Smlouva o dílo

uzavřená dle ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění, níže uvedeného dne, měsíce a roku, mezi:

AUTOCONT a.s.

Sídlo: Hornopolní 3322/34, 702 00 Ostrava – Moravská Ostrava
Jednající: Lukáš Jurča, ředitel krajského obchodního zastoupení
Bankovní spojení: Česká spořitelna a.s.
číslo účtu: 6563752/0800
IČ: 04308697
DIČ: CZ04308697
spisová značka OR: B 11012 vedená u Krajského soudu v Ostravě
číslo smlouvy Zhotovitele: RCS-230083
na straně jedné (dále jen jako „zhotovitel“)

a

Vojenská nemocnice Olomouc

Sídlo: Sušilovo nám. 1/5, Klášterní Hradisko, 779 00 Olomouc
IČ: 608 00 691
Zastoupena: plk. gšt. v. z. MUDr. Martin Svoboda, ředitel
na straně druhé (dále jen jako „objednatel“)

(dále společně zhotovitel a objednatel jen jako „smluvní strany“)

I.
Úvodní prohlášení

Smluvní strany prohlašují a činí nesporným, že tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem **„VN Olomouc – Zvýšení kyberbezpečnosti“, a to pro její část č. 1 „Segmentace sítě“**.

(dále jen jako „veřejná zakázka“)

II.

Dílo

Smluvní strany prohlašují a činí nesporným, že na základě této smlouvy se zhotovitel zavazuje provést pro objednatele na svůj náklad a nebezpečí dílo představující:

- dodávku dvou fyzických firewallů v HA režimu pro interní segmentaci sítě, dodávku switchů pro satelitní datové rozvaděče, s tím související nezbytné rozšíření stávajících centrálních switchů a dodávku propojovacího příslušenství a rozšíření licencí obslužných softwarů,
- dodávku prací tj. implementace do technologického prostředí zadavatele (instalace, konfigurace, převod konfigurace stávajících switchů na nově dodanou techniku, převod provozu a rozšíření technologie 802.1X do provozu celé nemocnice)

a to v souladu se zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, a objednatel se zavazuje řádně a včas provedené dílo převzít a zaplatit za něj zhotoviteli cenu.

(dále jen jako „dílo“)

III.
Cena díla a platební podmínky

Smluvní strany prohlašují a činí nesporným, že:

a) celková cena díla činí 13.318.180,00 Kč (slovy: třináctmilionůtřistaosmnácttisícjednostoosmdesátkorun) a je nejvýše přípustná (nepřekročitelná) a platná a účinná po celou dobu provádění díla na základě této smlouvy, která zahrnuje mj. dodávku hardwaru a softwaru a dodávku prací včetně servisní podpory výrobce od protokolárního předání díla po doby trvání uvedené ve specifikaci bez vad a nedodělků;

b) součástí ceny díla jsou tak i veškeré další související vynaložené náklady neuvedené v písm. a) tohoto čl. smlouvy nezbytné k řádnému a včasnému provedení díla s tím, že zhotovitel je oprávněn navýšit cenu díla o příslušnou sazbu DPH či jinou daň v souladu s platnými právními předpisy.

Objednatel prohlašuje a činí nesporným, že je povinen zaplatit zhotoviteli cenu díla na základě faktury – daňového dokladu, jejíž přílohou bude i předávací protokol ve smyslu čl. IV. písm. c) anebo e) této smlouvy, kterou je zhotovitel povinen vystavit v souladu s příslušnými právními předpisy

bezodkladně po provedení díla bez vad a nedodělků, a to bezhotovostním převodem na bankovní účet zhotovitele č. 6563752/0800, se splatností 21 dnů ode dne jejího vystavení.

Smluvní strany dále prohlašují a činí nesporným, že objednatel je oprávněn vrátit zhotoviteli vystavenou fakturu – daňový doklad v případě, že příslušná faktura – daňový doklad nebude mít některou ze zákonných či smluvních náležitostí či příloh s tím, že v takovém případě je zhotovitel povinen vystavit po doručení vrácené faktury – daňového dokladu bez zbytečného odkladu novou fakturu – daňový doklad se všemi zákonnými i smluvními náležitostmi včetně příloh. Od okamžiku doručení nové faktury – daňového dokladu dle předchozí věty počíná objednateli běžet nová doba splatnosti.

IV.
Místo a čas plnění

Smluvní strany prohlašují a činí nesporným, že:

a) zhotovitel je povinen provést na svůj náklad a nebezpečí dílo v sídle objednatele;

b) zhotovitel je povinen provést dílo do 30. 11. 2023 v souladu s harmonogramem prací, který se zhotovitel zavazuje vypracovat a předat objednateli v písemné podobě před započetím provádění díla;

c) o předání a převzetí díla bude sepsán a smluvními stranami podepsán předávací protokol, který musí obsahovat alespoň následující skutečnosti:

   - identifikace této smlouvy;
   - identifikace smluvních stran;
   - místo a datum provedení díla, resp. jeho dokončení a předání;
   - prohlášení objednatele, zda dílo přebírá s výhradami nebo bez výhrad;
   - případné vady a nedodělky díla a lhůtu pro jejich odstranění;

d) zhotovitel je povinen odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole dle písm. c) tohoto čl. smlouvy;

e) v případě odstranění vad a nedodělků ve smyslu písm. c) a d) tohoto čl. smlouvy, bude o předání a převzetí díla bez vad a nedodělků sepsán a smluvními stranami podepsán předávací protokol.

V.
Ostatní ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) v případě provádění byť jen části díla prostřednictvím poddodavatelů zhotovitele, je zhotovitel odpovědný i za případně vzniklou majetkovou újmu (škodu) objednatele v důsledku porušení smluvních či zákonných povinností daného poddodavatele, jako by ji způsobil sám, a zhotovitel je tak povinen takto vzniklou majetkovou újmu (škodu) objednateli v plném rozsahu nahradit;

b) zhotovitel je povinen být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), kdy příslušnou pojistku je zhotovitel povinen objednateli předložit bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy;

c) zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním;

d) zhotovitel je povinen archivovat originál této smlouvy včetně jejích případných dodatků a jejích příloh, dále veškeré originály účetních dokladů a dalších dokumentů souvisejících s prováděním díla po dobu minimálně deseti let od protokolárního předání díla objednateli bez vad a nedodělků;

e) v souladu se zásadou sociálně odpovědného zadávání dle § 6 odst. 4 zákona č. 134/216 Sb., o zadávání veřejných zakázek, v platném znění, je zhotovitel povinen při realizaci předmětu této smlouvy dodržovat a uplatňovat veškerá ustanovení zákona č. 435/2004 Sb., o zaměstnanosti, v platném znění, zejména pak ustanovení Hlavy II tohoto zákona., dále § 139, odst. 1. písm. c) a d) a § 140, odst. 1. písm. c) tohoto zákona. Zhotovitel je povinen při realizaci předmětu této smlouvy dodržovat vůči svým zaměstnancům vykonávajícím práci související s předmětem této smlouvy veškeré pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod. Pro případ, že příslušný kontrolní orgán (Státní úřad inspekce práce, Krajská hygienická stanice, atd.) zjistí svým pravomocným rozhodnutím v souvislosti s plněním předmětu této smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, má objednatel právo na snížení ceny díla o 10 %. Bude-li se zhotovitelem zahájeno správní řízení pro porušení pracovněprávních předpisů ze strany zhotovitele v souvislosti s plněním předmětu této smlouvy, je zhotovitel povinen zahájení takovéhoto řízení objednateli oznámit a objednatel má právo pozastavit výplatu 10 % ceny díla do okamžiku právní moci rozhodnutí s

tím, že po tuto dobu není v prodlení s úhradou ceny. Zhotovitel je povinen do 7 dnů ode dne právní moci takového rozhodnutí předat objednateli ověřenou kopii s vyznačením právní moci s tím, že bude-li pravomocně zjištěno v souvislosti s plněním předmětu této smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, objednatel jednostranně započte pozastavenou část ceny na závazek zhotovitele poskytnout slevu z ceny díla ve výši 10 %. Pro případ, že nebude ve správním řízení pravomocně zjištěno v souvislosti s plněním předmětu této smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, zavazuje se objednatel zadrženou část ceny díla vyplatit zhotoviteli do 15 dnů ode dne převzetí ověřené kopie rozhodnutí s vyznačením právní moci.

f) zhotovitel je ve smyslu zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), v platném znění, povinen:

- spolupůsobit při výkonu finanční kontroly, kdy zhotovitel si je vědom, že je povinen na žádost objednatele písemně poskytnout jakékoli doplňující informace související s prováděním díla, které si vyžádají kontrolní orgány, a to ve stanovené lhůtě;
- vytvořit podmínky k provedení kontroly vztahující se k realizaci projektu, resp. k provedení díla;
- poskytnout veškeré doklady vážící se k tomu, umožnit případné ověřování souladu údajů o realizaci projektu, resp. provádění díla, uváděných ve zprávách o realizaci projektu, resp. díla, se skutečným stavem a poskytnout součinnost všem osobám oprávněným k provádění kontroly (Ministerstvo obrany, územní finanční orgány, Ministerstvo financí, Nejvyšší kontrolní úřad, Evropská komise a Evropský účetní dvůr, případně další orgány oprávněné k výkonu kontroly);

g) zhotovitel je povinen archivovat originál této smlouvy včetně jejích případných dodatků a její přílohy, veškeré originály účetních dokladů a dalších dokumentů souvisejících s realizací díla po dobu min. 10 let od předání díla bez vad a nedodělků objednateli ve smyslu čl. IV. písm. d) anebo e) této smlouvy;

h) zhotovitel je povinen při realizaci předmětu této smlouvy:

- dodržovat a uplatňovat veškerá ustanovení zákona č. 435/2004 Sb., o zaměstnanosti, v platném znění, zejména pak ustanovení Hlavy II tohoto zákona, dále § 139 odst. 1. písm. c, d) a § 140 odst. 1. písm. c) tohoto zákona;

- dodržovat vůči svým zaměstnancům vykonávajícím práci související s předmětem této smlouvy veškeré pracovněprávní předpisy, a to zejména, nikoliv však výlučně, předpisy upravující mzdy zaměstnanců, pracovní dobu, dobu odpočinku mezi směnami, placené přesčasy, bezpečnost práce apod.;

i) pro případ, že příslušný kontrolní orgán (Státní úřad inspekce práce, Krajská hygienická stanice, atd.) zjistí svým pravomocným rozhodnutím v souvislosti s plněním smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, bude mít objednatel právo na snížení ceny díla dle této smlouvy o 10%;

j) bude-li se zhotovitelem zahájeno správní řízení pro porušení pracovněprávních předpisů ze strany zhotovitele v souvislosti s plněním této smlouvy, bude zhotovitel povinen zahájení takovéhoto řízení objednateli oznámit a objednatel bude mít právo pozastavit výplatu 10% ceny díla do okamžiku právní moci rozhodnutí s tím, že po tuto dobu není v prodlení s úhradou ceny, kdy zhotovitel bude povinen do 7 dnů ode dne právní moci takového rozhodnutí předat objednateli ověřenou kopii rozhodnutí s vyznačením právní moci s tím, že bude-li pravomocně zjištěno v souvislosti s plněním předmětu smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, objednatel bude mít právo jednostranně započíst pozastavenou část ceny na závazek zhotovitele poskytnout slevu z ceny díla ve výši 10%;

k) v případě, že nebude ve správním řízení ve smyslu písm. j) pravomocně zjištěno v souvislosti s plněním této smlouvy porušení pracovněprávních předpisů ze strany zhotovitele, je objednatel povinen zadrženou část ceny díla vyplatit zhotoviteli do 15 dnů ode dne převzetí ověřené kopie rozhodnutí s vyznačením právní moci;

l) v souladu se zásadou environmentálně odpovědného zadávání podle § 6 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, je zhotovitel povinen při plnění předmětu této smlouvy zajistit dodržování právních předpisů z oblasti práva životního prostředí, jež naplňuje cíle environmentální politiky související se změnou klimatu, využíváním zdrojů a udržitelnou spotřebou a výrobou, především zákona č. 114/1992 Sb., o ochraně přírody a krajiny, v platném znění, a zákona č. 17/1992 Sb., o životním prostředí, v platném znění, a zhotovitel je povinen přijmout veškerá opatření, která po něm lze rozumně požadovat, aby např. při používání dopravních prostředků chránil životní prostředí a omezil škody způsobené znečištěním, hlukem a jinými jeho činnostmi a musí zajistit, aby emise, půdní znečistění a odpadní vody z jeho činnosti nepřesáhly hodnoty stanovené příslušnými právními předpisy.

VI.
Záruka za jakost díla a servisní podpora

Zhotovitel prohlašuje a činí nesporným, že poskytuje na dílo záruku v délce dvacetičtyř měsíců, která počíná běžet okamžikem předání díla bez vad a nedodělků na základě předávacího protokolu ve smyslu čl. IV. této smlouvy.

Smluvní strany prohlašují a činí nesporným, že:

a) pokud objednatel v záruční době zjistí vadu díla, je povinen ji bezodkladně oznámit (postačí e-mailem) zhotoviteli na e-mailovou adresu: sd_sm@autocont.cz (dále jen jako „reklamace“) s tím, že zhotovitel je povinen vadu odstranit ve lhůtě patnácti dnů od okamžiku doručení reklamace a nahradit objednateli vzniklou majetkovou újmu (škodu) v plném rozsahu se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) doba od doručení „reklamace“ zhotoviteli do doby odstranění vytýkané vady na základě reklamace se do záruční doby nezapočítává a o tuto dobu se záruční doba prodlužuje.

VII.
Smluvní pokuta

Smluvní strany prohlašují a činí nesporným, že:

a) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. II. této smlouvy, resp. povinnost provést pro objednatele na svůj náklad a nebezpečí dílo v souladu se zadávacími podmínkami veřejné zakázky, nabídkou zhotovitele, požadavky a účelem zadavatele, a dále technickou specifikací, která tvoří přílohu č. 1 této smlouvy, vymezující podrobněji dílo na základě této smlouvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

b) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. IV. písm. a), b) anebo d) této smlouvy, resp. povinnost provést na svůj náklad a nebezpečí dílo v sídle objednatele, anebo povinnost provést dílo do 30. 11. 2023 v souladu s harmonogramem prací, který se zhotovitel zavazuje vypracovat a předat objednateli v písemné podobě před započetím provádění díla, anebo povinnost vypracovat a předat objednateli v písemné podobě před započetím provádění díla harmonogram prací, anebo povinnost odstranit vady a nedodělky díla ve lhůtě pro jejich odstranění uvedené v předávacím protokole, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši

0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

c) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. V. písm. b) této smlouvy, resp. povinnost být pojištěn po celou dobu účinnosti této smlouvy pro případ způsobení majetkové újmy (škody) třetím osobám v souvislosti se svou činností, resp. v souvislosti s prováděním díla, s minimálním pojistným plněním ve výši 3.000.000,- Kč (slovy: třimiliónykorunčeských), anebo povinnost předložit pojistku objednateli bezodkladně na požádání objednatele, nejpozději však do dvou pracovních dnů ode dne doručení výzvy, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

d) v případě, kdy zhotovitel poruší svou povinnost uvedenou v čl. V. písm. c) této smlouvy, resp. povinnost zachovávat mlčenlivost o všech skutečnostech, které se dozví při anebo v souvislosti s uzavřením této smlouvy a jejím plněním, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 1% z celkové ceny díla za každý případ takovéhoto porušení se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

e) v případě, kdy zhotovitel poruší byť jen jednu svou povinnost uvedenou v čl. VI. odst. 2 písm. a) této smlouvy týkající se záruky za jakost a servisní podpory, je objednatel oprávněn požadovat po zhotoviteli zaplacení smluvní pokuty ve výši 0,5% z celkové ceny díla za každý případ takovéhoto porušení a za každý byť jen započatý den prodlení se splněním dané povinnosti až do jejího úplného splnění se splatností pěti dnů ode dne doručení písemné výzvy k jejímu zaplacení;

f) ujednáním o smluvních pokutách ve smyslu písm. a) – e) tohoto článku smlouvy není dotčeno právo objednatele na náhradu majetkové újmy (škody) v plném rozsahu, kdy tímto smluvní strany vylučují ust. § 2050 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

VIII.
Odstoupení od smlouvy

Objednatel je oprávněn odstoupit od této smlouvy do doby provedení díla bez vad a nedodělků v těchto případech:

a) bude zahájeno insolvenční řízení ve věci zhotovitele jako dlužníka;

b) bude zahájeno anebo bude zjištěno jakékoliv exekuční řízení proti zhotoviteli jako povinnému;

c) zhotovitel bude v prodlení s provedením díla bez vad a nedodělků alespoň třicet kalendářních dnů;

d) zhotovitel bude provádět dílo v rozporu se zadávacími podmínkami anebo v rozporu s touto smlouvou, ačkoliv byl na tuto skutečnost ze strany objednatele alespoň jedenkrát upozorněn.

IX.
Převzetí nebezpečí změny okolností

Zhotovitel prohlašuje a činí nesporným, že na sebe převzal nebezpečí změny okolností ve smyslu ust. § 1765 zákona č. 89/2012 Sb., občanský zákoník, v platném znění.

X.
Závěrečná ujednání

Smluvní strany prohlašují a činí nesporným, že:

a) tato smlouva nabývá platnosti dnem podpisu obou smluvních stran, účinnosti dnem uveřejnění v registru smluv dle zákona č. 340/2015 Sb., zákon o registru smluv, v platném znění, kdy povinným subjektem je objednatel, a zavazuje se tak tuto smlouvu uveřejnit v registru smluv nejpozději do třiceti dnů ode dne podpisu této smlouvy oběma smluvními stranami;

b) tato smlouva je sepsána ve dvou vyhotoveních takto:

- 1x zhotovitel;
- 1x objednatel;

c) rozhodným právem pro tento závazkový vztah je právo české (právní řád České republiky);

d) tuto smlouvu je možné změnit pouze písemně, kdy pro účely této smlouvy se za písemnou formu nepovažuje výměna emailových či jiných elektronických zpráv;

e) vylučují přijetí nabídky s dodatkem nebo odchylkou ve smyslu ust. § 1740 zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

f) pokud nebylo v této smlouvě ujednáno jinak, řídí se právní vztahy vzniklé z této smlouvy příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník, v platném znění;

g) tato smlouva byla sepsána dle jejich vážné, pravé a svobodné vůle, kdy na důkaz toho po jejím přečtení činí vlastnoruční podpisy.

Příloha č. 1: technická specifikace

Příloha č. 2: plná moc Lukáš Jurča, zmocněnec

V Olomouci dne …….

Digitálně podepsal
Mgr. Lukáš Jurča
Datum: 2023.07.04
08:43:12 +02'00'

……

Lukáš Jurča
ředitel krajského obchodního zastoupení,
Zmocněnec na základě plné moci (zhotovitel)

V …….. dne …….

MUDr. Martin Svoboda

Digitálně podepsal
MUDr. Martin
Svoboda
Datum: 2023.08.07
16:15:26 +02'00'

……

Vojenská nemocnice Olomouc
plk. gšt. v. z. MUDr. Martin Svoboda, ředitel
(objednatel)

Příloha č. 1 Smlouvy o dílo, uzavírané v návaznosti na veřejnou zakázku s názvem „VN Olomouc – Zvýšení kyberbezpečnosti“, část č. 1 „Segmentace sítě“

Technická specifikace

1. Cíl projektu

Cílem této části veřejné zakázky je vyřešit problémy se správou segmentace sítě (definice VLAN a prostupů mezi nimi) **pořízením dvou firewallů** zapojených do clusteru kvůli zajištění vysoké dostupnosti.
Zakončení jednotlivých vnitronemocničních podsítí VLAN bude přemístěno z centrálních switchů právě na tyto firewally a prostupy mezi podsítěmi budou řízeny na nich, což umožní aplikovat na vnitronemocniční provoz plnou škálu kontrol obvykle aplikovaných na perimetru na internetový provoz.
Firewally musí splňovat požadavky na výkonnost pro zpracování toků dat ve vnitřní síti. **Centrální switche budou rozšířeny** o moduly s rychlostí 40 Gbit pro připojení firewallů k nim. Všechen příchozí datový provoz bude z centrálních switchů posílán na firewally, kde po filtraci, kontrole a uplatnění pravidel bude posílán zpět na centrální switche a doručován k cíli.
Bude **rozšířena licence stávajícího FortiAnalyzeru** sloužícího k logování a vyhodnocování provozu, protože firewally budou generovat nezanedbatelný objem záznamů o datových tocích.
Bude pořízeno 41 switchů disponujících technologií 802.1X, jako náhrada současných zastaralých switchů pořízených v průměru před 15 lety, které tuto technologii neumí. Budou pro ně pořízeny **licence Airwave** sloužící k jejich správě.
Rozšíření technologie 802.1X do provozu celé nemocnice zvýší flexibilitu sítě, zefektivní správu i zvýší její zabezpečení – neznámá zařízení či zařízení nesplňující přednastavené podmínky budou automaticky zařazeny do karanténní podsítě VLAN s omezeným přístupem. Technologii 802.1X lze uplatnit i na řízení přístupu uživatelů.
V popisu je uvedena poměrně vysoká pracnost 88 člověkodní, což je dáno relativně vysokým počtem VLAN provozovaných v nemocnici a množstvím různorodých zařízení do nich zapojených (kromě počítačů i např. různá zdravotnická technika, ovládání dveří, energetiky atd. atd.). Centrální správu 802.1X je potřeba „naučit“ tato zařízení, aby byla správně rozlišována, je potřeba pilotní provoz, doladění pravidel, dokumentace stavu. Celé řešení je požadováno jako „dodávka na klíč“ s minimální součinností zadavatele.
Dodávka zahrnuje potřebný HW, licence, drobný a spojovací materiál. Součástí dodávky je i **dodávka prací** tj. implementace do technologického prostředí zadavatele (instalace, konfigurace, převod konfigurace stávajících switchů na nově dodanou techniku, zprovoznění nových funkcí a převod provozu, vytvoření dokumentace) a zaškolení personálu Odd. informatiky.
Celá dodávka nové infrastruktury musí být navržena s ohledem na potřebnou vysokou dostupnost produkčního prostředí včetně propojení se stávající LAN technologií.
Zadavatel provozuje kritický informační systém, ve kterém nesmí dojít k neplánovaným výpadkům. Proto je dodavatel povinen plánovat a realizovat všechny práce, které mohou dostupnost informačního systému ohrozit, na dobu mimo hlavní pracovní dobu (víkendy nebo pozdní odpolední hodiny) a především po dohodě se zadavatelem a v termínech jím schválených.

2. Požadovaná dodávka hardware a software

Položka č.	Typ prvku	Umístění	Počet	Specifikace
1.	firewall	1x Datacentrum S1, 1x Datacentrum S2	2 ks	viz kapitola 4.1
2.	Prvky na propojení firewallů se stávajícími centrálními switchi	Datacentra S1 a S2	Komplet	viz kapitola 4.2
3.	Switch Model A 48 port 1Gbit non PoE	Podružné datové rozvaděče	6 ks	Viz kapitola 4.3
4.	Switch Model B 48 port 1Gbit PoE	Podružné datové rozvaděče	12 ks	Viz kapitola 4.3
5.	Switch Model C 24 port 1Gbit PoE	Podružné datové rozvaděče	8 ks	Viz kapitola 4.3
6.	Switch Model D 12 port 1Gbit PoE	Podružné datové rozvaděče	15 ks	Viz kapitola 4.3
7.	Drobný a propojovací materiál	Datacentra S1 a S2 a podružné datové rozvaděče	Komplet	viz kapitola 4.4
8.	Rozšíření licencí FortiAnalyzeru	Datacentra S1 a S2	Komplet	viz kapitola 4.5
9.	Rozšíření licencí Airwave	Datacentra S1 a S2	Komplet	viz kapitola 4.6
10.	Prodloužení podpory licencí ClearPass	Datacentra S1 a S2	Komplet	viz kapitola 4.7

Žádná z nabízených technologií nesmí být v okamžiku podání nabídky označena výrobcem jako končící = nesmí být označeny jako End of Sale nebo End of Support apod.

3. Požadovaná dodávka prací (instalace, konfigurace, uvedení do provozu)

Práce
1. fyzická montáž Firewallů, propojení FW, upgrade firmware na poslední vhodnou verzi 2. Osazení core switchů novými kartami a jejich konfigurace. 3. Výměna přístupových switchů – příprava konfigurace, fyzická výměna, ověření provozu. 4. Základní nastavení, vytvoření HA clusteru 5. Příprava bezpečnostních zón a interface 6. Příprava bezpečnostních politik - implementační analýza 7. Nastavení filtrování mezi VLAN, aktivace IPS a Antivir technologií 8. Aktivace pilotního provozu a dohled nad ním 9. Ověření nastavení stávající 802.1x technologie, instalace aktualizací a poslední vhodné verze, kontrola na návazné technologie (AD, PKI, GPO atd.), oprava případných nedostatků. 10. Kontrola šíření VLAN, zavedení a otestování s AAA servery. 11. Příprava autentizačních a autorizačních politik (metrics) na stávající technologii Aruba ClearPass – komunikace se zadavatelem. Testování politik. 12. Konfigurace vazby 802.1x technologie s dodávanými segmentačními firewally (například RSSO). 13. Příprava plánu změny režimu aktivních prvků v závislosti na aktivních prvcích a možnostech odstávek provozu. 14. Příprava testovacího prostředí pro ověření konfigurace koncových zařízení versus aktivní prvky a politiky 802.1x 15. Otestování 802.1x suplikanta u různých zařízení, případné update, opravy a nastavení zařízení.

16. Postupné rozšíření dynamického přiřazení do VLAN na segmenty s PC
17. Identifikace IP zařízení bez podpory suplikanta a jejich konfigurace v 802.1x, vytvoření seznamu, profilování.
18. Konfigurace bezdrátových profilů a přiřazení k SSID/VLAN
19. Analýza a návrh stavu přístupu přes VPN a jejich součinnost s 802.1x
20. Přepnutí bezpečnostních pravidel do běžného režimu.
21. Pilotní provoz, podpora ve zvýšeném SLA, komunikace s podporou výrobce Aruba/HPE/Fortinet/...
22. Dokumentace
23. Zaškolení

4. Výčet požadovaných vlastností dodávaného hardware a software

<u>Pokyny k vyplnění tabulek (analogické jako v nabídce):</u>
Dodavatel vyplní zeleně podbarvená políčka – název, typové označení a v pravém sloupci tabulky dodavatel vyplní „Ano“, jestliže nabízené řešení splňuje požadované parametry (musí splňovat).

4.1 Firewall

Název, typové označení	**FortiGate FG 1000F**	
Číslo	**Popis – firewall (fyzické hardwarové zařízení)**	**Splňuje**
	Základní technické požadavky	
1	Požadujeme platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází, …)	Ano
2	Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu 5 let. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.	Ano
3	Požadujeme dodání zařízení ve formátu HW appliance o velikosti 2RU	Ano
4	Požadujeme veškeré příslušenství (montážní prvky) pro montáž do RACKu	Ano
5	Firewally musí být schopny odesílat logy do stávajících technologií analýzy logů provozovaných zadavatelem – FortiAnalyzer a LogManager.	Ano
	HW parametry	
6	Počet síťových rozhraní copper, RJ45 100/1000/2500/5000/10G - min 8x	8 portů
7	Počet 10 GB SFP+ min 16x	16 portů
8	Počet 25 GB SFP28 min 8x	8 portů
9	Počet 100 GB QSFP28/ 40G QSFP+ min 2x	2 porty
10	Konzolový port pro management	Ano
11	Dedikovaný port RJ45 pro management	Ano
12	Dedikovaný port RJ45 pro HA konfiguraci	Ano
13	USB 3.0 port pro zálohu konfigurace	Ano
14	Redundantní napájecí zdroj	Ano
	Výkonnostní parametry	
15	Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 198Gbps, 196Gbps, 134Gbps	198 / 196 / 134 Gbps

16	Latence firewallu (64 B UDP paket) - max 4 mikro sec	3.45 µs
17	Počet naráz otevřených spojení – min 7,5 M	7.5 Million
18	Počet nových spojení za sekundu - min. 650 000	650 000
19	Počet firewall pravidel až 100 000	100 000
20	Podpora virtualizace (min 10 virtuálních kontextů)	10 kontextů
	Network a High Availibility	
21	Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru	Ano
22	Režim fungování L2 – transparentní režim, L3 – NAT/Router	Ano
23	Podpora VLAN	Ano
24	Podpora multicast, vytváření politiky pro multicast routování	Ano
25	Podpora 802.3ad link aggregation	Ano
26	Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading	Ano
27	Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace	Ano
28	Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP	Ano
29	Policy-based routing	Ano
30	Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky	Ano
	VPN	
	- **VPN – Funkce SSL VPN**	
31	Podpora klientského i bezklientského (portálového) režimu	Ano
32	Minimální počet současně navázaných SSL VPN tunelů: 10 000	10 000
33	Minimální propustnost SSL VPN: 5,3 Gbps	5,3Gbps
	- **VPN - Funkce IPSEC VPN**	
34	podpora site-to-site VPN	Ano
35	podpora klientských VPN	Ano
36	dostupnost VPN klienta pro koncové stanice (Windows, MacOS)	Ano
37	funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů. V opačném případě požadujeme dodání neomezené licence.	Ano
38	Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 20 000	20 000
39	Minimální počet klientských IPSEC VPN tunelů: 100 000	100 000
40	propustnost IPSec VPN min. 55 Gbps (měřeno při AES256-SHA256)	55Gbps
41	podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování	Ano
42	podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování	Ano
43	podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace	Ano
	- **VPN obecně**	
44	Podpora VXLAN	Ano
45	Podpora L2TP, PPTP, GRE	Ano
46	podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec	Ano
	UTM	
	- **UTM – Funkce detekce aplikací na L7 (Application Control)**	
47	Detekce známých aplikací na základě signatur	Ano
48	Signaturové databáze automaticky aktualizované výrobcem	Ano
49	alespoň 4000 podporovaných aplikací	Ano

50	pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci)	Ano
51	možnost tvorby vlastních signatur	Ano
52	detekované aplikace je možné: povolit, monitorovat, blokovat	Ano
53	na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci	Ano
54	funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše.	Ano
	- **UTM – Funkce detekce a potlačení narušení (IPS/IDS)**	
55	signatury automaticky aktualizované výrobcem	Ano
56	alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem	Ano
57	možnost tvorby vlastních signatur	Ano
58	funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům	Ano
59	propustnost funkce IPS včetně logování min. 19 Gbps (měřeno na komunikaci typu mix aplikací)	19Gbps
	- **UTM – Funkce antivirové kontroly**	
60	Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem	Ano
61	Signatury automaticky aktualizované výrobcem	Ano
62	požadujeme AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky)	Ano
63	možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW/SW appliance stejného výrobce	Ano
64	deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 10 Gbps	Ano
65	funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům	Ano
66	Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů	Ano
67	Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.	Ano
	- **UTM – Funkce kategorizace webových stránek**	
68	založená na centrálně spravované databázi výrobce	Ano
69	minimálně 70 filtračních kategorií	Ano
70	možnost definice vlastních kategorií	Ano
71	možnost definice vlastních seznamů zakázaných URL	Ano
72	kategorizace musí zahrnovat I české a slovenské internetové stránky	Ano
	- **UTM – Funkce DNS filtru**	
73	Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu)	Ano
74	Možnost definovat vlastní tzv. blacklist domén	Ano
75	Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL	Ano
76	Možnost importu seznamu blokovaných domén do DNS filtru	Ano
77	Detekce a blokování komunikace do botnet sítí	Ano
	- **UTM - Funkce ochrany před únikem citlivých informací (DLP)**	

78	možností analýzy běžných typů dokumentů a protokolů	Ano
79	možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum	Ano
	- **UTM obecně**	
80	Email filter - jednoduchá antispamová a antivirová inspekce elektronické pošty	Ano
81	Podpora SSL dekrypce/SSL inspekce s minimální propustností 10 Gbps	10Gbps
82	DoS Policy prevence proti základním útokům typu DoS	Ano
83	Firewall musí být vybaven bezpečnostním modulem pro ukládání citlivých informacích založeným na bázi HW (TPM)	Ano
	Firewall	
84	Možnost nastavovat firewall politiku na základě geografických údajů	Ano
85	Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem	Ano
86	Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud	Ano
87	Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru	Ano
88	Viditelnost do provozu na aplikační úrovni	Ano
89	Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo)	Ano
90	Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu	Ano
91	Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření.	Ano
92	Traffic Shaping, QoS s podporou priroritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii	Ano
93	Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu	Ano
94	Podpora funkce reverzní proxy	Ano
95	Podpora silné autentizace uživatelů – integrovaná podpora generátoru jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů	Ano
	- **Firewall – Explicit proxy**	
96	podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP)	Ano
97	podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos	Ano
98	funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta	Ano
99	Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru	Ano
	Virtualizace	
100	Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.	Ano
101	Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech)	Ano
102	Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů)	Ano
	Management	
103	FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici	Ano
104	Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě	Ano

105	Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury)	Ano
	Záruka a podpora	
106	Podpora výrobce v režimu 24x7 zahrnující aktualizaci a udržování všech požadovaných funkcí, technickou podporu, záruku na HW, to vše po dobu 5 let.	Ano

4.2 Prvky na propojení firewallů se stávajícími centrálními switchi „Aruba 5412R zl2 Switch J9822A“

Typ	Počet	Bude zapojeno do
QSFP+ 40Gbit SM modul	4	Dodávaný segmentační NGFW
SFP+ 10Gbit SM modul	4	Dodávaný segmentační NGFW
J9996A Aruba 2p 40GbE QSFP+ v3 zl2 Mod	2	Stávající core switch HPE 5412R zl2
JH232A HPE X142 40G QSFP+ LC LR4 SM Transceiver	4	Stávající core switch HPE 5412R zl2

Prvky musí být stejného výrobce jako zařízení (výrobce NGFW pro moduly vkládané do něj, HPE/Aruba v případě centrálního switche) a musí být pokryty stejnou zárukou a podporou výrobce jako vlastní prvky. Zadavatel nepřipouští dodávku neoriginálních modulů od jiných výrobců nebo z druhovýroby (OEM).
Dále jsou součástí dodávky veškeré kabely, zadavatel má na optických vanách konektory typu SC.

4.2 Switch (přepínač) model A, B, C a D

Název, typové označení	**A - HPE ANW 6200F 48G 4SFP+ Switch (JL726B)** **B - HPE ANW 6200F 48G CL4 4SFP+740W Switch (JL728B)** **C - HPE ANW 6200F 24G CL4 4SFP+370W Switch (JL725B)** **D - Aruba 6200F 12G CL4 2G/2SFP+ 139W (R8Q72A)**	
Číslo	**Popis – Switch (přepínač) model A, B, C a D**	**Splňuje**
	Požadavky pouze na switch (přepínač) model A (48 port 1Gbit non PoE)	
1	Počet 1 Gbit/s metalických portů: 48x 10/100/1000Mbps RJ45	Ano
2	Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4x	Ano
3	Minimální celková přepínací propustnost přepínače: 176Gbit/s	176Gbps
4	Minimální celkový paketový výkon přepínače: 130Mpps	130.9Mpps
5	Kapacita stohovacího propojení: 40Gbps	40Gbps
6	Podpora stohování různých typů přepínačů: Model A,B,C společně v různém mixu	Ano
	Požadavky pouze na switch (přepínač) model B (48 port 1Gbit PoE)	
7	Počet 1 Gbit/s metalických portů: 48x 10/100/1000Mbps RJ45	Ano
8	Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4x	Ano
9	Minimální celková přepínací propustnost přepínače: 176Gbit/s	176Gbps
10	Minimální celkový paketový výkon přepínače: 130Mpps	130.9Mpps
11	Kapacita stohovacího propojení: 40Gbps	40Gbps
12	Podpora stohování různých typů přepínačů: Model A,B,C společně v různém mixu	Ano
13	Podpora PoE+ dle standardu 802.3at	Ano
14	Podpora PoE dle standardu 802.3af	Ano
15	Dostupný výkon pro PoE+ napájení: 740W	Ano
	Požadavky pouze na switch (přepínač) model C (24 port 1Gbit PoE)	
16	Počet 1 Gbit/s metalických portů: 24x 10/100/1000Mbps RJ45	Ano

17	Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 4x	Ano
18	Minimální celková přepínací propustnost přepínače: 128Gbit/s	128Gbps
19	Minimální celkový paketový výkon přepínače: 95Mpps	95.2Mpps
20	Kapacita stohovacího propojení: 40Gbps	Ano
21	Podpora stohování různých typů přepínačů: Model A,B,C společně v různém mixu	Ano
22	Podpora PoE+ dle standardu 802.3at	Ano
23	Podpora PoE dle standardu 802.3af	Ano
24	Dostupný výkon pro PoE+ napájení: 370W	Ano
	Požadavky pouze na switch (přepínač) model D (12 port 1Gbit PoE)	
25	Počet 1 Gbit/s metalických portů: 12x 10/100/1000Mbps RJ45	Ano
26	Počet optických 10GE portů s volitelným fyzickým rozhraním (SFP+): 2x	Ano
27	Minimální celková přepínací propustnost přepínače: 68Gbit/s	68Gbps
28	Minimální celkový paketový výkon přepínače: 50Mpps	50.5Mpps
29	Kapacita stohovacího propojení: 20Gbps	Ano
30	Podpora stohování různých typů přepínačů: Model D jen sám se sebou	Ano
31	Podpora PoE+ dle standardu 802.3at	Ano
32	Podpora PoE dle standardu 802.3af	Ano
33	Dostupný výkon pro PoE+ napájení: 139W	Ano
34	Switche jsou tiché bezventilátorové (fanless)	Ano
	Společné požadavky na všechny modely A, B, C a D	
	- **Základní vlastnosti**	
35	Třída zařízení: přepínač	Ano
36	Formát zařízení do racku	Ano
37	Velikost zařízení: 1U	Ano
38	Interní AC zdroj	Ano
39	Minimální paketový buffer: 8MB	Ano
40	Maximální hloubka přepínače: 33 cm	Ano
	- **Vlastnosti stohování**	
41	Podporovaný počet přepínačů ve stohu: 8	Ano
42	Stoh podporuje distribuované přepínaní paketů	Ano
43	Stohování přes standartní uplink porty (možnost zapojení stohu na minimálně 10km)	Ano
44	Redundance řídícího prvku v rámci stohu	Ano
45	Jednotná konfigurace stohu (IP adresa, správa, konfigurační soubor)	Ano
46	Seskupení portů IEEE 802.3ad mezi různými prvky stohu (Multichassis LAG)	Ano
47	Stoh funguje jako jedno L3 zařízení (router, gateway, peer) včetně podpory dynamických směrovacích protokolů jako je OSPF	Ano
	- **Základní funkce a protokoly**	
48	Podpora "jumbo rámců" včetně velikosti 9198 Byte	Ano
49	Podpora linkové agregace IEEE 802.1AX	Ano
50	Konfigurovatelné rozkládání LACP zátěže podle L2, L3	Ano
51	Počet LACP skupin/linek ve skupině: 32/8	Ano
52	Minimální počet záznamů v tabulce MAC adres: 16 000	32 768
53	Minimální počet záznamů v tabulce ARP: 8 000	8 192
54	Protokol pro definici šířených VLAN: MVRP	Ano
55	Podpora VLAN podle IEEE 802.1Q, minimálně 2000 aktivních VLAN	Ano
56	Podpora zařazování do VLAN podle standardu 802.1v	Ano

57	IEEE 802.1s - Multiple Spanning Tree	Ano
58	STP instance per VLAN s 802.1Q tagováním BPDU (např. PVST+)	Ano
59	Detekce protilehlého zařízení pomocí LLDP a rozšíření LLDP-MED	Ano
60	Detekce jednosměrnosti optické linky (např. UDLD)	Ano
61	Podpora NTPv3	Ano
62	Statické směrování IPv4 a IPv6	Ano
63	Minimální počet IPv4 záznamů ve směrovací tabulce: 2 000	2048
64	Minimální počet IPv6 záznamů ve směrovací tabulce: 1 000	1024
65	Dynamické směrování OSPFv2, OSPFv3	Ano
66	Podpora Layer-3 routed port	Ano
67	IGMP v2 a v3	Ano
68	IGMP snooping	Ano
69	MLD v1 a v2	Ano
70	MLD snooping	Ano
71	Hardware podpora IPv4 a IPv6 ACL	Ano
72	ACL definice na základě skupiny fyzických portů	Ano
73	ACL aplikovatelný na interface, LAG, VLAN	Ano
74	BPDU a Root guard	Ano
75	DHCP snooping pro IPv4 a IPv6	Ano
76	HW ochrana proti zahlcení portu (broadcast/multicast/icmp) nastavitelná na kbps a pps	Ano
77	802.1X ověřování včetně více současných uživatelů na port, minimálně 32 uživatelů/port	Ano
78	Konfigurovatelná kombinace pořadí postupného ověřování zařízení na portu (IEEE 802.1x, MAC adresou)	Ano
79	Dynamické zařazování do VLAN a přidělení QoS podle RFC 4675	Ano
80	Podpora Critical VLAN	Ano
81	Podpora uživatelských rolí definujících pro konkrétní uživatele více tagovaných či netagovaných VLAN, ACL, QoS politiky a SDN tunely.	Ano
82	Podpora uživatelských rolí definovaných lokálně v přepínači, jejich aplikace na základě výsledku autorizace	Ano
83	Podpora uživatelských rolí dynamicky stahovatelných z RADIUS serveru, jejich aplikace na základě výsledku autorizace	Ano
84	Podpora Dynamic ARP protection	Ano
85	Port security	Ano
86	Konfigurovatelná ochrana control plane (CoPP) před DoS útoky na CPU	Ano
87	Podpora IPv4 a IPv6 QoS	Ano
88	IEEE 802.1p - minimální počet front: 8	Ano
	- **SDN funkce**	
89	Podpora technologie VXLAN	Ano
90	Podpora tunelování uživatelského provozu pomocí L2 GRE tunelů - schopnost izolovat více koncových zařízení na jednom portu do unikátních tunelů	Ano
91	Přiřazení koncového zařízení do tunelu na základě výsledku autorizace	Ano
	- **Analytické a automatizační nástroje**	
92	Podpora REST API pro automatizaci nastavení sítě.	Ano
93	Podpora skriptování v jazyce Python – lokální interpret jazyka v přepínači	Ano
94	Integrovaný nástroj na odchyt paketů (např. WireShark nebo ekvivalentní)	Ano
95	Interpretace uživatelských skriptů monitorujících definované parametry síťového provozu s možností automatické reakce na události	Ano

96	Grafické rozhraní pro zobrazení výsledků monitorování a analytických skriptů. Možnost zobrazení stavu monitorovaných metrik do grafů atp.	Ano
97	Root cause analysis v grafickém rozhraní – možnost vrácení se ke konkrétní funkční konfiguraci a stavu protokolů v čase.	Ano
98	Interní úložiště dat pro sběr provozních dat a pokročilou diagnostiku zařízení	Ano
99	Kapacita interního úložiště dat pro analytické účely minimálně 14 GB	16 GB
	- **Management**	
100	USB-C konzolový port	Ano
101	1xRJ45 OoB management port s podporou ethernetu	Ano
102	Konfigurace zařízení v člověku čitelné textové formě	Ano
103	Podpora automatických i manuálních snapshotů konfigurace systému	Ano
104	USB port pro diagnostiku, přenos konfigurace a firmware	Ano
105	Přímé bezdrátové připojení ke konzoli zařízení skrze bluetooth	Ano
106	Podpora managementu přes IPv4 i IPv6	Ano
107	SSHv2 a HTTPS pro IPv4 a IPv6	Ano
108	Podpora SNMPv2c a SNMPv3	Ano
109	RMON	Ano
110	Možnost omezení přístupu k managementu (SSH, SNMP) pomocí ACL	Ano
111	Lokálně vynucené RBAC na úrovni přepínače	Ano
112	Dualní flash image	Ano
113	Podpora UDP, TCP a TLS SYSLOG pro IPv4 a IPv6 s možností logováni do více syslog serverů	Ano
114	Podpora RADIUS včetně RADIUS CoA (RFC3576)	Ano
115	Podpora standardního Linux Shellu (BASH) pro debugging a skriptování	Ano
116	Podpora TACACS+	Ano
117	Analýza síťového provozu sFlow podle RFC 3176	Ano
118	Ochrana proti nahrání modifikovaného SW do zařízení prostřednictvím image signing a funkce secure boot, která ověřuje autentičnost a integritu OS zařízení prostřednictvím TPM chipu	Ano
119	Port mirroring, alespoň 4 různé obousměrné session: SPAN, ERSPAN	Ano
120	Podpora IP SLA pro měření zpoždění provozu VoIP	Ano
121	Podpora Zero Touch Provisioning (ZTP)	Ano
	- **Kompatibilita**	
122	Zadavatel provozuje monitoring a management nástroj Aruba Airwave. Nabízené a dodané switche musí být bez dalších nástrojů a investic s tímto nástrojem plně kompatibilní, a to minimálně v těchto bodech: • Airwave zajistí automatickou konfiguraci switchů • Airwave zajistí zálohu a obnovu konfigurace switchů • Airwave zajistí archivaci konfigurace pro potřeby auditu a řízení verzování konfigurací	Ano

Ostatní podmínky:

- Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství)
- Dodávka musí obsahovat veškeré potřebné licence bez časového omezení pro splnění požadovaných vlastností a parametrů.
- Je požadována záruka na hardware s výměnou v délce 60 měsíců. Tato záruka musí být garantovaná výrobcem zařízení.
- Jsou požadovány software aktualizace (nové verze programového vybavení) v minimální délce 60 měsíců.

- Je požadovaná technická podpora výrobce po dobu 60 měsíců.
- Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

4.4 Drobný a propojovací materiál

Zadavatel požaduje dodávku i potřebného propojovacího materiálu. Některé switche (skupiny) budou propojeny do Core Switchů pomocí 10Gb optických linek, některé switche budou propojeny pomocí 1Gbit SM a MM linek, přičemž se počítá s použitím stávajících modulů na straně core switchů.

Typ	Počet	Bude zapojeno do
SFP+ 10Gbit modul SM J9151E	10	Stávající core switch HPE 5412R zl2
SFP+ 10Gbit modul SM	10	Dodávané switche
10Gb SFP+ DAC kabel (0,5 - 1m)	41	Dodávané switche
SFP 1Gbit modul SM	30	Dodávané switche
SFP 1Gbit modul MM	26	Dodávané switche

Dodávané moduly musí být originální, stejný výrobce jako dodávané switche a plně podporované a kryté zárukou výrobce. Zadavatel nepřipouští moduly od jiného výrobce ani OEM.
Součástí dodávky je i veškerý další potřebný drobný a propojovací materiál, jako je spojovací a vyvazovací materiál, optické kabely, metalické kabely.

4.5 Rozšíření licencí FortiAnalyzeru

Zadavatel požaduje rozšíření stávajícího systému FortiAnalyzer pro ukládání a korelaci logů v síti zadavatele.
Systém musí být schopen příjmu a analýzy logů jak ze stávajících perimetrových firewallů FortiGate 200F, tak z nově dodávaných segmentačních firewallů dle bodu 4.1.
Dále musí být schopen poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.
Dodávka musí obsahovat licence na dobu 5 let a musí zvýšit kapacitu příjmu logů minimálně o 25GB/den.
Zadavatel požaduje funkci zpětné kontroly logů až 7 dnů zpět a zjištění, jestli systém nebyl napaden při přístupu na škodlivou webovou stránku. Logy jsou kontrolovány oproti pravidelně aktualizované databázi podezřelých IP adres, domén nebo webových URL adres.

Další požadované parametry rozšíření:

A. Hlavní parametry appliance
- Musí se jednat o virtuální appliance s podporou minimálně VMware
- Podpora minimálně 4 virtuálních interface
- Možnost škálovatelného navýšení kapacity úložiště na základě licence
- Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma
- Možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě

B. Multitenantnost
- Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení)

- Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků

C. Logovací funkce

- Musí se jednat o centrální logovací prvek pro všechny UTM firewally
- Musí umět ukládat jakékoliv Syslog zprávy
- Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day" malicious websites
- Vizualizace provozu nad všemi firewally
- Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy
- Realtime a historický náhled do logů
- Korelace logů
- Samostatná sekce týkající se hrozeb v síti
- Podpora prohlížení statistických údajů nad logy

D. Reporting

- Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF
- Generování reportů v pravidelných intervalech
- Předefinované vzory pro reporty na nejčastější použití
- Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze
- Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky

E. Další funkce

- Event Management – upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou
- Předvytvořený dashboard pro využití dohledovým centrem
- Možnost customizace rozhraní pro NOC/SOC dle konkrétních požadavků na dohlížené informace
- Incident Management – management incidentů vytvořených ze vzniklých eventů v SOC rozhraní
- PlayBook Automatizace – automatizované odpovědi na incidenty dle vzorových scénářů
- Outbreak služba – v případě rychle šířící se kybernetické hrozby vyhodnocené výrobcem systému může administrátor tohoto systému zobrazit varování a k tomu odpovídající event handlery a předdefinované reporty

F. Možnosti správy a komunikace

- Podpora SNMPv2, SNMPv3
- Podpora REST API
- Správa přes webové rozhraní HTTPS
- Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+)
- Podpora statického routování
- Možnost zašifrování spojení mezi zařízením které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace

4.6 Rozšíření licencí Airwave

Zadavatel aktuálně vlastní a provozuje tuto licenci monitoring a management nástroje Aruba Airwave:

Označení	Název licence	Počet
JW546AAE	Aruba LIC-AW Aruba Airwave 1 Device License E-LTU	70

Konec podpory pro stávající licence je květen 2024.
Zadavatel požaduje rozšíření tohoto nástroje o licence pro nově pořizované prvky (pro 41 kusů nových switchů modely A, B C a D viz výše) včetně sjednocení doby podpory již vlastněných licencí a její prodloužení na dobu 5 let od předání.

4.7 Prodloužení podpory licencí ClearPass

Zadavatel aktuálně vlastní a provozuje tyto licence software Aruba ClearPass:

Označení	Název licence	Počet
JZ399AAE	Aruba ClearPass Cx000V VM Appl E-LTU	2
H9WX9E	Aruba 5Y FC 24x7 ClearPass Cx000V VM SVC	2
JZ402AAE	Aruba ClearPass NL AC 1K CE E-LTU	1
H9XH9E	Aruba 5Y FC 24x7 ClearPass NL AC 1KCESVC	1

Konec podpory pro stávající licence je květen 2024.
Tato technologie je v síti Zadavatele využívána a bude hrát jednu z klíčových rolí v realizaci této části VZ. Proto Zadavatel požaduje prodloužení podpory těchto licencí po dobu udržitelnosti v délce 5 let.

4.8 Ostatní podmínky

Hardware musí být dodán zcela nový, plně funkční a kompletní (včetně příslušenství). Dodávka musí obsahovat veškeré potřebné licence pro splnění požadovaných vlastností a parametrů.
Uchazeč je povinen s dodávkou doložit oficiální potvrzení lokálního zastoupení výrobce o všech dodávaných zařízeních (seznam sériových čísel dodávaných zařízení) pro český trh.

5. Předávací kritéria

- Zařízení (Firewaly, switche) jsou namontována v místech určení a jsou propojena s provozní sítí LAN zadavatele
- Licence Firewallů jsou aktivovány, přiřazeny na portále výrobce pod účtem zadavatele, délka podpory koresponduje se smlouvou
- Switche jsou připojeny do dohledového nástroje Airwave, lze z nich vyčíst provozní údaje, informace o firmware atd.
- Firewally jsou v funkčním HA clusteru, ověřeno trhacími testy.
- Firewally mají zabezpečeny přístupy administrátorů, jsou nastavena bezpečná hesla, administrátorský přístup je možný pouze přes jump server a podobně dle analýzy a dohody se zadavatelem.
- Firewally mají zapnuté předávání logů do provozních logovacích systémů zadavatele (FortiAnalyzer, LogManager), lze dělat analýzy nad uloženými logy.
- Jsou nastaveny bezpečnostní politiky pro filtrování provozu mezi VLAN, jsou zapnuty technologie IPS, deep packet inspection tam kde to dává smysl dle schválené analýzy.
- Switche jsou v režimu „bezkonfiguračních portů“, probíhá automatické přiřazení VLAN k portu switche podle připojeného zařízení.
- Zařízení bez možnosti suplikanta jsou identifikována a zapojena do systému 802.1x vhodným způsobem (identifikace profilem/MAC adresou a podobně)
- Předána dokumentace skutečného stavu