrex

6.1.4.2 Profesionální služba O2 Managed Wifi – větší počet AP a Captive Portál

Profesionální služba O2 Managed WiFi může být dodána jako komplexní řešení, které zahrnuje dodávku a montáž většího počtu přístupových bodů (Access Point, AP) v lokalitě zákazníka a zajištění jejich provozu, řízení, správy a servisu na úrovni SLA. Řízení je zajištěno formou sdíleného hostovaného kontroléru (ve veřejném nebo privátním cloudu).

V rámci služby jsou k dispozici tři platformy řešení využívající zařízení produktových řad z produkce společností Cisco, Extreme Networks a HUAWEI.

Toto řešení obsahuje funkci O2 Captive Portál, který umožňuje zajištění řízení přístupu k WiFi prostřednictvím customizovaného webového portálu, a navíc vytváří podmínky pro marketingové a obchodní aktivity zákazníka.

7. Cenová nabídka

Všechny ceny jsou uvedeny bez DPH.

Ceny zahrnují: Zřízení plného přístupu k síti Internet, včetně zřízení přípojného vedení, konfigurace a instalace koncového zařízení na straně zákazníka, přidělení a registrace IP adresního prostoru.

Doplňkové služby jsou účtovány zvlášť, dle Ceníku doplňkových služeb.

Tabulka 2 – Kalkulace jednorázových a pravidelných poplatků za používání služby

Lokalita	Přístupová rychlost (Mb/s)	SLA	Jednorázová cena za zřízení	Měsíční cena celkem
Kunčice pod Ondřejníkem 569, 739 13	100/20 Mbps		1 Kč	1900 Kč

Tabulka 3 – Ceny volitelných doplňkových služeb

Lokalita	Typ služby	Jednorázová cena	Měsíční cena
Kunčice pod Ondřejníkem 569, 739 13	O2 Internet Mobile Backup LTE	1 Kč	490 Kč

8. Platební podmínky

- Veškeré ceny jsou stanoveny smluvně a uvedeny bez daně z přidané hodnoty.
- Cenová kalkulační je navržena s předpokladem uzavření kontraktu v délce 24 měsíců
- Přesné termíny plateb budou předmětem případné smlouvy.

9. Časový harmonogram zavedení služby

Realizace služby je podmíněna kladným výsledkem technického šetření a ověření dostupnosti sítě a technologie v lokalitách zákazníka.

Dodací lhůta je závislá na druhu a rozsahu požadované služby. Časově nejnáročnější je zřízení „poslední míle“, tj. přístupového okruhu či jiného alternativního přístupu (mikrovlna, optika...) mezi lokalitou zákazníka a přístupovým bodem sítě poskytovatele. V současnosti je typická zřizovací lhůta do tří týdnů od podpisu smlouvy (nevztahuje se na případy, kdy je nutno zajistit pokládku nové kabelové trasy).

V případě realizace bude zhotoven podrobný harmonogram všech prací, který bude odsouhlasen oběma stranami. Pro rozsáhlé akce je realizace řešena projektem.

10. Servisní, záruční a provozní podmínky

Ceny služeb nabízených poskytovatelem zahrnují servis, dohled a řízení.

Síť, kterou poskytovatel pro realizaci služby využívá, je koncipována na kruhových topologiích s automatickým přesměrováním na obchozí trasy v případě poruchy. Veškerá technologie v páteřní i přístupové síti je plně redundantní včetně zdrojové části. V případě poruchy napájení je technologie napájena ze záložních zdrojů. Poskytovatel zajišťuje dohled nad službami, které poskytuje zákazníkovi, prostřednictvím centrálního řídicího a dohledového centra v Praze, nepřetržitě 7 dní v týdnu, 24 hodin denně.

11. Technické prostředky poskytovatele – páteřní síť

Systém technických prostředků (přepínače, optické kabely, infrastruktura SDH, MPLS), které společnost poskytovatele využívá pro poskytování služeb koncovým zákazníkům, je řízen z dohledového centra, které je vybaveno prostředky pro monitorování okamžitého stavu a řízení sítě. Součástí řídicího centra jsou i subsystémy pro sběr statistických údajů, testování sítě, analýzu činností a plánování provozu a rozvoje sítě.

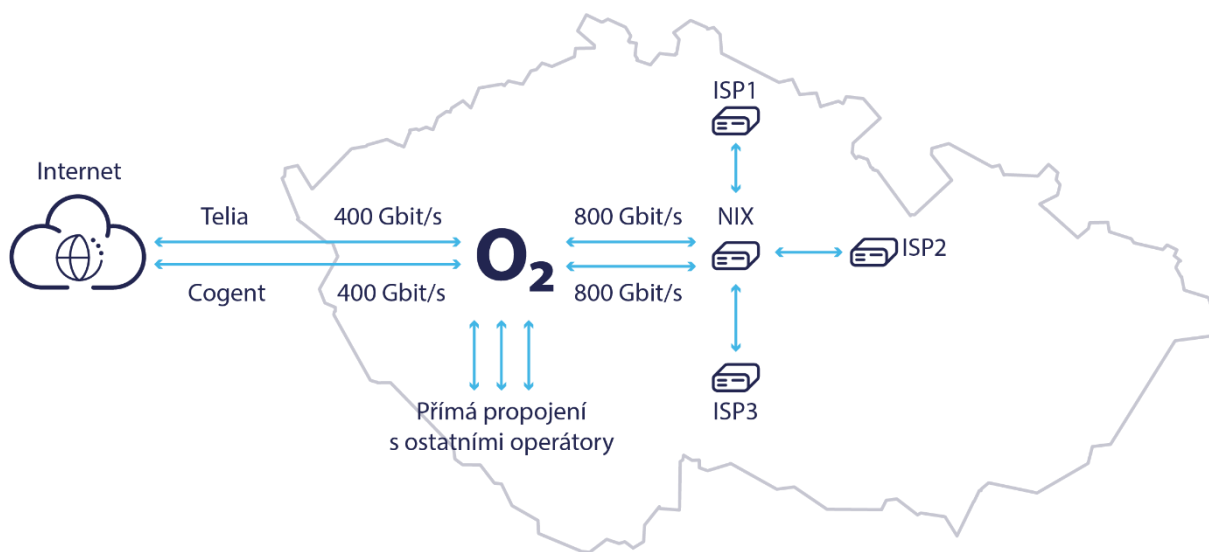
Bezchybný chod sítě je zajištěn pomocí specializovaného řídicího centra sítě NCC (Network Control Centre) umístěného v Praze s nepřetržitou službou 24 hodin denně, 7 dní v týdnu.

V případě přímého připojení sahá odpovědnost poskytovatele, v rámci poskytovaných služeb, na rozhraní modem – ukončující (koncové) zařízení zákazníka.

11.1.1 Konektivita

Společnost O2 Czech Republic a.s. aktuálně disponuje konektivitou 2x 800Gb/s do NIX.CZ realizovanou nezávislými trasami a dále pak propojením s celou řadou dalších poskytovatelů na úrovni privátního peeringu. Mezi těmito poskytovateli jsou například společnosti Microsoft, Google, MAFRA-iDnes, UPC apod.

Zahraniční konektivita je zajištěna poskytovateli Cogent (400 Gb/s) a Telia (400 Gb/s, připojeno přímo do uzlu ve Frankfurtu mimo IP infrastrukturu v ČR).



Obrázek 6 – Internetová konektivita

V rámci výše uvedených smluvních vztahů tak poskytovatel aktuálně disponuje konektivitou přesahující 2,4 Tb/s, z toho 2x 800Gb/s do NIX, což představuje jednoznačné prvenství v kapacitě připojení na českém trhu.

Konektivita je navíc realizována do různých uzlů, což znamená, že na trase není SPOF a i v případě, že by došlo k významnému výpadku některé konektivity, disponuje Poskytovatel dostatečnou kapacitou pro zajištění kvalitních služeb.

Smluvně zajištěné kapacity propojení pak současně nejsou konečné a jsou průběžně navyšovány a doplňovány tak, jak rostou potřeby zákazníků a vyvíjí se objem a struktura datových toků v síti.

12. Popis zákaznického řešení NGFW

Předmětem tohoto dokumentu je stručný popis služby O2 NGFW Dedicated. Služba je navržena jako flexibilní: pokud si ji zákazník vybere, umožní mu realizovat zásady jeho vlastní bezpečnostní politiky.

Pro realizaci O2 NGFW Dedicated byla zvolena koncepce rozproštění výkonných bezpečnostních HW prvků v lokalitě zákazníka; správa a dohled jsou centralizované (z jednoho místa). Tato koncepce je alternativou řešení O2 Next Generation Firewall, které je kompletně umístěno v datových centrech O2.

Poskytované služby nad komunikační infrastrukturou výrazným způsobem omezují možnosti průniku z vnějšího prostředí do interního IT prostředí zákazníka a vytvářejí podmínky pro koordinovaný postup zákazníka a poskytovatele proti potenciálním útočníkům.

O2 NGFW Dedicated poskytuje vysoce dostupnou bezpečnostní infrastrukturu, která je vhodná pro zajištění perimetru sítě v lokalitě zákazníka. Poskytovatel drží veškeré zálohy konfigurace služby dle předem schválené dohody, čímž je zajištěna vysoká dostupnost služby. V případě požadavku zákazníka je možné zajistit i plně redundantní řešení, které vysokou dostupnost ještě zvyšuje. Stejně tak je možné umístit dedikované prvky bezpečnostní infrastruktury v prostorech našich profesionálních datových center.

Služba je poskytovaná na dedikovaných (vyhrazených) zařízeních a má zcela shodné bezpečnostní funkcionality jako centrální řešení (O2 Next Generation Firewall) umístěné v datových centrech. Dedikovaná zařízení reflektují povahu konektivních služeb, v tomto případě jsou koncipována k internetovým službám v lokalitách zákazníka, které mají definovaný bezpečnostní perimetr přímo v místě zakončení konektivní služby.

Splnění požadavků na bezpečnost je garantováno po celou dobu plnění smluvního závazku.

Provoz je zajištěn v souladu s **ČSN ISO/IEC 17799:2005 Informační technologie – Soubor postupů pro řízení informační bezpečnosti**.

Poskytovatel má propracovaný a vyřešený systém bezpečnosti informací na základě normy **ISO/IEC 17799**, včetně bezpečnosti poskytovaných služeb.

Subdodavatelé poskytovatele splňují stejné podmínky jako poskytovatel.

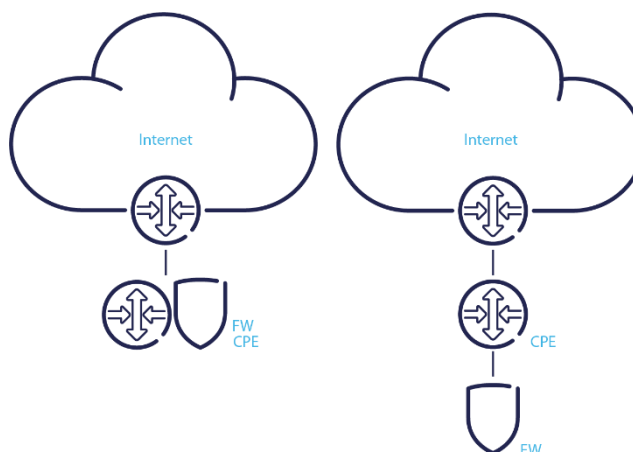
12.1 O2 Next Generation Firewall

O2 NGFW Dedicated nabízí komplexní bezpečnostní řešení formou služby, dodávané na rozhraní internetové přípojky a privátní sítě zákazníka (LAN či VPN) přímo v lokalitě zákazníka. Na internetu je dnes nepřeberné množství různých ohrožení, zranitelností (vulnerability) datových sítí, souborů apod. Malware (tj. viry, trojské koně, spyware, atd.), nevyžádaná pošta (spam), sítě napadených počítačů (botnety), podvodné emaily a stránky (phishing a pharming), organizované hackerské skupiny, a další představují potenciální ohrožení bezpečnosti pro firmy a jejich podnikání. Služba O2 NGFW Dedicated je poskytována primárně ke konektivním službám O2 Internet Business. Jejím cílem je realizace bezpečného připojení do internetu na definovaném perimetru sítě v lokalitě zákazníka.

O2 NGFW Dedicated umožňuje dva modely poskytování služby

- a) Dedikované (vyhrazené) univerzální CPE Fortinet (dále jen UniCPE) – jedná se o CPE dodávané ke konektivní službě umožňující aktivaci bezpečnostních NGFW funkcionalit v plném rozsahu zvolené varianty Advanced či Premium. Zařízení je vyhrazeno pouze pro jednoho konkrétního zákazníka.
- Na tomto zařízení jsou poskytovány konektivní služby spolu s dalšími službami typu bezpečnostního NGFW Dedicated či SD-WAN. V rámci tohoto modelu služby dostává uživatel přístup do konfiguračního rozhraní v omezeném režimu, a to pouze do bezpečnostních funkcionalit, které otevírá zvolená varianta Advanced či Premium.
- b) Dedikované (vyhrazené) HW zařízení FortiGate (dále jen NGFW box) – místo univerzálního CPE je do lokality zákazníka dodáno za standardní CPE ke konektivní službě samostatné zařízení FortiGate včetně licence, které umožňuje aktivaci bezpečnostních funkcionalit v plném rozsahu zvolené varianty Advanced či Premium. Zařízení je vyhrazeno pouze pro jednoho konkrétního zákazníka včetně plné konfigurace dle zvolené varianty Advanced či Premium.

V rámci služby NGFW Dedicated je zákazníkovi vyhrazeno konkrétní zařízení na celou dobu smluvního závazku. Toto zařízení může být umístěno buď v lokalitě zákazníka (model UniCPE i NGFW box) nebo v datovém centru poskytovatele do vyhrazeného prostoru zákazníka (pouze model NGFW box). V případě obou modelů je pro odběratele služby standardně dodáno jedno konkrétní zařízení. V případě potřeby je však možné zvolit i řešení typu Cluster, kdy jsou pro jednu službu použity dvě zařízení ve shodné konfiguraci a tím je dosaženo vysoké dostupnosti.



Obrázek 7 – Schéma řešení O2 Next Generation Firewall Dedicated

Úkolem služby je ochrana a případná filtrace dat na internetovém připojení zákazníka dle definované bezpečnostní politiky. Ochrana je víceúrovňová a obsahuje i aplikační zabezpečení v podobě:

- ochranu před útoky (firewall + IPS)
- ochranu nevyžádanými maily (antispam)
- ochranu před malware (antivir)
- obsahovou filtraci webu (webfiltering/content filtering/URL filtrace)
- řízení aplikací (application control)
- ochranu před únikem interních dat (DLP)
- VPN (IPSec i SSL, klientská i site-to-site)

- reporting

Služba NGFW je postavena na bezpečnostních produktech společnosti Fortinet, která patří k vedoucím společnostem v bezpečnostní oblasti. Konkrétně jde o perimetrové bezpečnostní řešení FortiGate (využívající ASIC technologii), emailové bezpečnostní řešení FortiMail a nástroje pro reporting FortiAnalyzer. Společnost Fortinet patří k vedoucím společnostem v bezpečnostní oblasti. Společnost O2 Czech Republic, a.s (poskytovatel služby) je certifikovaným partnerem společnosti Fortinet a disponuje specialisty s certifikací NSE – Network Security Expert.



Obrázek 8 – Firewall Fortigate

Veškerá příchozí i odchozí komunikace zákazníka prochází bezpečnostní platformou poskytovatele, který zajišťuje její ochranu a správu systémů zákazníka a dodržování definovaných bezpečnostních politik.

12.2 Přehled variant NGFW Dedicated

Tabulka 4 – Přehled variant NGFW Dedicated

NGFW Dedicated	Varianty hlavní služby		Doplňkové služby		
	Advanced	Premium	Antispam	Správa	2FA
Firewall	✓	✓	✗	✗	✗
IPS	✓	✓	✗	✗	✗
Antivirus a antimalware	✓	✓	✗	✗	✗
Webfiltering	✓	✓	✗	✗	✗
Application control	✓	✓	✗	✗	✗
VPN	✗	✓	✗	✗	✗
Data Loss Prevention (DLP)	✗	✓	✗	✗	✗
Reporting	✗	✓	✗	✗	✗
Antispam	✗	✗	✓	✗	✗
Správa	✗	✗	✗	✓	✗
2F Autentizace	✗	✗	✗	✗	✓ (Premium)

12.2.1 Nabízené služby

Firewall

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

IPS

IPS = Intrusion Protection System je systém pro prevenci narušení. Sleduje pomocí IPS senzorů síťový provoz na výskyt definovaných anomálií a signatur útoku. Anomálií je to, když útočník používá síťovou komunikaci jako zbraň. Typicky se jedná o zahlcující (flood) komunikace, jejichž cílem je odepření koncové služby (DoS – Denial of Service). IPS není ochranou proti distribuované variantě (DDoS, kdy není schopen se vyrovnat s násobně většími toky, obranou proti těmto útokům je další bezpečnostní služba O2 – AntiDDoS). Druhým typem obrany je obrana založená na signaturách. Každý útok je charakterizován specifickou sekvencí v komunikaci, kterou lze odhalit a na základě toho blokovat daný provoz. Tento typ se používá pro ochranu systémů, na které není aplikován (případně dostupný) softwarový patch, který danou zranitelnost řeší (zero day útoky apod.).

Antimalware (antivirus)

Antivirová funkcionality prohledává komunikaci na výskyt malwarových sekvencí v rozličných druzích komunikace: HTTP, FTP, IMAP, POP3, SMTP a NNTP, včetně šifrovaných variant. Skenuje na výskyt virů také souborové archivy (ZIP, RAR ...) včetně několásobně zanořených archivů (ZIP v ZIPu). Pracuje se všemi druhy malware, tedy nejen viry, ale také trojskými koni, spyware, síťovými červy apod. Pro detekci využívá neustále aktualizovanou databázi signatur.

Web filter

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

Tři hlavní části webového filtru jsou následující:

- obsahový filtr (Web Content Filter)
- URL Filter
- a služba FortiGuard Web Filtering,

Poskytují maximální kontrolu nad tím, co je možné na internetu navštěvovat a kým. Obsahový filtr hledá definovaná slova (specifikovaná divokými znaky či regulárními výrazy), URL filtr používá databázi vyjmenovaných domén a služba FortiGuard Web Filtering definuje desítky kategorií a do těchto kategorií řadí jednotlivé domény na denní bázi.

Opět je možné uplatnit několik akcí, co se má při návštěvě definované stránky stát, např. akce: **Allow** (povolit), **Monitor** (povolí návštěvu a provede záznam do logu, je možné využít ke kvótám), **Warning** (varování upozorňovací stránkou, po odsouhlasení je přesměrováno), **Authenticate** (před návštěvou stránky je nutné se autentizovat) a **Block** (zablokuje návštěvu).

Application Control

Jedná se o řízení síťových aplikací. Díky spojení se službou FortiGuard Application Control, NGFW rozeznává na základě parametrů více než tisíc různých síťových aplikací, které jsou řazeny do kategorií. Tyto kategorie jsou například Hry (Games), Botnet, P2P apod. Na tedy základě identifikace aplikace provádět různé akce (obdobu funkcionality u web filteringu).

VPN

Služba NGFW Dedicated umožňuje vytváření virtuálních privátních sítí (VPN) na bázi protokolu SSL a TLS. Podporuje různé verze těchto protokolů. VPN síť je možné vytvářet v několika formách, tzv. bezklientské či pouze webové formě – pro vybrané protokoly (http, CIFS, FTP apod.) je vytvořen zabezpečený webový portál na který jsou tyto služby publikovány a přistupující uživatel nepotřebuje instalaci žádného VPN klienta. K přístupu stačí pouze webový prohlížeč podporující SSL a TLS.

V základním režimu je podporován pouze klientský přístup na bázi SSL. Kromě SSL VPN zařízení umožňuje vytváření i IPSec VPN tunelů, včetně site-to-site VPN. Tato varianta IPSec VPN tunelů je dostupná na vyžádání a podléhá separátnímu zpoplatnění.

U obou variant je možnost volby různých autentizačních mechanismů, v případě doplnění o speciální zařízení (FortiToken) včetně dvou faktorové.

Data Leak Prevention (DLP)

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

Reporting

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

Antispam

Antispam je doplňkovou službou, která využívá prvky FortiMail pro detekci nevyžádané pošty. Opět jde o geograficky redundantní cluster rozmístěný ve dvou datových centrech. Kromě vlastní antispamové funkcionality nabízí také karanténu pro zachycené zprávy (pro eliminaci tzv. false positive). Službu je možné implementovat také samostatně bez nutnosti ostatních komponent NGFW.

Správa

Konfigurační a konzultační podpora, kdy zákazník nemá administrátorské oprávnění ke správě bezpečnostní platformy (VDM), ale veškeré konfigurační zásahy provádí na základě požadavků zákazníka vyškolený personál poskytovatele. Časová kapacita podpory se stanovuje individuálně, dle požadavku zákazníka.

2F autentizace

Dvoufaktorová autentizace je doplňkovou službou pro variantu NGFW Premium. K ověření je využíván softwarový kód skrze SMS/notifikaci nebo hardwarový FortiToken, generující jedinečný 60-vteřinový ověřovací kód, který je možný nosit na klíčkence.

Dostupnost a spolehlivost služby – SLA

U služby je standardně garantována minimální dostupnost 99,9 %. Výpočet dostupnosti je vztažen na dobu jednoho měsíce přepočítaného na 720 hodin (24 hodin × 30 dnů). Do doby dostupnosti nejsou započítávány pravidelné servisní odstávky služeb. Výpočet použitý pro stanovení dostupnosti je následující:

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

Kde vzorec pro výpočet obsahuje následující hodnoty:

Tabulka 5 – Hodnoty vstupující do výpočtu dostupnosti služby

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

Poskytovatel se zavazuje odstranit vady, v součinnosti se zákazníkem, v níže uvedených termínech:

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

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

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

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

Tabulka 6 – Sankce za nedodržení SLA

Dostupnost za měsíc	Maximální délka nedostupnosti	Sleva z měsíčního paušálu
99,9% – >99,5%	0,75 hodiny	10%
99,5% – >99,0%	3,6 hodiny	20%
99,0% – >98,0%	7,2 hodiny	30%
98,0% – > 97%	14,4 hodiny	50%
97,0% – > 95%	21,6 hodiny	75%
Méně než 95%	36 hodin	100%

Jiná náhrada (např. náhrada škody a ušlého zisku) nemůže být na základě Všeobecných obchodních podmínek poskytnuta a je řešena samostatně dle platných znění Obchodního a Občanského zákoníku.

Vrácení příslušné částky musí zákazník uplatnit písemně na adrese poskytovatele nejdéle však do 15 dnů od posledního dne trvání poruchy.

12.3 Hlavní výhody služby

Bezkonkurenční bezpečnost

- intelligence pro odhalování hrozeb je postavena na miliardách transakcí denně (FortiGuard)
- ochrana je zajištěna pro každý bajt webové transakce – příchozí i odchozí

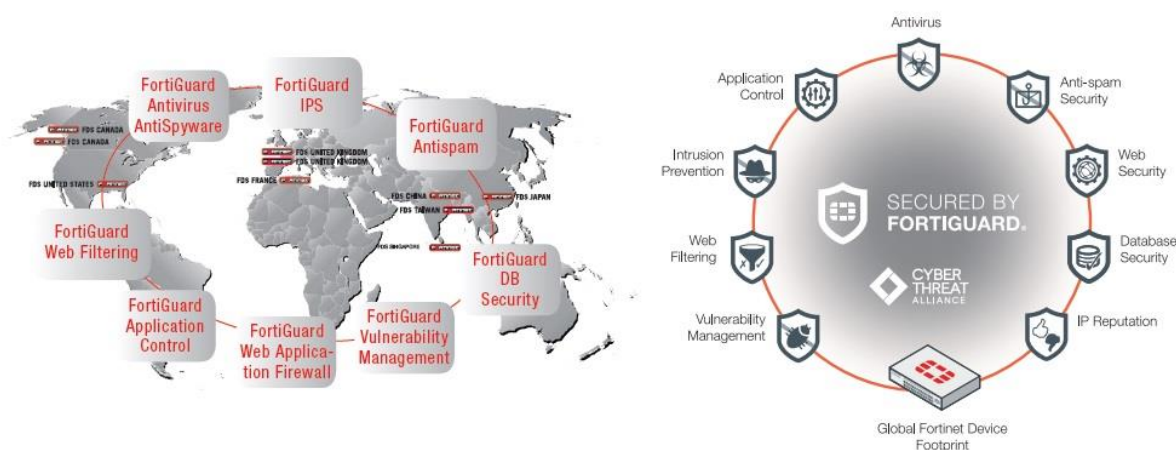
- nejmodernější a nejkompexnější zabezpečení webu s garancí SLA

Jednoduchost a účinnost

- odstranění složitosti a konsolidace samostatných zařízení v lokalitách
- přístup k řízení bezpečnostní politiky a reportingu
- flexibilní a škálovatelné řešení dle rostoucích potřeb
- snadná a rychlá implementace
- místo investičních nákladů (CAPEX) má zákazník pravidelné měsíční náklady (OPEX), které lze snadno plánovat
- přináší prokazatelný efekt již od prvního dne
- konsolidované sledování provozu v reálném čase a reporting

12.4 FortiGuard

FortiGuard je celosvětová síť firmy Fortinet, jak ukazuje následující schematický obrázek.



Obrázek 9 – Celosvětová síť FortiGuard

Tato síť má za úkol sledovat a analyzovat aktuální dění na internetu a na základě jeho stavu připravovat a následně doručovat aktualizace do jednotlivých zařízení FortiGate, aby byly schopné čelit bezprostředním bezpečnostním rizikům a hrozbám.

Jednotlivé laboratoře jsou umístěny v Kanadě, Číně, Francii, Japonsku, Malajsii a ve Spojených státech, kvůli rozložení rizik a také pro snadné pokrytí všech časových pásem (laboratoře fungují v režimu 24×7×365). Tým specialistů FortiGuard spolupracuje také s vedoucími světovými organizacemi, které monitorují aktuální hrozby (např. je jedním z členů Cyber Threat Alliance).

Pro představu, během běžného týdne FortiGuard přidá nebo aktualizuje průměrně:

- přes sto tisíc antivirových definic (signatur)
- několik desítek IPS definic
- přes půl milionů URL zařazení do webfiltering kategorií (v 65 jazycích)
- okolo třiceti miliónů antispamových signatur

Na stránkách FortiGuard lze snadno dohledat aktuální signatury a nastavení pro všechny nabízené ochrany.

13. Náklady na realizaci a provoz

Struktura cen:

- jednorázový poplatek za aktivaci a konfiguraci služby
- paušální poplatek za dedikovaný firewall
 - měsíční – uzavření smlouvy na 1, 2 nebo 3 roky
- paušální poplatek za funkcionalitu Antispam pro doménu prvního řádu (první a každou následující)
- cena závisí na těchto faktorech:
 - šířka pásma
 - model služby
 - zvolená varianta služby (ADVANCED, PREMIUM)
- příplatek za volitelné služby:
 - antispam
 - správa

Tabulka 7 – Ceny za službu NGFW v konkrétní konfiguraci

Služba	Parametry	Jednorázový poplatek za zřízení (bez DPH)	Pravidelný měsíční poplatek za používání služby (bez DPH)
Dedikovaný firewall	Šířka pásma připojení: 100/20 Mb/s Varianta: Dedicated ADVANCED / Uzavření smlouvy na: 2 roky	16 600 Kč	2900 Kč
Antispam – volitelná služba	Počet domén 1. řádu: xxxxxxxxx	xxxxxx Kč	xxxxxx Kč
Správa – volitelná služba	obsahuje libovolný počet hodin pracovního času měsíčně	xxxxxx Kč	xxxxxx Kč
2F autentizace – volitelná služba	Dvoufaktorové ověření pomocí 2FA tokenů	xxxxxx Kč	xxxxxx Kč

13.1 Platební podmínky

Obecné platební podmínky:

- Veškeré ceny jsou stanoveny smluvně a uvedeny bez daně z přidané hodnoty.
- Přesné termíny plateb budou předmětem případné smlouvy.

Podmínky pro objednání O2 NGFW:

- Minimální časový závazek pro objednání služby O2 NGFW je 1 rok.
- Změnit parametry (šířka pásma, jiná varianta) lze kdykoli v průběhu provozu služby. Tím dochází i k nové obnově minimálního časového závazku. Změna šířky pásma konektivní služby může mít dopad na volbu vhodného zařízení pro Dedikovaného (vyhrazeného) NGFW HW zařízení FortiGate.
- V případě předčasného ukončení dohodnutého časového závazku je účtována smluvní pokuta.

14. Servisní, záruční a provozní podmínky

14.1 Zákaznická podpora – Service Desk

Poskytovatel poskytuje ke službě O2 NGFW zákaznickou podporu na první a druhé úrovni.

Service Desk poskytovatele je jednotným kontaktním místem pro žádosti o zákaznickou podporu.

Service Desk zajišťuje především:

- zakládání a evidence incidentů
- poskytování informace o průběhu řešení incidentu zákazníkovi (na vyžádání)
- eskalace incidentu při nedodržení SLA
- Service Desk řeší odpovědi na běžné dotazy typu:
 - nedaří se mi přihlásit se do administračního webového rozhraní
 - v případě sjednané doplňkové služby Správa:
 - nemohu se dostat na stránku, na kterou chci i přesto, že ji mám v pravidlech povolenu
 - nefunguje blokáce na stránku, na kterou bych se podle nastavených pravidel neměl dostat

Požadavky na zákaznickou podporu jsou hlášeny pověřenými zástupci zákazníka (kontaktní osoby). Požadavky jsou v závislosti na jejich typu řešeny přímo poskytovatelem, nebo jsou postupovány dále na dodavatele / výrobce technologie.

Zákazník zajišťuje nultou úroveň podpory:

- provádí rutinní činnosti většinou spojené se správou uživatelů a definicí nových politik, monitoringem, reporty atd.
- poskytuje podporu vlastním uživatelům (zaměstnancům).

Zákaznická podpora poskytovaná ze strany poskytovatele zahrnuje:

- řešení nastalých provozních incidentů včetně případné eskalace na dodavatele nebo výrobce dané technologie.
- zajištění dostupnosti nabízeného řešení dle parametrů SLA pro jednotlivé poskytované služby včetně dohledů a pravidelné údržby těchto služeb na systémové a bezpečnostní úrovni.

Technická podpora nepokrývá žádné změnové požadavky zákazníka. Ty jsou řešeny vždy na základě objednávky a kalkulovány hodinovou sazbou.