**Rámcová dohoda č. 2100169/4600002324 na dodávku SW řízené přístupové vrstvy sítě VZP ČR**

**ID VZ: 2100169**

uzavřená ve smyslu § 131 a násl. zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, dle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů  
**(dále jen „Rámcová dohoda“)**

**Strany Rámcové dohody:**

**1. Všeobecná zdravotní pojišťovna České republiky**

se sídlem: Orlická 2020/4, 130 000 Praha 3

kterou zastupuje: Ing. Zdeněk Kabátek, ředitel VZP ČR

IČO: 411 97 518

DIČ: CZ41197518

bankovní spojení: XXXXXXXXXXX

čísla účtů: XXXXXXXXXXX

Zřízena zákonem č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky,

ve znění pozdějších předpisů

(dále jen „Objednatel“ nebo též „VZP ČR“)

a

**2.** **TOTAL SERVICE a.s.**

se sídlem: U Uranie 954/18, Holešovice, 170 00 Praha 7

kterou zastupuje/jí: Jiří Chovanec, člen představenstva

IČO: 256 18 067

DIČ: CZ25618067

bankovní spojení: XXXXXXXXXXX

číslo účtu: XXXXXXXXXXX

Zapsaná v [doplní Dodavatel] rejstříku vedeném Městským soudem v Praze, oddíl C, vložka 23580

(dále jen „Dodavatel“)

(společně též *„*Smluvní strany“)

**Článek I.**

**Úvodní ustanovení**

1. Tato Rámcová dohoda se uzavírá na základě otevřeného zadávacího řízení na uzavření Rámcové dohody s jedním Dodavatelem na veřejnou zakázku s názvem „**SW řízená přístupová vrstva sítě VZP ČR“**, evidovanou Objednatelem pod číslem 2100169 (dále jen „Veřejná zakázka“), jež byla zahájena odesláním oznámení o zahájení zadávacího řízení do Věstníku veřejných zakázek a Úředního věstníku Evropské unie dne 25. 6. 2021.
2. Dodavatel byl vybrán k uzavření této Rámcové dohody v souladu s § 122 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“), rozhodnutím ředitele VZP ČR ze dne 20. 8. 2021.
3. Dodavatel prohlašuje, že se náležitě seznámil se všemi zadávacími podmínkami této Veřejné zakázky, že jsou mu známy veškeré technické, kvalitativní a jiné podmínky plnění, že disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro poskytnutí plnění za dohodnuté jednotkové ceny uvedené v této Rámcové dohodě, a že je způsobilý ke splnění všech svých závazků podle této Rámcové dohody.
4. Ustanovení této Rámcové dohody, jakož i smluv na základě této Rámcové dohody uzavíraných, je třeba vykládat v souladu se zadávacími podmínkami výše uvedeného zadávacího řízení.

**Článek II.**

**Účel a předmět Rámcové dohody**

1. Účelem této Rámcové dohody je stanovení podmínek pro zadávání jednotlivých veřejných zakázek (dále jen „veřejná zakázka“) na dodávku SW řízené přístupové vrstvy sítě Objednatele včetně poskytování podpory na dobu 60 měsíců.
2. Předmět plnění musí být dodán jako technologický celek jednoho výrobce v souladu s podmínkami popsanými v Příloze č. 1 Rámcové dohody „Technická specifikace“ (dále jen „Příloha č. 1“).
3. Uzavření Rámcové dohody ve smyslu § 131 a násl. ZZVZ umožní Objednateli zadávat veřejné zakázky na sjednané plnění dle jeho aktuálních potřeb, čímž bude zajištěn rychlý a plynulý proces obměny předmětných zařízení.
4. Touto Rámcovou dohodou Smluvní strany mezi sebou ujednávají veškeré podmínky plnění veřejné zakázky ve smyslu § 131 ZZVZ, které jsou závazné po dobu trvání Rámcové dohody. Na základě Rámcové dohody budou zadávány veřejné zakázky v souladu s § 134 ZZVZ postupem podle podmínek stanovených v této Rámcové dohodě (viz čl. III. Rámcové dohody).
5. Předmětem této Rámcové dohody je na straně jedné rámcový závazek Dodavatele poskytovat Objednateli plnění specifikovaná v čl. IV. Rámcové dohody a v Příloze č. 1, a to za podmínek dále v této Rámcové dohodě uvedených.
6. Předmětem této Rámcové dohody je na straně druhé rámcový závazek Objednatele Dodavatelem řádně a včas poskytnutá plnění přijmout a zaplatit za ně cenu ve výši a za podmínek stanovených touto Rámcovou dohodou.
7. Předmětem plnění dle této Rámcové dohody jsou:
8. dodávky hardware (dále též jen „HW“) včetně souvisejícího standardního software v aktuální verzi (dále též jen „SW“), to vše dále též jen „zařízení“ a poskytnutí/zajištění licencí k příslušnému dodávanému SW;
9. pilotní provoz SW řízené přístupové vrstvy sítě;
10. poskytování 60 měsíční záruční podpory k dodaným HW zařízením SW řízené přístupové vrstvy sítě VZP ČR (dále též jen „Záruční podpora“);
11. zajištění školení certifikované výrobcem k administraci a konfiguraci dodané SW řízené přístupové vrstvy pro 3 pracovníky Objednatele v minimální délce 5 dnů v českém nebo slovenském jazyce;
12. bezplatný zpětný odběr stávajících vyřazovaných zařízení.
13. Předmětem plnění dle této Rámcové dohody nejsou činnosti spojené s přímou implementací SW řízené přístupové vrstvy sítě do síťové infrastruktury Objednatele. Implementaci SW řízené přístupové vrtsvy sítě bude Objednatel realizovat vlastními silami a prostředky, a to na základě výsledků Pilotního provozu. Ze strany Dodavatele jsou požadovány pouze činnosti spojené s realizací Pilotního provozu SW řízené přístupové vrtsvy sítě Objednatele.
14. Objednatel si vyhrazuje právo zadávat veřejné zakázky dle svých provozních potřeb. Tato Rámcová dohoda nezavazuje Objednatele k objednání plnění v jakémkoli minimálním množství a rozsahu (co do typu plnění nebo jeho finančního objemu).

**Článek III.**

**Veřejné zakázky zadávané na základě Rámcové dohody**

1. Jednotlivé smlouvy na plnění veřejných zakázek zadávaných na základě Rámcové dohody (dále jen „Smlouva“) budou uzavírány postupem dle této Rámcové dohody, tj. formou písemného návrhu Objednatele na uzavření Smlouvy (dále jen „návrh Smlouvy“) a písemného přijetí návrhu Smlouvy Dodavatelem, tj. podpisem návrhu Smlouvy Dodavatelem (dále jen „přijetí Smlouvy“). Dodavatel je povinen za podmínek a ve lhůtách stanovených touto Rámcovou dohodou Smlouvy s Objednatelem uzavírat. Veškeré Smlouvy budou Smluvní strany uzavírat pouze elektronicky.
2. Smluvní strany se dohodly, že oprávněná osoba Dodavatele podepíše vždy zaslaný návrh Smlouvy uznávaným elektronickým podpisem ve smyslu § 6 odst. 2 zákona č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „ZSVD“). Objednatel bude návrhy Smluv vždy podepisovat kvalifikovaným elektronickým podpisem, v souladu s § 5 výše citovaného zákona.
3. Smlouva je uzavřena podpisem Smlouvy oběma Smluvními stranami a nabývá účinnosti dnem jejího uveřejnění prostřednictvím registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.
4. Předmětem Smlouvy je závazek Dodavatele odevzdat Objednateli zařízení, která jsou předmětem plnění a umožnit mu nabýt vlastnické právo k nim a závazek Objednatele zařízení převzít a zaplatit Dodavateli sjednanou cenu, to vše za podmínek stanovených Rámcovou dohodou. Práva a povinnosti Smluvních stran neupravená touto Rámcovou dohodou se řídí příslušnými ustanoveními občanského zákoníku, zejména ustanoveními upravujícími kupní smlouvu (§ 2079 a násl. občanského zákoníku).
5. Smlouva bude zpravidla obsahovat:
6. číslo Smlouvy vygenerované z interního ekonomického systému Objednatele, které je Dodavatel povinen uvádět na příslušné faktuře a příslušném protokolu o předání a převzetí zařízení (dále jen „Předávací protokol“) nebo též na ostatních protokolech podepisovaných dle této Rámcové dohody;
7. identifikační údaje Dodavatele a Objednatele;
8. celý název této Rámcové dohody, na základě které se Smlouva uzavírá a číslo Rámcové dohody vygenerované z interního ekonomického systému, tj. číslo: 2100169/4600002324, které je Dodavatel povinen uvádět na příslušné faktuře a příslušném Předávacím/Akceptačním protokolu nebo Protokolu o uskutečnění školení;
9. specifikaci požadovaného plnění a jeho množství;
10. jednotkové ceny požadovaného plnění bez DPH a celkovou cenu plnění bez DPH;
11. lhůtu/dobu plnění;
12. jméno/jména osob Objednatele oprávněných zařízení převzít a podepsat příslušný Předávací protokol (dále též jen „Přebírající osoby“); oprávnění osob uvedených v čl. XV. odst. 6. této Rámcové dohody k těmto činnostem tímto není dotčeno;
13. ustanovení o nabytí účinnosti Smlouvy (viz odst. 3. tohoto článku);
14. jméno, příjmení a funkci osoby Objednatele, oprávněné k podpisu Smlouvy a její podpis;
15. jméno, příjmení a funkci osoby Dodavatele, oprávněné k podpisu Smlouvy a její podpis.
16. Objednatel zašle návrh Smlouvy v elektronické podobě do datové schránky Dodavatele.
17. Dokument je doručen dodáním do datové schránky adresáta (viz § 211 odst. 6 ZZVZ).
18. Dodavatel doručí Objednateli přijetí Smlouvy (tj. podepsanou Smlouvu) do datové schránky, a to nejpozději do 5 pracovních dnů ode dne doručení návrhu Smlouvy Dodavateli.
19. Osoby oprávněné k podpisu Smlouvy jsou osoby, jejichž oprávnění zastupovat Smluvní stranu je zřejmé z veřejného seznamu, případně osoby výslovně uvedené v článku XV. odst. 9. této Rámcové dohody.
20. Dodavatel je oprávněn nepřijmout Smlouvu pouze z objektivních důvodů, které nemůže Dodavatel ovlivnit nebo se jim vyhnout (ukončení výroby příslušného zařízení apod.). Dodavatel musí tyto důvody písemně sdělit Objednateli, a to stejnou formou a ve stejné lhůtě jako přijetí Smlouvy.

**Článek IV.**

**Předmět plnění**

* 1. Dodavatel se zavazuje dodávat VZP ČR níže uvedená zařízení a služby a převést na Objednatele vlastnické právo k dodaným zařízením za podmínek a způsobem dále v této Rámcové dohodě (viz zejména čl. V. Rámcové dohody) uvedeným.

Jedná se o následující zařízení a služby:

1. fixní přístupové přepínače,
2. modulární přístupové přepínače,
3. agregační přepínače,
4. bezdrátové přístupové body,
5. směrovače datového centra,

a to se standardním software, který je jejich součástí a potřebnými licencemi k jeho užití,

1. pilotní provoz SW řízené přístupové vrstvy,
2. školení administrace a konfigurace SW řízené přístupové vrstvy.
   1. Podrobná specifikace a parametry zařízení a služeb jsou uvedeny v Příloze č. 1 „Technická specifikace“ této Rámcové dohody.
   2. Dodavatel se zavazuje poskytovat všem dodaným zařízením Záruční podporu (tj. záruční podporu – viz čl. II. odst. 7. písm. c) Rámcové dohody) v délce 60 měsíců od data podpisu příslušného Předávacího protokolu oběma Smluvními stranami. Záruční podpora pokrývá veškeré opravy a případnou výměnu dodávaných zařízení.
   3. Náhradní díly pro dodávaná zařízení musí být originální (tj. vyrobené výrobcem příslušného zařízení, pro které jsou náhradní díly určeny, resp. výrobcem příslušného dílu originálního zařízení) nebo ekvivalentní k originálním a zcela kompatibilní s provozovanou technikou. Ekvivalentní náhradní díly musí být prokazatelně explicitně schváleny výrobcem zařízení nebo výrobcem originálního náhradního dílu k použití v předmětném zařízení, a to např. certifikátem, společným prohlášením o shodě, znaleckým posudkem či obdobným dokumentem, který objektivně nezavdá pochybnosti o shodě.
   4. Podrobná specifikace a způsob poskytování Záruční podpory jsou uvedeny v článku VIII. této Rámcové dohody.
   5. Dodavatel je povinen poskytnout/zajistit Objednateli jako součást plnění a za cenu zahrnutou v ceně zařízení licence k užívání softwaru, který je nedílnou a neoddělitelnou součástí poskytovaného plnění (včetně všech aktualizací získaných v rámci Záruční podpory), a to k užití v rámci VZP ČR. Licence budou jednotlivými Smlouvami poskytnuty jako nevýhradní a na dobu trvání majetkových autorských práv k příslušnému SW vč. zajištění přístupu Objednatele k aktuálním verzím SW prostřednictvím internetových stránek výrobce na adrese: <https://software.cisco.com> (nedohodnou-li se Smluvní strany v rámci Smluv na jiném způsobu jejich zpřístupnění Objednateli).
   6. Smluvní strany se dohodly, že licence poskytnuté dle této Rámcové dohody, resp. Smluv nelze vypovědět, a tedy že pro licenční ujednání podle této Rámcové dohody se nepoužije ani ustanovení § 2370 občanského zákoníku.
   7. Dodavatel se zavazuje dodat Objednateli zařízení řádně a včas bez faktických a právních vad. Dodavatel nese odpovědnost za to, že zařízení jsou ke dni dodání plně funkční, splňují minimální požadavky uvedené v tomto článku a v Příloze č. 1 této Rámcové dohody a odpovídají příslušné Smlouvě.
   8. Dodavatel se zavazuje zajistit a odpovídá za to, že dodávaná zařízení mají zejména následující vlastnosti (dále též jen „minimální vlastnosti“):
3. splňují všechny parametry uvedené v Příloze č. 1 této Rámcové dohody;
4. jsou originální, nová, nepoužitá, nerepasovaná a určená pro evropský trh;
5. všechna dodaná zařízení musí být od stejného výrobce, což značně zvýší efektivitu správy, managementu a eventuální výměny porouchaných prvků, či určování SW chyb;
6. v databázi výrobce musí být VZP ČR vedena jako první uživatel zařízení;
7. odpovídají závazným technickým normám;
8. jsou bez materiálových, konstrukčních, výrobních a vzhledových vad;
9. jsou bez právních vad;
10. jsou způsobilé pro použití k určenému účelu;
11. zařízení musí umožňovat vzdálenou správu s kompletní funkcionalitou   
    a plnou podporou prostřednictvím jednotného management SW;
12. zařízení musí být spravovatelné pomocí Cisco DNA centra (viz Příloha č. 1, bod 2. - Popis stávající sítě VZP ČR).
    1. Dodavatel je povinen dodat zařízení do místa plnění na své náklady a nebezpečí; způsob a podmínky dodání zařízení dle jednotlivých Smluv jsou uvedeny v čl. V. Rámcové dohody.
    2. Dodavatel se zavazuje poskytovat Objednateli po dobu trvání Záruční podpory všechny relevantní SW releases a verze SW nabízené výrobcem zařízení tak, aby dodané řešení vyhovovalo zadání Objednatele a fungovalo bez závad.
    3. Dodavatel se zavazuje včas a bez zbytečného odkladu informovat Objednatele o nových verzích SW a funkčnostech, které mohou rozšiřovat dodané řešení způsobem, který VZP ČR shledá ve shodě s potřebami dalšího rozvoje dodaného řešení.
    4. Objednatel musí mít možnost si sám legálně stahovat nové verze software přímo ze stránek nebo z dedikovaného úložiště výrobce.
    5. Dodavatel prohlašuje a odpovídá za to, že veškeré aktualizace a přechody na novější verze SW vztahující se k dodanému předmětu plnění budou respektovat oficiální doporučení výrobce zařízení a rovněž budou pocházet ze zdrojů určených výrobcem.
    6. Dodavatel se zavazuje zajistit Objednateli možnost zaregistrovat se na internetových stránkách výrobce na adrese: <https://tools.cisco.com/security/center/publicationListing.x> za účelem odběru automatických e-mailových zpráv týkajících se dodaných zařízení a upozorňujících s denní frekvencí především na:
       1. bezpečnostní incidenty, které vyžadují od Objednatele povýšení operačního systému/firmware či aplikování změny konfigurace či záplaty;
       2. konec prodeje či podpory;
       3. nové verze operačního systému/firmware;
       4. známé chyby operačního systému/firmware.
    7. Dodavatel se zároveň zavazuje informovat Objednatele o nových verzích SW a funkčnostech, které mohu rozšiřovat dodané řešení způsobem, který Objednatel shledá ve shodě s potřebami dalšího rozvoje dodaného řešení.
    8. Dodavatel prohlašuje a odpovídá za to, že plnění dle této Rámcové dohody, která jsou předmětem jakéhokoliv práva duševního vlastnictví, je oprávněn distribuovat a poskytovat třetím osobám (vč. Objednatele).
    9. Dodavatel se zavazuje předat vždy Objednateli současně se zařízením veškeré doklady nutné k převzetí, jakož i k provozování a užívání předmětného zařízení, tj. zejména dodací list a záruční list, návody k použití, uživatelské příručky a veškeré další doklady, nezbytné k řádnému užívání dodaného zařízení (dále jen „Nezbytné doklady k zařízení“). Veškeré Nezbytné doklady k zařízení musí být v českém nebo slovenském jazyce. Výjimkou jsou technické dokumentace výrobce, které mohou být i v anglickém jazyce a mohou být Objednateli poskytnuty i formou uvedení odkazu na internetové stránky. Dodavatel je povinen zajistit Objednateli přistup k znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
    10. Objednatel si vyhrazuje právo vyžádat si v případě potřeby od Dodavatele dodání překladu anglického textu do českého jazyka.
    11. Řádné dodání zařízení (za cenu zahrnutou v cenách zařízení) též zahrnuje zabalení zařízení, jejich přepravu do místa plnění a řádné předání Přebírající osobě Objednatele.
    12. Dodavatel se zavazuje zajistit bezplatný zpětný odběr stávajících zařízení Objednatele, která jsou již dále nevyužitelná a budou v rámci obměny zastaralých přístupových přepínačů a přístupových bodů vyřazena.
    13. Dodavatel není oprávněn dodat Objednateli větší, než Objednatelem ve Smlouvě požadované množství zařízení; postup dle § 2093 občanského zákoníku Smluvní strany tímto vylučují.
    14. Dodavatel se zavazuje provést Pilotní provoz SW řízené přístupové vrstvy sítě Objednatele. Toto plnění bude rozděleno na 3 samostatné části, které jsou blíže popsány v Příloze č. 1 této Rámcové dohody. Řádné provedení každé z těchto částí Pilotního provozu bude potvrzeno v příslušném akceptačním protokolu. Bližší specifikace požadavků na Pilotní provoz je uvedena v Příloze č. 1 této Rámcové dohody.
    15. Dodavatel se zavazuje zajistit realizaci školení v prostorách výrobcem certifikovaného školicího střediska, a to v minimálním rozsahu (trvání) pěti (5) dnů pro tři (3) pracovníky Objednatele na administraci a konfiguraci dodané SW řízené přístupové vrstvy.
    16. Řádné uskutečnění školení bude potvrzeno v příslušném dokumentu o realizaci školení (dále jen „Protokol o uskutečnění školení“) podepsaném k tomu Pověřenou osobou Objednatele, jehož součástí bude prezenční listina z uskutečněného školení.

**Článek V.**

**Doba, místo a podmínky plnění**

1. Místem dodání zařízení, poskytování Záruční podpory a místem plnění provedení Pilotního provozu jsou:

* Ústředí VZP ČR na adrese Orlická 2020/4, 130 00 Praha 3 a
* datové centrum ČD – Telematika a.s., na adrese Pod Táborem 369/8a, 190 00 Praha 9.

1. Dodavatel je povinen předat zařízení Objednateli v místě plnění na své náklady a nebezpečí. Lhůta dodání zařízení je do **90 kalendářních dnů** ode dne nabytí účinnosti příslušné Smlouvy.
2. Objednatel určí pro každou Smlouvu Přebírající osobu (osoby), která bude oprávněná v místě plnění zařízení převzít a podepsat Předávací protokol a uvede její kontaktní e-mail a telefon. Přebírající osoby budou uvedeny v příslušné Smlouvě nebo budou sděleny Dodavateli následně e-mailem zaslaným Pověřenou osobou Objednatele Pověřené osobě Dodavatele.
3. Dodavatel je povinen dohodnout s Přebírající osobou konkrétní datum a čas doručení zařízení v místě plnění. Tyto údaje Dodavatel následně písemně potvrdí elektronickou poštou na e-mail Přebírající osoby, a to nejméně 3 pracovní dny před datem doručení zařízení.
4. Nejpozději současně s doručením zařízení předá Dodavatel jednotlivým Přebírajícím osobám příslušný Předávací protokol podepsaný Pověřenou osobou Dodavatele (viz čl. XV. odst. 6. této Rámcové dohody); Předávací protokol lze zaslat v naskenované podobě také na e-mail Pověřené osoby Objednatele (viz čl. XV. odst. 6. této Rámcové dohody), nedohodnou-li se Smluvní strany v konkrétním případě jinak.
5. V dohodnutém termínu, čase a místě plnění předá Dodavatel zařízení Přebírající osobě, přičemž Přebírající osoba zkontroluje zařízení v zabaleném stavu, zejména soulad s údaji uvedenými v dodacím listu, množství přepravních jednotek (tj. krabic, kontejnerů apod.), neporušenost obalů, popisy na obalech apod. Následně Přebírající osoba potvrdí dodání zařízení podpisem dodacího listu. Pokud Přebírající osoba zjistí při kontrole zařízení v zabaleném stavu nedostatky nebo rozpor s dodacím listem, vyspecifikuje tyto nedostatky v dodacím listu.
6. Řádné dodání všech zařízení do místa plnění dle příslušné Smlouvy bude potvrzeno podpisem Předávacího protokolu Pověřenou osobou Dodavatele a Přebírající osobou Objednatele. V každém Předávacím protokolu bude uvedeno zejména označení a číslo této Rámcové dohody a příslušné Smlouvy, specifikace dodávaných zařízení včetně sériových čísel a jeho množství, datum, jméno a podpis Přebírající osoby Objednatele a Pověřené osoby Dodavatele. Podepsaný Předávací protokol zašle Přebírající osoba e-mailem Pověřené osobě Dodavatele.
7. Před podpisem Předávacího protokolu Přebírající osoba zkontroluje soulad předávaných zařízení s údaji uvedenými v příslušné Smlouvě (zejména Part number / název a počet) a dále zkontroluje, zda předávaná zařízení nemají zjevné vady. V případě zjištění jakýchkoli vad Objednatel vadné zařízení nepřevezme. Zjištěné vady zařízení, jakož i případná chybějící zařízení Objednatel vyspecifikuje v Předávacím protokolu (dále jen „**Předávací protokol s výhradou**“). Závazek Dodavatele dodat zařízení dle příslušné Smlouvy tak zůstává nesplněn až do dne řádného dodání všech zařízení dle příslušné Smlouvy do místa plnění.
8. Podpisem příslušného Předávacího protokolu Objednatelem přechází na VZP ČR vlastnické právo k zařízení a nebezpečí škody na zařízení.
9. Objednatel je povinen do 5 pracovních dnů od doručení zařízení do místa plnění podpisem příslušného Předávacího protokolu ve 2 vyhotoveních potvrdit řádné dodání zařízení s tím, že 1 podepsané vyhotovení příslušného Předávacího protokolu zašle neprodleně zpět Dodavateli (viz též odst. 7. tohoto článku).
10. Závazek Dodavatele dodat zařízení podle příslušné Smlouvy je splněn podpisem všech Předávacích protokolů bez výhrad, resp. podpisem posledního Předávacího protokolu bez výhrad Objednatelem dle příslušné Smlouvy. Následně je Dodavatel oprávněn vystavit za dodaná zařízení fakturu dle příslušných ustanovení této Rámcové dohody.
11. Dodavatel se zavazuje k bezplatnému zpětnému odběru stávajících vyřazovaných zařízení, a to na základě písemné (elektronické) výzvy Objednatele nejpozději do 24 měsíců ode dne nabytí účinnosti Rámcové dohody a dnem jejího uveřejnění prostřednictvím registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů.

**Článek VI.**

**Cena plnění**

1. Objednatel se zavazuje zaplatit Dodavateli za řádné poskytnutí plnění cenu ve výši a lhůtách splatnosti dohodnutých touto Rámcovou dohodou.
2. Dodavatel se zavazuje poskytovat Objednateli plnění na základě této Rámcové dohody a Smluv   
   za jednotkovou cenu, která je uvedena v Příloze č. 2 této Rámcové dohody.
3. Jednotková cena za plnění bez daně z přidané hodnoty (dále jen „DPH“) je stanovena v souladu se zákonem č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, na základě cenové nabídky Dodavatele předložené v rámci zadávacího řízení na uzavření Rámcové dohody. Jednotková cena bez DPH je stanovena jako maximální, nejvýše přípustná a nepřekročitelná   
   a zahrnuje veškeré náklady Dodavatele nutné k řádnému poskytnutí plnění dle podmínek stanovených v této Rámcové dohodě včetně odměny za poskytnuté licence.
4. K jednotkové ceně bez DPH, uvedené v Příloze č. 2, bude Dodavatelem účtována daň   
   z přidané hodnoty v zákonem stanovené výši platné ke dni uskutečnění zdanitelného plnění. Za správnost stanovení sazby DPH a vyčíslení výše DPH odpovídá Dodavatel.
5. Součástí jednotkové ceny jsou i související služby či dodávky, které v zadávací dokumentaci této Veřejné zakázky nebo v této Rámcové dohodě nejsou výslovně uvedeny, ale Dodavatel jakožto odborník o nich ví nebo má vědět, že jsou nezbytné pro řádné poskytnutí plnění. Na eventuální dodatečné vícenáklady a/nebo požadavky Dodavatele zejména na úhradu víceprací a/nebo úhrady spojené s pohybem cen, pohybem měnových kurzů a podobně nebude brán zřetel a Dodavatel nemá právo na jejich úhradu. S tím Dodavatel projevuje svůj výslovný a bezvýhradný souhlas.
6. Objednatel neposkytuje Dodavateli na předmět plnění dle této Rámcové dohody jakékoliv zálohy.

**Článek VII.**

**Fakturační a platební podmínky**

1. Úhrady za plnění, poskytnutá na základě Smluv a v souladu s touto Rámcovou dohodou, budou Objednatelem prováděny bezhotovostním převodem na bankovní účet Dodavatele, uvedený v záhlaví Rámcové dohody, a to na základě daňových dokladů – faktur vystavených Dodavatelem (dále jen „faktura“) a zaslaných Objednateli. Smluvní strany se dohodly, že bankovní účty uvedené u jejich identifikačních údajů v záhlaví Rámcové dohody mohou být měněny pouze formou písemných smluvních dodatků k této Rámcové dohodě, podepsaných oprávněnými zástupci Smluvních stran.
2. Jednotlivé faktury bude Dodavatel zasílat Objednateli v listinné podobě na adresu sídla Objednatele uvedenou v záhlaví této Rámcové dohody nebo v elektronické podobě do datové schránky Objednatele.
3. Dodavatel je oprávněn vystavit fakturu za plnění dle čl. II, odst. 7, písm. a) a d) až po poskytnutí veškerého plnění dle příslušné Smlouvy, tj. po podpisu příslušného Předávacího protokolu / Protokolu o uskutečnění školení Objednatelem, kterým bude řádné poskytnutí příslušného plnění stvrzeno. Kopie příslušného protokolu musí být přílohou vystavené faktury, jinak faktura nezakládá povinnost Objednateli uhradit uvedenou cenu. Cena za plnění dle čl. II. odst. 7. písm. c) je započtena v cenách za jednotlivá zařízení.
4. Smluvní strany se dohodly, že Dodavatel Objednateli cenu dílčích plnění Pilotního provozu dle čl. II, odst. 7, písm. b) vyfakturuje postupně, a to po ukončení jednotlivých částí následovně:

|  |  |  |  |
| --- | --- | --- | --- |
| Část | Fakturační milník | Podíl z ceny | Cena bez DPH  [Kč] |
| Analytická část | Akceptační protokol | 30%  z ceny | 1 665 000,- |
| Provedení pilotního provozu | Akceptační protokol | 50%  z ceny | 2 775 000,- |
| Dokumentace k migračnímu procesu | Akceptační protokol | 20%  z ceny | 1 110 000,- |

1. Úhrady za plnění budou prováděny v českých korunách. Peněžitá částka se považuje za zaplacenou (tj. peněžitý závazek se považuje za splněný) okamžikem jejího odepsání z účtu Objednatele ve prospěch účtu Dodavatele. Dodavatel není oprávněn nárokovat bankovní poplatky nebo jiné náklady vztahující se k převodu poukazovaných částek mezi Smluvními stranami na základě této Rámcové dohody.
2. Každá faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných zákonných ustanovení, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a § 435 občanského zákoníku.
3. Každá faktura musí též obsahovat číslo této Rámcové dohody, tj. číslo 2100169/4600002324 a číslo příslušné Smlouvy. Obě čísla budou vždy uvedena v příslušné Smlouvě (viz též čl. III. odst. 5. této Rámcové dohody). Pro fakturaci plnění dle čl. II., odst. 7. písm. d) navíc i číslo 2100169/4100057796.
4. Na veškerých fakturách musí být vždy jako odběratel uvedena Všeobecná zdravotní pojišťovna České republiky, Orlická 2020/4, 130 00 Praha 3.
5. Smluvní strany se dohodly, že splatnost každé faktury je 30 kalendářních dnů ode dne jejího doručení Objednateli.
6. Objednatel je oprávněn před uplynutím lhůty splatnosti vrátit bez zaplacení fakturu, která neobsahuje zákonem nebo touto Rámcovou dohodou stanovené náležitosti, obsahuje nesprávné údaje, není doplněna dohodnutými přílohami nebo má jiné vady v obsahu podle této Rámcové dohody nebo podle příslušných právních předpisů. V takovém případě je Objednatel povinen zároveň uvést důvod vrácení faktury. Dodavatel je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. Vrácením faktury přestává běžet původní lhůta splatnosti. Celá 30 denní lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury Objednateli.
7. Dodavatel prohlašuje, že účet uvedený v záhlaví Rámcové dohody je účtem zveřejněným správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 zákona o DPH.
8. V případě, že Dodavatel nebude mít v době uskutečnění zdanitelného plnění bankovní účet uvedený v záhlaví Rámcové dohody tímto způsobem zveřejněn, uhradí Objednatel Dodavateli v dohodnutém termínu splatnosti příslušné faktury pouze částku představující dohodnutou cenu plnění bez DPH. Částku rovnající se výši DPH z ceny plnění fakturované Dodavatelem uhradí Objednatel, v souladu s § 109a zákona o DPH, finančnímu úřadu místně příslušnému Dodavateli. Dodavatel výslovně prohlašuje, že příslušnou cenu plnění bude považovat tímto za zaplacenou.
9. Pokud v době uskutečnění příslušného zdanitelného plnění bude Dodavatel uveden v aplikaci „Registr DPH“ jako Nespolehlivý plátce, dohodly se Smluvní strany, že Objednatel bude postupovat při úhradě ceny příslušného plnění způsobem uvedeným v odst. 12. tohoto článku.

**Článek VIII.**

**Odpovědnost za vady, Záruční podpora a záruční doba**

1. Dodavatel se zavazuje realizovat předmět plnění této Rámcové dohody v souladu s příslušnými právními předpisy a s maximální péčí a v kvalitě odpovídající jeho odborným znalostem a zkušenostem, kterou lze od něj vzhledem k jeho profesnímu zaměření právem očekávat.
2. Dodavatel odpovídá za veškeré právní vady i faktické vady (společně též jen „vady“) zařízení, které bude mít zařízení (či jeho dílčí část) v době převzetí Objednatelem nebo které budou zjištěny v záruční době.
3. Dodavatel odpovídá za to, že zařízení (či jeho dílčí části) v době jeho převzetí Objednatelem a po celou záruční dobu:

* nebude mít žádné právní vady (zjevné či skryté), zejména pak, že nebude zatíženo právy třetích osob, ze kterých by pro Objednatele vyplynuly jakékoli další finanční nebo jiné povinnosti ve prospěch třetích stran;
* nebude mít žádné faktické vady (zjevné či skryté), zejména pak, že bude splňovat veškeré funkční, technické a jiné vlastnosti a specifikace dohodnuté v této Rámcové dohodě a vlastnosti obvyklé, a dále že bude splňovat veškeré požadavky stanovené příslušnými právními předpisy a technickými normami.

1. Dodavatel poskytuje Objednateli na dodané zařízení záruku za jakost (dále též jen „**záruka**“) v délce 60 měsíců. Záruční doba začne běžet ode dne podpisu příslušného Předávacího protokolu oběma Smluvními stranami.
2. Zárukou za jakost se Dodavatel zavazuje, že zařízení bude po celou záruční dobu způsobilé pro použití ke smluvenému, popř. obvyklému účelu a že si zachová smluvené, popř. obvyklé vlastnosti.
3. Ustanovení § 2112 občanského zákoníku, stanovící důsledky neoznámení vad zařízení bez zbytečného odkladu, se pro účely této Rámcové dohody nepoužije; záruka se vztahuje na veškeré vady zařízení, které Objednatel uplatní v záruční době.
4. V rámci poskytování Záruční podpory se Dodavatel zavazuje odstraňovat veškeré vady opravou nebo výměnou vadného zařízení za nové, a to při dodržení všech podmínek a ustanovení Rámcové dohody, příslušné Smlouvy na plnění a technických požadavků na zařízení.
5. Dodavatel se zavazuje poskytovat Objednateli po celou záruční dobu, tj. 60 měsíců od podpisu příslušného Předávacího protokolu oběma Smluvními stranami, Záruční podporu k veškerým dodaným zařízením (viz čl. IV. odst. 1. písm. a) – e) Rámcové dohody). Cena Záruční podpory je zahrnuta v jednotkové ceně zařízení, uvedené v Příloze č. 2 této Rámcové dohody.
6. Poskytování Záruční podpory spočívá v povinnosti Dodavatele odstraňovat veškeré vady dodaných zařízení vzniklé při provozu zařízení a nefunkčnost některé ze služeb (dále dohromady též jen „vady“) **v režimu 7x24**. Pro vyloučení pochybností Smluvní strany uvádějí, že poskytování Záruční podpory zahrnuje cenu nového zařízení, spotřebního materiálu a dopravu nového zařízení do místa plnění.
7. Standardní komunikace mezi Objednatelem a Dodavatelem při poskytování Záruční podpory bude probíhat prostřednictvím aplikace Service Desk Objednatele v českém nebo slovenském jazyce. Tento způsob komunikace bude použit pro nahlášení vady (tj. poskytování požadované Záruční podpory), sledování průběhu odstraňování vady zařízení a odstranění vady zařízení.
8. Objednatel bude hlásit každou vadu zjištěnou v záruční době při provozu zařízení prostřednictvím svého Service Desku (e-mail: [servicedesk@vzp.cz](mailto:servicedesk@vzp.cz), telefon: 952 220 000) na servisní kontaktní místo Dodavatele (e-mail: [helpdesk@totaservice.cz](mailto:helpdesk@totaservice.cz), telefon: 270 002 800).
9. Komunikace se Service Deskem (dále též „SD") Objednatele bude probíhat primárně na bázi elektronické komunikace formou servisních požadavků (dále též jako „SP“). Použití telefonické či distanční formy elektronické komunikace (např. prostřednictvím MS Teams, Webex apod.) při zadání, řešení či vyřešení SP je možné pouze v případě, kdy nelze využít e-mailovou komunikaci. V případě komunikace prostřednictvím telefonu či distanční formy elektronické komunikace bude i tato komunikace následně potvrzena prostřednictvím e-mailu.
10. Komunikace mezi Objednatelem a Dodavatelem bude obsahovat minimálně tyto kroky:
    * 1. Zadání servisního požadavku Objednatelem – nahlášení vady Dodavateli vč. jejího podrobného popisu a vč. uvedení typu služby („Bussines critical“ nebo „Normal“) (zaslání e-mailu Dodavateli).
      2. Automatické potvrzení doručení servisního požadavku (e-mailu) Dodavateli, potvrzující doručení servisního požadavku VZP ČR na e-mail Dodavatele (zaslání e-mailu Objednateli).
      3. Potvrzení přijetí servisního požadavku Dodavatelem – (zaslání e-mailu Objednateli) do 4 hodin (reakční doba) od automatického potvrzení doručení servisního požadavku Dodavateli.
      4. V případě odmítnutí servisního požadavku Dodavatelem – (zaslání e-mailu Objednateli); součástí odmítnutí musí být jeho řádné odůvodnění, a to ve stejné lhůtě jako potvrzení přijetí SP.
      5. Oznámení o vyřešení servisního požadavku Dodavatelem (zaslání e-mailu Objednateli); v oznámení musí být uvedeno, kdy byla vada odstraněna. Přílohou e-mailu musí být kopie podepsaného Protokolu o odstranění vady.
11. Objednatel si vyhrazuje možnost dotazu (e-mailem) na stav nevyřešeného požadavku, na nějž Dodavatel odpoví nestrukturovaným e-mailem.
12. Okamžikem vyřešení SP se rozumí datum a čas uvedený v protokolu o odstranění vady, který bude souáčastí e-mailu „Oznámení o vyřešení servisního poždavku Dodavatelem“, který bude poslán Objednateli při vyřešení servisního požadavku (viz odst. 13. písm. e) tohoto článku).
13. Lhůty pro odstranění vady v rámci poskytování Záruční podpory jsou stanoveny ve dvou režimech (službách), a to „Bussines critical“ a „Normal“. Ve službě „Bussines critical“ je lhůta pro odstranění vady do 24 hodin od automatického potvrzení doručení servisního požadavku Dodavateli, ve službě „Normal“ je lhůta pro odstranění vady do 2 pracovních dnů od automatického potvrzení doručení servisního požadavku Dodavateli.
14. Služba „Bussines critical“ slouží k řešení bussines critical incidentů v SW řízené přístupové vrstvě, které mají významný dopad do činnosti VZP ČR. Za významný dopad se rozumí ovlivnění práce více než 20 % uživatelů. Služba „Normal“ slouží k řešení ostatních incidentů.
15. Odstranění vady bude potvrzeno v Protokolu o odstranění vady, podepsaném Pověřenými osobami Smluvních stran při předání opraveného nebo nového zařízení, ve kterém bude mj. uvedeno označení převzatého nového zařízení a jeho množství a datum a čas odstranění vady. Podpisem Protokolu o odstranění vady Pověřenou osobou Objednatele je odstranění vady považováno za dokončené. Následně pak Dodavatel pošle e-mail o vyřešení servisního požadavku, kde uvede datum a čas odstranění vady a bude přiložena kopie podepsaného Protokolu o odstranění vady.
16. Neodstraní-li Dodavatel vadu zařízení ve stanoveném či dohodnutém termínu je Objednatel oprávněn odstranit vadu sám nebo pověřit odstraněním této vady třetí osobu, a to bez ztráty oprávnění ze záruky podle této Rámcové dohody. Veškeré takto vzniklé náklady je Dodavatel povinen Objednateli uhradit. Možnost Objednatele vyúčtovat Dodavateli smluvní pokutu za prodlení s odstraňováním vad při poskytování Záruční podpory v záruční době dle čl. XIII. odst. 4. Rámcové dohody tím není dotčena.

**Článek IX.**

**Odpovědnost za škodu**

1. Odpovědnost za škodu se řídí ustanovením § 2894 a násl. občanského zákoníku, zejména pak ustanovením § 2913 občanského zákoníku.
2. Smluvní strana, která poruší svoji povinnost vyplývající z této Rámcové dohody nebo ze Smlouvy, je povinna nahradit škodu tím způsobenou druhé Smluvní straně. Povinnosti k náhradě škody se zprostí, prokáže-li, že jí ve splnění povinnosti dočasně nebo trvale zabránila mimořádná nepředvídatelná a nepřekonatelná překážka vzniklá nezávisle na její vůli. Škoda, způsobená zaměstnanci příslušné Smluvní strany nebo třetími osobami, které příslušná Smluvní strana pověří plněním svých závazků dle Rámcové dohody, bude posuzována jako škoda způsobená příslušnou Smluvní stranou.
3. Není-li v této Rámcové dohodě stanoveno jinak, odpovídá příslušná Smluvní strana za jakoukoli škodu, která druhé Smluvní straně vznikne v souvislosti s porušením povinností příslušné Smluvní strany podle Rámcové dohody či Smlouvy.
4. Překážka vzniklá z osobních poměrů příslušné Smluvní strany nebo vzniklá až v době, kdy byla příslušná Smluvní strana s plněním smluvené povinnosti v prodlení, ani překážka, kterou byla příslušná Smluvní strana podle Rámcové dohody povinna překonat, jí však povinnosti k náhradě škody nezprostí.
5. Smluvní strana, která porušila právní povinnost, nebo Smluvní strana, která může a má vědět, že ji poruší, oznámí to bez zbytečného odkladu druhé Smluvní straně, které z toho může újma vzniknout, a upozorní ji na možné následky. Splní-li oznamovací povinnost, nemá poškozená Smluvní strana právo na náhradu té újmy, které mohla po oznámení zabránit.
6. V případě, že Dodavatel použije k plnění svých závazků vyplývajících z této Rámcové dohody / Smlouvy poddodavatele, odpovídá Dodavatel za jeho/jejich plnění tak, jako by plnil sám.
7. Smluvní strany se dohodly, že celková výše náhrady škody vzniklé Smluvním stranám při plnění závazků nebo v souvislosti s plněním závazků Rámcové dohody nebo Smluv nepřesáhne v úhrnu pro každou Smluvní stranu částku 25 000 000 Kč (slovy dvacet pět miliónů korun českých). Uvedené omezení se netýká škod způsobených úmyslně.

**Článek X.**

**Ochrana informací, osobních údajů a dat**

1. S odkazem na § 24a zákona č. 551/1991 Sb., o Všeobecné zdravotní pojišťovně České republiky, ve znění pozdějších předpisů, zákon č. 110/2019 Sb., o zpracování osobních údajů, Nařízení Evropského parlamentu a Rady (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 (obecné nařízení o ochraně osobních údajů), a dále na zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, se Dodavatel zavazuje učinit taková opatření, aby veškeré osoby, které se podílejí na realizaci jeho závazků z této  Rámcové dohody a Smluv, zachovávaly mlčenlivost o veškerých osobních údajích, jakož i o technicko-organizačních opatřeních k jejich ochraně, o nichž se při plnění závazků dozvěděly, včetně těch, které Objednatel eviduje pomocí výpočetní techniky, či jinak. Toto ujednání platí i v případě nahrazení uvedených právních předpisů předpisy jinými.
2. Dodavatel se dále zavazuje zajistit, aby veškeré osoby, které se podílejí na realizaci jeho závazků z této Rámcové dohody / Smluv, zachovávaly mlčenlivost o veškerých dalších skutečnostech, údajích a datech, o nichž se při plnění těchto závazků dozvěděly, a které nejsou veřejně známé nebo veřejně dostupné.
3. Za porušení závazků uvedených v odst. 1. a 2. tohoto článku se považuje i využití těchto skutečností, údajů a dat, jakož i dalších vědomostí pro vlastní prospěch Dodavatele, prospěch třetí osoby nebo pro jiné důvody.
4. Poskytnutí informací na základě povinností stanovených Smluvním stranám obecně závaznými právními předpisy České republiky včetně přímo použitelných předpisů Evropské unie není považováno za porušení povinností Smluvních stran sjednaných v tomto článku.
5. Za porušení závazku uvedeného v odstavci 1. tohoto článku je Dodavatel povinen zaplatit Objednateli v každém jednotlivém případě smluvní pokutu ve výši 1 000 000 Kč (slovy: jeden milion korun českých). Ujednáním o smluvní pokutě ani zaplacením smluvní pokuty není dotčeno právo VZP ČR na náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje.
6. Za porušení závazku uvedeného v odstavci 2. tohoto článku je Dodavatel povinen zaplatit Objednateli v každém jednotlivém případě smluvní pokutu ve výši 100 000 Kč (slovy: jedno sto tisíc korun českých). Ujednáním o smluvní pokutě ani zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu škody vzniklé z porušení povinnosti, ke kterému se smluvní pokuta vztahuje.
7. Závazky Smluvních stran uvedené v tomto článku trvají i po skončení tohoto smluvního vztahu.

**Článek XI.**

**Uveřejnění Rámcové dohody**

1. Smluvní strany jsou si plně vědomy zákonné povinnosti Smluvních stran uveřejnit dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), tuto Rámcovou dohodu, Smlouvy, které budou uzavřeny na základě této Rámcové dohody, včetně všech případných dohod, kterými se tato Rámcová dohoda / Smlouva doplňuje, mění, nahrazuje nebo ruší, prostřednictvím registru smluv.
2. Uveřejněním Rámcové dohody / Smlouvy dle odst. 1. tohoto článku se rozumí uveřejnění elektronického obrazu textového obsahu Rámcové dohody / Smlouvy v otevřeném a strojově čitelném formátu a rovněž metadat, podle § 5 odst. 1 zákona o registru smluv, prostřednictvím registru smluv.
3. Smluvní strany se dohodly, že tuto Rámcovou dohodu zašle správci registru smluv k uveřejnění prostřednictvím registru smluv Objednatel. Dodavatel je povinen zkontrolovat, že Rámcová dohoda včetně všech příloh a metadat byla řádně v registru smluv uveřejněna. V případě, že Dodavatel zjistí jakékoli nepřesnosti či nedostatky, je povinen neprodleně o nich Objednatele informovat. Výše uvedený postup se Smluvní strany zavazují dodržovat i pro Smlouvy, nedohodnou-li se v konkrétní Smlouvě výslovně jinak.
4. Postup uvedený v odst. 3. tohoto článku se Smluvní strany zavazují dodržovat i v případě uzavření dodatků k této Rámcové dohodě, jakož i v případě jakýchkoli dalších dohod, kterými se tato Rámcová dohoda doplňuje, mění, nahrazuje nebo ruší.
5. Dodavatel bere na vědomí a souhlasí s tím, že Objednatel rovněž uveřejní tuto Rámcovou dohodu (tj. celé znění včetně všech příloh) včetně všech jejích případných dodatků, jakož i všechny Smlouvy, na svém profilu zadavatele.
6. Dodavatel výslovně souhlasí s tím, že s výjimkou ustanovení znečitelněných v souladu se zákonem o registru smluv bude uveřejněno úplné znění Rámcové dohody.
7. VZP ČR výslovně souhlasí s tím, že s výjimkou ustanovení znečitelněných v souladu se zákonem o registru smluv bude uveřejněno úplné znění Rámcové dohody.

**Článek XII.**

**Pojištění**

1. Dodavatel se zavazuje, že bude po celou dobu poskytování plnění na základě této Rámcové dohody / Smluv, jakož i po celou záruční dobu (tj. dobu poskytování Záruční podpory k dodanému zařízení), pojištěn pro případ vzniku odpovědnosti za škodu.
2. Uvedené pojištění musí být sjednáno pro případ odpovědnosti Dodavatele za škodu, která může vzniknout Objednateli nebo třetí osobě při plnění závazků Dodavatele dle této Rámcové dohody / Smluv, resp. v souvislosti s plněním těchto závazků. Pojištění musí být sjednáno s pojistnou částkou ne nižší než 25 000 000 Kč (slovy: dvacet pět milionů korun českých).
3. Dodavatel je povinen na výzvu Pověřené osoby Objednatele doložit, že je pojištěn pro případ odpovědnosti za škodu v požadovaném rozsahu, a to vždy nejpozději do 10 pracovních dnů od doručení výzvy Objednatele. Dodavatel k prokázání splnění tohoto požadavku předloží Objednateli dokumenty, ze kterých bude splnění požadavku na pojištění vyplývat, tj. buď pojistnou smlouvu nebo pojistku a doklad o zaplacení pojistného na příslušné období nebo pojistný certifikát, či obdobný doklad vydaný příslušnou pojišťovnou.
4. V případě nesplnění povinnosti Dodavatele stanovené v odst. 1. a 2. tohoto článku je VZP ČR oprávněna vyúčtovat Dodavateli smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých), a to za každý i jen započatý kalendářní den, kdy porušení této povinnosti trvá a Dodavatel je povinen tuto částku uhradit.
5. V případě nesplnění povinnosti Dodavatele stanovené v odst. 3. tohoto článku je VZP ČR oprávněna vyúčtovat Dodavateli smluvní pokutu ve výši 5 000 Kč (slovy: pět tisíc korun českých) za každý i jen započatý kalendářní den prodlení a Dodavatel je povinen tuto částku uhradit.
6. VZP ČR je oprávněna uplatnit právo na zaplacení smluvních pokut dle odst. 4. a 5. tohoto článku souběžně.

**Článek XIII.**

**Sankční ujednání**

1. V případě prodlení Dodavatele s doručením přijetí Smlouvy Objednateli dle čl. III. odst. 8. Rámcové dohody, je Objednatel oprávněn vyúčtovat Dodavateli smluvní pokutu ve výši 0,02 % z ceny za plnění uvedené ve Smlouvě (bez DPH), s jejímž přijetím je Dodavatel v prodlení, a to za každý i jen započatý kalendářní den prodlení a Dodavatel je povinen tuto smluvní pokutu zaplatit.
2. V případě prodlení Dodavatele s řádným dodáním zařízení dle příslušné Smlouvy je Objednatel oprávněn vyúčtovat Dodavateli smluvní pokutu ve výši 0,05 % z ceny za plnění uvedené ve Smlouvě (bez DPH), a to za každý i jen započatý kalendářní den prodlení a Dodavatel je povinen tuto smluvní pokutu zaplatit.
3. V případě prodlení Dodavatele s odesláním potvrzení přijetí servisního požadavku Dodavatelem dle čl. VIII. odst. 13. písm. c) Rámcové dohody je Objednatel oprávněn vyúčtovat Dodavateli smluvní pokutu ve výši 200 Kč (slovy: dvě stě korun českých) za každou i jen započatou hodinu prodlení a Dodavatel je povinen tuto smluvní pokutu zaplatit.
4. V případě prodlení Dodavatele s odstraněním vady při poskytování Záruční podpory dle čl. VIII. odst. 16. Rámcové dohody je Objednatel oprávněn vyúčtovat Dodavateli smluvní pokutu ve výši 200 Kč (slovy: dvě stě korun českých) za každou i jen započatou hodinu prodlení a Dodavatel je povinen tuto smluvní pokutu zaplatit.
5. V případě prodlení Dodavatele s realizací Pilotního provozu, tj. s prodlením plnění dle kapitoly 6 písm. a) – c) Přílohy č. 1 této Rámcové dohody, a to každé její jednotlivé části samostatně, je Objednatel oprávněn vyúčtovat Dodavateli smluvní pokutu ve výši 0,1 % z ceny za plnění uvedené ve Smlouvě (bez DPH), a to za každý i jen započatý kalendářní den prodlení a Dodavatel je povinen tuto smluvní pokutu zaplatit.
6. V případě prodlení Objednatele s úhradou řádně a oprávněně vystavené faktury je Dodavatel oprávněn vyúčtovat Objednateli úrok z prodlení ve výši 0,02 % z nezaplacené částky předmětné faktury za každý kalendářní den prodlení a Objednatel je povinen tuto sankci uhradit.
7. Sjednáním smluvní pokuty ani jejím zaplacením není dotčeno právo oprávněné Smluvní strany na náhradu škody (v souladu s limitací sjednanou v článku IX. odst. 7. Rámcové dohody), vzniklé v důsledku porušení povinnosti, ke kterému se smluvní pokuta vztahuje. Zaplacením smluvní pokuty ani náhrady škody není dotčena povinnost příslušné Smluvní strany splnit své závazky dle této Rámcové dohody a příslušné Smlouvy.

**Článek XIV.**

**Ostatní ujednání**

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Rámcové dohody/Smluv.
2. Objednatel je povinen poskytovat Dodavateli součinnost nezbytnou ke splnění jeho závazků vyplývajících z Rámcové dohody, jakož i Smluv; ustanovení § 2591 občanského zákoníku se pro účely této Rámcové dohody nepoužije.
3. Dodavatel se zavazuje, že na poskytování plnění dle této Smlouvy se budou podílet výhradně členové servisního týmu Dodavatele, jehož jmenné složení je uvedeno v Příloze č. 3 této Rámcové dohody. Dodavatel se zavazuje, že po celou dobu poskytování plnění dle Smlouvy/Smluv uzavřené/uzavřených na základě této Rámcové dohody, bude počet členů servisního týmu minimálně dvě osoby.
4. Služby budou všemi členy servisního týmu poskytovány v českém nebo slovenském jazyce. Jestliže kterýkoli z členů týmu nehovoří českým nebo slovenským jazykem na úrovni potřebné pro řádné poskytování servisních služeb, je Dodavatel povinen ve vztahu k takovému členovi servisního týmu využít služeb tlumočníka/překladatele, přičemž v takovém případě uhradí veškeré náklady spojené s využitím služeb tlumočníka/překladatele Dodavatel.
5. V případě potřeby změnit člena servisního týmu z důvodu na straně Dodavatele je Dodavatel povinen informovat Objednatele nejméně 5 pracovních dnů před plánovanou změnou a požádat Objednatele o písemný souhlas se zařazením nového člena do servisního týmu.
6. V případě potřeby změnit člena servisního týmu z důvodů, které Dodavatel nebyl schopen ani s náležitou péčí předem předvídat a jim zabránit, je Dodavatele povinen informovat Objednatele o nutnosti této změny a požádat jej o písemný souhlas se zařazením nového člena do servisního týmu nejpozději do 5 pracovních dnů od zjištění potřeby změny člena servisního týmu, nedohodnou-li se v konkrétním případě Pověřené osoby obou Smluvních stran písemně jinak.
7. Nový člen servisního týmu musí splňovat zejména veškeré požadavky na kvalifikaci, stanovené pro nahrazovaného člena týmu a tuto kvalifikaci prokázat. Požadavky na kvalifikaci členů týmu jsou uvedeny v Příloze č. 3 této Smlouvy. Zhotovitel je povinen spolu se žádostí o souhlas Objednatele s výměnou člena realizačního týmu, doložit dokumenty v souladu s Přílohou č. 3 této Smlouvy.
8. Smluvní strany se zavazují, že o každé změně Pověřených osob, uvedených v čl. XV. odst. 6. Rámcové dohody nebo jejich kontaktních údajů se budou bez zbytečného odkladu navzájem informovat; uzavření písemného smluvního dodatku není v těchto případech třeba (viz též čl. XV. odst. 5. věta druhá).
9. Tato Rámcová dohoda může být ukončena písemnou dohodou Smluvních stran podepsanou oprávněnými zástupci obou Smluvních stran při dodržení pravidel ZZVZ.
10. Každá ze Smluvních stran může od této Rámcové dohody/Smlouvy odstoupit v případech stanovených touto Rámcovou dohodou nebo zákonem, zejména pak dle ustanovení § 1977 a násl. a § 2001 a násl. občanského zákoníku. Účinky odstoupení nastávají dnem doručení oznámení o odstoupení příslušné Smluvní straně.
11. Pro účely odstoupení od Rámcové dohody/Smlouvy se za podstatné porušení smluvních povinností považuje:
12. prodlení Dodavatele s přijetím Smlouvy (viz čl. III. odst. 8. Rámcové dohody) o více než 30 kalendářních dnů;
13. prodlení Dodavatele s dodáním zařízení dle příslušné Smlouvy o více než 30 kalendářních dnů;
14. porušení závazku Dodavatele na dodržení požadovaných vlastností zařízení dle čl. IV. odst. 4. a odst. 9. Rámcové dohody;
15. prokazatelné porušení povinností Dodavatele zajistit ochranu osobních údajů, jejichž správcem či zpracovatelem je VZP ČR, dle čl. X. odst. 1. Rámcové dohody.
16. VZP ČR je oprávněna v případě potřeby vypovědět Rámcovou dohodu / příslušnou Smlouvu. Výpovědní lhůta činí 3 měsíce od data doručení výpovědi Dodavateli do jeho datové schránky.
17. Předčasným ukončením Rámcové dohody ani jejím ukončením v souladu s tímto čl. XIV. Rámcové dohody není dotčena platnost ustanovení, z jejichž povahy vyplývá, že mají být pro Smluvní strany závazná i po skončení Rámcové dohody (tj. zejména ustanovení týkající se záruky a Záruční podpory, odpovědnosti za vady, odpovědnosti za škodu, povinnosti mlčenlivosti, řešení sporů apod.).
18. Ukončení Rámcové dohody nemá vliv na platnost a účinnost Smluv uzavřených v době trvání Rámcové dohody.

**Článek XV.**

**Závěrečná ustanovení**

1. Tato Rámcová dohoda se uzavírá písemně v elektronické podobě. Rámcová dohoda je podepsána elektronickým podpisem dle ZSVD. Smluvní strany se dohodly, že Dodavatel podepíše Rámcovou dohodu uznávaným elektronickým podpisem ve smyslu § 6 odst. 2 ZSVD; VZP ČR Rámcovou dohodu podepíše v souladu s § 5 ZSVD kvalifikovaným elektronickým podpisem. Rámcová dohoda nabývá platnosti dnem jejího podpisu poslední Smluvní stranou a účinnosti dnem jejího uveřejnění prostřednictvím registru smluv v souladu se zákonem o registru smluv.
2. Tato Rámcová dohoda se uzavírá se na dobu určitou v délce trvání 48 měsíců počínaje dnem nabytí její účinnosti. Veřejné zakázky na základě Rámcové dohody mohou být zadávány po celou dobu trvání Rámcové dohody.
3. Nahrazení Dodavatele jiným dodavatelem je možné pouze za podmínek stanovených v § 222 odst. 10 ZZVZ.
4. Smluvní strany se dohodly, že vylučují možnost přijetí návrhu na uzavření Smlouvy dle této Rámcové dohody s dodatkem či jakoukoli jinou odchylkou od textu návrhu Smlouvy.
5. Tato Rámcová dohoda může být měněna a doplňována pouze v souladu se ZZVZ, formou písemných, vzestupně číslovaných smluvních dodatků, podepsaných oprávněnými zástupci obou Smluvních stran. Uzavření písemného smluvního dodatku není třeba pouze v případech výslovně stanovených touto Rámcovou dohodou.
6. Osobami pověřenými k jednání ve věcech plnění závazků Smluvních stran dle této Rámcové dohody a Smluv (dále jen „**Pověřené osoby**“) jsou:

Za Objednatele:

|  |  |
| --- | --- |
| Jméno a příjmení: | XXXXXXXXXXX |
| E-mail: | XXXXXXXXXXX |
| Mobilní telefon: | XXXXXXXXXXX |

nebo

|  |  |  |
| --- | --- | --- |
| Jméno a příjmení: | XXXXXXXXXXX |  |
| E-mail: | XXXXXXXXXXX |  |
| Mobilní telefon: | XXXXXXXXXXX |  |

|  |  |  |
| --- | --- | --- |
| Jméno a příjmení: | XXXXXXXXXXX |  |
| E-mail: | XXXXXXXXXXX |  |
| Mobilní telefon: | XXXXXXXXXXX |  |

Za Dodavatele:

|  |  |  |
| --- | --- | --- |
| Jméno a příjmení: | XXXXXXXXXXX |  |
| Funkce: | XXXXXXXXXXX |  |
| E-mail: | XXXXXXXXXXX |  |
| Mobilní telefon: | XXXXXXXXXXX |  |

1. Je-li Pověřených osob určeno více, může každá z nich jednat samostatně, neurčuje-li tato Rámcová dohoda v konkrétním případě jinak. Pověřené osoby nemohou uzavírat Smlouvu na plnění ani měnit tuto Rámcovou dohodu, nestanoví-li tato Rámcová dohoda v konkrétním případě jinak.
2. Změnu Pověřených osob nebo jejich kontaktních údajů je každá Smluvní strana povinna bez zbytečného odkladu písemně oznámit druhé Smluvní straně, a to:
3. e-mailem zaslaným Pověřenou osobou jedné Smluvní strany Pověřené osobě druhé Smluvní strany, ve kterém bude změna oznámena;

nebo

1. oznámením zaslaným druhé Smluvní straně do její datové schránky.

Dodatek k Rámcové dohodě se v tomto případě neuzavírá; změna Pověřené osoby či jejích kontaktních údajů je účinná okamžikem, kdy je oznámení o změně druhé Smluvní straně řádně doručeno.

1. K uzavírání Smluv jsou vždy oprávněny osoby, jejichž oprávnění zastupovat příslušnou Smluvní stranu je zřejmé z veřejného seznamu.

K uzavírání Smluv jsou dále oprávněni:

Za Objednatele:

|  |  |
| --- | --- |
| Funkce: | *náměstek ředitele VZP ČR pro informatiku* |

Za Dodavatele:

|  |  |
| --- | --- |
| Jméno a příjmení: | Jiří Chovanec |
| Funkce: | člen představenstva |

1. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Rámcové dohody/Smluv nebo v souvislosti s touto Rámcovou dohodou/Smlouvami, včetně sporů o jejich výklad či platnost, a usilovat o jejich vyřešení především smírnou cestou. Nedojde-li k dohodě Smluvních stran smírnou cestou, budou se tyto spory řešit u věcně a místně příslušného soudu v České republice.
2. Pokud některé z ustanovení této Rámcové dohody je nebo se stane neplatným, neúčinným či zdánlivým, neplatnost, neúčinnost či zdánlivost tohoto ustanovení nebude mít za následek neplatnost Rámcové dohody jako celku ani jiných jejích ustanovení, pokud je takovéto ustanovení oddělitelné od zbytku této Rámcové dohody. Smluvní strany se zavazují takovéto neplatné, neúčinné či zdánlivé ustanovení nahradit novým platným a účinným ustanovením, které svým obsahem bude co nejvěrněji odpovídat podstatě a smyslu původního ustanovení.
3. Tato Rámcová dohoda jakož i Smlouvy a vztahy z nich vyplývající se řídí právním řádem České republiky.
4. Nedílnou součástí této Rámcové dohody jsou následující přílohy:

* Příloha č. 1 – „Technická specifikace“.
* Příloha č. 2 – „Specifikace ceny plnění“.
* Příloha č. 3 – „Jmenný seznam členů servisního týmu Dodavatele“.
* Příloha č. 4 - „Podmínky pro přístup Dodavatele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR“

1. Pro případ kontradikce se jako závazná použijí prioritně příslušná ustanovení této Rámcové dohody a následně příslušná ustanovení jednotlivých příloh, a to ve výše uvedeném pořadí.
2. Smluvní strany prohlašují, že si před podpisem tuto Rámcovou dohodu včetně jejích příloh řádně přečetly, textu porozuměly a s jejím obsahem souhlasí, což stvrzují svými podpisy.

Ing. Zdeněk Kabátek Jiří Chovanec

ředitel člen představenstva

Všeobecná zdravotní pojišťovna České republiky TOTAL SERVICE a.s.

**Příloha č. 1 – Technická specifikace**

*Ustanovení této přílohy vymezují technické požadavky a podmínky VZP ČR na předmět Rámcové dohody.*

## Obecné požadavky na předmět plnění

Veškeré níže uvedené technické podmínky a požadavky Objednatele na poskytování plnění představují minimální úroveň poskytovaného plnění, která musí být Dodavatelem dodržena a zajištěna po celou dobu trvání Rámcové dohody.

## Požadavky VZP ČR na kompatibilitu prostředí:

Dodaný předmět plnění musí být plně kompatibilní se stávajícím technologickým prostředím, nezpůsobil žádné nároky na dodatečné investice či náklady ze strany Objednatele spojené se zařazením do stávající infrastruktury (jako jsou náklady/investice na monitoring, náklady/investice na úpravy datových center, náklady na úpravy provozovaných aplikací, aj.) a jeho implementace byla provázána na stávající technologie tak, aby mohla být využita co nejefektivněji stávající technologie,

Dodaná řešení byla co možná nejjednotnější a umožňovala co nejjednodušší a nejefektivnější správu s automatizovanými prvky včetně vysoké dostupnosti a bezporuchový provoz v nejvyšší možné míře. Objednatele k tomu vede jeho zájem na ochranu již vynaložených investic, k minimalizaci nákladů na monitoring a k minimalizaci nákladů na přeškolení administrátorů, nákladů na úpravy datových center a nákladů na provozování aplikací.

## Popis stávající sítě VZP ČR

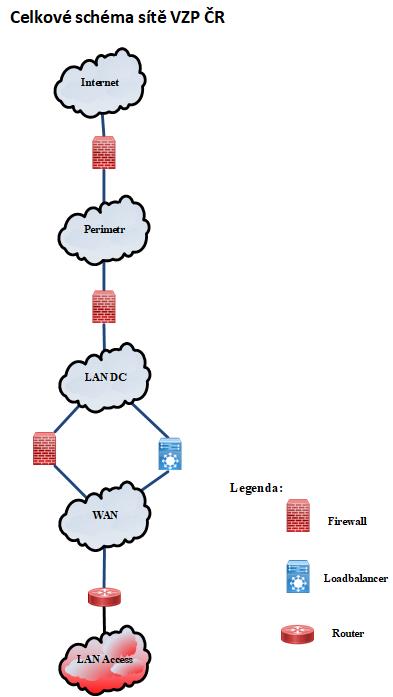
Síť VZP ČR je možné dle funkčnosti rozdělit do několika celků:

1. Připojení do Internetu a perimetr

LAN sítě datových center

1. WAN sítě
2. Přístupová vrstva - LAN sítě ústředí, regionálních poboček a kliprů
3. Řídící kontrolér fabriky

Celkové schéma sítě VZP ČR je zobrazena na následujícím obrázku:



V rámci této veřejné zakázky požaduje VZP ČR zajistit komplexní řešení přístupové vrstvy, tj. LAN sítí ústředí, regionálních poboček a kliprů. Ve výše uvedeném obrázku se jedná o červeně podbarvený blok LAN Access.

* 1. **Připojení do Internetu a perimetr**

Perimetr je zabezpečená oblast podnikové sítě, která zajišťuje přístup uživatelů do Internetu a prezentaci služeb VZP ČR externím uživatelům prostřednictvím Internetu. Zahrnuje další síťové a bezpečnostní složky (hraniční směrovače, firewally, IDS systémy, zařízení VPN, přepínače).

Sítě v perimetru jsou odděleny pomocí bezpečnostních bran (firewallů) do dvou oddělených bezpečnostních zón:

* vnější perimetr – bezpečnostní oddělení externích sítí (Internetu) od sítě VZP ČR
* vnitřní perimetr – bezpečnostní oddělení veřejně vystavených služeb VZP ČR od vnitřní (uživatelské) sítě VZP ČR

Součástí řešení je i VPN přístup do VZP ČR. VPN slouží pro vzdálený přístup zaměstnanců a externích kontraktorů do sítě VZP ČR z Internetu.

* 1. **Sítě datových center**

VZP ČR provozuje dvě geograficky oddělená datová centra:

* DC1 na adrese Orlická 2020/4, 130 00 Praha 3
* DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9

Obě datová centra jsou propojena dvěma nezávislými optickými trasami technologií DWDM s kapacitou optických tras 2x 100 Mb/s pro LAN, 2x 16 Mb/s pro SAN a 2x 10Mb/s pro perimetr.

Síťová infrastruktura datových center je postavena na technologii Cisco ACI (Application Centric Infrastructure) a je znázorněna na následujícím obrázku:



ACI infrastruktura je rozdělená na POD1 (DC2) a POD2 (DC1). Pody jsou vzájemně propojeny přes nezávislou IPN (Inter-Pod Network). IPN používá pro vzájemné propojení mezi lokalitami DWDM.

Součástí DC jsou i čtyři hraniční L3 přepínače Cisco Nexus 7706. Ty zajišťují propojení a logicky odděluji ostatní části sítě VZP:

Každé z datových center VZP ČR je vytvořeno dle architektury Spine and Leave a je možné zařadit ho mezi tzv. aplikačně řízené infrastruktury (Application Centric Infrastructure ACI), které umožňují integrovat do řízení síťového provozu datového centra vlastní logiku jednotlivých aplikací z pohledu jejich požadavků na síťovou konektivitu, bezpečnost a L4-L7 služby (load balancing, firewalling atd.). Aplikační požadavky na konektivitu, bezpečnost a L4-L7 služby jsou definovány prostřednictvím aplikačních politik (Application Policy), které formou logického modelu popisují jak jednotlivé aplikace, resp. jak aplikační vrstvy mají komunikovat navzájem nebo s okolním prostředím (WAN síť, Internet…). Fyzické nebo virtuální aplikační servery sdílející stejnou bezpečnostní a síťovou politiku jsou konsolidovány do logických skupin (EPG = End Point Group) a současně je definována jejich vzájemná komunikace (která aplikační komunikace je povolená, jaké vyžaduje QoS parametry a jaké vyžaduje L4-L7 služby).

K datu zveřejnění VZ byly provedeny plné integrace systému ACI s:

* Cisco firewally ASA 5585-X
* VMWare ESX vSphere 6.7, vCenter Server Appliance 6.7
  1. **WAN sítě**

VZP ČR provozuje privátní datovou síť WAN na přenosových prostředcích dodavatele datového připojení pomocí technologie MPLS. Pro zajištění bezpečnosti přenášených dat je použito šifrování na síťové vrstvě mezi koncovými zařízeními ve správě VZP ČR pomocí protokolu IPSec.

Šifrování se provádí na regionálních pobočkách na směrovačích Cisco C4551, na klientských pracovištích KLIPR1 na směrovačích Cisco C4551 a C4331, na klientských pracovištích KLIPR2 na směrovačích Cisco C1111. V datových centrech se pro vystavení tunelů (šifrování) používají směrovače Cisco řady ASR1002-X.

Pobočkové routery tvoří spolu s centrálními routery nedílnou součást jednotného řešení technologie Cisco SD-WAN, pro kterou jsou veškeré routery licenčně pokryté.

Cisco SD-WAN je nasazena v on-prem řešení, kontroléry jsou umístěné v datových centrech VZP ČR v prostředí VMWare. Základní design je navrhnutý na využití dvou přenosových infrastruktur WAN sítě – MPLS a Internetu. Dále SD-WAN využívá Certifikační autoritu VZP ČR.

SD-WAN odděluje kontrolní a management vrstvu WAN sítě, které v tradičních WAN sítích jsou společně s datovou vrstvou sloučené ve směrovačích na pobočkách / datových centrech.

SD-WAN kontrolní a management vrstvu centralizuje do kontrolérů v datových centrech, pobočkové / datacentrové směrovače zajištují pouze datovou vrstvu a jsou centrálně řízeny kontroléry.

SD-WAN se skládá z následujících částí:

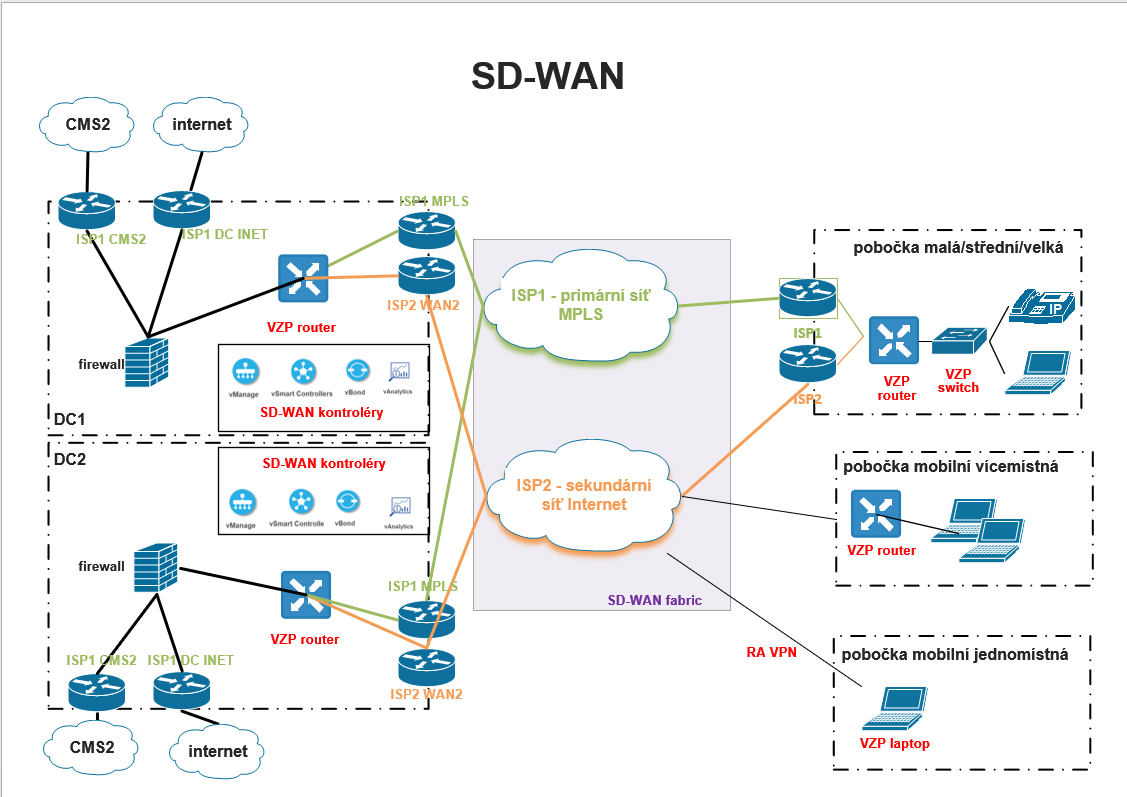
**vManage** NMS (network management systém) je kontrolér zajištující management vrstvu – centrální správu, nastavení, monitoring a analýzu SD-WAN sítě.

**vBond** je kontrolér zajištující orchestrační vrstvu (orchestraci konektivity), každá komponenta SD-WAN (kontrolér i router) se musí před připojením do overlay sítě registrovat a ověřit. Dále vBond slouží i jako NAT-traversal orchestrátor.

**vSmart** je kontrolér zajištující kontrolní vrstvu. Na úrovni síťových a bezpečnostních politik. Je to centrální mozek celého SD-WAN řešení.

Jednotlivé routery nemají v paměti celé routovací tabulky a nepřepočítávají routing – pracují s next-hop jednotlivých transportních sítí.

**vEdge** / WAN edge zařízení / router – jsou fyzická nebo virtuální zařízení (routery) na pobočkách / v datových centrech / v cloudu. Zajištují datovou vrstvu – transmisi jednotlivých datových packetů.



* 1. **Přístupová vrstva - LAN sítě ústředí, regionálních poboček a kliprů**

VZP ČR má lokalit rozděleny dle počtu uživatelů na:

* Ústředí – centrální pobočka s L3 přepínači řady Cisco Catalyst 6500 ve VSS, přístupovými přepínači Cisco Catalyst 4500.
* Regionální pobočky (RP) se středně velkou LAN nad 100 uživatelů s L3/L2 přepínači Cisco Catalyst 4500.
* Klientská pracoviště (KLIPR1) se středně velkou LAN do 100 uživatelů s L3/L2 přepínači řady Cisco Catalyst 4500 nebo Cisco Catalyst C3650. K L3 switchi jsou dále připojeny přístupové switche Cisco 2960X.
* klientská pracoviště (KLIPR1) do 25 uživatelů s L3/L2 přepínači řady Cisco Catalyst C3650. K L3 switchi jsou dále připojeny přístupové switche Cisco 2960X.
* klientská pracoviště (KLIPR2) do 5 uživatelů s routerem Cisco C1111. V ojedinělých případech je doplněn přepínač Cisco 2960X.

Správa síťových prvků, tj. směrovačů a přepínačů se provádí prostřednictvím Cisco PRIME Infrastructure a Cisco DNA centrum. Řízení přístupu do sítě je realizováno pomocí Cisco ISE. VZP ČR požaduje, aby nově dodávaná zařízení byla spravovatelná (administrovatelná) těmito systémy.

* + 1. **LAN Ústředí**

Pro zajištění vysoké dostupnosti jsou použity dva L3 přepínače Catalyst C6509 zapojené do VSS, které slouží k ukončení L2 provozu a zároveň zde jsou připojeny přístupové přepínače. Pro přístup koncových uživatelů do sítě se používají přepínače C3560 ve vertikálním zapojení (rozdělení sítě do pater budovy) a C2960 v horizontálním zapojení (zapojení patra). Přepínač C3560 umožňuje napájení IP telefonů pomocí Ethernetu a pomocí vhodného SFP modulu budou redundantně připojeny k centrálním přepínačům. Přepínač C2960 slouží k připojení serverů nebo zařízení bez nutnosti PoE napájení. Počet přístupových přepínačů je dán konkrétními požadavky (počet pater, počet uživatelů, počet IP telefonů…). Za účelem připojení datového centra (ACI) jsou mezi router ASR1002-X a přepínače C6509 vloženy přepínače Nexus 7706.

* + 1. **LAN regionálních poboček**

Pro připojení uživatelů a zařízení do sítě VZP ČR jsou použity buď modulární přepínače řady Cisco C4500 nebo přepínače Cisco C3560. Pro zvýšení počtu přístupových portů jsou použity i přepínače Cisco C2960. Počet přepínačů je dán konkrétními požadavky jednotlivých poboček (počet pater, počet uživatelů, počet IP telefonů,…).

* + 1. **LAN poboček KLIPR1**

Pro připojení koncových uživatelů do sítě se používají přepínače Cisco C3560 a C2960. Dle velikosti pobočky je tato vybavena jedním nebo dvěma přepínači C3560, na nichž se provádí inter VLAN routing. Z důvodu navýšení přístupových portů jsou některé pobočky vybaveny i přepínači Cisco C2960. Počet těchto přepínačů je dán konkrétními požadavky jednotlivých poboček (počet pater, počet uživatelů, počet IP telefonů, …).

* + 1. **LAN poboček KLIPR2**

Pobočky KLIPR2 jsou vybaveny routerem Cisco C1111. Na tomto routeru se šifruje odchozí provoz a dešifruje příchozí provoz, podle důležitosti a priorit se zde značkuje provoz do tříd. Pro přístup koncových uživatelů do sítě se použije vestavěný 8-portový přepínač se čtyřmi porty s možností napájení PoE.

Pobočky typu KLIPR2, kde pro připojení zařízení nedostačuje vestavný 8 portový switch, jsou navíc vybaveny 24 portovými switchi Cisco C2960X-24PD-L, případně 48 portovými switchi Cisco C2960X-48PD-L.

* + 1. **Významné pobočky v Praze**

Na území hlavního města Prahy se nacházejí tři pobočky, které jsou významné buď svojí velikostí nebo funkcí. Jedná se o pobočky:

* Regionální pobočka Praha, Na Perštýně 6
* Pobočka Crystal, Vinohradská 178
* Call Centrum, Kutvirtova 339/5

Pobočky RP Praha a Crystal jsou připojeny jedním optickým vláknem do datového centra DC2, pobočka Kutvirtova je připojena dvěma optickými vlákny, do každého datového centra po jednom. Optické vlákno je nenasvícené a je v každé lokalitě ukončeno v centrálním přepínači. U RP Praha je centrálním přepínačem dvojice přepínačů řady Cisco Catalyst 6509E ve VSS, u poboček Crystal a Kutvirtova se jedná o dvojici přepínačů Cisco C3650 spojených do clusteru.

Pobočky Crystal a RP Praha jsou pro zvýšení počtu portů vybaveny přepínači řady Cisco 4500, C3650 a C2960X

* 1. **Bezdrátová WiFi síť**

VZP ČR provozuje celkem 4 kusy bezdrátových kontrolérů, které slouží pro řízení centrální a pobočkové sítě bezdrátových přístupových bodů (dále AP). Z důvodu vysoké dostupnosti je v každém datovém centru umístěna dvojice kontrolerů (Cisco AIR-CT5520), které jsou zapojeny do HA konfigurace (viz obrázek).



VZP ČR provozuje následující přístupové body (AP):

|  |  |  |
| --- | --- | --- |
| **Produktové číslo** | **Druh zařízení** | **Počet** |
| AIR-CAP2602I-E-K9 | Access Point | 42 |
| AIR-CAP2702I-E-K9 | Access Point | 123 |
| AIR-CAP3502I-E-K9 | Access Point | 2 |
| AIR-CAP3602I-E-K9 | Access Point | 5 |
| ISR-AP1100AC-E | ISR1111 | 110 |

Síť ve VZP ČR využívá konfiguraci infrastruktury v několika variantách:

* WLAN\_DATA – síť určená pro standardní uživatele interní sítě VZP ČR, je veřejně inzerovaná;
* WLAN\_ADMIN – síť určená pouze pro administrátory sítě. Síť není veřejně inzerovaná (má vypnuto vysílání SSID), aby bylo znemožněno jeho odposlechnutí;
* WLAN\_TECH – síť určená pro IoT
* WLAN\_GUEST – síť určená pro připojení externích uživatelů s přístupem pouze na Internet. Tato síť je veřejně inzerovaná;

Přístup do sítí WLAN\_DATA a WLAN\_ADMIN je ověřován pomocí strojového (WLAN\_DATA) resp. uživatelského (WLAN\_ADMIN) certifikátu.

Autentizace probíhá pomocí EAP (Extensible Authentication Protocol), a to konkrétně EAP – TLS

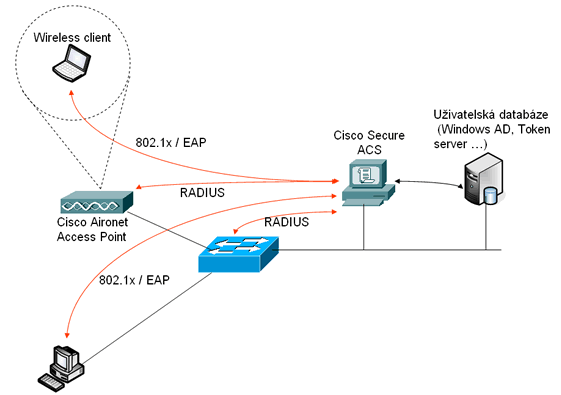
* EAP - Transport Layer Security - používá certifikáty pro autentizaci obou stran, vyžaduje RADIUS nebo jiný autentizací server, je velmi bezpečný, ale vyžaduje certifikát na straně klienta.

Zabezpečení je zajištěno protokolem IEEE 802.1x na druhé vrstvě, kde ověřování identity ve WLAN provádí přístupový bod pro klienty na základě jejich výzvy pomocí seznamu nebo externího autentizačního systému (serveru Cisco ACS – Cisco Access Control System). Tento systém se může ještě dotázat na ověření Microsoft AD. Pouze ověřený uživatel má možnost přístupu k bezdrátové síti.

Připojení k bezdrátové síti WLAN\_TECH je uskutečněné protokolem WPA2 a zabezpečené heslem o délce 20 znaků, které bude neměnné a bude stejné na všech lokalitách.

Komunikace mezi AP a mobilním platebním terminálem (PT) je šifrována pomocí protokolu WPA2 a AES algoritmu.

Ověření PT je zajištěno pomocí autentizace MAC adres připojovaných zařízení proti databázi MAC adres uložených na autentizačním serveru RADIUS. Pouze PT, které má odpovídající MAC adresu má oprávnění přístupu do sítě VZP ČR.



Přístup hostů nebo kontraktorů je zajištěn pomocí WLAN\_GUEST. K autentizaci přístupu do sítě WLAN\_GUEST se používá webová autentizace, kdy se klient po připojení se do sítě má k dispozici pouze protokol DHCP a veškerý webový provoz je přesměrovaný na https přihlašovací portál vytvořený pomocí Cisco ISE (ostatní provoz je zakázán). Klient zadáním svých přihlašovacích údajů, které získá od operátorů přístupu (tzv. Lobby operátorů), se autentizuje a tím se autentizuje i jeho session a veškerý povolený provoz přes firewall do internetu je povolen. V rámci tohoto způsobu přístupu je povolen pouze WWW provoz pomocí protokolu HTTP do Internetu. WLAN\_GUEST je ukončena v centrálním perimetru, kde jsou za tímto účelem umístěné AIR-CT-5580 (v každém perimetru po jednom kuse). Datový provoz je dále směrován do VLAN Guest\_VLAN. Guest\_VLAN je neroutovaná a je L3 ukončená na FW v DMZ perimetru.

* 1. **Řízení přístupu do sítě VZP ČR**

Pro správu a řízení přístupu do sítě používá VZP ČR řešení od firmy Cisco - Identity Services Engine (ISE).

Pro přístupy na administrativní rozhraní prvků síťové infrastruktury VZP ČR používá autentizaci pomocí protokolu TACACS+.

Pro přístupy uživatelů a zařízení do sítě zadavatele je použit standard IEEE 802.1x, který je určen pro řízení přístupu k síti.

Zabezpečení přístupu koncových zařízení (KZ) do LAN je zajištěno:

* Protokolem IEEE 802.1x pro koncová zařízení typu PC nebo notebook zařazená do MS domény na základě ověření platnosti certifikátu v Active Directory autentizačním serverem (Cisco ISE). Certifikát byl přidělen při zařazení PC nebo notebooku do MS domény VZP ČR (Machine Cerificate). Cisco ISE server následně zkontroluje ověřovací atributy oproti Microsoft AD doméně, aby zjistil, zda daný certifikát odpovídá doménovému počítači. V případě úspěšného ověření je počítači umožněn přístup do sítě a port na LAN prvku je zařazen do VLANy na základě autorizačních atributů. Po ověření certifikátu, které provádí přístupový přepínač pomocí protokolu RADIUS, je port přístupového přepínače zařazen do VLAN umožňující přístup do sítě VZP ČR. Pro neautentizovaná PC nebo notebooky, tj. při neúspěšném ověření certifikátu je port přístupového přepínače zařazen do VLAN\_ GUEST (210).
* MAC adresou pro KZ, která neumožňují autentifikaci protokolem IEEE 802.1x dle bodu a), tj. většinou tiskárny, scannery, technologická zařízení apod. KZ je ověřeno oproti databázi MAC adres, která je spravována na autentizačním serveru (Cisco ISE).
* Servery a jejich management porty jsou zařazovány do vyhrazených VLAN a jsou jim přidělovány fixní IP adresy. Servery musí být umístěny v zabezpečených prostorách.
* Pro administrátorský přístup jsou vytvořeny specializované VLAN, administrátorský přístup je umožněn na základě osobního certifikátu administrátora.
* Z internetu je do vymezených částí sítě VZP ČR umožněn VPN přístup na základě ověření platnosti osobního certifikátu vydaného interní CA VZP. Část sítě, kam je pracovníkovi přístup povolen, je dána jeho oprávněními.

Celkový počet současných požadavků na autentizaci se pohybuje kolem 10 000 klientů.

V současnosti provozuje VZP ČR celkem 2 kusy ISE serverů v datových centrech, které slouží pro autentizaci a autorizaci přístupů do sítě VZP ČR.

**VZP ČR požaduje, aby nově dodávaná zařízení byla plně kompatibilní s provozovaným systémem Cisco ISE.**

* 1. **Software a licence pro správu sítě.**

Za účelem dosažení vysokého stupně automatizace a rychlé odezvy na vzniklé problémy používá VZP ČR pro administraci, dohled a řešení problémů celou řadu nástrojů. Přehled těchto SW je uveden v následující tabulce:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Výrobce** | **Zkratka** | **Produkt** | **Verze** | **Použití** |
| Cisco | ACI | Application Policy Infrastructure Controller | 4.2(4i) | Správa SW řízených datových center |
| Infoblox | DDI | Grid manager | 8.4.3-383835 | Správa DHCP, DNS, IP address |
| Cisco | ISE | Identity Services Engine | 2.7.0.356 | Správa identit pro řízení přístupu do sítě VZP ČR |
| Cisco | Prime | Cisco Prime Infrastructure | 3.9 | Správa přepínačů, směrovačů a přístupových bodů |
| Cisco | DNA | DNA Center | 2.1.2.5 | Správa SW řízené přístupové vrstvy |
| Cisco | SD-WAN | vManage | 20.4.1 | Správa SD-WAN |
| Cisco | CUCM | Unified Communications Manager | 10.5.2.12900-14 | Správa IP telefonie |

**VZP ČR požaduje, aby nově dodávaná zařízení byla kompatibilní a podporovaná těmito SW nástroji.**

Správa síťových prvků, tj. směrovačů a přepínačů se provádí prostřednictvím Cisco PRIME Infrastructure a Cisco DNA centrum. DNA Centrum má zadavatel nasazeno v HA režimu na 3 HW appliancích v dostatečné kapacitě pro řízení softwarově definované přístupové vrstvy sítě VZP ČR.

**VZP ČR** provozuje systém DNS, DHCP a správy IP adresního prostoru (DDI) od firmy Infoblox.

**VZP ČR** je vlastníkem celé řady licencí od firmy Cisco. Přehled těchto licencí, které mají vztah k přístupové vrstvě sítě VZP ČR, je uveden v následující tabulce:

|  |  |  |
| --- | --- | --- |
| **Název licence** | **Zkratka** | **Počet ks.** |
| 16 port 1/10G FEX License for ACI | ACI | 14 |
| ACI Base License for 10/25/40+G leaf | ACI | 9 |
| ACI Essential License for 10+G Leaf | ACI | 24 |
| ACI Essential License for 1G Leaf | ACI | 10 |
| Aironet DNA Advantage Term Licenses | DNA | 308 |
| C2960X-48P DNA Essentials | DNA | 10 |
| C3650-DNA-E-24 | DNA | 12 |
| C3650-DNA-E-48 | DNA | 74 |
| C4500E DNA Essential License | DNA | 22 |
| DNA Advantage For SDWAN | DNA | 194 |
| ISE Apex Session Licenses | ISE | 3 500 |
| ISE Base Session Licenses | ISE | 17 175 |
| ISE Plus License | ISE | 8 000 |
| Maximum number of nodes entitled to TACACS+ transactions | ISE | 100 |
| Prime Infrastructure 3.x Assurance Lic. | PRIME | 635 |
| Prime Infrastructure 3.x BASE Lic. | PRIME | 1 |
| Prime Infrastructure 3.x Lifecycle Lic. | PRIME | 2 135 |
| ASR1000-HX Built-In 10GE 2-port License | SD-WAN | 4 |
| Cisco 1100 Series with 8 LAN Ports AppX License | SD-WAN | 206 |
| Cisco 1100 Series with 8 LAN Ports Security License | SD-WAN | 206 |
| ISR\_4331\_Application | SD-WAN | 88 |
| ISR\_4331\_Security | SD-WAN | 88 |
| ISR\_4400\_Application | SD-WAN | 84 |
| ISR\_4400\_Hsec | SD-WAN | 84 |
| ISR\_4400\_Security | SD-WAN | 84 |
| AP Perpetual Networkstack Advantage | WiFi | 300 |
| WLC 5520 or WLC 8540 or WLC 3504 Access Point License | WiFi | 308 |
| C3650\_24\_Ipbase |  | 8 |
| C3650\_48\_Ipbase |  | 17 |
| Cisco AnyConnect Apex License |  | 1 000 |
| LAN license for Nexus 9300-XF |  | 8 |
| NetworkServices\_Nexus9300\_XF |  | 8 |
| SDWAN Umbrella Provision Cloud Advantage |  | 2 |

**Z důvodu minimalizace nákladů na tvorbu SW řízené přístupové vrstvy sítě požaduje VZP ČR v maximální míře využít již nakoupené licence.**

* 1. **Požadavky na integraci.**

**VZP ČR** požaduje integraci SW řízené přístupové vrstvy s následujícími systémy pro správu sítě:

* ISE, Cisco Identity Services Engine.
* ACI, integrace na úrovni centrálního kontrolérů Application Policy Infrastructure Controller.
* SD-WAN, integrace na úrovni centrálního management SW vManage.
* DDI, integrace na úrovni Infoblox Grid manager.

Integrace SW řízené přístupové vrstvy se systémy ACI a SD-WAN musí zajistit, že skupiny uživatelů/zařízení klasifikované v SW řízené přístupové vrstvě se objeví jako EPG (End Point Group) v ACI a naopak politiky definované v ACI budou uplatněny v SW řízené přístupové vrstvě.

**Z důvodu ochrany vynaložených investic VZP ČR požaduje, aby přístupová vrstva sítě VZP ČR byla spravována již nakoupeným a používaným Cisco DNA centrem (Řídící kontrolér fabriky).**

* 1. **Řídící kontrolér fabriky**

VZP ČR požaduje, aby všechna zařízení vyjmenovaná v čl IV., odst. 1., písm „a“ až „e“ této Rámcové dohody, dodávaná v rámci plnění, byla plně kompatibilní a v maximální míře využívala všechny funkční a technické vlastnosti řídícího kontroléru fabriky, a to včetně již existujících licencí. Současný řídící kontrolér fabirky Cisco DNA Centrum, které VZP ČR vlastní a plně využívá, poskytuje zejména následující funkce:

|  |
| --- |
| **Popis parametru** |
| **Funkce kontroléru softwarově definované sítě** |
| Zařízení funguje jako kontroléry softwarově definované sítě k automatizaci vytváření drátové  a bezdrátové síťové fabriky. |
| Kontrolér zajišťuje i monitoring fabriky a jejich zařízení. |
| Kontrolér navádí správce doporučeným postupem při odstraňování problémů infrastruktury fabriky  i připojovaných koncových zařízení a uživatelů. |
| Pro vývoj relevantních nadstavbových aplikací a pro integraci do IT prostředí poskytuje kontrolér otevřená a dokumentovaná aplikační rozhraní (API). |
| Kontrolér umožňuje integraci se systémy používanými již ve VZP ČR   * Cisco ACI * IPAM od firmy Infoblox. * Cisco ISE * Cisco SD-WAN |
| Kontrolér není v cestě datového toku. To znamená, že veškerý datový provoz koncových bodů neprochází kontrolérem pro jakoukoli komunikaci s jinými koncovými body fabriky ani s koncovými body v externích sítích. |
| Kontrolér softwarově definované fabriky umožňuje vizualizovat komunikační vztahy mezi skupinami (reprezentovanými skupinovými značkami) navzájem komunikujícími v rámci fabriky. |
| Kontrolér zobrazuje používané komunikační protokoly a porty pro komunikaci mezi skupinami v rámci fabriky, aby bylo možné optimalizovat politiku pro podrobnější segmentaci sítě. |
| Centralizovaný síťový kontrolér a management systém pro drátovou a bezdrátovou (LAN i WLAN) infrastrukturu. |
| Kontrolér podporuje integraci s dalšími bezpečnostními zařízeními prostřednictvím Platform Exchange GRID (pxGrid), který využívá mnoho dodavatelů zabezpečení, jako jsou Checkpoint, LogRhythm, Splunk, Huntsman, Infoblox, Ping Identity, Cisco ISE a mnoho dalších. |
| Kontrolér poskytuje podrobný soupis a inventář zařízení uspořádaný podle typu zařízení, jména,  IP adresy, MAC adresy, firmware, sériového čísla a konfigurace. Tento inventář je možno automaticky aktualizovat minimálně po každých 30 minutách. |
| Kontrolér má integrovaný modul síťové analýzy a také funkce kognitivní analýzy prostřednictvím Machine Learning pro řešení problémů se sítí. |
| Kontrolér poskytuje webové rozhraní pro jednotnou správu drátové a bezdrátové sítě poskytující integrovaný pohled na drátovou i bezdrátovou síť. Poskytuje správci rychlý a snadný pohled na stav sítě, umožňující snadnou identifikaci výpadků, izolaci problémů v síti a obsahující doporučení pro identifikaci nápravy hlavních příčin. |
| Kontrolér umožňuje jednoduchou a centralizovanou definici síťových a bezpečnostních politik. |
| Automatizace poskytovaná platformou je založená na politikách. Zjednodušuje a abstrahuje od složitosti správy sítě při nasazování a vynucování politiky v celé síti. |
| Kontrolér poskytuje grafické zobrazení topologie sítě s možností vyhledávání a exportu, vytvoření mapy fyzické topologie sítě lokality na základě rolí jednotlivých síťových prvků softwarově definované sítě. Možnost umístění lokality do mapy na základě adresy lokality nebo GPS souřadnice. Možnost organizovat síťovou hierarchii organizace do oblastí, budov a pater. |
| Kontrolér umožňuje nahrání uložené mapy se síťovou hierarchií z Prime Infrastructure. |
| Kontrolér poskytuje mapy síly signálu bezdrátové sítě včetně „heatmap“ síly signálu a jeho kvality. |
| Kontrolér umožňuje lokalizování polohy klientů po integraci s volitelným lokalizačním serverem. |
| Kontrolér poskytuje centrální správu bezdrátových sítí (SSID) pro jednotlivé lokality. |
| Kontrolér umožňuje automatizaci nastavení standardních síťových služeb (DNS, DHCP, AAA, přístupová oprávnění, monitoring) pro síťová zařízení podle lokality. |
| Kontrolér podporuje automatické zprovoznění nových zařízení – jejich nalezení, zajištění bezpečné komunikace s kontrolérem, zavedení do inventáře a pod správu, konfigurace s využitím základní konfigurační šablony. |
| Kontrolér podporuje centralizovanou správu standardních konfigurací s využitím konfiguračních šablon. |
| Kontrolér umožňuje automatizaci provozních změn – modifikaci chování síťového zařízení aplikací konfigurační šablony. |
| Přístup ke kontrolérům je na základě rolí (pouze čtení, povolené změny a administrátor). |
| Kontrolér poskytuje informace o provedených změnách (kdo, co, kdy) – auditní logy. |
| Kontrolér podporuje následující standardní protokoly, které umožňují komunikovat se síťovými zařízeními: NETCONF, SSH, SNMP, HTTP(S) |
| Kontrolér podporuje autentizaci pomocí TACACS a RADIUS. |
| Kontrolér poskytuje otevřená rozhraní API pro vytváření inteligentní, otevřené a programovatelné sítě/fabriky pro konfiguraci pokročilých automatizačních služeb. |
| Kontrolér poskytuje otevřená rozhraní API pro zasílání událostí z monitoringu |
| Kontrolér podporuje rozhraní API REST (Representational State Transfer). |
| Kontrolér poskytuje multivendor SDK k vytváření balíčků zařízení a přidání podpory pro síťová zařízení třetích stran. |
| Kontrolér podporuje automatické aktualizování software kontroléru z cloudu přes cloud tethering. |
| Kontrolér podporuje automatické aktualizace aplikací kontroléru prostřednictvím cloudového tetheringu. |
| Kontrolér podporuje režim redundance N + 1 s plnou perzistencí dat pro vysokou dostupnost. |
| Kontrolér poskytuje podporu stávajících provozovaných přepínačů Objednatele, viz. Popis aktuálního stavu. |
| Kontrolér poskytuje podporu stávajících provozovaných směrovačů v tradičnim i SD-WAN režimu. |
| Kontrolér podporuje správu obrazů softwaru aktivních prvků, udržuje centrální úložiště obrazů softwaru a softwarových oprav (patch) a umožňuje aplikovat je jednotlivě i najednou na více zařízení ve fabrice (například ve stohu) i mimo fabriku. |
| Kontrolér softwarově definované sítě umožňuje definovat softwarovou politiku, jaký konkrétní obraz softwaru aktivního prvku je v síti a/nebo v lokalitě standardem pro rodinu zařízení a / nebo roli zařízení (přístup, distribuce, jádro). |
| Kontrolér umožňuje operátorovi jednoduchou identifikaci aktivních prvků, které vyžadují změnu obrazu software z důvodu změny v softwarové politice nebo protože stávající obraz aktivního prvku není v souladu se platnou politikou. |
| Funkce správy obrazu softwaru podporuje provádění předběžných kontrol inventáře zařízení ohledně dostupnosti doporučeného prostoru ve flash paměti. Po nasazení (aktualizaci softwarového obrazu) musí zkontrolovat úspěšnou aktivaci nainstalovaného obrazu. |
| Kontrolér podporuje HTTPS, SFTP a SCP pro distribuci softwarových obrazů. |
| Kontrolér podporuje plánování distribuce a aktivace obrazů softwaru na jednotlivá síťová zařízení ve fabrice i mimo fabriku. Distribuci a aktivaci umožňuje provést v rozdílný čas. |
| Kontrolér je schopen indikovat, že software provozovaný na síťovém zařízení je zasažen bezpečnostní zranitelností a umožňuje tento incident řešit. |
| Kontrolér podporuje sladění charakteristik softwarového obrazu se softwarovou politikou u nově zprovozňovaných zařízení. |
| **Funkce kontroléru - Monitoring a analýza stavu sítě, řešení výpadků a potíží se sítí** |
| Zobrazení informace o monitorované síti / vybrané části sítě |
| Zobrazení informace o monitorovaných aktivních prvcích |
| Zobrazení informace o připojených drátových a bezdrátových koncových stanicích a uživatelích |
| Zobrazení informace o využívaných aplikacích |
| Zobrazení informace o aplikacích používaných drátovými i bezdrátovými klienty |
| Zobrazení informace o využití napájení v rámci sítě (PoE) |
| Detekce problémů s klientem / koncovým bodem |
| Detekce problémů se síťovými zařízeními |
| Uvedení doporučených nápravných kroků pro každý zjištěný výpadek nebo problém |
| Uchování 30 denní provozní historie sítě umožňující analýzu a řešení výpadků a problémů, ke kterým došlo v minulosti, stejnými postupy jako u právě probíhajících výpadků |
| Detailní zobrazení stavu a provozní historie síťového zařízení, souvisejících událostí, problémů a topologie připojení sousedních aktivních prvků v analyzovaném čase |
| Detailní zobrazení stavu a provozní historie klienta / koncového bodu, souvisejících událostí, problémů, detail síťového připojení v analyzovaném čase a přehled využívaných aplikací |
| Umožňuje využití metody strojového učení (Machine Learning) lokálně nebo v cloudu výrobce (Artificial Intelligence) |
| Umožňuje integrované proaktivní testy bezdrátové sítě s využitím bezdrátových senzorů |

## Specifikace předmětu plnění

VZP ČR požaduje v průběhu trvání Rámcové dohody dodat následující zařízení v těchto předpokládaných počtech:

**Předpokládané počty**

|  |  |  |
| --- | --- | --- |
| **Kód** | **Popis** | **Počet** |
| S1 | Fixní přístupový 48 portový přepínač | 92 |
| S2 | Fixní přístupový 48 portový přepínač | 74 |
| S3 | Fixní přístupový 48 portový přepínač | 18 |
| S4 | Fixní přístupový 24 portový přepínač | 18 |
| S5 | Fixní přístupový 24 portový přepínač | 30 |
| S6 | Fixní přístupový 24 portový přepínač | 110 |
| SM1 | Stohovací modul pro fixní přepínače S1 až S6 | 85 |
| RZ1 | Redundantní napájecí zdroj pro přepínače S1 až S6 | 50 |
| RZ2 | Redundantní napájecí zdroj pro přepínače S1 až S6 | 50 |
| S7 | Modulární 7 slotový přepínač | 13 |
| S8 | Modulární 10 slotový přepínač | 2 |
| RŘM | Redundantní řídící modul do modulárního přepínače S7 a S8 | 15 |
| C1 | 48 portová karta do modulárního přepínače S7 a S8 | 15 |
| C2 | 48 portová karta do modulárního přepínače S7 a S8 | 32 |
| C3 | 48 portová karta do modulárního přepínače S7 a S8 | 26 |
| S9 | Fixní agregační 24 portový přepínač | 2 |
| S10 | Fixní agregační 48 portový přepínač | 2 |
| AP1 | Přístupový bod | 300 |
| AP2 | Přístupový bod | 150 |
| R1 | Směrovač datového centra | 4 |

Popis požadovaných parametrů je uveden přehledně v tabulkách v následujících kapitolách.

Parametry uvedené v níže uvedených tabulkách jsou povinné.

## Přehled zařízení

* 1. **Fixní přístupové přepínače** 
     1. **Společné parametry fixních přístupových přepínačů**

Níže uvedené parametry musí splňovat všechny dodávané fixní přístupové přepínače, tj. typ S1 až S6.

|  |  |
| --- | --- |
| **Popis parametru** | **Splněno (ANO)** |
| Typ přepínače: L2/L3 přepínač | **Ano** |
| Formát přepínače: Stohovatelný | **Ano** |
| Možnost rozšíření o stohování (doplňkovým interním HW modulem)   * minimální počet dedikovaných stohovacích portů: 2 * počet zařízení ve stohu minimálně: 8 * minimální kapacita sběrnice stohu: 300 Gb/s | **Ano** |
| Stateful Switch Over v rámci stohu | **Ano** |
| Non-stop Forwarding | **Ano** |
| Možnost instalovat interní redundantní napájecí zdroj | **Ano** |
| Redundantní ventilátory | **Ano** |
| Redundantní ventilátory vyměnitelné za chodu zařízení | **Ano** |
| Velikost MAC address tabulky: 30000 | **Ano** |
| Min. počet IPv4 routes: 32000 | **Ano** |
| Min. počet IPv6 routes: 16000 | **Ano** |
| Min. počet konfigurovatelných security ACL: 5000 | **Ano** |
| Min. velikost sdíleného systémového bufferu: 16MB | **Ano** |
| IEEE 802.3ad (Link Aggregation) | **Ano** |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | **Ano** |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | **Ano** |
| Minimální počet konfigurovatelných Link Aggregation Group trunků: 128 | **Ano** |
| IEEE 802.1Q | **Ano** |
| Minimální počet aktivních VLAN: 1000 | **Ano** |
| IEEE 802.1x | **Ano** |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | **Ano** |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | **Ano** |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | **Ano** |
| RADIUS CoA | **Ano** |
| Podpora instance spanning-tree protokolu per VLAN | **Ano** |
| IEEE 802.1w - Rapid Spanning Tree Protocol | **Ano** |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | **Ano** |
| Podpora jumbo rámců (min. 9198 bytes) | **Ano** |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | **Ano** |
| Směrování protokolů IPv4 a IPv6 v hardware | **Ano** |
| OSPFv2 | **Ano** |
| OSPFv3 | **Ano** |
| ISIS | **Ano** |
| Směrování dle škálovatelné adresace, dle vícero adresních prostorů (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830 nebo funkčně ekvivalentní) | **Ano** |
| BGPv4 | **Ano** |
| VXLAN s BGP EVPN | **Ano** |
| Policy based routing uvnitř VRF | **Ano** |
| Graceful Insertion and Removal | **Ano** |
| IP Multicast (PIM SSM, PIM SM) | **Ano** |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | **Ano** |
| MPLS VPN | **Ano** |
| MPLS VPN přes GRE tunely | **Ano** |
| MPLS VPN - 6VPE | **Ano** |
| VXLAN enkapsulace | **Ano** |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | **Ano** |
| Reverse path check (uRPF) pro IPv4 i IPv6 | **Ano** |
| IGMPv2, IGMPv3 | **Ano** |
| IGMP snooping | **Ano** |
| MLD snooping | **Ano** |
| DHCP relay | **Ano** |
| Minimální počet HW QoS front: 8 | **Ano** |
| QoS classification – ACL, DSCP, CoS based | **Ano** |
| QoS marking - DSCP, CoS | **Ano** |
| QoS - Strict Priority Queue | **Ano** |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | **Ano** |
| QoS Policing | **Ano** |
| QoS-Per Flow policing | **Ano** |
| QoS-Hierarchical QoS: min. 2 úrovně | **Ano** |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | **Ano** |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | **Ano** |
| IPv6 QoS | **Ano** |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | **Ano** |
| IPv6 Port ACL, VLAN ACL | **Ano** |
| Možnost definovat povolené MAC adresy na portu | **Ano** |
| PACL, VACL | **Ano** |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | **Ano** |
| IEEE 802.1ae na uplink portech | **Ano** |
| IEEE 802.1ae (AES-GCM-256) na uplink portech | **Ano** |
| IEEE 802.1ae na všech portech | **Ano** |
| IEEE 802.1ae (AES-GCM-256) na všech portech | **Ano** |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | **Ano** |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | **Ano** |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | **Ano** |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | **Ano** |
| Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní) | **Ano** |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | **Ano** |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | **Ano** |
| SUDI (IEEE 802.1AR) autentizace | **Ano** |
| Schopnost poskytovat PoE napájení připojeným zřízením i během restartu přepínače | **Ano** |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | **Ano** |
| IEEE 802.3az | **Ano** |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | **Ano** |
| Správa prostřednictvím Prime Infrastructure 3.x a DNA Center ve verzi 2.x. | **Ano** |
| Multicast DNS (mDNS) gateway | **Ano** |
| Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) | **Ano** |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | **Ano** |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | **Ano** |
| Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS | **Ano** |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | **Ano** |
| SSHv2 | **Ano** |
| CLI rozhraní | **Ano** |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | **Ano** |
| Python scripting | **Ano** |
| Linux shell | **Ano** |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | **Ano** |
| Application hosting | **Ano** |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | **Ano** |
| Streaming telemetrie prostřednictvím NETCONF/XML | **Ano** |
| SNMPv2/v3 | **Ano** |
| Podpora network boot (iPXE) pres IPv4 i IPv6 | **Ano** |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | **Ano** |
| Vzdálený port mirroring (ERSPAN) | **Ano** |
| NTPv3 server | **Ano** |

* + 1. **Fixní přístupový 48 portový přepínač, typ S1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-48UXG-4X-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S1** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 36 | **Ano** | |
| Minimální počet portů 1/2.5/5/10 Gbase-T s PoE napájením: 12 | **Ano** | |
| Minimální PoE budget: 650W | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at, IEEE 802.3bt | **Ano** | |
| Minimální počet uplink portů: 4x10GE SFP+ | **Ano** | |

* + 1. **Fixní přístupový 48 portový přepínač, typ S2**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-48P-4X-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S2** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 48 | **Ano** | |
| Minimální PoE budget: 500W | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at | **Ano** | |
| Minimální počet uplink portů: 4x10GE SFP+ | **Ano** | |

* + 1. **Fixní přístupový 48 portový přepínač, typ S3**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-48P-4G-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S3** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 48 | **Ano** | |
| Minimální PoE budget: 500W | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at | **Ano** | |
| Minimální počet uplink portů: 4x1GE SFP | **Ano** | |

* + 1. **Fixní přístupový 24 portový přepínač, typ S4**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-24UXG-4X-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S4** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 16 | **Ano** | |
| Minimální počet portů 1/2.5/5/10 Gbase-T s PoE napájením: 8 | **Ano** | |
| Minimální PoE budget: 850W | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at, IEEE 802.3bt | **Ano** | |
| Minimální počet uplink portů: 4x10GE SFP+ | **Ano** | |

* + 1. **Fixní přístupový 24 portový přepínač, typ S5**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-24P-4X-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |
| --- | --- |
| **Popis parametru** | **Splněno (ANO)** |
| **Typ-S5** | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** |
| Maximální velikost zařízení 1RU | **Ano** |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 24 | **Ano** |
| Minimální PoE budget: 500W | **Ano** |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at | **Ano** |
| Minimální počet uplink portů: 4x10GE SFP+ | **Ano** |

* + 1. **Fixní přístupový 24 portový přepínač, typ S6**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-24P-4G-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |
| --- | --- |
| **Popis parametru** | **Splněno (ANO)** |
| **Typ-S6** | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** |
| Maximální velikost zařízení 1RU | **Ano** |
| Minimální počet portů 10/100/1000 Base-TX s PoE napájením: 24 | **Ano** |
| Minimální PoE budget: 500W | **Ano** |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at | **Ano** |
| Minimální počet uplink portů: 4x1GE SFP | **Ano** |

* 1. **Stohovací modul do fixních přepínačů S1 až S6, typ SM1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9300L-STACK-KIT=**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-SM1** | | |
| Stohovací modul plně kompatibilní s přepínači S1 až S6 včetně 0,5m stohovacího kabelu | **Ano** | |

* 1. **Redundantní napájecí zdroj pro přepínače S1 až S6, typ RZ1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**PWR-C1-715WAC-P=**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-RZ1** | | |
| Interní redundantní napájecí zdroj 230V AC do přepínačů S1 až S6, min. 700W, včetně napájecích kabelů | **Ano** | |

* 1. **Redundantní napájecí zdroj pro přepínače S1 až S6, typ RZ2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Základní údaje** | **Nabízená hodnota** | | | |
| Výrobce zařízení | [**Cisco**] | | | |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**PWR-C1-1100WAC-P=**] | | | |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9300-series-switches/nb-06-cat9300-ser-data-sheet-cte-en.html)] | | | |
| **Popis parametru** | | | **Splněno (ANO)** |
| **Typ-RZ2** | | | |
| Interní redundantní napájecí zdroj 230V AC do přepínačů S1 až S6, min. 1000W, včetně napájecích kabelů | | **Ano** | |

* 1. **Modulární přístupové přepínače**
     1. **Společné vlastnosti modulárních přístupových přepínačů**

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Společné vlastnosti** | | |
| Typ přepínače: L2/L3 přepínač | **Ano** | |
| Formát přepínače: modulární | **Ano** | |
| Možnost redundantního řídícího modulu | **Ano** | |
| Výpadek redundantního řídícího modulu nesmí snížit přenosovou kapacitu přepínače | **Ano** | |
| Stateful Switch Over | **Ano** | |
| Non-stop Forwarding mezi řídícími moduly | **Ano** | |
| ISSU | **Ano** | |
| Min. velikost sdíleného systémového bufferu: 96MB | **Ano** | |
| Velikost MAC address tabulky: 60000 | **Ano** | |
| Min. počet IPv4 routes: 128000 | **Ano** | |
| Min. počet IPv6 routes: 50000 | **Ano** | |
| Min. počet konfigurovatelných security ACL záznamů: 16000 | **Ano** | |
| Podpora jumbo rámců (min. 9198 bytes) | **Ano** | |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | **Ano** | |
| IEEE 802.3ad (Link Aggregation) | **Ano** | |
| IEEE 802.3ad přes více karet v šasi | **Ano** | |
| IEEE 802.3ad přes více šasi | **Ano** | |
| Minimálně 8 linek jako součást Link Aggregation Group trunku | **Ano** | |
| Minimální počet konfigurovatelných Link Aggregation Group trunků: 64 | **Ano** | |
| IEEE 802.1Q | **Ano** | |
| Minimální počet VLAN ID: 4000 | **Ano** | |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | **Ano** | |
| Podpora instance spanning-tree protokolu per VLAN | **Ano** | |
| IEEE 802.1w - Rapid Spanning Tree Protocol | **Ano** | |
| Směrování protokolů IPv4 a IPv6 v hardware | **Ano** | |
| OSPFv2 | **Ano** | |
| OSPFv3 | **Ano** | |
| ISIS | **Ano** | |
| Směrování dle škálovatelné adresace (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830 nebo funkčně ekvivalentní) | **Ano** | |
| BGPv4 | **Ano** | |
| VXLAN s BGP EVPN | **Ano** | |
| Policy based routing uvnitř VRF | **Ano** | |
| Graceful Insertion and Removal | **Ano** | |
| IP Multicast (PIM SSM, PIM SM) | **Ano** | |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | **Ano** | |
| MPLS VPN | **Ano** | |
| MPLS VPN přes GRE tunely | **Ano** | |
| MPLS VPN - 6VPE | **Ano** | |
| VXLAN enkapsulace | **Ano** | |
| First Hop Redundancy Protokol (např. VRRP, HSRP) | **Ano** | |
| First Hop Redundancy Protokol pro IPv6 (HSRP nebo VRRP) | **Ano** | |
| Reverse path check (uRPF) pro IPv4 i IPv6 | **Ano** | |
| IGMPv2, IGMPv3 | **Ano** | |
| IGMP snooping | **Ano** | |
| MLD snooping | **Ano** | |
| DHCP relay | **Ano** | |
| Minimální počet HW QoS front: 8 | **Ano** | |
| QoS classification – ACL, DSCP, CoS based | **Ano** | |
| QoS marking - DSCP, CoS | **Ano** | |
| QoS - Strict Priority Queue | **Ano** | |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | **Ano** | |
| QoS Policing | **Ano** | |
| QoS-Per Flow policing | **Ano** | |
| QoS-Hierarchical QoS: ANO, min. 2 úrovně | **Ano** | |
| IPv6 services (Telnet, SSH, Syslog, DHCP) | **Ano** | |
| IPv6 QoS | **Ano** | |
| IPv6 First Hop Security (RA guard, DHCPv6 snooping, IPv6 source guard) | **Ano** | |
| IPv6 Port ACL, VLAN ACL | **Ano** | |
| IEEE 802.1x | **Ano** | |
| Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou, Web autentizací) | **Ano** | |
| Integrace IEEE 802.1x s IP telefonním prostředím (802.1x Multi-domain authentication) | **Ano** | |
| Možnost provozu 802.1x v tzv. audit módu bez omezování přístupu koncových uživatelů | **Ano** | |
| RADIUS CoA | **Ano** | |
| Možnost definovat povolené MAC adresy na portu | **Ano** | |
| PACL, VACL | **Ano** | |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | **Ano** | |
| IEEE 802.1AE na všech portech | **Ano** | |
| IEEE 802.1ae (AES-GCM-256) | **Ano** | |
| Bezpečnostní funkce umožňující ochranu proti podvržení zdrojové MAC a IP adresy | **Ano** | |
| Bezpečnostní funkce umožňující ochranu proti připojení neautorizovaného DHCP serveru | **Ano** | |
| Bezpečnostní funkce umožňující inspekci provozu protokolu ARP | **Ano** | |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | **Ano** | |
| Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní) | **Ano** | |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | **Ano** | |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | **Ano** | |
| SUDI (IEEE 802.1AR) autentizace | **Ano** | |
| IEEE 802.3af | **Ano** | |
| IEEE 802.3at | **Ano** | |
| Inteligentní PoE management - zajištění napájení připojeného zařízení podle konkrétních požadavků daného typu zařízení | **Ano** | |
| IEEE 802.3az | **Ano** | |
| Automatická aplikace specifické konfigurace pro dané zařízení po detekci jeho připojení na portu | **Ano** | |
| Správa prostřednictvím Prime Infrastructure 3.x a DNA Center ve verzi 2.x. | **Ano** | |
| Multicast DNS (mDNS) gateway | **Ano** | |
| Application Visibility - Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) | **Ano** | |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | **Ano** | |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | **Ano** | |
| Application Visibility – Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS | **Ano** | |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | **Ano** | |
| SSHv2 | **Ano** | |
| CLI rozhraní | **Ano** | |
| Vzdálená identifikace komponent zařízení pomocí "Blue Beacon" mechanismu | **Ano** | |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | **Ano** | |
| Python scripting | **Ano** | |
| Linux shell | **Ano** | |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | **Ano** | |
| Application hosting | **Ano** | |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | **Ano** | |
| Streaming telemetrie prostřednictvím NETCONF/XML | **Ano** | |
| SNMPv2/v3 | **Ano** | |
| Podpora network boot (iPXE) | **Ano** | |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | **Ano** | |
| Vzdálený port mirroring (ERSPAN) | **Ano** | |
| NTPv3 server | **Ano** | |

* + 1. **Modulární 7 slotový přepínač, typ S7**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9407R**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S7** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Výška šasi: max. 10RU | **Ano** | |
| Hloubka šasi: max. 43cm | **Ano** | |
| Počet slotů v šasi pro moduly rozhraní: minimálně 5 | **Ano** | |
| Interní redundantní napájecí zdroje v režimu N+1 i N+N | **Ano** | |
| ventilátory vyměnitelné z přední strany šasi | **Ano** | |
| ventilátory vyměnitelné ze zadní strany šasi | **Ano** | |
| Počet a typ uplink slotů z řídícího modulu: 8x10GE+2x40GE | **Ano** | |
| Požadovaná minimální přenosová kapacita slotu: 120 Gbit/s | **Ano** | |

* + 1. **Modulární 10 slotový přepínač, typ S8**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9410R**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S8** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Výška šasi: max. 13RU | **Ano** | |
| Hloubka šasi: max. 43cm | **Ano** | |
| Počet slotů v šasi pro moduly rozhraní: minimálně 8 | **Ano** | |
| Interní redundantní napájecí zdroje v režimu N+1 i N+N | **Ano** | |
| ventilátory vyměnitelné z přední strany šasi | **Ano** | |
| ventilátory vyměnitelné ze zadní strany šasi | **Ano** | |
| Počet a typ uplink slotů z řídícího modulu: 8x10GE+2x40GE | **Ano** | |
| Požadovaná minimální přenosová kapacita slotu: 80 Gbit/s | **Ano** | |

* + 1. **48 portová karta do modulárního přepínače S7 a S8, typ C1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9400-LC-48UX=**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-series-line-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-C1** | | |
| Karta plně kompatibilní s přepínači typu S7 a S8 | **Ano** | |
| Minimálně 24x port IEEE 802.3bz, multigigabit 1/2,5/5/10GBase-T s PoE napájením | **Ano** | |
| Minimálně 24x port 10/100/1000 s PoE napájením | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at, IEEE 802.3bt | **Ano** | |

* + 1. **48 portová karta do modulárního přepínače S7 a S8, typ C2**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9400-LC-48U=**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-series-line-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-C2** | | |
| Karta plně kompatibilní s přepínači typu S7 a S8 | **Ano** | |
| Minimálně 48x port 10/100/1000 s PoE napájením | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at, IEEE 802.3bt | **Ano** | |

* + 1. **48 portová karta do modulárního přepínače S7 a S8, typ C3**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9400-LC-48P**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-series-line-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-C3** | | |
| Karta plně kompatibilní s přepínači typu S7 a S8 | **Ano** | |
| Minimálně 48x port 10/100/1000 s PoE napájením | **Ano** | |
| Všechny PoE porty splňují standardy IEEE 802.3af, IEEE 802.3at | **Ano** | |

* + 1. **Redundantní řídící modul do modulárního přepínače S7 a S8, typ RŘM**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9400-SUP-1XL=**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9400-series-switches/nb-06-cat9400-ser-sup-eng-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-RŘM** | | |
| Redundantní řídící modul plně kompatibilní s přepínači typu S7 a S8 | **Ano** | |
| Minimálně 8x uplink port 10 GE | **Ano** | |
| Minimálně 2x uplink port 40 GE | **Ano** | |

* 1. **Fixní agregační přepínače**
     1. **Společné vlastnosti fixních agregačních přepínačů**

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Společné vlastnosti** | | |
| Typ přepínače: L2/L3 přepínač | **Ano** | |
| Min. velikost sdíleného systémového bufferu: 36MB | **Ano** | |
| Velikost MAC address tabulky: 80000 | **Ano** | |
| Min. počet IPv4 routes: 100000 | **Ano** | |
| Min. počet IPv6 routes: 100000 | **Ano** | |
| Min. počet konfigurovatelných security ACL: 27000 | **Ano** | |
| Flexibilní alokace SRAM a TCAM zdrojů | **Ano** | |
| IEEE 802.3ad (Link Aggregation - LAG) | **Ano** | |
| IEEE 802.3ad přes více přepínačů ve stohu nebo více šasis | **Ano** | |
| ISSU | **Ano** | |
| Minimální počet aktivních VLAN: 4000 | **Ano** | |
| IEEE 802.1w - Rapid Spanning Tree Protocol | **Ano** | |
| Podpora instance spanning-tree protokolu per VLAN | **Ano** | |
| Podpora jumbo rámců (min. 9198 bytes) | **Ano** | |
| Detekce protilehlého zařízení (např. CDP nebo LLDP) | **Ano** | |
| Protokol MVRP nebo VTP pro definici a správu VLAN sítí | **Ano** | |
| OSPFv2, OSPFv3 | **Ano** | |
| ISIS | **Ano** | |
| Směrování dle škálovatelné adresace, dle vícero adresních prostorů (např. Locator/Identifier Separation Protocol (LISP) dle RFC 6830 nebo funkčně ekvivalentní) | **Ano** | |
| BGPv4 | **Ano** | |
| VXLAN s BGP EVPN | **Ano** | |
| Policy based routing uvnitř VRF | **Ano** | |
| Graceful Insertion and Removal | **Ano** | |
| IP Multicast (PIM SSM, PIM SM) | **Ano** | |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | **Ano** | |
| Min. počet oddělených (nezávislých) směrovacích tabulek: 10 | **Ano** | |
| MPLS VPN | **Ano** | |
| MPLS VPN - 6VPE | **Ano** | |
| VXLAN enkapsulace | **Ano** | |
| First Hop Redundancy Protokol (např. VRRP, HSRP) pro IPv4 i IPv6 | **Ano** | |
| Reverse path check (uRPF) | **Ano** | |
| Minimální počet HW QoS front: 8 | **Ano** | |
| QoS - Strict Priority Queue | **Ano** | |
| QoS classification – ACL, DSCP, CoS based | **Ano** | |
| QoS marking - DSCP, CoS | **Ano** | |
| QoS Policing | **Ano** | |
| QoS-Hierarchical QoS | **Ano** | |
| Automatické nastavení QoS parametrů (AutoQoS nebo ekvivalentní) | **Ano** | |
| IPv6 First Hop Security (RA guard, DHCPv6 guard, IPv6 source guard) | **Ano** | |
| Port ACL, VLAN ACL | **Ano** | |
| Paketové filtry (ACL) jsou stále aplikovány a filtrují i v případě, že jsou na nich prováděny změny | **Ano** | |
| Klasifikace bezpečnostní role přistupujícího uživatele nebo koncového zařízení a její propagace sítí (např. Scalable-Group Tag eXchange Protocol dle RFC draft-smith-kandula-sxp-10 nebo funkčně ekvivalentní). | **Ano** | |
| Hardwarová filtrace (access list) podle bezpečnostních rolí uživatelů propagovaných sítí přistupujících k různým skupinám síťových prostředků (např. SGACL, role-based ACL nebo funkčně ekvivalentní) | **Ano** | |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak bootloaderu, tak i samotného operačního systému zařízení prostřednictvím interních HW prostředků - tzv. trusted modulů | **Ano** | |
| HW trusted modul využíván pro bezpečné uložení hesel a šifrovacích klíčů | **Ano** | |
| Podpora SUDI (IEEE 802.1AR) autentizace | **Ano** | |
| IPv6 Port ACL, VLAN ACL | **Ano** | |
| IEEE 802.1AE na všech portech | **Ano** | |
| IEEE 802.1ae (AES-GCM-256) na všech portech | **Ano** | |
| NAT v rámci VRF | **Ano** | |
| IGMPv2/v3 snooping | **Ano** | |
| MLD snooping | **Ano** | |
| Multicast DNS (mDNS) gateway | **Ano** | |
| Application Visibility - Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | **Ano** | |
| Application Visibility - Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, hodnota TTL, ICMP kód, IGMP type | **Ano** | |
| Správa prostřednictvím Prime Infrastructure 3.x a DNA Center ve verzi 2.x. | **Ano** | |
| Export monitorovaných dat ve formátu NetFlow v9 nebo IPFIX | **Ano** | |
| SSHv2 | **Ano** | |
| CLI rozhraní | **Ano** | |
| Vzdálená identifikace zařízení pomocí "Blue Beacon" mechanismu | **Ano** | |
| Model-driven programovatelnost prostřednictvím RESTCONF, NETCONF/YANG | **Ano** | |
| Python scripting | **Ano** | |
| Linux shell | **Ano** | |
| Interpretace uživatelských skriptů a jejich aktivace asynchronní událostí v systému zařízení | **Ano** | |
| Aplikace softwarových záplat, nikoli povyšování celého firmware | **Ano** | |
| Streaming telemetrie prostřednictvím NETCONF/XML | **Ano** | |
| SNMPv2/v3 | **Ano** | |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | **Ano** | |
| Vzdálený port mirroring (ERSPAN) pro IPv4 i IPv6 | **Ano** | |
| NTPv3 server | **Ano** | |

* + 1. **Fixní agregační 24 portový přepínač, typ S9**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9500-24Y4C-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S9** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28: 24 | **Ano** | |
| Uplink porty: 4x100GE QSFP28 | **Ano** | |
| Interní redundantní napájecí zdroj | **Ano** | |

* + 1. **Fixní agregační 48 portový přepínač, typ S10**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [**C9500-48Y4C-A**] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/switches/catalyst-9500-series-switches/nb-06-cat9500-ser-data-sheet-cte-en.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-S10** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60 cm – hloubka rozvaděče 100-115 cm | **Ano** | |
| Maximální velikost zařízení 1RU | **Ano** | |
| Minimální počet neblokovaných portů 1/10/25GE s volitelným fyzickým rozhraním typu SFP28: 48 | **Ano** | |
| Uplink porty: 4x100GE QSFP28 | **Ano** | |
| Interní redundantní napájecí zdroj | **Ano** | |

* 1. **Bezdrátové přístupové body**
     1. **Společné vlastnosti bezdrátových přístupových bodů**

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Společné vlastnosti** | | |
| AP určený pro instalaci na strop/podhled | **Ano** | |
| Typ antén - Integrované pro obě pásma | **Ano** | |
| Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | **Ano** | |
| Minimální počet inzerovaných SSID (BSSID) per radio - 8 | **Ano** | |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11ac/ax klientům (Tx Beam Forming) | **Ano** | |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | **Ano** | |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | **Ano** | |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | **Ano** | |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | **Ano** | |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí SSH | **Ano** | |
| AP uzavřené konstrukce bez větracích otvorů | **Ano** | |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem | **Ano** | |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | **Ano** | |
| Plná podpora AP na stávajících bezdrátových kontrolerech Zadavatele | **Ano** | |
| Správa prostřednictvím Prime Infrastructure 3.x a DNA Center ve verzi 2.x. | **Ano** | |
| Plná podpora AP s bezdrátovým kontrolerem běžícím na všech poptávaných typech přepínačů v režimu softwarově definované fabriky. | **Ano** | |
| Pro připojení AP k bezdrátovým kontrolerům bude využito stávajících AP licencí Zadavatele | **Ano** | |
| AP zalicencováno pro lokalizaci připojených klientů pomocí triangulace síly signálu | **Ano** | |
| AP zalicencováno pro lokalizaci cizích AP a klientů pomocí triangulace síly signálu | **Ano** | |
| AP zalicencováno pro lokalizaci a korelaci zdrojů rušení bezdrátové sítě | **Ano** | |
| AP zalicencováno pro lokalizační metriky/analytika chování připojených klientů | **Ano** | |
| AP zalicencováno pro porovnání metrik chování připojených klientů mezi logicky vytvořenými zónami (lokalita) | **Ano** | |
| AP zalicencováno pro integraci údajů o lokalizaci připojených klientů s DNA Center | **Ano** | |
| AP zalicencováno pro OpenRoaming | **Ano** | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| AP určený pro instalaci na strop/podhled | **Ano** | |
| Typ antén - Integrované pro obě pásma | **Ano** | |
| Podpora standardů 802.11a/b/g/n/ac a Wi-Fi6 (802.11ax) | **Ano** | |
| Minimální počet inzerovaných SSID (BSSID) per radio - 8 | **Ano** | |
| Podpora mechanismu pro optimalizaci fáze vysílaného bezdrátového signálu směrem k 802.11ac/ax klientům (Tx Beam Forming) | **Ano** | |
| Podpora mechanismu pro přepojení klientů z 2,4GHz do 5GHz pásma | **Ano** | |
| Access Pointy obsahují X.509 certifikát s lokální platností pro nasazeni PKI | **Ano** | |
| Podpora autentizace Access Pointu do LAN sítě pomocí 802.1x, AP obsahují 802.1x supplikant | **Ano** | |
| Podpora detekce a monitorování problémů WLAN odchytáváním provozu na AP a jeho zasíláním do Ethernetového analyzátoru (např. Wireshark) | **Ano** | |
| Podpora přímého přístupu na příkazovou řádku AP přes serial konzoli a přes IPv4 pomocí SSH | **Ano** | |
| AP uzavřené konstrukce bez větracích otvorů | **Ano** | |
| AP je fyzicky zabezpečitelné/zamknutelné k okolním pevným částem | **Ano** | |
| Důvěryhodný HW/SW – AP používá bezpečný zavaděč OS, ověřování podpisu OS, kontrolu autentičnosti HW a mechanizmy pro ochranu SW a HW proti útokům | **Ano** | |

* + 1. **Přístupový bod, typ AP1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [C9120AXI-E] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9120ax-series-access-points/datasheet-c78-742115.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-AP1** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Dvě rádia pracující v režimu 2,4 a 5 GHz pro standardní prostředí nebo duální 5 GHz pro HD nasazení, možnost statické i dynamické volby režimu | **Ano** | |
| Samostatné rádio pro monitorování 2,4 a 5 GHz RF spektra – detailní spektrální analýza, detekce útoků na bezdrátovou sít, lokalizace klientů | **Ano** | |
| Podpora minimálně 4x4 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 160 MHz kanál pro 802.11ax | **Ano** | |
| Hardwarová podpora spektrální analýzy s podporou 160 MHz kanálů (detekce zdroje rušivého signálu – interference) | **Ano** | |
| Podpora rozpoznání zdroje rušivého signálu podle signatur | **Ano** | |
| Access Point obsahuje radio podporující BLE 5.0, ZigBee, Thread a USB 2.0 port | **Ano** | |
| 1 x 100/1000/2500 Mbit/s RJ45 ethernet rozhraní kompatibilní s 802.3bz | **Ano** | |
| Možnost PoE napájení AP z přepínače nebo injectoru – plná funkce AP při použití 802.3at, v případě 802.3af AP běží minimálně v režimu 1x1 MIMO pro obě rádiová pásma bez sníženého vysílacího výkonu | **Ano** | |
| AP je kompatibilní s plechovými úchyty stávajících AP Zadavatele, výměna AP tak nevyžaduje vrtací práce | **Ano** | |

* + 1. **Přístupový bod, typ AP2**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [C9105AXI-E] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/wireless/catalyst-9100ax-access-points/datasheet-c78-744062.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-AP2** | | |
| Zařízení je uvedeno v matici kompatibility výrobce nabízené fabriky | **Ano** | |
| Dvě rádia pracující v režimu 2,4 a 5 GHz | **Ano** | |
| Podpora minimálně 2x2 MIMO, MU-MIMO, UL/DL OFDMA, TWT, BSS Coloring a až 80 MHz kanál pro 802.11ax | **Ano** | |
| Access Point obsahuje radio podporující BLE 5.0 | **Ano** | |
| 1 x 100/1000 Mbit/s RJ45 ethernet rozhraní | **Ano** | |
| Možnost PoE napájení AP z přepínače nebo injectoru – plná funkce AP při použití 802.3af | **Ano** | |
| Součástí AP je plechový úchyt pro instalaci na strop nebo stěnu | **Ano** | |

* 1. **Směrovač datového centra**
     1. **Směrovač datového centra, typ R1**

|  |  |
| --- | --- |
| **Základní údaje** | **Nabízená hodnota** |
| Výrobce zařízení | [**Cisco**] |
| Produktové číslo (typ) nabízeného zařízení (v případě, že je zařízené popsáno více produktovými čísly, uvede Dodavatel hlavní produktové číslo nabízeného zařízení) | [C8500-12X4QC-DNA] |
| Odkaz na www stránky výrobce zařízení, kde je k dispozici detailní technická specifikace (DataSheet) v českém nebo anglickém jazyce | [[DataSheet](https://www.cisco.com/c/en/us/products/collateral/routers/catalyst-8500-series-edge-platforms/datasheet-c78-744089.html)] |

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Typ-R1** | | |
| Zařízení montovatelné do standardního 19inch stojanového rozvaděče – standardní Rack (IS EIA310D) - šířka rozvaděče 60cm – hloubka rozvaděče 100-115cm | **Ano** | |
| Formát zařízení: Fixní | **Ano** | |
| Interní redundantní AC napájecí zdroj 230V vyměnitelný za provozu | **Ano** | |
| Minimálně 8 portů 1/10 GigabitEthernet s volitelným fyzickým rozhraním typu SFP+ | **Ano** | |
| Minimálně 2 porty 40 GigabitEthernet s volitelným fyzickým rozhraním typu QSFP+ | **Ano** | |
| Minimálně 2 porty 40/100 GigabitEthernet s volitelným fyzickým rozhraním typu QSFP28 | **Ano** | |
| Oddělený procesor pro funkce směrování a forwardování paketů | **Ano** | |
| Propustnost systému minimálně 190Gb/s | **Ano** | |
| Minimální počet záznamů ve směrovací tabulce - IPv4 : 4M | **Ano** | |
| Minimální počet záznamů ve směrovací tabulce – IPv6 : 4M | **Ano** | |
| IEEE 802.3ad | **Ano** | |
| OSPFv2, OSPFv3 | **Ano** | |
| BGPv4, MP-BGP | **Ano** | |
| IS-IS v4, IS-IS v6 | **Ano** | |
| Podpora 4 byte AS numbers in BGP | **Ano** | |
| GRE (Generic Routing Encapsulation) | **Ano** | |
| Policy-based routing podle ACL | **Ano** | |
| IP Multicast (PIM SSM, PIM SM) | **Ano** | |
| IGMPv2, IGMPv3 | **Ano** | |
| uRPF pro IPv4 i IPv6 | **Ano** | |
| DHCP relay pro IPv4 i IPv6 | **Ano** | |
| First Hop Redundancy Protokol pro pro IPv4 i IPv6 | **Ano** | |
| MPLS L3 VPN | **Ano** | |
| IPv6 MPLS VPN (6VPE) | **Ano** | |
| mLDP based Multicast VPN | **Ano** | |
| L2 VPN with BGP-EVPN control plane (RFC 7432) | **Ano** | |
| VXLAN Group Policy Option nebo ekvivalentní | **Ano** | |
| IPv6 Multicast (MLDv1 & v2) | **Ano** | |
| IPv6 Multicast (PIM SM, PIM SSM) | **Ano** | |
| QoS classification – ACL, DSCP, CoS, MPLS Exp based | **Ano** | |
| QoS marking - DSCP, CoS, MPLS Exp | **Ano** | |
| QoS Shaping | **Ano** | |
| QoS Policing – 2 rate, 3 color policer | **Ano** | |
| Congestion avoidance - WRED | **Ano** | |
| Class Based and Priority queuing | **Ano** | |
| Priority queuing – min. 2 priority queues | **Ano** | |
| Možnost aplikovat queuing policy na port-channel rozhranní | **Ano** | |
| Rate Limiting | **Ano** | |
| Hierarchical QoS: min. 3 úrovně | **Ano** | |
| Virtualizace směrovacích tabulek - např. Virtual Routing and Forwarding (VRF) | **Ano** | |
| Minimální počet oddělených (nezávislých) směrovacích tabulek: 1000 | **Ano** | |
| Podpora protokolů a služeb per VRF (OSPF, TACACS+, VRRP nebo HSRP, SNMP, Syslog) | **Ano** | |
| IPSec AES-GCM-256 | **Ano** | |
| Hardwarová akcelerace šifrování pro IPSec AES-GCM-256 | **Ano** | |
| QoS pre-classification pro IPSec | **Ano** | |
| Šifrovací výkon pro IPSec AES-GCM-256: minimálně 130Gb/s | **Ano** | |
| IPSec IKEv2 | **Ano** | |
| VRF aware IPSec | **Ano** | |
| SHA-2 (SHA-256, SHA-512) | **Ano** | |
| Vytváření šifrovaných Hub&Spoke VPN s možností dynamicky sestavovat tunely mezi „spoke“ lokalitami | **Ano** | |
| Vytváření šifrovaných VPN bez potřeby tunelů dle RFC 3547 (GDOI based VPN) s centrální správou šifrovacích klíčů | **Ano** | |
| Podpora Suite-B šifrovacích algoritmů (RFC 6379) ve spojení s GDOI based VPN | **Ano** | |
| VRF aware GDOI group member (selektivní šifrování provozu per IP VPN) | **Ano** | |
| ACL na rozhraní IN/OUT | **Ano** | |
| Schopnost práce s bezpečnostními značkami (SGT) | **Ano** | |
| Schopnost inline přenosu bezpečnostních značek (SGT) v záhlaví ethernetových rámců | **Ano** | |
| Vytváření a enforcement ACL založených na bezpečnostních značkách (SGACL) | **Ano** | |
| Podpora ACL založených na bezpečnostních značkách v hardware | **Ano** | |
| Podpora přenosu mapování mezi bezpečnostními značkami (SGT) a IP adresami definovaného v Cisco ISE do jednotlivých VRF | **Ano** | |
| Podpora alespoň 1500 relací pro přenos mapování mezi bezpečnostními značkami (SGT) a IP adresami do ostatních směrovačů a přepínačů v síti | **Ano** | |
| IEEE 802.1AE (GCM-AES-256) na všech 1/10/40/100GE portech | **Ano** | |
| Pokročilá detekce a klasifikace jednotlivých přenášených aplikací (DPI na 7. vrstvě OSI modelu dle aplikačních signatur) včetně možnosti definovat signatury pro vlastní aplikace | **Ano** | |
| Monitorování aplikačních toků (všech paketů) prostřednictvím technologie NetFlow nebo ekvivalentní | **Ano** | |
| Možnost definice klíčových atributů a parametrů monitorovaných toků včetně parametrů: zdrojová/cílová MAC adresa, zdrojová/cílová IP adresa, zdrojová/cílová VLAN, TCP flags, TCP sekvenční čísla, hodnota TTL, ICMP kód, IGMP type | **Ano** | |
| Schopnost detekce bezpečnostních hrozeb v šifrovaném provozu, např. v HTTPS, bez nutnosti dešifrování paketů | **Ano** | |
| Export NetFlow dat dle formátu NetFlow v9 nebo IPFIX | **Ano** | |
| Interní nástroje pro on-line měření kvality síťové infrastruktury, např. IP SLA nebo ekvivalentní | **Ano** | |
| Ochrana proti nahrání modifikovaného software do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu jak samotného operačního systému, tak i bootloaderu, a to prostřednictvím nemodifikovatelných interních HW prostředků - tzv. hardware anchores | **Ano** | |
| Podpora funkce umožňující administrátorovi ověřit, že zařízení skutečně nabootovalo důvěryhodný operační systém, tzv. Boot Integrity Visibility | **Ano** | |
| Operační systém zařízení využívá tzv. Runtime Defenses nástroje, které znemožňují injektovat škodlivý kód do běžícího systému | **Ano** | |
| Ochrana proti modifikaci HW prostředků zařízení využívající X.509 SUDI certifikát pro ověření autentičnosti HW prostředků zařízení. Možnost zobrazení SUDI certifikátu administrátorem, např. prostřednictvím konzole zařízení | **Ano** | |
| SSHv2 | **Ano** | |
| CLI rozhraní | **Ano** | |
| Programovatelnost prostřednictvím NETCONF/YANG | **Ano** | |
| Python scripting | **Ano** | |
| Software patching | **Ano** | |
| Model-driven telemetrie pro real-time streaming informací o stavu zařízení | **Ano** | |
| SNMPv2/v3 | **Ano** | |
| TACACS+ nebo RADIUS klient pro AAA (autentizace, autorizace, accounting) | **Ano** | |
| NTPv3 server | **Ano** | |

## Podrobná specifikace SW řízené přístupové vrstvy

Veškerá výše specifikované přepínače a přístupové body budou součástí a musí být spravovatelné pomocí SW řízené přístupové vrstvy. SW řízená přístupová vrstva je dodána ve formě fabriky skládající se z podkladové přenosové vrstvy (underlay), zajišťující základní L2, L3 konektivitu a překryvné (overaly) vrstvy zajišťující řídící a management komunikaci. Fabrika je řízena centrálním kontrolérem, DNA centrem, který je nedílnou součástí SW řízené přístupové vrstvy.

* 1. **Obecné vlastnosti softwarově definované přístupové sítě (fabriky)**

|  |  |  |
| --- | --- | --- |
| **Popis parametru** | | **Splněno (ANO)** |
| **Obecné vlastnosti softwarově definované přístupové sítě (fabriky)** | | |
| Fabrika má dvě oddělené vrstvy – “underlay”, poskytující základní L3 komunikační infrastrukturu a “overlay”, vytvářející překryvnou strukturu poskytující inteligentní funkce jako je segmentace a bezpečnostní politiky založené na identitě uživatelů a vlastnostech koncových bodů. | **Ano** | |
| Ověřování, automatické rozpoznávání a klasifikace připojovaných zařízení, včetně nových a fabrice dosud neznámých. | **Ano** | |
| Ověřování identity a klasifikace uživatelů přistupujících do fabriky. | **Ano** | |
| Automatické rozpoznání a klasifikace přenášených aplikací spolu s detekcí toků v síti. | **Ano** | |
| Rozpoznání bezpečnostních incidentů na základě detekce toků v síti. | **Ano** | |
| Detekce škodlivého kódu skrytého v šifrovaném provozu připojených klientů proti interním i externím serverům a kryptografické auditu tohoto šifrovaného provozu bez nutnosti jeho dešifrování. | **Ano** | |
| Definice politik přístupu připojovaných zařízení podle jejich klasifikace a identity jejich aktuálního uživatele. | **Ano** | |
| Vynucování politik přístupu a segmentace automaticky a dynamicky, dle dynamické klasifikace připojovaných zařízení i uživatelů. Staticky je možné řešit pouze výjimečné situace. | **Ano** | |
| Vynucování politik přístupu a segmentace jednotně a nezávisle na vlastní fyzické topologii “underlay” infrastruktury. | **Ano** | |
| Vynucování politik přístupu a segmentace jednotně a nezávisle na fyzickém místě a způsobu připojení. | **Ano** | |
| Vytvořené segmenty musí být v dané lokalitě rozprostřené přes fyzickou topologii “underlay” infrastruktur a musí umožňovat existenci více IP subnetů uvnitř daného segmentu a rovněž rozprostření všech těchto IP subnetů přes L3 “underlay” infrastrukturu. | **Ano** | |
| Fabrika umožňuje nasazení přístupu “zero-trust”, kdy dané zařízení je do sítě připojeno na základě úspěšné (v případě potřeby i multifaktorové) autentizace a na základě jejího výsledku je mu přidělen odpovídající přístup k síti a jejím zdrojům. | **Ano** | |
| Segmentace a bezpečnostní politiky založené na identitě uživatelů a vlastnostech koncových bodů definují pravidla pro komunikaci a omezují možnost šíření hrozeb mezi koncovými zařízeními, a to jak mezi segmenty, v rámci jednoho společného segmentu mezi skupinami sdílejícími společnou klasifikaci a rovněž mezi členy stejné skupiny. | **Ano** | |
| Segmentace a bezpečnostní politiky jsou jednotné pro přístup uživatele a zařízení v pevné i integrované bezdrátové přístupové síti. | **Ano** | |
| Segmentace a bezpečnostní politika se „přesouvá“ spolu s koncovým zařízením a uživatelem. | **Ano** | |
| Pro definici segmentace a bezpečnostní politiky a ovládání celé fabriky je využíváno konceptu “intent-based” (“řízení záměrem”). Definice segmentace a bezpečnostní politiky i řízení fabriky se provádí z uživatelského grafického rozhraní kontroléru nikoli z příkazové řádky. | **Ano** | |
| Pří nastavování fabriky se jednotlivým zařízením pouze přiřazují jejích role ve fabrice a doplňují se jenom nezbytné parametry pro její funkci. Díky abstrakci není třeba ručně připravovat pro jednotlivá zařízení individuální konfigurace, ale tyto jsou automaticky generovány kontrolérem. | **Ano** | |
| Při sestavování fabriky se využívají automatizační přístupy jako zero-touch provisioning, plug&play a guided workflows. | **Ano** | |
| Automatizace segmentace zabezpečení, vytváření VRF pro síťovou fabriku. | **Ano** | |
| Na síťové fabrice nesmí být žádné ruční konfigurace VLAN. Mohou být součástí automatizace. | **Ano** | |
| Automatizace vytváření skupinových bezpečnostních značek, které musí být umožněno klientům přiřazovat dynamicky nebo staticky. Granulární segmentace zabezpečení musí umožnit odepření vzájemné komunikace klientů ze stejné podsítě, drátové i bezdrátové. | **Ano** | |
| Automatizace konfigurací přístupových portů přepínačů pro bezpečné připojení uživatelů a jejich koncových stanic na základě autentizace, rozpoznání identity uživatele a jeho zařízení, autorizace a dalších atributů. | **Ano** | |
| Síťová fabrika musí být nezávislá na topologii, což znamená, že mohou být podporovány jakékoli 2 vrstvé, 3 vrstvé, mesh, semi-mesh topologie sítě. | **Ano** | |
| Protokol směrování „underlay“ sítě fabriky musí být automatizován kontroléry softwarově definované sítě. | **Ano** | |
| Síťová fabrika musí mít jednotnou pevnou a bezdrátovou síť. To znamená, že bezdrátový provoz koncových stanic nemusí být nutně přenášen přes kontrolér bezdrátové sítě. Bezdrátový provoz musí být možné ukončit prostřednictvím přístupového přepínače, který bude poskytovat připojení k přístupovému bodu (distribuovaný datový model). | **Ano** | |
| Síťová fabrika musí podporovat multicast. Konfigurace multicastu musí být automatizována prostřednictvím kontrolerů softwarově definované sítě. | **Ano** | |
| Softwarově definovaná sít musí podporovat automatizaci konfigurací QoS end-to-end v rámci fabriky pro drátové i bezdrátové sítě prostřednictvím jednoduchého postupu uživatelského rozhraní bez nutnosti používat příkazový řádek. | **Ano** | |
| Automatizace pro vytvoření underlay sítě prostřednictvím kontrolérů softwarově definované sítě musí být založena na grafickém uživatelském rozhraní bez nutnosti používat příkazový řádek. | **Ano** | |
| Architektura fabriky musí umožnit nasazení v centrálních lokalitách i areálech s desítkami tisíc koncových zařízení, stejně jako implementaci v malé vzdálené lokalitě s jednotkami koncových zařízení při zachování jednotné segmentace a bezpečnostní politiky pro všechny lokality. | **Ano** | |
| Nabízené řešení musí umožnit sdílení identit, politik přístupu a segmentace vně fabriky, do navazujících infrastrukturních oblastí, tedy do WAN a datových center, případně i do zařízení třetích stran jako jsou firewally. | **Ano** | |
| **Vlastnosti “Overlay” sítě** | | |
| Pro dosažení vyšší flexibility, stability, dostupnosti služeb a snížení provozního rizika při provádění změn jsou bezpečnostní politiky a segmentace a jejich přesuny (spolu s koncovým zařízením a uživatelem) zajištěny pomocí virtuální překryvné sítě (virtual network overlay), která je logicky oddělená od underlay sítě, která poskytuje pouze transportní funkci. | **Ano** | |
| Overlay síť musí být segmentovatelná na virtuální sítě s plně oddělěným směrovacím kontextem (VRF). Komunikace mezi nimi musí být zajištěna na zařízení vně fabriku, které zároveň zabezpečuje bezpečnostní politiku mezi nimi (směrovač nebo firewall). | **Ano** | |
| Overlay síť musí umožňovat vytvoření alespoň 60 virtuálních sítí. | **Ano** | |
| Při připojení koncového zařízení do překryvné sítě jsou informace nutné pro síťovou komunikaci s ním zaregistrovány řídícím protokolem do řídícího uzlu fabriky.  Tyto informace předá řídící protokol překryvné sítě pouze těm ostatním prvkům fabriky, které danou informaci pro zajištění síťové komunikace potřebují.  Při přesunu koncového zařízení z jednoho prvku na druhý aktualizuje řídící protokol překryvné sítě pouze informace pro prvky, které ji vyžadují, nikoli všechny prvky fabriky. | **Ano** | |
| Pro zvýšení odolnosti proti výpadkům komunikace může být v případě potřeby řídící uzel překryvné sítě zdvojen. | **Ano** | |
| Pro zajištění vysoké škálovatelnosti řešení není síťový provoz mezi zařízeními připojenými do různých prvků fabriky a patřících do stejné virtuální sítě tunelován do řídícího uzlu překryvné sítě nebo jiného centralizovaného bodu fabriky, pokud k němu jedno z těchto koncových zařízení není přímo připojeno. | **Ano** | |
| Jednotné politiky přístupu a segmentace jsou aplikovány stejně, i když se uživatel přesune mezi pevnou a bezdrátovou sítí a naopak. Jednotná aplikace politik je možná díky sjednocení provozu z pevné a bezdrátové sítě na úrovni přístupového prvku. Uživatelský provoz z připojeného bezdrátového přístupového bodu je prvkem posílán přímo do překryvné sítě fabriky, stejné jako uživatelský provoz z pevného přístupového portu téhož prvku. Řídící protokoly překryvné a bezdrátové sítě jsou prointegrovány. | **Ano** | |
| Forwarding uživatelských dat (data plane) je distribuovaný pro eliminaci úzkých hrdel a negativních dopadů případných výpadků. Každý přístupový prvek překryvné sítě aplikuje politiky na uživatelský provoz, označuje ho přislušnou značkou určující příslušnost do skupiny a přeposílá (forwarduje) ho lokálně. | **Ano** | |
| Overlay síť poskytuje dvouúrovňovou segmentaci. První úrovní segmentace je členění fabriky na logické nebo organizační celky (virtuální sítě). Druhou úrovní je rozdělení virtuální sítě na skupiny sdružující jednotlivé koncové uživatele, uživatelské stanice a k síti připojená zařízení podle klíče, který umožní efektivní tvorbu politik mezi těmito skupinami a odráží roli těchto skupin v rámci sítě. Politika může zacházet až do úrovně jednotlivých komunikačních protokolů a portů. Politikou lze i povolit nebo zakázat komunikaci mezi všemi jednotlivými uživateli či zařízeními v rámci stejné skupiny. | **Ano** | |
| Segmentace zavadí nový nezávislý identifikátor (skupinovou značku) využívaný ve fabrice a přenositelný i mimo fabriku. Tato značka může být přidělena bez ohledu na tradiční segmentační přístupy jako je například členění sítě do VLAN. Tato značka se může měnit i když IP adresa stanice a její příslušnost do VLAN zůstává stejná, například tehdy, přihlásí-li se k ní jiný uživatel. | **Ano** | |
| Ve fabrice není třeba konfigurovat žádný seznam řízení přístupu IP pro účely segmentace sítě. | **Ano** | |
| Overlay síť podporuje šíření multicast, broadcast i unknown unicast provozu. | **Ano** | |
| Overlay síť podporuje vytvoření rozprostřeného komunikačního L2 segmentu koncových zařízení přes L3 infrastrukturu bez závislosti a omezení daných technologií Spanning Tree protokolu. | **Ano** | |
| Pro připojování návštěvníků (Guest access) může fabrika poskytovat oddělenou logickou infrastrukturu (segment) s dedikovaným řídícím uzlem a vyústěním v DMZ. | **Ano** | |
| **Vlastnosti “Underlay” sítě** | | |
| Pro dosažení maximální robustnosti, stability a jednoduchosti je „underlay“ síť realizována jako kompletně IP směrovaná až do úrovně přepínače přístupové vrstvy (L3 access). | **Ano** | |
| Směrovací protokol je konfigurován pro dosažení rychlé konvergence v případě výpadku trasy. | **Ano** | |
| Underlay nevyužívá Spanning tree protokol. | **Ano** | |
| Pro dosažení maximální robustnosti, stability a jednoduchosti „underlay“ síť využívá všech redundantních spojů tak, jak jsou definovány v topologii jednotlivých lokalit. | **Ano** | |
| Pro využití redundantních spojů ve fabrice se využívá rozkládání zátěže pomocí mechanizmu Equal Cost Multi Path (ECMP) s pokročilým algoritmem rozkladu. Všechny redundantní trasy jsou aktivní. | **Ano** | |
| Pro rychlou detekci výpadků spojení a rychlou reakci na ně je využit protokol BFD. | **Ano** | |
| Nastavení a konfigurace “underlay” vrstvy je automatizována centrálním řídícím kontrolérem fabriky. | **Ano** | |
| “Underlay” vrstva poskytuje dostatečnou velikost MTU pro transport “overlay” sítě bez nutnosti fragmentace a to minimálně 1800 bajtů, ideálně alespoň 9100 bajtů. | **Ano** | |
| “Underlay” vrstva poskytuje mechanizmy pro směrování a přenos multicast paketů, kterých je využíváno pro efektivní šíření multicast, broadcast i unknown unicast provozu v overlay vrstvě sítě. | **Ano** | |
| **Funkce fabriky - Automatizace a provoz fabriky** | | |
| Řešení poskytuje nástroje pro správu sítě v hierarchické struktuře založenou na profilech. | **Ano** | |
| Řešení umožňuje centralizovanou správu bezdrátových sítí, jejich nastavení a aktivaci v jednotlivých lokalitách síťové hierarchie. | **Ano** | |
| Řešení umožňuje centralizované nastavení parametrů provozního a bezpečnostního monitoringu z kontroléru softwarově definované sítě. | **Ano** | |
| Kontrolér softwarově definované sítě musí poskytovat funkce pro automatické sestavení „underlay“ sítě fabriky ve spravované lokalitě. | **Ano** | |
| Řešení umožňuje automatické vyhledání nových přístupových síťových přepínačů připojených v lokalitě k jednomu nebo dvěma podporovaným a spravovaným „seed“ přepínačům. | **Ano** | |
| Řešení umožňuje automatickou alokaci IP adres rozhraní přepínače přidávaného do „underlay“ sítě fabriky z přiděleného IP rozsahu s využitím automatizace. | **Ano** | |
| Řešení umožňuje konfiguraci přidávaných přepínačů „underlay“ sítě fabriky s využitím výrobcem doporučených konfigurací – včetně směrování a zabezpečení zařízení. | **Ano** | |
| Řešení podporuje zavedení automaticky přidávaných zařízení do inventáře zařízení spravovaných systémem pro řízení fabriky a archivaci jejich konfigurací. | **Ano** | |
| Řešení podporuje konfiguraci zařízení jako součásti „underlay“ sítě s využitím zákaznické šablony pro případy, kdy není výrobcem doporučená konfigurace vhodná či žádoucí. | **Ano** | |
| Řešení podporuje možnost rozšíření stávající „underlay“ sítě v lokalitě přidáním dalšího zařízení s využitím automatizovaného postupu. | **Ano** | |
| Řešení umožňuje definici rolí jednotlivých zařízení fabriky z grafického prostředí kontroléru softwarově definované sítě. | **Ano** | |
| Součástí řešení je pomocník pro výběr metody ověřování a řízení přístup do sítě v rámci fabriky v dané lokalitě. | **Ano** | |
| Součástí řešení je pomocník pro aktivaci segmentů sítě v rámci fabriky v dané lokalitě. | **Ano** | |
| Součástí řešení je pomocník pro aktivaci bezdrátových sítí v rámci fabriky v dané lokalitě. | **Ano** | |
| Součástí řešení je pomocník pro nastavení multicast provozu tam, kde je ve fabrice vyžadován. | **Ano** | |
| Řešení umožňuje nastavení specifické konfigurace portu, který vyžaduje odlišné parametry, než jsou dány centrální politikou. | **Ano** | |
| Řešení poskytuje podporu pro migraci klientů ze stávající infrastruktury do sítě v režimu fabriky. IP subnet může být po dobu migrace rozprostřen mezi stavající infrastrukturou a fabrikou. | **Ano** | |
| Řešení softwarově definované sítě musí poskytovat nástroje a rozhraní pro monitoring funkcí softwarově definované fabriky. | **Ano** | |
| Řešení poskutuje podporu pro řešení výpadků a problémů souvisejících s provozem fabriky a připojením koncových stanic do fabriky. | **Ano** | |
| **Funkce fabriky – Bezpečnost** | | |
| Kontrolér automatizuje konfiguraci pro podporu detekce bezpečnostních incidentů monitorováním síťového provozu. | **Ano** | |
| Kontrolér automatizuje konfiguraci pro podporu detekce šifrovaného škodlivého provozu. | **Ano** | |
| Kontrolér softwarově definované sítě musí podporovat pro drátové i bezdrátové připojení na všech přístupových přepínačích a bezdrátových přístupových bodech ve fabrice automatizovanou konfiguraci bez nutnosti používat příkazový řádek pro 802.1x a MAB (ověření na základě MAC adresy). | **Ano** | |
| Kontrolér softwarově definované sítě musí podporovat pro drátové i bezdrátové připojení na všech přístupových přepínačích a bezdrátových přístupových bodech ve fabrice automatizovanou konfiguraci bez nutnosti používat příkazový řádek pro webové ověření pro návštěvnický přístup. | **Ano** | |
| Navržené řešení softwarově definované sítě musí podporovat profilování jednotlivých připojovaných koncových zařízení a musí umět odeslat informace o koncových zařízeních nastavenému serveru s politikami za účelem klasifikace zařízení. Konfigurace příslušných aktivních síťových prvků musí být automatizována kontrolérem. | **Ano** | |
| Navržené řešení softwarově definované sítě musí podporovat identifikaci a profilování koncových a IoT zařízení na základě analýzy jejich komunikace a chování v sítí s cílem omezit výskyt neznámých zařízení v sítí. | **Ano** | |
| **Funkce fabriky – Segmentace** | | |
| Řešení softwarově definované sítě musí implementovat virtuální sítě (segmenty) založené na Virtual Routing Forwarding (VRF), aby zajistilo bezpečnou segmentaci sítě v rámci síťové fabriky. | **Ano** | |
| Veškeré vytváření virtuálních sítí musí být plně automatizováno kontroléry softwarově definované sítě bez nutnosti používat příkazový řádek. | **Ano** | |
| Přiřazení příslušné virtuální sítě je ověřenému koncovému bodu / uživateli provedeno automaticky během připojování do sítě na základě jeho role. | **Ano** | |
| Vytvoření virtuálních sítí a také přiřazení skupinových značek musí být možno v grafickém prostředí kontrolérů softwarově definované sítě a nesmí vyžadovat manuální konfigurační zásah. | **Ano** | |
| Vytvoření politik pro segmentaci sítě musí být možno jen a výhradně kontrolérem softwarově definované sítě. Kontrolér následně naprogramuje nástroj pro správu politik a řízení přístupů na základě toho, co bylo nakonfigurováno. | **Ano** | |
| Kontrolér softwarově definované fabriky musí umožnit vizualizovat komunikační vztahy mezi skupinami (reprezentovanými skupinovými značkami) navzájem komunikujícími v rámci fabriky. | **Ano** | |
| Kontrolér musí zobrazit používané komunikační protokoly a porty pro komunikaci mezi skupinami v rámci fabriky, aby bylo možné optimalizovat politiku pro podrobnější segmentaci sítě. | **Ano** | |
| **Způsob připojování koncových zařízení k fabrice** | | |
| Fabrika ověřuje připojovaná zařízení pomocí IEEE 802.1x mechanismů. | **Ano** | |
| Ověření koncového zařízení lze dynamicky znovu vynutit ze strany fabriky. | **Ano** | |
| Pokud to skupina koncových zařízení vyžaduje, využije fabrika ověření na základě MAC adresy. | **Ano** | |
| Koncové zařízení včetně jeho datového provozu je fabrikou profilováno a následně pomocí mechanismů strojového učení klasifikováno. Tímto jsou aplikovány relevantní politiky na nová, neznámá koncová zařízení. | **Ano** | |
| Fabrika aplikuje své centrálně definované politiky na provoz koncového zařízení na základě jeho ověření a příslušnosti k definované skupině. | **Ano** | |
| Koncové zařízení obdrží nastavení IP parametrů vždy z jemu příslušného IP rozsahu dle autorizačních politik. | **Ano** | |
| Fabrika využívá principu Anycast Gateway. IP i MAC adresa výchozí brány pro daný IP subnet je stejná na všech jejích uzlech. | **Ano** | |
| Pokud to skupina koncových zařízení vyžaduje, poskytuje fabrika koncovým zařízením na jejich vzájemné propojení jeden komunikační L2 segment bez ohledu na to, ve kterém místě fabriky jsou koncová zařízení fyzicky připojena. | **Ano** | |
| Fabrika poskytuje přístupová místa pro návštěvníky organizace (Guest Access) a jejich oddělení (dedikovaný segment) od interního provozu organizace. | **Ano** | |
| Fabrika poskytuje připojení pevným i bezdrátovým koncovým zařízením. | **Ano** | |
| Přístupová vrstva síťové fabriky musí podporovat připojení IP kamer a dalších ne-uživatelských zařízení. | **Ano** | |
| Přístupová vrstva síťové fabriky musí v případě potřeby podporovat připojení serverů. | **Ano** | |
| Fabrika automaticky detekuje a do sebe začlení i připojovaný bezdrátový přístupový bod. | **Ano** | |
| Fabrika připojí koncová zařízení i přes externí L2 přepínač (např. umístěný v kancelářských prostorech) a i na datový provoz mezi těmito koncovými zařízeními jsou aplikovány příslušné centrální politiky/segmentace. | **Ano** | |
| **Řízení přístupů do fabriky** | | |
| Řešení zajistí bezpečné připojení uživatelů a jejich koncových stanic na základě procesu autentizace (rozpoznání identity uživatele a jeho zařízení) a autorizace (zpřístupnění konkrétních datových zdrojů podle uživatelské role, stavu koncového zařízení) a dalších atributů v rámci kontextu uživatele. | **Ano** | |
| Řešení poskytne centrální bod pro správu přístupových politik, monitorování a řešení problémů z pohledu drátového, bezdrátového nebo VPN připojení do sítě. | **Ano** | |
| Řešení softwarově definované sítě poskytne integrované funkce zajišťují komunikaci s AAA serverem (RADIUS) a umožňují nastavovat komplexní a unifikované bezpečnostní politiky pro autentizaci, autorizaci a accounting. | **Ano** | |
| Řešení poskytne flexibilní způsoby ověřování (FlexAuth), včetně ověřování IEEE 802.1X, webového ověřování (WebAuth) a technologie MAC Authentication Bypass (MAB). | **Ano** | |
| Všichni uživatelé (mobilní zaměstnanci, ale i dodavatelé nebo prodejci) budou vždy jednoznačně identifikováni a prostřednictvím přidělených rolí jim bude zajištěn bezpečný přístup ke všem informacím v síti, na které mají nárok. Budou zařazeni do jim příslušné virtuální sítě/segmentu a bude jim přiřazena relevantní skupinová značka, čímž je poskytnuta podpora pro požadovanou dvouúrovňovou segmentaci. | **Ano** | |
| Připojení pro hosty do Guest sítě a jejich správu prostřednictvím plně přizpůsobitelných mobilních nebo desktop portálů, které jsou lehce vytvořitelné během několika minut s dynamickým vizuálním workflow. | **Ano** | |
| Řešení dokáže ověřit, zda stanice, které se připojují do sítě, vyhovují bezpečnostním pravidlům stanoveným ve firmě. Prověřované parametry týkající se třeba aktivované a aktualizované antivirové ochrany nebo jestli koncové stanice mají nainstalovány nezbytné opravy a aktualizace operačního systému. Přístup stanic, které definovaným pravidlům nevyhovují, bude omezen síťovým zařízením do té doby, než budou odstraněny nedostatky. Po odstranění nedostatků získá stanice opět plný přístup do sítě. | **Ano** | |
| Řešení umožní, aby již připojené koncové stanice bylo možné dynamicky přesunout do jiného pracovního segmentu (ale i např. karantény) nebo uplatnit přístupové filtry tzv. „za běhu“ pomocí řízení CoA (Change of Authorization = proces aplikace pravidel pomocí rozšíření protokolu RADIUS, popsaném v RFC) na základě aktuálního vyhodnocení vstupních parametrů (typ koncového zařízení, jeho stav apod.). | **Ano** | |
| Řešení poskytne podporu pro BYOD a Enterprise Mobility se snadným „out-of-the-box“ nastavením a správou certifikátů pro interní zařízení s jednotným a přehledným managementem. | **Ano** | |
| Řešení umožní pokročilé integrace s několika dodavateli systémů Mobile Device Management, jakými jsou například Cisco Meraki SM, AirWatch, Good Technology, MobileIron a Zenprise. | **Ano** | |
| Řešení poskytuje zjednodušenou správu bezpečnostních politik a umožňuje tak jejich konzistentní nastavení v rámci celé sítě. | **Ano** | |
| Komponenty centrálního bezpečnostního managementu, s vazbou na externí autentizační databáze, např. AD, LDAP jsou využitelné i pro přiřazení bezpečnostních politik na dalších zařízeních (např. firewall) na základě uživatelské identity nebo jeho skupinové bezpečnostní role. | **Ano** | |
| Nástroj řízení přístupu do fabriky musí být výrobcem uveden jako podporovaný pro řešení nabízené fabriky. | **Ano** | |
| **Interakce fabriky s okolním síťovým prostředím** | | |
| Fabrikou zjištěná příslušnost koncového zařízení/uživatele ke skupině a segmentu je sdílena s technologií Cisco ACI, která tvoří fabriku v datovém centru organizace, a ta danou skupinu a segment pro politiky a segmentaci v datovém centru využívá. | **Ano** | |
| Značkám reprezentujícím skupinu v LAN fabrice mohou být v datacentrové ACI fabrice namapovány 1:1 příslušné EPG značky. A rovněž naopak EPG značky mohou být namapovány do značek používaných LAN fabrikou. Dosáhne se tím jednotné identifikace uživatelů/skupin a aplikací napříč systémy. | **Ano** | |
| Příslušnost koncového zařízení/uživatele ke skupině a segmentu lze sdílet s technologií SD-WAN pro připojení vzdálených lokalit organizace. | **Ano** | |
| Segment je mapován do SD-WAN sítě tak, že je přenášen v oddělené virtuální síti. | **Ano** | |
| Značka reprezentující identitu/skupinu ve fabrice je v SD-WAN přenášena jako dodatečná informace v záhlaví SD-WAN overlay na vzdálenou lokalitu. | **Ano** | |
| Příslušnost koncového zařízení/uživatele ke skupině (skupinovou značku) lze přenášet okolním síťovým prostředím jak in-band/inline v datovém provozu (metadata), tak i out-of-band protokolem určeným pro tento přenos. | **Ano** | |
| Segmentace provozu při přenosu okolním síťovým prostředím je zajištěna nativními prostředky přenosové technologie. | **Ano** | |
| Příslušnost koncového zařízení/uživatele ke skupině (skupinová značka) je sdílena s externími zařízeními a ty je využívají pro svou funkci (např. firewall pro firewallová pravidla). | **Ano** | |
| Síťová fabrika musí poskytovat interoperabilitu se síťovými zařízeními od různých výrobců mimo tuto fabriku (např. firewall). | **Ano** | |
| Fabriku lze s ostatními oblastmi sítě propojit na L3 (směrovaný propoj, oddělení L2 domén). | **Ano** | |
| Fabriku lze s ostatními oblastmi sítě propojit na L2 (protažení vybraných L2 segmentů vně fabriky). V tomto případě je možné umístit výchozí bránu i mimo fabriku. | **Ano** | |
| Sdílené síťové služby (například AAA, DHCP, DNS, ...), není nutné implementovat pro každý segment fabriky zvlášť. Lze je realizovat 1x a bezpečně propojit s každým odděleným segmentem. | **Ano** | |
| Fabrika používá naimplementovaný AAA systém Cisco ISE nativně bez pomocných produktů 3tích stran. | **Ano** | |
| Řešení poskytuje automatizaci pro správu IP adresních rozsahů segmentů síťové fabriky v jednotlivých lokalitách. | **Ano** | |
| Řešení umožňuje integraci s používaným IPAM systémem od firmy Infoblox. | **Ano** | |

## Pilotní provoz SW řízené přístupové vrstvy sítě VZP ČR (dále jen Pilotní provoz)

Pilotní provoz SW řízené přístupové vrstvy sítě (plnění dle čl. II. odst.7. písm. b) této Rámcové dohody) VZP ČR se skládá z těchto částí:

1. **Analytické části**
   1. Návrh řešení (High Level Design) - dokument popisující celé řešení, včetně všech síťových detailů;
   2. Návrh pilotního provozu – dokument popisující provedení pilotního provozu;
   3. Návrh testovacích scénářů sloužících k ověření výsledků dosažených pilotním provozem.
2. **Provedení pilotního provozu**
   1. Nasazení řídícího HW a SW (management) nástroje v DC VZP ČR včetně jeho konfigurace;
   2. Implementace HW a SW ve třech předem domluvených pobočkách VZP ČR;
   3. Realizace testovacích aktivit podle scénářů vypracovaných v analytické části, které prokáží nade vší pochybnost vhodnost a funkčnost celého řešení, a to v předem definovaných parametrech.
3. **Dokumentace k migračnímu procesu**
   1. Popis procesu migrace - dokument popisující proces migrace do SW řízené přístupové vrstvy, tj. nasazování, procesy, postupy, principy, návaznosti, podmínky a závislosti;
   2. Podrobný popis migrace, tj. dokument popisující detailní konfiguraci všech zařízení, které jsou předmětem dodávky, včetně podrobných instalačních, implementačních a konfiguračních manuálů.
   3. **Doba a podmínky plnění Pilotního provozu**

Předmět plnění dle čl. IV. odst. 1. písm f), tj. pilotní provoz SW řízené přístupové vrstvy bude realizován dle Smlouvy uzavřené na základě této Rámcové dohody (dále jen „Smlouva na pilotní provoz“).

Objednatel připouští elektronickou verzi všech požadovaných dokumentů včetně předávacích a akceptačních protokolů.

Elektronická komunikace bude probíhat mezi Pověřenými osobami obou Smluvních stran.

* + 1. **Doba a podmínky plnění Analytické části**

1. Dodavatel je povinen poskytnout plnění řádně a včas. Řádně poskytnutým plněním se rozumí poskytnutí plnění v rozsahu a za podmínek stanovených touto Rámcovou dohodou nejpozději do 90 kalendářních dní ode dne nabytí účinnosti Smlouvy na pilotní provoz. Plnění této části se považuje za řádně poskytnuté dnem podpisu Akceptačního protokolu analytické části.
2. Řádně vypracovaná dokumentace analytické části, tzn. dokumenty:
   * Návrh řešení (High Level Design)
   * Návrh pilotního provozu
   * Návrh testovacích scénářů

bude předána Objednateli v elektronické verzi v editovatelném formátu (tj. .doc, .docx, .txt, .rtf, .ppt, .xls, .xlsx), a to v termínu (viz odst. 1. tohoto článku 6.1.1.).

1. Před akceptací dokumentace analytické části proběhne akceptační procedura popsaná v odst. 4. až 9. tohoto článku. Případná nutnost opakovat akceptační proceduru nemá vliv na povinnost Dodavatele poskytnout plnění řádně a včas dle odst. 1. tohoto článku.
2. O předání a převzetí dokumentace analytické části bude sepsán Předávací protokol analytické části, který bude podepsán Pověřenými osobami obou Smluvních stran.
3. Podepsáním Předávacího protokolu se zahajuje akceptační řízení, ve kterém Objednatel předloží připomínky k vypracované dokumentaci analytické části do osmi (8) kalendářních dnů od podepsání příslušného Předávacího protokolu analytické části.
4. V případě, že Objednatel dokumentaci analytické části neakceptuje nebo bude mít k analytické části výhrady, zavazuje se Dodavatel bez zbytečného odkladu provést veškeré potřebné úpravy dokumentace analytické části dle výhrad a připomínek Objednatele a takto upravenou dokumentaci analytické části předat Objednateli opětovně k akceptaci.
5. Dokud Dodavatel nevypořádá veškeré připomínky Objednatele, nebude dokumentace analytické části akceptována a bude postupováno obdobně dle ustanovení odst. 4. až 7. tohoto článku.
6. Akceptace řádně vypracované dokumentace analytické části bude po vypořádání všech připomínek Objednatele potvrzena podpisem Akceptačního protokolu analytické části Pověřenými osobami obou Smluvních stran.
7. Objednatel se zavazuje poskytovat Dodavateli součinnost při plnění závazků Dodavatele dle této Rámcové dohody, a to zejména poskytovat Dodavateli veškeré informace a podklady potřebné pro vypracování dokumentace analytické části.
   * 1. **Doba a podmínky plnění Provedení pilotního provozu**
8. Zhotovitel je povinen poskytnout plnění řádně a včas. Řádně poskytnutým plněním této části (provedení pilotního provozu) se rozumí poskytnutí plnění v rozsahu a za podmínek stanovených touto Rámcovou dohodou nejpozději do 180 kalendářních dní ode dne nabytí účinnosti Smlouvy na pilotní provoz. Plnění se považuje za řádně poskytnuté dnem podpisu Akceptačního protokolu o provedení pilotního provozu.
9. Provedení pilotního provozu SW řízené přístupové vrstvy bude proveden ve třech pobočkách Objednatele, které budou odsouhlaseny oběma stranami v Analytické části pilotního provozu. Dodavatel provede migraci těchto třech poboček do SW řízené přístupové vrstvy a od této doby bude probíhat pilotní provoz v těchto třech pobočkách, který bude trvat minimálně 30 kalendářních dnů.
10. V průběhu pilotního provozu budou provedeny testy na základě testovacích scénářů odsouhlasených v Analytické části za účasti Dodavatele a Objednatele.
11. V případě, že Objednatel neakceptuje vysledky testů provedených na základě testovacích scénářů, zavazuje se Dodavatel bez zbytečného odkladu provést veškeré potřebné úpravy v SW řízené přístupové vrstvě pilotního provozu dle výhrad a připomínek Objednatele. Po provedení potřebných úprav se budou opakovat testovací scénáře dle bodu 3., a to opakovaně až do úplné akceptace bez výhrad.
12. Po provedení testovacích scénářů bude sepsán Akceptační protokol o provedení pilotního provozu, který bude podepsán Pověřenými osobami obou Smluvních stran.
13. VZP ČR se zavazuje poskytovat Dodavateli součinnost při plnění závazků Dodavatele dle této Rámcové dohody, a to zejména poskytovat Dodavateli veškeré informace a podklady potřebné pro Provedení pilotního provozu.
14. Objednatel se zavazuje poskytnout Dodavateli po dobu plnění této části Provedení pilotního provozu testovací prostředí v rozsahu jedné pobočky Objednatele. Testovací prostředí bude umístěno v Ústředí VZP ČR, Orlická 2020/4, Praha 3.
    * 1. **Doba a podmínky plnění Dokumentace k migračnímu procesu**
15. Zhotovitel je povinen poskytnout plnění řádně a včas. Řádně poskytnutým plněním této části Dokumentace migračního procesu se rozumí poskytnutí plnění v rozsahu a za podmínek stanovených touto Rámcovou dohodou nejpozději do 240 kalendářních dní ode dne nabytí účinnosti Smlouvy na pilotní provoz. Plnění se považuje za řádně poskytnuté dnem podpisu Akceptačního protokolu Dokumentace k migračnímu procesu.
16. Řádně vypracovaná dokumentace k migračnímu procesu, tzn. dokumenty:
    * + Popis procesu migrace
      + Podrobný popis migrace

bude předána Objednateli v elektronické verzi v editovatelném formátu (tj. .doc, .docx, .txt, .rtf, .ppt, .xls, .xlsx), a to v termínu (viz odst. 1. tohoto článku 6.1.3.).

1. Před akceptací dokumentace k migračnímu procesu proběhne akceptační procedura popsaná v odst. 4. až 9. tohoto článku. Případná nutnost opakovat akceptační proceduru nemá vliv na povinnost Dodavatele poskytnout plnění řádně a včas dle odst. 1. tohoto článku.
2. O předání a převzetí dokumentace k migračnímu procesu bude sepsán Předávací protokol dokumentace k migračnímu procesu, který bude podepsán Pověřenými osobami obou Smluvních stran.
3. Podepsáním Předávacího protokolu se zahajuje akceptační řízení, ve kterém Objednateli předloží připomínky k vypracované dokumentaci k migračnímu procesu do osmi (8) kalendářních dnů od podepsání příslušného Předávacího protokolu dokumentace k migračnímu procesu.
4. V případě, že Objednatel dokumentaci k migračnímu procesu neakceptuje nebo bude mít k dokumentaci k migračnímu procesu výhrady, zavazuje se Dodavatel bez zbytečného odkladu provést veškeré potřebné úpravy dokumentace k migračnímu procesu dle výhrad a připomínek Objednatele a takto upravenou dokumentaci k migračnímu procesu předat Objednateli opětovně k akceptaci.
5. Dokud Dodavatel nevypořádá veškeré připomínky Objednatele, nebude dokumentace k migračnímu procesu akceptována a bude postupováno obdobně dle ustanovení odst. 4. až 7. tohoto článku.
6. Akceptace řádně vypracované dokumentace k migračnímu procesu bude po vypořádání všech připomínek Objednatele potvrzena podpisem Akceptačního protokolu dokumentace k migračnímu procesu Pověřenými osobami obou Smluvních stran.
7. Objednatel se zavazuje poskytovat Dodavateli součinnost při plnění závazků Dodavatele dle této Rámcové dohody, a to zejména poskytovat Dodavateli veškeré informace a podklady potřebné pro vypracování dokumentace k migračnímu procesu.

## Školení

Objednatel požaduje zajistit výrobcem dodávaných zařízení certifikované školení k problematice administrace a konfigurace SW řízené přístupové vrstvy a všech dodaných zařízení, a to pro 3 pracovníky Objednatele na dobu 5 dnů v akreditovaném školícím zařízení na území ČR v českém nebo slovenském jazyce.

## Technická podpora

Dodavatel se zavazuje poskytovat Záruční podporu v délce 60 měsíců ode dne podpisu příslušného Předávací protokolu. Poskytovaná technická podpora musí zajistit bezporuchový provoz stávající infrastruktury sítě Objednatele a nezpůsobit Objednateli žádné dodatečné náklady spojené s podporou stávající infrastruktury.

Po celou dobu poskytování technické podpory musí být Dodavatelem zajištěno:

1. Technická podpora pokrývá veškeré opravy na dodávaných zařízeních včetně ceny náhradních dílů, nákladů dopravy a práce techniků;
2. Náhradní díly pro použití v provozované technice musí být originální (tj. vyrobené výrobcem příslušného zařízení, pro které jsou náhradní díly určeny, resp. výrobcem příslušného dílu originálního zařízení) nebo ekvivalentní k originálním a zcela kompatibilní s provozovanou technikou. Ekvivalentní náhradní díly musí být prokazatelně explicitně schváleny výrobcem zařízení nebo výrobcem originálního náhradního dílu k použití v předmětném zařízení, a to např. certifikátem, společným prohlášením o shodě, znaleckým posudkem či obdobným dokumentem, který objektivně nezavdá pochybnosti o shodě;
3. Dodavatel je odpovědný za vyřešení servisního požadavku;
4. Dodavatel je odpovědný za případné otevření dalších sekundárních servisních požadavků potřebných ke zprovoznění zařízení;
5. Objednatel musí mít možnost otevřít servisní požadavek u výrobce, i když si není jist, že se jedná o závadu, a to i bez nutnosti její předchozí diagnostiky.

## SLA (Service level agreement) – Smlouva o úrovni služeb

Služby technické podpory budou poskytovány v **SLA parametrech**.

Jedná se o následující požadovanou službu v minimálně níže uvedených požadovaných anebo lepších než požadovaných SLA parametrech. Lepšími parametry se rozumí stejná anebo lepší hodnota parametru pro všechny Objednatelem specifikované a požadované parametry.

Poskytování Záruční podpory spočívá v povinnosti Dodavatele odstraňovat veškeré vady dodaných zařízení vzniklé při provozu zařízení a nefunkčnost některé ze služeb (dále dohromady též jen „vady“) **v režimu 7x24**.

## Služba „Bussines critical“

|  |  |
| --- | --- |
| **Parametr** | **Hodnota** |
| Dostupnost podpory | 7x24 |
| Reakční doba | 4 hodiny od automatického potvrzení doručení servisního požadavku (e-mailu) |
| Maximální doba pro odstranění závady | 24 hodin od automatického potvrzení doručení servisního požadavku (e-mailu) |
| Místa plnění | DC1 na adrese Orlická 2020/4, 130 00 Praha 3  DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9 |

### **Popis služby**:

Služba slouží k řešení bussines critical vad v SW řízené přístupové vrstvě, které mají významný dopad do činnosti Objednatele. Za významný dopad se rozumí ovlivnění práce více než 20% uživatelů.

Reakční doba (Response Time) bude maximálně 4 hodiny od nahlášení vady službou Service Desk. Dodavatel poskytne pracovní sílu, náhradní díly a materiály, které jsou potřebné k tomu, aby SW řízená přístupová vrstva byla uvedena opět do normálního funkčního stavu. Dodavatel identifikuje a opraví špatné funkce a závady. Vyměněné vadné díly se stanou majetkem Dodavatele. Objednatel zajistí a bude zajišťovat od okamžiku nahlášení incidentu případný fyzický přístup Dodavatele k zařízení.

## Služba „Normal“

|  |  |
| --- | --- |
| **Parametr** | **Hodnota** |
| Dostupnost podpory | 7x24 |
| Reakční doba | 4 hodiny od automatického potvrzení doručení servisního požadavku (e-mailu) |
| Maximální doba pro odstranění závady | 2 pracovní dny od automatického potvrzení doručení servisního požadavku (e-mailu) |
| Místa plnění | DC1 na adrese Orlická 2020/4, 130 00 Praha 3  DC2 na adrese ČD Telematika a.s., Pod Táborem 369/8a, 190 00 Praha 9 |

**Popis služby**:

Služba slouží k řešení vad v SW řízené přístupové vrstvě vyjma bussines critical incidentů.

Reakční doba (Response Time) bude maximálně 4 hodiny od automatického potvrzení doručení servisního požadavku (e-mailu) . Dodavatel poskytne pracovní sílu, náhradní díly a materiály, které jsou potřebné k tomu, aby SW řízená přístupová vrstva byla opět uvedena do normálního funkčního stavu. Dodavatel identifikuje a opraví špatné funkce a závady zařízení. Vyměněné vadné díly se stanou majetkem Dodavatele. Objednatel zajistí a bude zajišťovat od okamžiku nahlášení vady fyzický přístup Dodavatele k zařízení.

## Záruky/garance požadované doby opravy (Fix Time) po uplatnění Servisního požadavku

* Dodavatel zajistí, aby bylo zařízení znovu uvedeno do provozu do požadované doby od nahlášení vady formou servisního požadavku.
* Odstranění vady je považováno za dokončené tím, že Dodavatel jeho odstranění ověří k tomu nejvhodnějším a nejprokazatelnějším způsobem a metodou. Okamžikem vyřešení servisního požadavku se rozumí datum a čas uvedený v protokolu o odstranění vady, který bude součástí e- mailu „Oznámení o vyřešení servisního poždavku Dodavatelem“, který bude poslán Objednateli při vyřešení servisního požadavku.
* Ověření může být dosaženo například provedením autodiagnostického testu, samostatného diagnostického testu nebo vizuálním ověřením řádného provozu. Dodavatel podle svého vlastního uvážení určí míru testování nezbytného k ověření, že zařízení bylo opraveno.
* Podle svého vlastního uvážení může Dodavatel dočasně nebo trvale nahradit výrobek za účelem splnění závazku opravy. Náhradní zařízení musí být nové a/nebo ekvivalentní anebo lepší, co do stáří, výkonu a spolehlivosti a musí splňovat veškeré požadavky stanovené touto Rámcovou dohodou. Nahrazená zařízení se stanou vlastnictvím Dodavatele.

**Příloha č. 2 - Specifikace ceny plnění**

|  |  |  |
| --- | --- | --- |
| **Pořadové číslo** | **Popis položky** | **Cena za kus** |
| 1. | **S1 - Fixní přístupový 48 portový přepínač** | 206 069,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S1 - Fixní přístupový 48 portový přepínač |
| Licence k 1 kusu S1 - Fixní přístupový 48 portový přepínač | 86 441,00 Kč |
| 2. | **S2 - Fixní přístupový 48 portový přepínač** | 140 934,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S2 - Fixní přístupový 48 portový přepínač |
| Licence k 1 kusu S2 - Fixní přístupový 48 portový přepínač | 86 441,00 Kč |
| 3. | **S3 - Fixní přístupový 48 portový přepínač** | 117 124,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S3 - Fixní přístupový 48 portový přepínač |
| Licence k 1 kusu S3 - Fixní přístupový 48 portový přepínač | 86 441,00 Kč |
| 4. | **S4 - Fixní přístupový 24 portový přepínač** | 129 206,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S4 - Fixní přístupový 24 portový přepínač |
| Licence k 1 kusu S4 - Fixní přístupový 24 portový přepínač | 53 548,00 Kč |
| 5. | **S5 - Fixní přístupový 24 portový přepínač** | 95 884,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S5 - Fixní přístupový 24 portový přepínač |
| Licence k 1 kusu S5 - Fixní přístupový 24 portový přepínač | 53 548,00 Kč |
| 6. | **S6 - Fixní přístupový 24 portový přepínač** | 72 073,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S6 - Fixní přístupový 24 portový přepínač |
| Licence k 1 kusu S6 - Fixní přístupový 24 portový přepínač | 53 548,00 Kč |
| 7. | **S7 - Modulární 7 slotový přepínač** | 490 527,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S7 - Modulární 7 slotový přepínač |
| Licence k 1 kusu S7 - Modulární 7 slotový přepínač | 304 115,00 Kč |
| 8. | **S8 - Modulární 10 slotový přepínač** | 616 024,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S8 - Modulární 10 slotový přepínač |
| Licence k 1 kusu S8 - Modulární 10 slotový přepínač | 304 115,00 Kč |
| 9. | **S9 - Fixní agregační 24 portový přepínač** | 366 434,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S9 - Fixní agregační 24 portový přepínač |
| Licence k 1 kusu S9 - Fixní agregační 24 portový přepínač | 148 746,00 Kč |
| 10. | **S10 - Fixní agregační 48 portový přepínač** | 396 606,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu S10 - Fixní agregační 48 portový přepínač |
| Licence k 1 kusu S10 - Fixní agregační 48 portový přepínač | 242 371,00 Kč |
| 11. | **SM1 - Stohovací modul pro fixní přepínače S1 až S6** | 17 960,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu SM1 - Stohovací modul pro fixní přepínače S1 až S6 |  |
| 12. | **RZ1 - Redundantní napájecí zdroj pro přepínače S1 až S6** | 15 379,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu RZ1 - Redundantní napájecí zdroj pro přepínače S1 až S6 |  |
| 13. | **RZ2 - Redundantní napájecí zdroj pro přepínače S1 až S6** | 23 349,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu RZ2 - Redundantní napájecí zdroj pro přepínače S1 až S6 |  |
| 14. | **RŘM - Redundantní řídící modul do modulárního přepínače S7 a S8** | 314 611,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu RŘM - Redundantní řídící modul do modulárního přepínače S7 a S8 |  |
| 15. | **C1 - 48 portová karta do modulárního přepínače S7 a S8** | 142 010,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu C1 - 48 portová karta do modulárního přepínače S7 a S8 |  |
| 16. | **C2 - 48 portová karta do modulárního přepínače S7 a S8** | 164 798,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu C2 - 48 portová karta do modulárního přepínače S7 a S8 |  |
| 17. | **C3 - 48 portová karta do modulárního přepínače S7 a S8** | 91 491,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu C3 - 48 portová karta do modulárního přepínače S7 a S8 |  |
| 18. | **AP1 - Přístupový bod** | 23 889,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu AP1 - Přístupový bod |
| Licence k 1 kusu AP1 - Přístupový bod | 15 750,00 Kč |
| 19. | **AP2 - Přístupový bod** | 11 436,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu AP2 - Přístupový bod |
| Licence k 1 kusu AP2 - Přístupový bod | 15 435,00 Kč |
| 20. | **R1 - Směrovač datového centra** | 2 254 779,00 Kč |
| Záruční podpora v délce 60 měsíců k 1 kusu R1 - Směrovač datového centra |
| Licence k 1 kusu R1 - Směrovač datového centra | 934 547,00 Kč |
| 21. | **Školení certifikované výrobcem pro 3 pracovníky VZP ČR v minimální délce 5 dnů** | 250 000,00 Kč |
| 22. | **Pilotní provoz SW řízené přístupové vrstvy sítě - Analytická část** | 1 665 000,00 Kč |
| 23. | **Pilotní provoz SW řízené přístupové vrstvy sítě - Provedení pilotního provozu** | 2 775 000,00 Kč |
| 24. | **Pilotní provoz SW řízené přístupové vrstvy sítě - Dokumentace k migračnímu procesu** | 1 110 000,00 Kč |

**Příloha č. 3 – Jmenný seznam členů servisního týmu Dodavatele**

**Dodavatel se zavazuje,** žeode dne nabytí účinnosti první Smlouvy uzavřené na základě této Rámcové dohody, mít k dispozici servisní tým, a to po celou dobu plnění poskytovaného na základě Smluv uzavřených dle této Rámcové dohody. Servisní tým, který se bude podílet na plnění (poskytování Záruční podpory a Pilotní provoz) poskytovaného na základě příslušných Smluv dle této Rámcové dohody, bez ohledu na to, zda jde o zaměstnance Dodavatele nebo jsou osoby v jiném vztahu k Dodavateli (dále též jen „servisní tým“).

**Dodavatel se zavazuje, že** plnění dle Rámcové dohody bude poskytováno pouze členy servisního týmu, kteří jsou uvedeni v této Příloze č. 3 Rámcové dohody.

Všichni členové servisního týmu musí splňovat „Obecné požadavky na členy servisního týmu“.

**Obecné požadavky na členy servisního týmu**

Všichni členové servisního týmu musí být schopni komunikovat písemně i ústně v českém nebo slovenském jazyce na velmi dobré úrovni, tj. na úrovni potřebné pro správné a přesné pochopení komunikace s Objednatelem při poskytování plnění. Dodavatel může tento požadavek splnit tak, že pro případného člena servisního týmu, který výše uvedený požadavek na jazykové znalosti nesplňuje, zajistí Dodavatel překladatele, resp. při mluvené komunikaci tlumočníka s jazykovými znalostmi na takové úrovni překládaného českého či slovenského jazyka, aby nemohlo dojít k nedorozuměním při poskytování plnění v důsledku překladu, resp. tlumočení a aby případné překládání/tlumočení probíhalo způsobem, kterým nedojde k porušení podmínek Rámcové dohody, tj. nebude snížena kvalita Dodavatelem poskytovaných služeb. Za nedorozumění a případné škody způsobené překladem nebo jazykovým nedorozuměním odpovídá plně Dodavatel. Finanční náklady na případného překladatele/tlumočníka se považují za náklady Dodavatele zahrnuté v ceně za poskytnuté služby.

**Požadavky na odbornost členů servisního týmu:**

Dodavatel se zavazuje mít v servisním týmu takové technické specialisty, aby v souhrnu splňovali (tj. zajišťovali) všechny požadavky na odbornost členů servisního týmu (viz písm. a) až c) níže). Každý člen servisního týmu musí splňovat alespoň jednu odbornost, může však splňovat i více odborností zároveň. **Servisní tým Dodavatele pro zajištění předmětu plnění musí sestávat z minimálně 2 (dvou) odborných pracovníků splňujících v souhrnu všechny níže uvedené požadavky na odbornou kvalifikaci.** Konkrétní počet členů servisního týmu stanoví dle svých možností Dodavatel. Nikdo kromě těchto členů týmu není oprávněn servisní služby provádět. Konkrétní počet členů servisního týmu se může v průběhu trvání Rámcové dohody měnit, vždy však musí být splněny veškeré Objednatelem stanovené požadavky na servisní tým a počet členů nesmí klesnout pod 2.

**Jednotlivé požadavky na odbornost:**

1. 1 technický specialista s minimálně 3 roky praxe v oblasti správy a podpory bezdrátových (WiFi) sítí;
2. 1 technický specialista s minimálně 3 roky praxe v oblasti správy a podpory přepínačů;
3. 1 technický specialista s minimálně 3 roky praxe v oblasti bezpečnosti počítačových sítí.

**Všichni členové servisního týmu musí mít certifikát potvrzující certifikaci k servisní práci na provozovaných zařízeních Cisco v úrovni Cisco Certified Internetwork Expert. Certifikát nesmí být ve stavu „expired“.**

|  |  |
| --- | --- |
| Certifikace: | CCIE #55858 Routing & Switching (Enterprise)  [www.cisco.com/go/verifycertificate](http://www.cisco.com/go/verifycertificate)  Verification Code: 427994169610AMZM |
| Jméno, příjmení: | XXXXXXXXXXX |
| E-mail: | XXXXXXXXXXX |
| Telefon: | XXXXXXXXXXX |
| Plynulá komunikace v českém/slovenském jazyce: | ANO |
| Praxe: | 06/2019 – doposud  Team Leader, DC Networking  ALEF NULA, a.s., Pernerova 691/42, 18600 Praha 8  Information and communication technologies  07/2016 – 06/2019  Senior Systems Engineer  ALEF NULA, a.s., Pernerova 691/42, 18600 Praha 8  Information and communication technologies  07/2015 – 06/2016  Senior ICT Engineer  T-Systems Slovakia s.r.o., Žriedlová 13, 040 01 Košice, Slovenská republika  Information and communication technologies  Date: 09/2013 – 01/2016  Linux Network Software Developer  University of Žilina, Univerzitná 8215/1, 010 26 Žilina, Slovenská republika  Information and communication technologies  Splňuje požadavek na nejméně 3 roky praxe v oblasti správy a podpory bezdrátových (WiFi) sítí, přepínačů a v oblasti bezpečnosti počítačových sítí.  **Certifikace**  CCIE #55858 Routing & Switching (Enterprise)  CCNP Datacenter  CCNP Devnet  Cisco DevNet Specialist - Data Center Automation and Programmability  AWS Certified Solution Architect – Associate  AWS Certified Developer – Assocaite  AWS Authorized Instructor  Cisco Certified Instructor (CCSI) #35493  ITIL Foundation |

|  |  |
| --- | --- |
| Certifikace: | CCIE #55892 Routing & Switching (Enterprise)  [www.cisco.com/go/verifycertificate](http://www.cisco.com/go/verifycertificate)  Verification Code: 428064172601BSVG |
| Jméno, příjmení: | XXXXXXXXXXX |
| E-mail: | XXXXXXXXXXX |
| Telefon: | XXXXXXXXXXX |
| Plynulá komunikace v českém/slovenském jazyce: | ANO |
| Praxe: | 2015 - dosud  Senior System Engineer  ALEF NULA, a.s.  Informační a komunikační technologie    2013 - 2015  System Engineer  ALEF NULA, a.s.  Informační a komunikační technologie    **Nejvyšší dosažené vzdělání**  2009 - 2012  Univerzita Pardubice, Fakulta elektrotechniky a informatiky  Vysokoškolské, magisterské  Splňuje požadavek na nejméně 3 roky praxe v oblasti správy a podpory bezdrátových (WiFi) sítí, přepínačů a v oblasti bezpečnosti počítačových sítí.  **Certifikace**  CCIE Routing & Switching  CCNP Routing & Switching  CCNA Routing & Switching |

**Změna členů servisního týmu**

Změna člena servisního týmu je upravena v čl. XIV. odst. 5. a násl. této Rámcové dohody. Při každé změně člena servisního týmu musí být dále splněny níže uvedené podmínky:

* Nový člen servisního týmu musí splňovat všechny **Obecné požadavky na členy servisního týmu**;
* Nový člen servisního týmu musí prokázat splnění požadavků na člena servisního týmu:
* Vyplněním tabulky, která je součástí této Přílohy č. 3;
* Předložením strukturovaného profesního životopisu, který bude obsahovat alespoň jméno, příjmení, přehled relevantní praxe a znalostí k prokázání splnění požadavků Objednatele a seznam profesní certifikace;
* Doložením příslušného povinného certifikátu k prokázání technické kvalifikace nebo jeho kopii (tento certifikát může být i v anglickém jazyce, Objednatel si však vyhrazuje možnost vyžádat si od Dodavatele překlad takového certifikátu do českého jazyka).

**Příloha č. 4 – Podmínky pro přístup Dodavatele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR**

**Podmínky pro přístup Dodavatele do vnitřní sítě VZP ČR  
prostřednictvím VPN VZP ČR**

**(dále jen „Podmínky“ nebo „dokument“)**

Pro zajištění řádného plnění Dodavatele podle příslušné Smlouvy uzavřené na základě této Rámcové dohody (dále jen „Smlouvy“), jejíž přílohou jsou tyto Podmínky a za účelem současného zajištění bezpečnosti vnitřní sítě VZP ČR a jejích informačních systémů (dále jen „IS VZP ČR“) jsou těmito Podmínkami stanoveny vzájemné povinnosti Smluvních stran, které souvisejí se vzdáleným přístupem Dodavatele do vnitřní sítě VZP ČR, IS VZP ČR a k informacím prostřednictvím VPN VZP ČR (dále též jen „VPN přístup“).

**Čl I. Použité zkratky**

|  |  |
| --- | --- |
| Zkratka | Význam |
| CA VZP ČR | Interní certifikační autorita VZP ČR vydává certifikáty určené pro VPN přístup Uživatelů a řídí životní cyklus těchto certifikátů. |
| VPN VZP ČR | Virtuální privátní síť VZP ČR |
| VZP ČR | Všeobecná zdravotní pojišťovna České republiky |

**Čl. II. Použité pojmy**

|  |  |
| --- | --- |
| **Pojem** | **Význam** |
| Uživatel | Fyzická osoba, která se na plnění závazků Dodavatele dle Smlouvy přímo podílí a k tomu potřebuje VPN přístup. Uživatel není ve smluvním vztahu k VZP ČR, ale k Dodavateli, popř. k jeho poddodavateli. |
| Certifikát | Digitální prostředek sloužící k ověření elektronické identity Uživatele při VPN přístupu. |
| Privátní klíč | Část šifrovacího klíče certifikátu, který slouží k asymetrickému šifrování informací. |
| VPN přístup | Vzdálený přístup realizovaný mezi koncovým zařízením Uživatele připojeným z veřejné sítě Internet a přístupovým bodem VZP ČR umožňujícím přístup do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR. |
| Validační e-mail | E-mailová zpráva zasílaná VZP ČR na e-mail Uživatele uvedený v Žádosti, ověřující, zda Uživatel je stále na tomto e-mailu dostupný. |

**Čl. III. Předmět**

1. VZP ČR zřídí Dodavateli VPN přístup a zajistí jeho využití po určenou dobu, a to za podmínek dále uvedených v tomto dokumentu.
2. VPN přístup bude Dodavatelem využíván prostřednictvím Dodavatelem určených osob, které se podílejí nebo budou podílet na plnění závazků Dodavatele podle Smlouvy (dále jen „Uživatel“).
3. VZP ČR zřídí VPN přístup Dodavateli pouze v případě, bude-li to pro plnění Dodavatele podle Smlouvy potřebné.

**Čl. IV. Zřízení VPN přístupu**

1. Zřízením VPN přístupu Dodavateli se rozumí proces, kterým je Uživateli vydán certifikát a předány autentizační údaje, pomocí nichž může Uživatel přistupovat do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR.
2. Dodavatel žádá o zřízení VPN přístupu pro konkrétního Uživatele písemně prostřednictvím formuláře „Žádost o zřízení VPN přístupu (dále jen „Žádost“), viz Příloha A těchto Podmínek.
3. Dodavatel odpovídá za to, že všechny údaje uvedené v Žádosti jsou správné a platné. V případě, že dojde ke změně některého z údajů uvedených v bodu 2) Žádosti, je Dodavatel povinen nejpozději do 8 kalendářních dnů od změny předložit číslovaný dodatek k Žádosti s vyznačením požadovaných změn (dále jen „Dodatek“). Dodatek Dodavatel předkládá v souladu s první větou odst. 7. tohoto článku. Dodatek posoudí VZP ČR obdobně jako Žádost (k tomu viz odst. 8. tohoto článku).
4. Dodavatel žádá o VPN přístup pro Uživatele maximálně na dobu účinnosti Smlouvy.
5. Pokud se jedna a tatáž fyzická osoba podílí na plnění podle více smluv uzavřených mezi Dodavatelem a VZP ČR, předkládá Dodavatel VZP ČR vždy samostatnou Žádost pro Uživatele pro každou takovou smlouvu.
6. Dodavatel musí v Žádosti u Uživatele uvést vždy číslo jeho mobilního telefonu a jeho   
   e-mailovou adresu.
7. Vyplněnou Žádost zasílá Dodavatel prostřednictvím elektronické pošty na e-mailovou adresu Service Desku VZP ČR [servicedesk@vzp.cz](mailto:servicedesk@vzp.cz), přičemž e-mailová zpráva musí být podepsána uznávaným elektronickým podpisem Pověřené osoby uvedené ve Smlouvě za Dodavatele. E-mailovou zprávu zasílá Dodavatel nejpozději 10 pracovních dnů před datem, od kterého Dodavatel požaduje zřídit Uživateli VPN přístup.
8. VZP ČR doručenou Žádost posoudí z hlediska potřebnosti VPN přístupu pro předmětné plnění Dodavatele, formálních a věcných náležitostí, případně požádá Dodavatele o doplnění (opravu) Žádosti.
9. VZP ČR zašle Dodavateli a v kopii Uživateli prostřednictvím elektronické pošty informaci o schválení/schválení s omezením/neschválení Žádosti.

Přičemž v případě:

* 1. schválení Žádosti s omezením:

VZP ČR uvede změny oproti Žádosti (např. omezení doby požadovaného VPN přístupu apod.) a zdůvodnění;

* 1. neschválení Žádosti:

VZP ČR neschválení zdůvodní.

1. V případě schválení Žádosti nebo schválení Žádosti s omezením zasílá VZP ČR následně na e-mailovou adresu Uživatele též informace potřebné pro zřízení VPN přístupu, tj.  postup, jakým způsobem si Uživatel vygeneruje certifikát pro VPN přístup, postup, jakým způsobem si Uživatel obnoví certifikát a postup pro změnu jemu přiděleného výchozího hesla na přihlašovací heslo/resp. obnovu platného přihlašovacího hesla, včetně pravidel pro jeho tvorbu a dobu platnosti. Informace obsahují rovněž údaj o době platnosti certifikátu.
2. VZP ČR zasílá Uživateli na jeho e-mailovou adresu uvedenou v Žádosti přidělené uživatelské jméno a zároveň na jeho mobilní telefonní číslo uvedené v Žádosti výchozí heslo.
3. Veškeré údaje uvedené v odst. 10. a 11. tohoto článku přebírá Uživatel jménem Dodavatele.

**Čl. V. Znemožnění VPN přístupu**

1. Znemožněním VPN přístupu se rozumí stav, kdy Uživatel nemůže přistupovat do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR.
2. VPN přístup je Uživateli znemožněn (nikoliv ukončen):
   1. z důvodu, že si Uživatel včas v době platnosti certifikátu neobnovil certifikát, tj. Uživateli vypršela doba platnosti jeho certifikátu (k tomu srov. Čl. VIII., odst. 6., písm. h.);
   2. z důvodu, že si Uživatel včas nezměnil své přihlašovací heslo, které mu slouží k VPN přístupu, tj. Uživateli vypršela doba platnosti jeho přihlašovacího hesla.
3. O znemožnění VPN přístupu dle odst. 2. tohoto článku **není** VZP ČR povinna Uživatele ani Dodavatele informovat.
4. VPN přístup, jenž byl znemožněn dle odst. 2., písm. a. a písm. b. tohoto článku, si Uživatel obnovuje sám (tj. na základě vlastní iniciativy prostřednictvím VZP ČR). Nečinnost Uživatele nebo Dodavatele v tomto směru nemůže jít k tíži VZP ČR. Obnovení VPN přístupu lze Uživatelem provést v rámci doby, na kterou byl VPN přístup podle Žádosti schválen.

# Čl. VI. Pozastavení VPN přístupu

1. Pozastavením VPN přístupu se rozumí jednostranný proces na straně VZP ČR, kterým VZP ČR z dále uvedených důvodů **dočasně** znemožní Uživateli přístup do vnitřní sítě VZP ČR zablokováním jeho účtu v doméně VZP ČR / zneplatněním certifikátu apod.
2. VZP ČR si vyhrazuje právo pozastavit Uživateli VPN přístup:

#### v případě zjištění porušení nebo podezření na nedodržení některého ustanovení tohoto dokumentu, příp. při nereakci na validační e-mail nebo při podezření na bezpečnostní událost nebo bezpečnostní incident související s osobou Uživatele/ Dodavatele, příp. VPN přístupem (dále jen „Událost“);

#### z důvodu provozní nebo technické odstávky VPN VZP ČR realizované VZP ČR (dále vše jen „Odstávka“).

1. VZP ČR informuje Dodavatele o pozastavení VPN přístupu Uživateli formou e-mailové zprávy zaslané Dodavateli se zdůvodněním svého postupu, a pokud je to možné, i o předpokládané době pozastavení VPN přístupu v případě Odstávky.
2. Po vyhodnocení Události informuje VZP ČR Dodavatele **o opětovném umožnění** **VPN přístupu** Uživateli nebo **o ukončení VPN přístupu** Uživatele, přičemž uvede zdůvodnění svého postupu a své zjištění.
3. Dodavatel může požádat o pozastavení VPN přístupu Uživateli.

# Čl. VII. Ukončení VPN přístupu

1. Ukončením VPN přístupu se rozumí proces, kdy Uživatel/ Dodavatel pozbývá možnosti přístupu do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR, **tj. Uživateli je trvale zneplatněn jeho certifikát a zablokován jeho účet v doméně VZP ČR**.
2. VZP ČR ukončí Uživateli/ Dodavateli VPN přístup:
   1. v případě uplynutí doby, na kterou byl VPN přístup podle Žádosti schválen;
   2. dnem ukončení účinnosti Smlouvy;
   3. na základě žádosti Dodavatele;
   4. na základě žádosti Uživatele;
   5. dle Čl. VI., odst. 4. tohoto dokumentu (po příslušném vyhodnocení Události);
   6. na základě žádosti Dodavatele dle odst. 3., písm. d., e. a f. tohoto článku.
3. Dodavatel je povinen vždy prostřednictvím Service Desku VZP ČR na e-mail: servicedesk@vzp.cz nebo telefonicky na tel.: 950 220 000,

bezodkladně informovat VZP ČR v případech, když:

* 1. došlo ke ztrátě/podezření na ztrátu, k podezření na kompromitaci privátního klíče Uživatele;
  2. došlo k podezření na kompromitaci přihlašovacího hesla k přidělenému uživatelskému jménu Uživatele sloužícímu pro VPN přístup;
  3. došlo k podezření na ztrátu/odcizení nebo ke ztrátě/ odcizení koncového zařízení Uživatele, z něhož realizuje VPN přístup;

bezodkladně žádat VZP ČR o ukončení VPN přístupu v případech, když:

* 1. došlo/dojde k ukončení smluvního vztahu mezi Uživatelem a Dodavatelem;
  2. Uživatel se přestal/přestane podílet na plnění závazků Dodavatele dle Smlouvy;
  3. došlo/dojde k ukončení smluvního vztahu mezi Dodavatelem a jeho podDodavatelem, je-li Uživatel ve smluvním vztahu k tomuto podDodavateli.

**Odpovědnost za veškeré činnosti realizované pod přiděleným účtem příslušného Uživatele v doméně VZP ČR nese do splnění příslušné povinnosti podle tohoto odstavce Dodavatel.**

1. VPN přístup bude v případech uvedených:
   1. pod písm. a. nebo b. odst. 2. tohoto článku ukončen příslušným dnem;
   2. pod písm. c. nebo d. odst. 2. tohoto článku do 3 pracovních dnů od doručení žádosti o ukončení VPN přístupu, pokud nebude v žádosti o ukončení VPN přístupu požadováno pozdější datum ukončení;
   3. pod písm. e. nebo f. odst. 2. tohoto článku po vyhodnocení Události /po doručení žádosti VZP ČR.
2. V případě ukončení VPN přístupu dle odst. 2., písm. d., tohoto článku je **Uživatel** povinen o této skutečnosti neprodleně informovat Dodavatele; splnění této jeho povinnosti si zajistí Dodavatel.

# Čl. VIII. Povinnosti Dodavatele a Uživatele

1. Dodavatel je povinen dodržovat všechna ustanovení tohoto dokumentu a zajistit jejich dodržování jednotlivými Uživateli Dodavatel.
2. **Dodavatel je povinen:**
   1. prokazatelně **seznámit** Uživatele s  právy a povinnostmi vyplývajícími pro něj z tohoto dokumentu a prokazatelně Uživatele **poučit** o jeho povinnostech uvedených v tomto dokumentu, a to nejpozději v den podání příslušné Žádosti a na vyzvání VZP ČR tuto skutečnost také VZP ČR ve lhůtě uvedené v příslušné písemné výzvě, která nebude kratší než 10 pracovních dnů, doložit;
   2. zajistit, aby Uživatel dodržoval povinnosti a postupy vyplývající pro něj z tohoto dokumentu;
   3. zajistit, že jsou Uživatelem dodržována taková bezpečnostní opatření, která zamezí narušení nebo ohrožení bezpečnosti vnitřní sítě VZP ČR, IS VZP ČR a jejich informací.
3. Dodavatel nese plnou odpovědnost za nedodržení povinností Uživatelem daných Uživateli tímto dokumentem.
4. VZP ČR je oprávněna kontrolovat plnění ustanovení tohoto dokumentu na straně Dodavatele. Dodavatel je povinen poskytnout VZP ČR nezbytné podklady, součinnost, případně umožnit kontrolu na místě.
5. Dodavatel je dále povinen zajistit, aby Uživatel realizoval VPN přístup pouze z koncového zařízení, které:
6. je chráněno antivirovou a antimalwarovou ochranou a má aktuální virovou databázi;
7. má instalováno a má aktivní (zapnuto) firewalové řešení operačního systému, příp. HIDS/HIPS;
8. má instalovány dostupné bezpečnostní záplaty a aktualizace zveřejněné výrobcem operačního systému a aplikací a operační systém je podporovaný výrobcem;
9. má nastaveno uzamčení koncového zařízení v případě nečinnosti Uživatele;
10. má chráněn přístup do BIOS koncového zařízení;
11. má šifrován pevný disk koncového zařízení;
12. umožňuje přístup ke koncovému zařízení pouze po zadání přihlašovacích údajů.
13. Povinnosti Uživatele:
14. realizovat přístup do vnitřní sítě VZP ČR pouze prostřednictvím VPN VZP ČR;
15. před prvním přístupem do vnitřní sítě VZP ČR si musí změnit výchozí heslo předané VZP ČR na přihlašovací heslo;
16. pro přístup do vnitřní sítě VZP ČR používat jako přihlašovací heslo unikátní, tj. heslo, které není shodné s jinými hesly používanými Uživatelem (kdekoliv);
17. nesmí sdílet s třetími osobami své přístupové údaje ani vydaný certifikát určený pro VPN přístup;
18. nesmí sdílet VPN připojení s jiným zařízením prostřednictvím sdílení připojení na síťové úrovni;
19. zajistit ochranu privátního klíče a vydaného certifikátu proti jeho zneužití;
20. generovat certifikát pro VPN přístup na koncové zařízení se silnou ochranou privátního klíče;
21. obnovit si vydaný certifikát nejdříve měsíc před uplynutím doby jeho platnosti;
22. neukládat své přihlašovací údaje pro VPN přístup do koncového zařízení;
23. nezasahovat do konfiguračních souborů a nastavení VPN klienta dodaného ze strany VZP  ČR;
24. ukončit VPN přístup (navázané spojení) v případě, že koncové zařízení nechává bez dozoru;
25. nepokoušet se narušit bezpečnost vnitřní sítě VZP ČR;
26. **bezodkladně** žádat VZP ČR prostřednictvím Service Desk VZP ČR tel.: 952220000 v době PO - PA od 8:30 do 16:30 nebo kdykoliv na e-mail: servicedesk@vzp.cz:
    * 1. o zneplatnění platného certifikátu v případě podezření na kompromitaci privátního klíče;
      2. o zneplatnění platného certifikátu a zablokování přístupových údajů sloužících k VPN přístupu v případě podezření na kompromitaci/ ztrátu/odcizení koncového zařízení nebo přístupových údajů;
      3. o zablokování přístupových údajů k VPN přístupu v případě zjištění dalších hrozeb narušení bezpečnosti vnitřní sítě VZP ČR, např. výskyt spywaru.

Odpovědnost za veškeré činnosti realizované pod přiděleným účtem příslušného Uživatele v doméně VZP ČR nese do splnění příslušné povinnosti podle tohoto písm. m. Dodavatel.

1. chránit informace získané při VPN přístupu a to i tehdy, pokud přímo nesouvisejí s plněním dle Smlouvy, za což nese i osobní odpovědnost;
2. zachovávat mlčenlivost o všech skutečnostech, se kterými se seznámil v rámci plnění Smlouvy a které nejsou veřejně známé nebo veřejně dostupné;
3. vzít na vědomí, že VZP ČR je oprávněna monitorovat přístupy Uživatele do systémů a vnitřní sítě VZP ČR a je oprávněna pozastavit/ukončit Uživateli VPN přístup v případě nesplnění jeho povinností a požadavků uvedených v tomto dokumentu;
4. vzít na vědomí, že osobní údaje uvedené v Žádosti VZP ČR zpracovává z titulu oprávněného zájmu k zajištění účelu poskytnutí přihlašovacích údajů Uživateli a jednoznačnému přidělení vydaného certifikátu pro VPN přístup;
5. odpovědět na validační e-mail VZP ČR nejpozději do 14 kalendářních dnů ode dne, kdy mu byl doručen.

# Čl. IX. Sankce a náhrada škody

1. Pokud Dodavatel nesplní své povinnosti stanovené v Čl. VIII., odst. 2., písm. a. tohoto dokumentu, tj. že ve lhůtě uvedené v příslušné písemné výzvě nedoloží VZP ČR příslušné skutečnosti, je Dodavatel povinen za každý den prodlení zaplatit VZP ČR smluvní pokutu ve výši 5 000 Kč.
2. Za porušení jednotlivých povinností daných tímto dokumentem Dodavateli:
3. v Čl. IV., odst. 3. tohoto dokumentu nebo
4. v Čl. VII., odst. 3., písm. a. až f. tohoto dokumentu nebo
5. v Čl. VIII., odst. 2., písm. a. tohoto dokumentu, tj. že Uživatele neseznámí s jeho právy a povinnostmi nebo nepoučí Uživatele o jeho povinnostech vyplývajících pro Uživatele z tohoto dokumentu nebo
6. v Čl. VIII., odst. 2., písm. c. nebo d. tohoto dokumentu nebo
7. v Čl. VIII. odst. 5. písm. a. až g. tohoto dokumentu

je Dodavatel povinen zaplatit VZP ČR v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 100 000 Kč, a to i opakovaně.

1. Za porušení jednotlivých povinností daných tímto dokumentem Uživateli v Čl. VIII., odst. 6., písm. a. až l. tohoto dokumentu je Dodavatel povinen zaplatit VZP ČR v každém jednotlivém případě porušení příslušné povinnosti smluvní pokutu ve výši 100 000 Kč, a to i opakovaně.
2. Pokud dojde současně k porušení jedné a téže povinnosti uložené tímto dokumentem Dodavateli i Uživateli, lze příslušnou sankci uplatnit vůči Dodavatel pouze 1x; tím není vyloučena možnost opakovaného postihu Dodavatele, pokud opětovně k porušení jedné a téže povinnosti dojde.
3. Odpovědnost za škodu se řídí ustanovením § 2894 a násl. občanského zákoníku. Sjednáním ani zaplacením smluvní pokuty není dotčeno právo oprávněné smluvní strany na náhradu škody v celém rozsahu.
4. Za škodu způsobenou porušením povinností stanovených tímto dokumentem odpovídá Dodavatel, a to jak za škody způsobené porušením jeho povinností, tak za škody způsobené porušením povinností Uživatelem. Uživatel se pro účely tohoto ustanovení považuje za pomocníka Dodavatele ve smyslu § 2914 věta první občanského zákoníku.

# Čl. X. Závěrečná ustanovení

1. Pokud není v těchto Podmínkách výslovně stanoveno jinak, komunikují Dodavatel a VZP ČR ve věci VPN přístupu prostřednictvím oprávněných osob uvedených ve Smlouvě.
2. V případě, že v době trvání Smlouvy bude nutné přijmout takové bezpečnostní opatření, které vyvolá potřebu upravit tyto Podmínky, zejména bude-li se jednat o bezpečnostní opatření směřující ke zlepšení systému řízení bezpečnosti informací ve VZP ČR, řešení kybernetického bezpečnostního incidentu a s tím spojené potřeby minimalizace vzniklého bezpečnostního rizika nebo o povinnost přijmout opatření vydané Úřadem dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů, zavazují se smluvní strany Smlouvy vyvinout maximální součinnost směřující k uzavření dodatku ke Smlouvě, kterým budou tyto Podmínky odpovídajícím způsobem upraveny.
3. Uzavírání dodatku ke Smlouvě, jakož i jeho uveřejňování se řídí příslušnými ustanoveními Smlouvy.

**Příloha A**

**k Podmínkám pro přístup Dodavatele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR**

***(Formulář)***

**Žádost o zřízení/pozastavení/ukončení**2) **VPN přístupu   
Dodavatele do vnitřní sítě VZP ČR**

1. ***Smlouva, na základě které je/byl VPN přístup pro Dodavatele prostřednictvím Uživatele požadován:***

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Č. j. Smlouvy |  | | Dodavatel: |  |
| Účinnost Smlouvy od: |  | | Účinnost Smlouvy do: |  |
| Jméno a příjmení Pověřené osoby Dodavatele dle Smlouvy: | | |  | |
| Zdůvodnění potřebnosti zřízení VPN přístupu | |  | | |

1. ***Fyzická osoba, pro niž je/byl VPN přístup požadován (Uživatel):***

|  |  |  |  |
| --- | --- | --- | --- |
| Jedná se o fyzickou osobu: | | ve vztahu k Dodavateli/podDodavateli 1) | |
| Jméno: |  | Příjmení, titul: |  |
| E-mail: |  | | |
| Mobilní telefon: |  | | |
| Zaměstnán u Dodavatele/jiný vztah k Dodavateli: |  | IČO podDodavatele:  IČO fyzické osoby |  |

*1) nehodící škrtněte, pokud uvedete podDodavatele, doplňte jeho název*

1. ***VPN přístup:***

|  |  |  |
| --- | --- | --- |
| VPN přístup požadován zřídit/ pozastavit/ukončit: 2) | od: | do: |

*2) nehodící škrtněte*

…………………………………

datum a podpis

*Pověřené osoby uvedené v Rámcové dohodě na straně Dodavatele*