SMLOUVA O DODÁVCE A IMPLEMENTACI OBNOVY INFRASTRUKTURY FIREWALLŮ

uzavřená dle zákona č. 89/2012 Sb., občanského zákoníku

mezi:

Odběratelem				
Název:	**Fakultní nemocnice Ostrava**			
Sídlo:	17. listopadu 1790, 708 52 Ostrava-Poruba			
IČ:	00843989	**DIČ:**	CZ00843989	je plátcem DPH
Zřizovací listina MZ ČR ze dne 25. listopadu 1990 č. j. OP-054-25.11.90				
Zastoupena:	MUDr. Jiřím Havrlantem, MHA, ředitelem			
Bankovní spojení:	Česká národní banka, č. ú. 43 - 65137761/0710			

a

Dodavatelem				
u právnické osoby				
Obchodní firma:	**ALEF NULA,a.s.**			
Sídlo:	Praha 8, Pernerova 691/42, PSČ 186 00, Česká republika			
IČ:	61858579	**DIČ:**	CZ61858579	je plátcem DPH
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze oddíl B, vložka 2727				
Jednající:	Ing. Milan Zinek, předseda představenstva			
Bankovní spojení:	51-3717150237/0100			

Odběratel a Dodavatel jsou dále souhrnně označeni jako „**Smluvní strany**" nebo jednotlivě „**Smluvní strana**"

I.
Základní ustanovení

1. Odběratel a dodavatel uzavírají tuto Smlouvu o dodávce a implementaci obnovy infrastruktury firewallů (dále také jen „**Smlouva**") na základě výsledku výběru nejvhodnější nabídky veřejné zakázky „**Obnova infrastruktury firewallů**" (dále také jen „**Veřejná zakázka**"), na základě které má Dodavatel provést obnovu technologické infrastruktury firewallů, včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů, jež budou integrovány v rámci firewallů, a to včetně instalace, implementace, plné konfigurace a uvedení do provozu (dále také jen „**Infrastruktura firewallů**" nebo „**Řešení**") dle zadávací dokumentace Veřejné zakázky (dále také jen „**Zadávací dokumentace**"), jejíž součástí je mimo jiné technická specifikace Infrastruktury firewallů, která tvoří rovněž přílohu č. 1 této Smlouvy (dále také jen „**Technická specifikace**").
2. Veřejná zakázka „**Obnova infrastruktury firewallů**" byla vyhlášena podle zákona č. 134/2016 Sb. o zadávání veřejných zakázek, ve znění platném ke dni vyhlášení veřejné zakázky.
3. Dodávka, instalace a implementace Infrastruktury firewallů včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů, příslušných licencí, zaškolení, zhotovení dokumentace a zajištění záručního servisu v rámci standardu záruky za jakost , které jsou předmětem této Smlouvy, jsou spolufinancovány v rámci Integrovaného regionálního operačního programu, specifického cíle 3.2 – Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT, 10. výzva „Kybernetická

bezpečnost" a v souladu s projektem Odběratele *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"* (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023). Zajištění rozšíření doby technické (servisní) podpory ve smyslu dle čl. V. odst. 2 písm. a) až d) této Smlouvy po dobu 3. – 5. roku je hrazeno z vlastních zdrojů Odběratele, nikoliv z poskytnutých prostředků regionálního operačního programu.

4. Součástí plnění Smlouvy je krom dodání technických zařízení, vybavení a jejich příslušenství (dále také jen „**Hardware**" nebo „**Technická zařízení**") a převodu vlastnického práva k tomuto vybavení na Odběratele, také mimo jiné dodání všech potřebných licencí a subskripcí (dále také jen „**Licence**") pro počítačové programy (včetně operačních systémů) potřebné pro řádný chod celého Řešení (dále také jen „**Software**"), instalace, nastavení, a zprovoznění Řešení dle Zadávací dokumentace a požadavků Odběratele do ostrého provozu (dále také jen „**Implementace**") v rámci počítačového prostředí – IT infrastruktury Odběratele (dále také jen „**IT Infrastruktura**"), provedení školení personálu Odběratele (dále také jen „**Školení**") a poskytování standardní záruční technické podpory celého Řešení (dále také jen „**Technická podpora**"). Technická podpora bude poskytována v délce 2 (slovy: dvou) let s možností rozšíření její doby o další 3 (slovy: tři) roky na celkovou dobu 5 (slovy: pět) let.

II.
Předmět smlouvy

1. Dodavatele se zavazuje poskytnout a provést Odběrateli následující plnění dle Zadávací dokumentace, které zahrnuje:
   a) dodávku Hardware (včetně převodu vlastnického práva k Hardware na Odběratele);
   b) dodávku a poskytnutí všech potřebných Licencí pro řádný chod celého Řešení;
   c) provedení Implementace a uvedení celého Řešení do ostrého provozu;
   d) provedení Školení;
   e) poskytování Technické podpory;
   f) další plnění dle Zadávací dokumentace;

   (dále souhrnně také jen „**Předmět plnění**"), přičemž detaily a rozsah jsou vymezeny v Technické specifikaci, která je přílohou č. 1 této Smlouvy a v příloze č. 2 této Smlouvy – Položkový rozpočet předmětu plnění (dále také jen „**Rozpočet**").

2. V rámci Předmětu plnění bude Odběrateli dodán Hardware, který je originální, nový a nepoužitý. V databázi výrobce Hardware a Software bude Odběratel veden jako první uživatel dodaného Hardware/Licence. Dodavatel je povinen doložit do 7 (slovy: sedmi) pracovních dnů od doručení žádosti Odběratele potvrzení výrobce o určení dodávaného Hardware pro evropský trh, včetně sériových čísel dodávaného Hardware, případně jiný doklad výrobce prokazující pro dodaná Technická zařízení provozovaná na území ČR poskytnutí plné podpory výrobce při řešení technických problémů (požadavek uvedený v Technické specifikaci). Před převzetím Hardware si Odběratel vyhrazuje právo kontroly dle sériových čísel (pokud jsou přidělena) u výrobce. Shodně pro Software je Dodavatel povinen na výzvu poskytnout doklad o poskytnutí plné záruky a podpory výrobce při řešení technických problémů. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Odběratel (a to historicky), bude se jednat o podstatné porušení této Smlouvy.

3. Veškeré potřebné Licence budou Dodavatelem dodány v rozsahu potřebném pro řádné užívání celého Řešení včetně možnosti jeho správy a konfigurace. Časový rozsah těchto Licencí bude na celou dobu trvání majetkových autorských práv k dodanému Software.

4. Předmět plnění zahrnuje rovněž vyhotovení a dodání instalační, administrační a provozní dokumentace Řešení (dokumentace bude zpracována nejméně v rozsahu potřebném pro zajištění užívání, správy a údržby

Řešení Odběratelem a dále bude obsahovat popis skutečného provedení Řešení včetně jeho vazeb na další části IT Infrastruktury).

III.
Místo a způsob poskytnutí Předmětu plnění

1. Místem dodání Předmětu plnění je:
   a) v areálu sídla Odběratele - Fakultní nemocnice Ostrava – prostory ve správě Útvaru náměstka ředitele pro informační technologie;
   b) v areálu detašovaného pracoviště Odběratele – Léčebna pro dlouhodobě nemocné Klokočov, Klokočov 59, Vítkov – Klokočov, PSČ 747 47;
   c) detašované pracoviště Odběratele - odběrové pracoviště Krevního centra FNO, AVION Shopping Park Ostrava, Rudná 114, Ostrava - Zábřeh, PSČ 700 30, 2. podlaží

   (dále souhrnně také jen „**Místo plnění**" nebo jednotlivá místa uvedená pod body a) až c) výše dále také jen "Lokalita").
2. Náklady na dodání Předmětu plnění a jeho částí do místa dodání hradí Dodavatel.
3. Předmět plnění včetně dodání veškerého Hardware, Licencí a provedení Implementace a uvedení Řešení do ostrého provozu bude provedeno nejpozději do 90 (slovy: devadesáti) kalendářních dnů ode dne podpisu této Smlouvy oběma Smluvními stranami (dále také jen „**Termín plnění**"), a to dle vzájemně odsouhlaseného harmonogramu (dále také jen „**Harmonogram**"). Harmonogram bude zpracován Dodavatelem a musí mimo jiné zohlednit roli Odběratele jako provozovatele základní služby podle vyhlášky č. 437/2017 Sb. o kritériích pro určení provozovatele základní služby a implementační práce tak musí mít minimální dopad na provoz Odběratele.
4. Termín plnění může být posunut pouze o délku případného prodlení zaviněného na straně Odběratele, a to formou písemného dodatku k této Smlouvě.
5. Náhrada stávajících firewallů za dodávané Řešení bude probíhat v objektech Odběratele za plného provozu a musí být provedena tak, aby měla na provoz Odběratele minimální dopad. Maximální celková doba akceptovatelného výpadku síťových služeb poskytovaných firewally v jedné Lokalitě během jejich náhrady je 1 (slovy: jedna) hodina. Vlastní výměna firewallů bude provedena ve večerních hodinách (18:00 – 24:00 h) po předchozí dohodě s Odběratelem.
6. Součástí implementace musí být i případné související konfigurace síťových prvků nebo management nástrojů v síti Odběratele a nastavení automatického zálohování konfigurace, ke kterému je možné využít stávající nástroje Odběratele (Prime Infrastructure).
7. Součástí fyzické instalace v rámci Implementace je odpojení patch kabelů, demontáž stávajících zařízení, montáž nových zařízení (Hardware), zapojení patch kabelů, kabelový management, kontrola zapojení, zapojení na centrální management. Součástí nasazení firewallů musí být také migrace příslušných pravidel ze stávajících firewallů, jejich optimalizace z pohledu správy i výkonu, propojení na zdroje identit (AD, ISE) a kontrola funkčnosti řešení a jednotlivých pravidel.
8. Smluvní strany se dohodly, že po instalaci a uvedení Řešení do provozu, budou Dodavatelem v místě plnění provedeny zkoušky provozu, činnosti a veškerých funkcí Řešení (dále také jen „**Akceptační testy**"). Odběratel je oprávněn se Akceptačních testů zúčastnit. Termín provádění Akceptačních testů je povinen Dodavatel sdělit Odběrateli nejméně 2 (slovy: dva) pracovní dny před plánovaným dnem jejich provádění; v případě, že by takto navržený termín Odběrateli z relevantních důvodů nevyhovoval, je oprávněn požadovat odložení Akceptačních testů o nejvýše 4 (slovy: čtyři) pracovní dny. V případě, že Řešení nebo jeho příslušenství bude vykazovat vady, není Řešení způsobilé předání a Odběratel nemá povinnost jej převzít. Po provedení

Akceptačních testů, dle kterých bude Řešení bez vad, bude spuštěno do ostrého provozu (dále také jen „**Ostrý provoz**").

9. Předmět plnění je způsobilý předání Odběrateli, pokud budou provedeny všechny plnění, které jsou jeho součástí, tj. zejména dodání Hardware a jeho příslušenství, dodání a poskytnutí Licencí (včetně dodání dokumentů ohledně oprávnění Odběratele k užívání Software na základě Licencí), dodání veškeré dokumentace, instalace a uvedení Řešení do Ostrého provozu (Implementace) v Místě plnění a v rámci Akceptačních testů nebude Řešení vykazovat jakékoliv vady nebo nedostatky. Předmět plnění se považuje za řádně dodaný podpisem akceptačního protokolu Odběratelem (dále také jen „**Akceptační protokol**") po uvedení Řešení do Ostrého provozu. Nárok na úhradu ceny za Předmět plnění sjednané v čl. IV. odst. 3 písm. A/ této Smlouvy vzniká Dodavateli podpisem Akceptačního protokolu Odběratelem.

10. Přechod nebezpečí škody a vlastnického práva

10.1. Nebezpečí škody na dílčích částech Předmětu plnění (typicky jednotlivého Hardware) přechází na Odběratele převzetím jednotlivých dílčích částí Předmětu plnění Odběratelem a podpisem protokolu o takovém převzetí k tomu oprávněným zástupcem Odběratele (dále také jen „**Protokol o dodání dílčí části**"). Protokol o dodání dílčí části slouží pouze pro evidenční účely, že došlo k dovozu/provedení dílčí části Předmětu plnění, neboť není fakticky možné, aby byl celý Předmět plnění dodán najednou.

10.2. Převzetí dílčích částí Předmětu plnění dle odst. 10.1 tohoto článku výše, ani podepsání Protokolu o dodání dílčí části, nelze považovat za částečné plnění předmětu této Smlouvy Dodavatelem. Dodavatel v této souvislosti bere na vědomí, že Odběratel požaduje dodání Předmětu plnění jako celku, když očekává plně funkční Řešení a dílčí plnění pro něj nemají žádný význam ani užitek.

10.3. Vlastnické právo k movitým věcem dodaným Odběrateli na základě této Smlouvy přechází na Odběratele podpisem Akceptačního protokolu.

11. Realizační tým

11.1. Dodavatel bude Předmět plnění realizovat majoritně za účasti (prostřednictvím) osob, které jsou uvedeny v příloze č. 3 této Smlouvy – Realizační tým dodavatele. V případě, že dojde ke změně těchto osob je Dodavatel povinen tuto skutečnost oznámit Odběrateli nejpozději do 5 (slovy: pěti) pracovních dnů od vzniku této skutečnosti. Nová osoba, která bude součástí realizačního týmu, musí splňovat podmínky, které Odběratel stanovil v Zadávací dokumentaci. Zároveň s oznámením o změně osoby tak budou doručeny doklady, které budou prokazovat osvědčení o vzdělání a odborné kvalifikaci této nové osoby. O této změně bude vyhotoven písemný dodatek k této Smlouvě.

12. Dodavatel je povinen realizovat Předmět plnění tak, aby se vyhnul jednání, které způsobí nebo by mohlo způsobit narušení, ohrožení či přerušení IT infrastruktury Odběratele nebo narušení integrity či kvality služeb poskytovaných IT infrastrukturou Odběratele.

13. Odběratel oznámí písemně Dodavateli osoby odpovědné a oprávněné komunikovat jeho jménem s Dodavatelem ve věci plnění této Smlouvy.

IV.
Cena a platební podmínky

1. Cena Předmětu plnění (dále také jen „**Cena**") je stanovena jako nejvýše přípustná a nepřekročitelná a zahrnuje veškeré náklady, rizika, zisk a finanční vlivy (např. inflace nebo vývoj kurzu české měny vůči zahraničním měnám), a to po celou dobu realizace zakázky v souladu s podmínkami uvedenými v Zadávací dokumentaci. Ceny jsou závazné a nejvýše přípustné.

2. Cena zahrnuje veškeré náklady spojené s realizací Předmětu plnění dle čl. II. této Smlouvy včetně dodání/poskytnutí Licencí.

3. V souladu se zněním zákona č. 526/1990 Sb., o cenách se Smluvní strany dohodly na celkové Ceně za Předmět plnění ve výši:

Nabídková cena bez DPH	**18 337 218,88 Kč**
DPH 21%	**3 850 815,96 Kč**
Nabídková cena celkem vč. DPH	**22 188 034,84 Kč**

přičemž

A/ z projektu Odběratele *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"* (reg. č.: CZ.06.3.05/0.0/0.0/15_011/0007023 bude uhrazena částka za dodávku, instalace a implementace infrastruktury firewallů, včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů, příslušných licencí, zaškolení a zhotovení dokumentace a zajištění záručního servisu v rámci standardu záruky za jakost v prvních dvou letech ve výši:

Nabídková cena bez DPH	16 933 218,88 Kč
DPH 21 %	3 555 975,96 Kč
Nabídková cena celkem vč. DPH	20 489 194,84 Kč

Podrobný položkový Rozpočet Předmětu plnění je uveden v příloze č. 2 této Smlouvy.

B/ Z vlastních zdrojů Odběratele bude uhrazena částka za zajištění Technické podpory dle čl. V. odst. 2. písm. a) až d) této Smlouvy nad rámec prvních 2 (slovy: dvou let), přičemž cena za zajištění Technické podpory po dobu následujících 3 (slovy: tří) let od uplynutí prvních dvou let doby poskytování Technické podpory činí:

Nabídková cena bez DPH **za 3 roky**	1 404 000,00 Kč
DPH 21 %	294 840,00 Kč
Nabídková cena celkem **za 3 roky** vč. DPH	1 698 840,00 Kč
Nabídková cena bez DPH **za rok**	468 000,00 Kč
DPH 21 %	98 280,00 Kč
Nabídková cena celkem **za rok** vč. DPH	566 280,00 Kč

a tato cena bude hrazena ročně, vždy na 1 (slovy: jeden) rok trvání Technické podpory nad rámec prvních dvou let trvání Technické podpory, tj. od 3 (slovy: třetího) roku.

4. Zálohy nebudou poskytovány.

5. Dodavatel vyúčtuje Cenu nebo její část v souladu se Smlouvou, daňovým dokladem – fakturou (dále také jen „**Faktura**"), která bude vystavena na základě Akceptačního protokolu podepsaného odpovědnými zástupci obou Smluvních stran.

6. Dodavatel výslovně prohlašuje, že je ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, plátcem DPH, resp. pro oblast přijatého plnění osobou povinnou k dani. Dodavatel se zavazuje při účtování dodávky uvést na faktuře odpovídající kód nomenklatury celního sazebníku. V případě, že se na dodávku Předmětu plnění vztahuje přenesená daňová povinnost, uvede Dodavatel na faktuře pouze platnou sazbu DPH a sdělení, že výši daně je povinen vypočítat, doplnit a přiznat Odběratel, pro kterého je plnění uskutečněno (§92f)".

7. Splatnost Faktury se sjednává do **60** (slovy: šedesát) kalendářních dnů od doručení Faktury Odběrateli.

8. Faktura musí splňovat mimo náležitostí podle ust. § 28 zákona č. 235/2004 Sb., o dani z přidané hodnoty, dále níže uvedené náležitosti:

   a. předmět plnění je spolufinancován z prostředků Integrovaného regionálního operačního programu. Na Faktuře musí být vždy uveden:

      - název projektu: *„Kybernetická bezpečnost ICT Fakultní nemocnice Ostrava"*;
      - registrační číslo projektu: *CZ.06.3.05/0.0/0.0/15_011/0007023*;

- věta *„Projekt je spolufinancován v rámci Integrovaného regionálního operačního programu"*,

b. dále bude Faktura obsahovat:

- IČ;
- den splatnosti;
- označení peněžního ústavu a číslo účtu, ve prospěch kterého má být provedena platba, konstantní a variabilní symbol;
- odvolávka na smlouvu, číslo smlouvy, Dodavatele a Odběratele;
- razítko a podpis osoby oprávněné k vystavení účetního dokladu;
- přílohou Faktury bude kopie potvrzeného Akceptačního protokolu.

Smluvní strany se v souladu s ust. § 26, odst. 3, zákona č. 235/2004 Sb., o dani z přidané hodnoty, dohodly, že Dodavatel bude zasílat Fakturu, včetně příloh výhradně e-mailem na adresu: efakturace-inv@fno.cz.

Dodavatel se zavazuje při této komunikaci dodržovat následující pravidla:

- v jednom e-mailu budou jako přílohy zaslány dokumenty vztahující se pouze k jedné Faktuře, platí tedy pravidlo "jeden e-mail = jedna faktura a související dokumenty";
- všechny přiložené dokumenty budou výhradně ve formátu PDF a v pořadí dokladů: faktura, ostatní související dokumenty;
- Odběratel se zavazuje akceptovat takto zasílané dokumenty, pokud splňují ostatní náležitosti dané zákonem.

Pouze výjimečně je možné zasílat Fakturu v papírové podobě.

9. Za okamžik uhrazení Faktury se považuje datum, kdy byla předmětná částka odepsána z účtu Odběratele.

10. V případě, že Faktura nebude obsahovat výše uvedené náležitosti, je Odběratel oprávněn Fakturu vrátit do doby její splatnosti způsobem, který prokazuje, že do tohoto data Dodavatel vrácený daňový doklad od Odběratele převzal. V takovém případě je Dodavatel povinen Fakturu opravit a v případě, že by oprava činila Fakturu nepřehlednou, vystavit Fakturu nový. Opravená nebo nová Faktura musí být znovu zaslán Odběrateli a začíná běžet nová lhůta splatnosti.

V.
Technická podpora

1. Dodavatel zajistí Technickou podporu po dobu prvních 2 (slovy: dvou) let trvání Záruční doby ve smyslu čl. VI. odst. 4.1 této Smlouvy a případného rozšíření doby Technické podpory až o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let) a to za cenu sjednanou v čl. IV. odst. 3 písm. B/ této Smlouvy. Odběratel si vyhrazuje právo nevyužít případné rozšíření doby Technické podpory o další 3 (slovy: tři) roky (tj. na celkovou dobu 5 let). V tomto případě odešle Odběratel v prvních 2 letech trvání Záruční doby sdělení Dodavateli, že o rozšířenou dobu Technické podpory již nemá zájem.

2. Technická podpora bude poskytnuta v následujícím rozsahu:

a) možnost eskalace případné závady na technickou podporu výrobce přímo Odběratelem;

b) on-line přístup Odběratele k dokumentaci a znalostní bázi přímo na stránkách výrobce;

c) poskytnutí všech relevantních verzí Software, aktualizace geolokačních databází, signatur malware a IDS (Intrusion Detection System), databází IP adres a URL nabízené výrobcem tak, aby dodané Řešení vyhovovalo zadání Odběratele a fungovalo bez závad;

d) možnost Odběratele, aby se sám registroval na stránkách výrobce s možností samostatného stahování nových verzí Software a registrace k odběru automatických e-mailových zpráv týkajících se dodávaných zařízení a upozorňující na tyto skutečnosti:

- bezpečnostní incidenty, které vyžadují od Odběratele povýšení operačního systému / firmware či aplikování změny konfigurace či opravy (záplaty);
- konec prodeje či podpory;
- nové verze operačního systému / firmware;
- známé chyby operačního systému / firmware.

3. Technická podpora bude poskytnuta v režimu servis v místě instalace (tzv. on-site service).
4. Technická podpora bude poskytována v režimu 7 x 24 x 365 (7 dnů v týdnu a 24 hodin každého dne) na celé dodané Řešení.
5. Odběratel bude hlásit požadavky na poskytnutí Technické podpory (dále také jen „**Požadavky**") přes helpdesk systém Dodavatele (dále také jen „**Helpdesk**") dostupný na internetové adrese [redacted] nebo telefonicky na telefonní číslo servisního střediska Dodavatele [redacted]. Dodavatel bude veškeré Požadavky evidovat v Helpdesku a Odběratel bude mít k evidenci Požadavků přístup.
6. Dodavatel je povinen reagovat na jednotlivé Požadavky do 4 (slovy: čtyř) hodin od jejich nahlášení Dodavateli postupem dle odst. 4 tohoto článku výše (dále také jen „**Reakční doba**"). V rámci Reakční doby je Dodavatel povinen (i) potvrdit přijetí Požadavku a zahájit jeho řešení, (ii) v případě nemožnosti či nevhodnosti řešení Požadavku prostřednictvím vzdáleného přístupu se dostavit na místo, kde se nachází Infrastruktura firewallů, způsob řešení požadavku musí být odsouhlasen odpovědným pracovníkem Odběratele.
7. Dodavatel se zavazuje vyřešit Požadavek v následujících lhůtách:
   a) v případě, že Požadavek je zapříčiněn poruchou či závadou Hardware, zavazuje se Dodavatel k vyřešení Požadavků včetně odstranění případné závady (oprava) do 8 (slovy: osmi) hodin od přijetí Požadavku Dodavatelem, pokud odpovědný pracovník Odběratele písemně nepotvrdí souhlas s prodloužením doby vyřešení, v takovém případě musí být součástí písemného souhlasu i konkrétní termín vyřešení;
   b) v případě, že Požadavek je zapříčiněn jiným důvodem, než dle bodu a) výše, pokud se Smluvní strany nedohodnou jinak, bude Požadavek vyřešen do 14 (slovy: čtrnácti) kalendářních dnů ode dne jeho nahlášení, to vše, pokud není v této Smlouvě stanoveno jinak. V případě závad nebo problémů, které závažně ovlivňují služby poskytované dodaným systémem, musí Dodavatel, do doby finální opravy, zajistit do 8 hodin od nahlášení zjištěné závady funkcionalitu náhradním řešením.
8. Požadavek se považuje za vyřešený akceptací jeho řešení Odběratelem.
9. Po celou dobu zajišťování technické podpory dle odst. 1. tohoto článku výše, je Dodavatel povinen v případě dostupnosti nových verzí software/firmware nebo jejich oprav (tzv. patche), které řeší závažné bezpečnostní problémy nebo novou funkcionalitu řešení, po předchozím schválení Odběratelem, tyto aktualizace či opravy aplikovat, a to minimálně jednou ročně.
10. V případě, že Požadavek nebude vyřešen ve lhůtách sjednaných v tomto článku Smlouvy, je Odběratel oprávněn uplatnit požadavek na odstranění závady Infrastruktury firewallů přímo u výrobce.

VI.
Vady Předmětu plnění, jejich uplatnění a záruka

1. Vady Předmětu plnění

1.1. Předmět plnění vykazuje vady, nemá-li vlastnosti sjednané v této Smlouvě včetně jejich příloh, tj. zejména neodpovídá-li Technické specifikaci.

2. Právní vady

2.1. Dodavatel odpovídá za to, že jím poskytnutá plnění dle této Smlouvy nebudou zatíženy právem třetí osoby.

2.2. V případě, že k plněním poskytnutým Odběrateli na základě této Smlouvy uplatní právo jakákoliv třetí osoba, zavazuje se Dodavatel nahradit Odběrateli veškerou újmu takto způsobenou, jakož i náklady vynaložené na obranu práv Odběratele. Dodavatel se v takovém případě dále zavazuje na svůj náklad poskytnout Odběrateli veškerou možnou součinnost k ochraně jeho práv. Dodavatel je povinen na své náklady vypořádat veškeré nároky třetích osob uplatněné vůči Odběrateli z titulu právních vad plnění dodaného na základě této Smlouvy. V případě soudního sporu je Dodavatel povinen zajistit řádné a svědomité vedení takového sporu a činit veškeré potřebné úkony tak, aby práva Odběratele nebyla zpochybněna z důvodu nedostatečné procesní obrany; Odběratel se zavazuje poskytnout Dodavateli potřebnou součinnost při vedení takového sporu.

3. Reklamace vad

3.1. Jakákoliv reklamace vad Předmětu plnění musí být Odběratelem provedena bez zbytečného odkladu, nejpozději do 5 (slovy: pěti) pracovních dnů, co se Odběratel o vadě dozvěděl. Uplynutím této lhůty nedochází ke ztrátě nároků Odběratele z vad Předmětu plnění.

3.2. Reklamace bude prováděna písemně. Za písemnou formu pro účely reklamace vad Předmětu plnění považují Smluvní strany rovněž e-mailovou komunikaci.

3.3. V rámci písemné reklamace musí Odběratel sdělit popis reklamované vady včetně doložení případných fotografií, pokud je má Odběratel k dispozici.

4. Záruka za jakost a možnost rozšíření její doby

4.1. Záruka za jakost na celé Řešení a jeho dílčí části (dále také jen „**Záruka**") je 2 roky (dále také jen „**Záruční doba**") a začíná plynout ode dne převzetí Infrastruktury firewallů na základě podepsání Akceptačního protokolu Odběratelem. V případě, že dojde k rozšíření doby Technické podpory dle č. V. odst.1 a čl. IV. odst. 3 písm. B/ této Smlouvy, prodlužuje se Záruční doba i na celou dobu trvání rozšířené doby Technické podpory.

4.2. Dodavatel se zavazuje, že po dobu trvání Záruky bude mít dodané Řešení vlastnosti požadované Odběratelem v rámci Technické specifikace a vlastnosti obvyklé.

4.3. Případné náklady související s odstraněním vad dodaného Řešení včetně dílů a materiálu pro jejich odstranění, jsou v případě odstranění vad v rámci Záruky, neseny Dodavatelem.

VII.
Sankční ustanovení

1. V případě, že Dodavatel nesplní povinnost dle čl. II. odst. 2 této Smlouvy, vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

2. V případě, že Dodavatel nedodrží maximální dobu výpadku dle čl. III. odst. 5 této Smlouvy, vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 100.000,- Kč (slovy: jedno sto tisíc korun českých) za každé

jednotlivé nedodržení maximální doby výpadku síťových služeb poskytovaných firewally ve smyslu druhé věty čl. III. odst. 5 této Smlouvy. Úhradou smluvní pokuty není dotčeno právo na náhradu škody.

3. V případě, že v průběhu trvání Záruky Odběratel zjistí, že vlastnosti (zejména technické parametry) Hardware nebo Software jsou prokazatelně v rozporu s touto Smlouvou (zejména nesplňují minimální požadované parametry uvedené v Technické specifikaci uvedené v příloze č. 1 této Smlouvy), vzniká Odběrateli nárok vůči Dodavateli na smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Úhradou smluvní pokuty není dotčeno právo na náhradu škody. Rovněž porušení povinnosti zakládající nárok na smluvní pokutu dle tohoto odstavce představuje podstatné porušení této Smlouvy.

4. V případě prodlení Dodavatele s poskytnutím Technické podpory, tj. se splněním Reakční doby a/nebo splnění lhůty pro vyřešení Požadavku, vzniká Odběrateli nárok na smluvní pokutu vůči Dodavateli v následujícím rozdělení: (i) ve výši 2.000,- Kč (slovy: dva tisíce korun českých) za každou i jen započatou hodinu o kterou je překročena Reakční doba dle článku V. odst. 6 této Smlouvy, (ii) ve výši 5.000,- Kč (slovy: pět tisíc korun českých) za každou i jen započatou hodinu, o kterou je překročena doba dle článku V. odst. 7 písm. a) této Smlouvy a (iii) ve výši 50.000,- Kč (slovy: padesát tisíc korun českých) za každých i jen započatých 24 hodin, o které je překročena doba dle článku V. odst. 7 písm. b) této Smlouvy.

5. Odběratel se zavazuje při prodlení se zaplacením ceny Předmětu plnění zaplatit Dodavateli úrok z prodlení ve výši stanovené zákonem č. 89/2012 Sb., občanským zákoníkem.

6. V případě prodlení Dodavatele s plněním Termínu plnění vzniká Odběrateli vůči Dodavateli nárok na smluvní pokutu ve výši 0,5% (slovy: pět desetin procenta) z ceny Předmětu plnění za každý započatý den prodlení. Úhradou smluvní pokuty není dotčeno právo na náhradu škody.

7. Smluvní pokuty dle tohoto článku Smlouvy jsou splatné 3. (slovy: třetí) den od doručení výzvy k jejich úhradě druhé Smluvní straně.

VIII.
Ochrana osobních údajů a důvěrných informací

1. Smluvní strany se zavazují při zpracování osobních údajů dodržovat nařízení Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016, obecného nařízení o ochraně osobních údajů (dále jen „**GDPR**"). Smluvní strany berou na vědomí, že cílem této Smlouvy není zpracování osobních údajů třetích osob (ve smyslu tohoto odstavce jsou třetími osobami chápáni i zaměstnanci smluvních stran). Za předpokladu, že se i přes tuto skutečnost dostane Dodavatel do kontaktu s osobními údaji třetích osob, zavazuje se tyto zpracovávat v minimálním možném rozsahu a v souladu s GDPR a případnou smlouvou o zpracování osobních údajů uzavřenou mezi Smluvními stranami.

2. Smluvní strany se vzájemně zavazují zachovávat mlčenlivost o všech podstatných skutečnostech získaných při své činnosti vyplývající z této Smlouvy (dále jen „**Povinnost mlčenlivosti**"), a to zejména o skutečnostech, které tvoří jejich obchodní tajemství ve smyslu ust. § 504 Občanského zákoníku a důvěrné informace (dále také jen „**Důvěrné informace**").

3. Za Důvěrné informace Odběratele Smluvní strany považují zejména (nikoliv výlučně):
   a) strukturu počítačových systémů a programů Odběratele;
   b) popis procesů Odběratele;
   c) přístupové údaje k počítačovým systémům a programů Odběratele;
   d) data Odběratele;
   e) informace o plánovém rozvoji struktury počítačových systémů a programů Odběratele.

4. Za Důvěrné informace Dodavatele Smluvní strany považují detailní funkční specifikaci Řešení.

5. Za Důvěrné informace kterékoliv Smluvní strany se dále považují informace a údaje, které poskytující Smluvní strana výslovně a zřetelně označí jako „důvěrné".

6. Za porušení Povinnosti mlčenlivosti je kvalifikováno jednání, jímž jedna smluvní strana jiné osobě neoprávněně sdělí, zpřístupní, pro sebe nebo pro jiného využije obchodní tajemství či Důvěrné informace získané při své činnosti od jiné Smluvní strany, pokud je to v rozporu se zájmy jiné Smluvní strany, a učiní tak bez jejího souhlasu.

7. Porušením závazku mlčenlivosti není:

   a) poskytnutí obchodního tajemství a/nebo Důvěrných informací v nezbytném rozsahu orgánům nebo osobám majícím ze zákona právo na tyto informace a kontrolu činnosti Smluvních stran;

   b) poskytnutí obchodního tajemství a/nebo Důvěrných informací osobám, které mají ze zákona uloženou povinnost mlčenlivosti (notář, advokát, daňový poradce);

   c) poskytnutí obchodního tajemství a/nebo Důvěrných informací Smluvní strany či umožnění přístupu k němu třetím osobám v souvislosti s plněním této Smlouvy, pouze však v nezbytném rozsahu, přičemž příslušná Smluvní strana je povinna poučit tyto třetí osoby o tom, že jde o obchodní tajemství a/nebo Důvěrné informace jiné Smluvní strany a zavázat takové třetí osoby k mlčenlivosti nejméně ve stejné rozsahu v jakém je k mlčenlivosti vázána dle této Smlouvy Smluvní strana, třetí osobě takové informace sdělující;

   d) použití obchodního tajemství a/nebo Důvěrných informací v souladu s touto Smlouvou nebo na základě výslovného souhlasu příslušné Smluvní strany, popř. jiné použití důvěrných informací, které se staly veřejně dostupnými nikoliv v důsledku porušení závazku mlčenlivosti povinnou Smluvní stranou;

   e) použití a/nebo sdělení obchodního tajemství a/nebo Důvěrných informací Odběratelem třetí osobě za účelem správy, údržby, rozšíření, úprav, změn, oprav a dalšího nakládání se Software prováděného pro Odběratele takovou třetí osobou.

8. Veškeré důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její vlastní důvěrné informace.

9. Povinností mlčenlivosti jsou Smluvní strany vázány po dobu trvání skutečností zakládajících tuto Povinnost mlčenlivosti, pokud nebudou mlčenlivosti zproštěny nebo se nestanou dané informace veřejně dostupnými jinak než porušením Povinnosti mlčenlivosti některou ze Smluvních stran.

10. V případě porušení Povinnosti mlčenlivosti Dodavatelem, vzniká Odběrateli nárok na smluvní pokutu ve výši 100.000,- Kč (slovy: sto tisíc korun českých) za každé jednotlivé porušení Povinnosti mlčenlivosti. Tato smluvní pokuta je splatná do 10 (slovy: deseti) kalendářních dnů od doručení výzvy k její úhradě. Úhradou této smluvní pokuty není dotčen nárok Odběratele na náhradu škody ani nárok na případné sankce ze závislých smluv na této Smlouvě.

IX.
Ukončení Smlouvy

1. Odběratel je oprávněn od této Smlouvy odstoupit kromě podmínek daných zákonem č. 89/2012 Sb., občanským zákoníkem a případů sjednaných v této Smlouvě, rovněž v následujících případech, které se považují za podstatné porušení této Smlouvy:

   a) prodlení Dodavatele s dodáním Hardware, Licencí nebo jiných plnění dle této Smlouvy, které je delší než 30 (slovy: třicet) kalendářních dnů;

   b) prodlení s Technickou podporou o více než 7 (slovy: sedm) kalendářních dnů.

2. V případě odstoupení od Smlouvy jsou si Smluvní strany povinny vrátit vše, co si v souvislosti s touto Smlouvou plnily, přičemž Smluvní strany se dohodly, že dojde-li k odstoupení v druhém nebo dalším roce trvání platnosti této Smlouvy, není Dodavatel povinen vracet tu část uhrazené Ceny, po jaký počet měsíců trvala tato Smlouva s tím, že tato částka, kterou nebude Dodavatel povinen vracet, bude určena z ceny Technické podpory dle čl. IV. odst. 3 písm. B/ jako její poměrná část.

3. Zánikem Smlouvy z důvodu odstoupení od Smlouvy nezanikají nároky na smluvní pokuty sjednané v čl. VII. této Smlouvy, stejně jako nezaniká právo na náhradu škody.

X.
Závěrečná ustanovení

1. Pohledávky vyplývající z této Smlouvy nemohou být postoupeny třetí osobě bez předchozího písemného souhlasu druhé Smluvní strany.
2. V souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole, je Dodavatel osobou povinnou spolupůsobit při výkonu finanční kontroly. Tato povinnost se vztahuje na právnickou nebo fyzickou osobu, podílející se na dodávkách zboží nebo služeb hrazených z veřejných rozpočtů nebo z veřejné finanční podpory.
3. Dodavatel je povinen archivovat veškerou dokumentaci související s realizací Předmětu plnění, zejména originální vyhotovení Smlouvy, její dodatky, originály účetních dokladů a dalších dokladů vztahujících se k realizaci Předmětu plnění této Smlouvy po dobu 10 (slovy: deseti) let od zániku závazku vyplývajícího ze Smlouvy a po tuto dobu je Dodavatel rovněž povinen umožnit kontrolu těchto dokladů osobám oprávněným k výkonu kontroly Předmětu plnění a vytvořit těmto osobám podmínky k provedení kontroly vztahující se k realizaci Předmětu plnění a poskytnout jim při provádění kontroly součinnost.
4. Smluvní strany se dohodly, že 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), tuto Smlouvu, včetně případných dodatků, v Registru smluv uveřejní Odběratel.
5. Veškeré změny a doplňky této Smlouvy je možné činit písemně, a to formou číslovaných dodatků.
6. Tato Smlouva se uzavírá písemně elektronickými prostředky, a to zaručeným elektronickým podpisem oprávněných zástupců obou smluvních stran.
7. Veškeré právní vztahy touto Smlouvou neupravené se řídí obecně závaznými právními předpisy České republiky, zejména zákona č. 89/2012 Sb., občanským zákoníkem.
8. Tato Smlouva nabývá platnosti podpisem obou Smluvních stran a účinnosti od data zveřejnění v Registru smluv.
9. Jestliže jednotlivá ustanovení této Smlouvy jsou nebo se stanou zcela nebo částečně neplatnými nebo jestliže v této Smlouvě nějaké ustanovení zcela chybí, není tím dotčena platnost ostatních ustanovení. Namísto neplatného či chybějícího ustanovení dohodnou Smluvní strany takové platné ustanovení, které nejvíce odpovídá smyslu a účelu neplatného či chybějícího ustanovení.

Přílohy:

Příloha č. 1 - Technická specifikace Předmětu plnění;
Příloha č. 2 – Položkový rozpočet Předmětu plnění
Příloha č. 3 – Realizační tým Dodavatele

V Ostravě, dne: dle elektronického podpisu

MUDr. Jiří Havrlant

Digitálně podepsal MUDr. Jiří Havrlant
Datum: 2021.08.27 14:10:42 +02'00'

Fakultní nemocnice Ostrava
MUDr. Jiří Havrlant, MHA
Ředitel

V Praze, dne: dle elektronického podpisu

Ing. Milan Zinek

Digitally signed by Ing. Milan Zinek
Date: 2021.08.18 13:35:06 +02'00'

ALEF NULA,a.s.
Ing. Milan Zinek
Předseda představenstva

Příloha č. 1

Technická specifikace předmětu plnění

Obnova infrastruktury firewallů – technická specifikace

Popis požadavku
Motivace požadavku
Zajištění ochrany perimetru datové sítě zadavatele, zabezpečení koncových bodů datové sítě a centrální správa celého systému. Řešení tak napomáhá splnění požadavků daných §18 Bezpečnost komunikačních sítí a §21 Ochrana před škodlivým kódem Vyhlášky o kybernetické bezpečnosti č. 82 /2018 Sb.

POPIS SOUČASNÉHO STAVU
Lokalita FNO
V prostředí Fakultní nemocnice Ostrava (dále jen "**FNO**" nebo "**Zadavatel**") jsou nyní provozována dvě nezávislá datová centra DC1 a DC2 vzájemně propojená LAN konektivitou. LAN konektivita je postavena na dvou chassis Cisco 9606R zapojených do clusteru (StackWise Virtual).
Stávající firewally Cisco ASA5585-X s modulem SFR řízené centrálním managementem FMC, umístěné v obou datových centrech, filtrují síťový provoz na vrstvách L3 – L7 OSI modelu, jsou zapojeny v režimu vysoké dostupnosti a zajišťují připojení do sítě Internet v rámci samostatných kontextů (virtuálních instancí firewallů) přes 3 nezávislé ISP s následující konektivitou:

- ISP1 – 1Gb/1Gb
- ISP2 – 1Gb/1Gb
- ISP3 – 50Mb/50Mb

Lokalita LDN Klokočov
V rámci detašovaného pracoviště LDN Klokočov jsou provozována 2 datová centra vzájemně propojená na druhé vrstvě modelu OSI. V těchto datových centrech jsou umístěny firewally Cisco ASA5506-X s moduly SFR řízené centrálním managementem FMC, které jsou zapojené v režimu vysoké dostupnosti, a které zajišťují filtraci síťového provozu na vrstvách L3 – L7 OSI modelu a připojení do sítě Internet přes 2 nezávislé ISP s následující konektivitou:

- ISP1 – 100Mb/100Mb
- ISP2 – 16Mb/16Mb

Firewall také navazuje site to site VPN s lokalitou FNO v režimu vysoké dostupnosti.
Lokalita KC Avion
V detašovaném pracovišti KC Avion je připojení do sítě Internet a filtrace síťového provozu na vrstvách L3 – L7 OSI modelu zabezpečena firewallem Cisco ASA5506-X s modulem SFR řízeným centrálním managementem FMC přes jednoho ISP s následující konektivitou:

- ISP1 – 20Mb/20Mb

Firewall také navazuje site to site VPN s lokalitou FNO.
Management firewallů
Centrální správa a sběr informací z jednotlivých firewallů je zajištěna centrálním management systémem Cisco FMC (Firepower Management Center).
Jednotlivá pravidla firewallů využívají identifikaci uživatelů a jejich členství ve skupinách AD ve spolupráci se systémem pro správu identit Cisco Identity Services Engine (ISE) a autentizací koncových zařízení protokolem 802.1x.
Monitoring firewallů pak zabezpečuje systém Cisco Prime Infrastructure, systém Zabbix a síťová analytická platforma IP Fabric pomocí síťových protokolů SNMP, ICMP a SSH.
Ochrana koncových zařízení – počítačů
Ochrana koncových zařízení je zajištěna lokálně nainstalovaným antivirovým řešením ESET Endpoint Security a ESET Endpoint Antivirus bez integrace na stávající firewally nebo jejich management.

Obecný popis požadovaného řešení
Předmětem plnění této veřejné zakázky je obnova technologické infrastruktury firewallů, včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů, jež bude integrována v rámci firewallů.
Systém firewallů bude dodán včetně instalace, implementace, plné konfigurace, uvedení do provozu, zajištění technické podpory, zajištění záruky, zajištění dostupnosti softwarových aktualizací, a to na všechny části a komponenty dodaného systému (HW, SW i licence). Za kvalitu a včasnost provádění servisu ručí vždy Dodavatel.
Systém bude nasazen v datových centrech umístěných ve třech lokalitách Zadavatele – areálu FN Ostrava v sídle Zadavatele, LDN Klokočov a KC Avion.
Zadavatel požaduje od Dodavatele o plnění veřejné zakázky (dále jen také „Dodavatel", „Účastník") následující plnění:

- Obnovit firewally, které v současnosti přestaly být podporovány výrobcem a jejich používání již není pro Zadavatele ekonomické ani bezpečné. Zadavatel požaduje dodání firewallů s nástrojem pro jejich

centrální management, které splňují požadavky na technické parametry, jež jsou popsány v tabulkách níže. Poskytování podpory všech komponent v tomto bodě bude 24 + (dalších) 36 měsíců ode dne dodání celého předmětu veřejné zakázky a náklady s ní spojené musí být součástí ceny (odděleně 24 a dalších 36 měsíců).

- Je poptáván systém pro centrální správu soutěžených bezpečnostních technologií Zadavatele, tzn. Firewally a Endpoint klienty. Systém musí být plně kompatibilní s dodávanými zařízeními.
- Je poptáváno řešení ochrany endpoint klientů před zero-day škodlivým kódem, viry a malware. Dodávané řešení musí být plně integrováno s dodávaným firewallem a nástrojem pro jejich centrální správu.
- Vlastní dodávku zařízení.
- Požadavky na zařízení jsou rozděleny do několika skupin podle typu zařízení. Parametry pro jednotlivé typy poptávaných technologií jsou uvedeny níže v tabulkách.

Obecné požadavky a parametry

- Všechny v zadání zmíněné parametry jsou definovány jako minimální, není-li uvedeno jinak.
- Veškeré dodávané HW a SW produkty musí být Dodavatelem získány legálně a umožnit využití těchto produktů Zadavatelem, jako koncovým zákazníkem, v souladu s distribučními a licenčními podmínkami výrobce.
- V případě dodání HW a SW produktů Zadavateli, jako koncovému zákazníkovi, nesmí být Zadavatel nijak omezen ve svých nárocích vyplývajících ze záruky výrobce dodávaných zařízení/software a z produktové podpory, kterou tento výrobce k dodávaným HW a SW produktům poskytuje. Uvedené musí zahrnovat i nárok Zadavatele na přístup k relevantním SW releases a novým verzím SW po celou dobu trvání podpory výrobce.
- Musí být umožněn online přístup Zadavatele k dokumentaci výrobce HW/SW a znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- Vzhledem k tomu, že Zadavatel provozuje informační systém základní služby a protože zařízení budou součástí bezpečnostní infrastruktury, musí být součástí nabídky doklad výrobce či odkaz na veřejně dostupné webové stránky výrobce, z jejichž obsahu bude nad veškerou pochybnost zřejmé, že výrobce nabízených aktivních síťových prvků má implementován tzv. "SDL - secure development lifecycle" při vývoji svých produktů a tzv. "SIRT - Security Incident Response Team" pro reportování bezpečnostních incidentů spojených s nabízenými produkty.
- Zadavatel musí mít možnost eskalovat závady přímo k technické podpoře výrobce HW/SW, včetně možnosti si sám a přímo otevřít požadavek na technickou podporu, provádět změny priority požadavků a případné eskalace pracovníky Zadavatele. A to po celou dobu požadované podpory.
- V databázi výrobce musí být Zadavatel veden jako první uživatel zboží a licencí / subscripcí / operačních systémů. Zadavatel požaduje originální a nová zařízení určená pro evropský trh. Před převzetím zboží si Zadavatel vyhrazuje právo kontroly dle sériových čísel u výrobce. Pokud v databázi výrobce bude uveden jiný koncový uživatel než Zadavatel nebo jiné určení než pro evropský trh, bude se jednat o porušení této podmínky.
- Dodavatel musí garantovat, že v případě dodání zboží Zadavateli, jako koncovému zákazníkovi, bude Dodavatelem poskytnuta k dodávanému zařízení záruka a produktová podpora v plném, minimálně výrobcem poskytovaném rozsahu.
- V případě, že Dodavatel nesplní povinnost do 7 pracovních dnů od doručení žádosti Zadavatele předložit potvrzení výrobce o určení dodaného zboží pro evropský trh případně jiného dokladu výrobce nebo jím pověřené osoby prokazující pro dodaná zařízení provozovaná na území ČR poskytnutí plné podpory výrobce nebo jím pověřené osoby při řešení technických problémů (požadavek uvedený v ZD), může Zadavatel požadovat po Dodavateli jednorázovou smluvní pokutu ve výši 500.000, - Kč. Současně bude mít zadavatel právo odstoupit od smlouvy z důvodu jejího podstatného porušení.
- Předmětné plnění musí být dodáno oficiálním distribučním a prodejním kanálem výrobce dle nařízení Komise (EU) č. 330/2010 o selektivní distribuci.
- V případě, že v průběhu záruční lhůty Zadavatel zjistí, že vlastnosti (zejm. technické parametry) dodaného zboží nebo software jsou prokazatelně v rozporu s technickou specifikací uvedenou v zadávací dokumentaci veřejné zakázky (nesplňují minimální požadované parametry uvedené v zadávací dokumentaci), má Zadavatel nárok uplatnit vůči Dodavateli jednorázovou smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých). Současně má Zadavatel právo odstoupit od smlouvy, na základě které byla provedena dodávka předmětu veřejné zakázky z důvodu podstatného porušení takové smlouvy.
- Zaplacení smluvní pokuty výše uvedené se nedotýká nároku Zadavatele na náhradu škody, kterou Dodavatel porušením povinnosti výše uvedených způsobil, a to v plné výši.
- Součástí všech zařízení musí být dodávka SW a firmware v aktuální nebo dohodnuté verzi.
- Součástí dodávky musí být poskytnutí práva užívat nabízeného software (dále též „licence").
- U každého dodávaného zařízení Dodavatel uvede v nabídce jeho přesnou specifikaci, obchodní název, výrobce a identifikátor zboží (part number).

Počet požadovaných zařízení

Zařízení	Počet ks
NGFW Appliance, Typ A	3
NGFW Appliance, Typ B	2
Management Center	1
EndPoint Malware Protection (integrován s NGFW)	3000

Detailní popis požadovaného HW a SW a požadovaných vlastností je uveden níže.

Technické požadavky na poptávanou technologii
Požadavky na Firewall typ A

- Šasi pro montáž do standardního racku (včetně příslušných dílů pro montáž), výška 1RU;
- Minimálně 1 port 1Gb/RJ-45 určený pro management;
- Minimálně 8 standardně osazených portů 1Gb/RJ-45 určených pro data (LAN/WAN);
- Minimálně 2 porty ze standardně osazených portů budou PoE+;
- Minimálně 1 console port RJ-45 (RS-232) a 1 port USB 3.0;
- Minimálně 100.000 současně otevřených spojení při využití AVC (funkcionalita NextGen Firewallu se zajištěním aplikační visibility a deep packet inspection);
- Minimálně 6.000 nových spojení za sekundu při využití AVC;
- Propustnost stavového firewallu (multiprotokolový režim) minimálně 2 Gbps;
- Minimálně 50 podporovaných VLAN na interface;
- Minimální propustnost 650 Mbps při využití AVC;
- Minimální propustnost 650 Mbps při využití AVC a IPS;
- Podpora L2 (transparentního) módu s podporou NAT a PAT;
- Podpora L3 (routovaného) módu s podporou NAT a PAT;
- Podpora vysoké dostupnosti v režimu Active/Standby včetně případně potřebných licencí;
- Propustnost VPN koncentrátoru (šifrování 3DES/AES) minimálně 300 Mbps;
- Minimálně 75 současných šifrovaných spojení.

Požadavky na Firewall typ B

- Šasi pro montáž do standardního racku (včetně příslušných dílů pro montáž), výška 1RU;
- Minimálně 1 port 1Gb/RJ-45 určený pro management;
- Minimálně 24 osazených portů 10Gb/SFP+ určených pro data (LAN/WAN);
- Redundantní zdroje (Hot-Swappable);
- Minimálně 25.000.000 současně otevřených spojení při využití AVC (funkcionalita NextGen Firewallu se zajištěním aplikační visibility a deep packet inspection);
- Minimálně 265.000 nových spojení za sekundu při využití AVC;
- Propustnost stavového firewallu (multiprotokolový režim) minimálně 45 Gbps;
- Minimálně 1024 podporovaných VLAN na interface;
- Podpora vysoké dostupnosti v režimu Active/Standby včetně případně potřebných licencí;
- Minimální propustnost 40 Gbps při využití AVC;
- Minimální propustnost 35 Gbps při využití AVC a IPS;
- Podpora L2 (transparentního) módu s podporou NAT a PAT;
- Podpora L3 (routovaného) módu s podporou NAT a PAT;
- Podpora zvyšování výkonu pomocí sloučení firewallů do jednoho logického clusteru složeného z minimálně 6 firewallů, kde cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP;
- Podpora virtuálních bezpečnostních kontextů (virtuálních firewallů) s licencí pro minimálně 10 instancí;
- Minimální propustnost firewallu jako VPN koncentrátoru (šifrování 3DES/AES) 14 Gbps;
- Minimálně 20.000 současných šifrovaných spojení.

Požadavky na EndPoint funkcionalitu

- Software pro ochranu koncových stanic/zařízení (dále také jen "**Endpoint SW**") musí vyžadovat na koncové stanici nejvýše 100 MB datového prostoru na lokální pevném disku a musí podporovat manuální i bezobslužnou instalaci;
- Instalace (nasazení) **Endpoint SW** musí být možné také pomocí nástrojů pro správu systémů 3. stran;
- Endpoint SW musí být podporován na následujících platformách:
    - Windows 7 až 10, server 2008 až 2019
    - Mac OS
    - Linux Red Hat Enterprise
    - Android, iOS
- Analýza hlavní příčiny na podezřelých koncových stanicích musí poskytovat min. následující funkce:

  - Sekvenční a chronologické stopy událostí s detaily, včetně hostitele, uživatelského jména, IP adresy a klientské aplikace;
  - Podrobnosti musí obsahovat informaci o tom, který soubor, proces, nebo služby byly ovlivněny.
- Endpoint SW musí umožňovat sdílení informací o počítačových hrozbách mezi bezpečnostními řešeními pomocí frameworku STIX za účelem zmírnění kompromitace, nebo pro vyžádání izolace koncového bodu v síti;
- Endpoint SW musí spolupracovat se systémem pro správu identit ISE a na základě korelování informací umět provést akce zabraňující šíření malware v síti;
- Endpoint SW musí umět importovat malware události detekované na koncovém zařízení (bodu) do centrálního managementu NGFW aby mohly tyto události spravovány spolu s malwarovými událostmi generovanými kompatibilním NGFW systémem;
- Importovaná data pro tyto malware události musí zahrnovat informace o skenování, detekci malwaru, informace o karanténě, provedené blokaci, náznaky kompromitace (IOC) hostitele, které kompatibilní NGFW monitoruje;
- Endpoint SW musí podporovat sledování podezřelých souborů (malware) a poskytnout vizualizaci na úrovni sítě: postižené uživatele, systémy, Patient Zero – Day Zero (způsob a místo jakým hrozba pronikla do sítě);
- Endpoint SW musí podporovat sledování chování souboru, aktivity jednotlivých procesů a musí umět automaticky generovat výstrahy při prvních známkách škodlivého chování;
- Řešení musí podporovat průběžné a neustálé monitorování souborů pro retrospektivní náhled detekce / blokování hrozby (malware). Musí být tak možné retrospektivně dohledat a vysledovat šíření (trajektorii) malware přes soubory a jednotlivá zařízení včetně informací o identitách spojených s těmito zařízeními pomocí integrace s ISE;
- Řešení musí umět identifikovat zranitelný software a chyby zabezpečení na koncovém bodu;
- Řešení musí podporovat úplnou analýzu souborů v zabezpečené karanténě (sandboxu) poskytující podrobnou zprávu o podezřelém chování souboru (malware)
- Součástí řešení musí být přístup k dashboardu sandboxové analýzy, pokud se nejedná o primární dashboard řešení;
- Řešení musí zajišťovat pokročilou detekci a reakci koncových bodů (EDR);
- Software pro koncové body musí být schopen blokovat CnC komunikaci, Sniffer / Dropper aktivity a obsah pro šíření škodlivého kódu;
- Reakce na událost a její náprava na koncových stanicích musí min. obsahovat:
  - Sledování a zachytávání souborů s možností vyhledat škodlivé soubory na podezřelých koncových bodech
  - Blokování souborů, procesů nebo služeb, které vykazují škodlivé chování
  - Detekce Dropper aktivit a blokování stahování přes URL / web stránky
  - Možnost odeslat podezřelé škodlivé soubory pro další analýzu
- Součástí řešení musí být centrální správa umožňující přehled o bezpečnostních incidentech přes zařízení, hosty, aplikace, uživatele, soubory a geolokační informace.

Jednotné požadavky na NGFW a společný MNG

Obecné požadavky

- Dynamické směrování – podpora alespoň RIP, OSPF, BGP
- Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP
- Podpora Policy based Routing
- Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací apod.
- Podpora filtrace IPv4, IPv6
- Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD
- Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích
- Podpora inspekce IPv6 provozu
- Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v internetu
- Stateful inspekce minimálně těchto aplikačních protokolů: HTTP, FTP, Instant Messenger, File Sharing, SIP, H.323, SCCP, SMTP, ESMPT, DNS, RPC, CIFS, MSRPC, NETBIOS
- Podpora NAT64 a DNS64
- Možnost integrace cloudových bezpečnostních bran s transparentním směrováním určitého provozu na tyto prvky a zde prováděnou inspekci na škodlivý kód, případně pro řízení přístupu podle uživatelské identity, typu aplikace apod.
- Bezpečnostní pravidla musí kromě adres a portů zohlednit i identitu uživatele
- Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech
- API rozhraní pro sdílení kontextových informací s dalšími systémy
- Možnost začlenit do SDN řešení – kontrolérem řízená infrastruktura (APIC)

Funkce IPS

- Možnost definovat typ provozu předávaný k inspekci do IPS
- Podpora také IDS režimu – pasivního monitorování (TAP režim)
- Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)
- Možnost obejití IPS funkcí při zahlcení nebo nedostupnosti
- Podpora 802.1Q tagovaných rámců
- Inspekce pro IPv4 i IPv6
- Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému
- IPS musí obsahovat filtry/signatury popisující exploity, zranitelnosti, krádeže identity, spyware, viry, průzkumné aktivity, ochranu síťové infrastruktury, IM aplikace, P2P sítě a nástroje na kontrolu toku multimédií
- Automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací
- Podpora aplikace pro psaní zákaznických filtrů
- Podpora importu komunitních filtrů/signatur Snort
- IPS musí umět detekovat a blokovat útoky průzkumných aktivit
- IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS
- IPS musí umět detekovat a blokovat útoky na základě IP adresy, nebo DNS jména „known bad host" jako je spyware, phishing nebo Botnet C&C
- IPS musí umět detekovat a blokovat útoky proti síťové infrastruktuře firmy, jako jsou přepínače, routery, firewall, bezdrátové přepínače a podobně. Dále musí poskytovat i ochranu pro protokoly využívané v IP telefonii
- Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události
- Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku
- Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive
- Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí
- Možnost definice uživatelské vrstvy politik
- Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik
- Různé politiky lze sdílet a aplikovat na různé senzory
- Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů
- Ochrana před malware typu „zero day attack" které nelze detekovat tradičními antiviry
- Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, musí být IPS schopna reagovat
- Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole
- Možnost ochrany před malware až do úrovně koncových stanic s centralizovanou správou bezpečnostních politik, blacklistů pro aplikace, řízení spouštění aplikací, přesun malware do karantény, blacklistů pro síťovou komunikaci apod.
- Retrospektivní ochrana koncových stanic (chytré telefony), stanice s Windows, Mac OS – pokud je později SW kód rozpoznán v operačním centru dodavatele jako malware, je na koncových stanicích okamžitě přesunut do karantény
- Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice
- IPS musí být plně transparentní k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků
- Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation"
- Možnost automatické i manuální klasifikace stanice jako "kritické" se zohledněním v pravidlech, reportech apod.
- Podpora automaticky spouštěných příkazů na základě definovaných kritérií, pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování apod. včetně otevřeného rozhraní (API) pro uživatelsky definované příkazy a jejich posloupnosti.
- Podpora databází reputací adres v internetu (Security Intelligence)

Funkce Next Generation Firewallu

- Možnost definovat typ provozu předávaný k inspekci do Next Generation Firewallu
- Podpora pasivního monitorování (TAP režim)
- Možnost definovat režim provozu při zahlcení nebo nedostupnosti Next-Gen FW funkcí (fail open, fail close)

- Možnost obejití Next-Gen FW funkcí při zahlcení nebo nedostupnosti
- Podpora 802.1Q tagovaných rámců
- Podporovaných min. 4000 různých aplikací
- Kategorie aplikací (nebezpečné, důležité apod.)
- Podporovaných min. 80 různých URL kategorií
- Podporovaných min. 280 milionů kategorizovaných světových URL
- Řízení přístupu k WWW – Web Usage Control (WCU)
- Filtrace podle typů aplikací webových i ne-webových
- Filtrace podle reputace serverů
- SSL inspekce (dekrypce/enkrypce)
- Security Inteligence database – známé uzly botnet sítí C&C
- Security Inteligence database – známé adresy anonymních proxy, otevřených mail relay, apod.
- Možnost integrovat vlastní reputační databáze
- Podpora komunitních, otevřených standardů popisu apliací (OpenAppID)
- Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)
- Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě (Network Behavior Analysis – NBA)
- Řešení musí být schopné pasivního sběru informací o síťových zařízení a zobrazení:
    - Typ zařízení
    - Operační systém
    - Dodavatel OS
    - Použité síť. protokoly
    - Použité síť. služby
    - Otevřené porty síť. služeb
    - Potenciální zranitelnosti
- Přehled o síťových spojení má poskytovat minimálně tyto informace:
    - Čas startu a konce flow
    - Akce (allow, deny,..)
    - Důvod případného blokování
    - Zdrojová a cílová adresa
    - Vstupní a výstupní zóna
    - Vstupní a výstupní rozhraní
    - Zdrojový a cílový port
    - Aplikační protokol
    - IPS událost, pokud vznikne
    - Riziková úroveň IPS události
    - Použitá síťová aplikace
    - Rizikovost aplikace
    - „Business impact" aplikace
    - Množství přenesených dat

Funkce VPN

- Podpora IPSec VPN
- IPsec VPN s podporou standardů: RFC 2408 - Internet Security Association and Key Management Protocol (ISAKMP), RFC 2409 - The Internet Key Exchange (IKE), RFC 2412 - OAKLEY Key Determination Protocol
- Podpora nového protokolu pro výměny klíčů IKEv2
- Podpora šifrovacích metod – minimálně: DES, 3DES, AES-128, AES-192, AES-256
- Podpora kontrolních mechanizmů: MD5, SHA
- Podpora NextGen šifrovacích algoritmů: AES-GCM/GMAC-128, AES-GCM/GMAC-192, AES-GCM/GMAC-256
- Podpora komponentu Suite-B: SHA-2 mechanizmu s metodami: SHA-256, SHA-384
- Podpora šifrovacích algoritmů eliptických křivek (součást Suite-B): ECDH, ECDSA
- Podpora SSL VPN
- Jednotný klient pro IPsec (IKEv2) i SSL VPN
- SSL VPN klient k dispozici pro všechny běžné desktopové OS: Windows 7 - 10 (32-bit a 64-bit), MAC OS X(10.5 - 10.8.x), Linux
- Podpora TLS i DTLS pro SSL připojení
- Podpora SSL VPN v tunelovém režimu s distribucí VPN klientského SW přímo z FW
- Podpora současné autentizace koncové stanice i uživatele
- Podpora definice pravidel pro VPN přístup přímo prostředky FW a jejich automatická distribuce VPN připojeným klientům
- Jednotná správa VPN přístupů pro různé mobilní platformy a různé OS, včetně smart-phone a tabletů

- Možnost definovat specifická přístupová oprávnění (bezpečnostní politiky, ACL atd.) podle identity nebo skupiny uživatele (např. v AD)
- Podpora definice různých LDAP nebo AD serverů podle mapování uživatelů na skupiny s využitím RADIUS, LDAP nebo hodnot v certifikátu
- Možnost dynamického přiřazení bezpečnostních politik (způsob a možnosti přístupu) podle aktuálního stavu koncové stanice: detekce instalovaných verzí bezpečnostního SW, detekce typu platformy a operačního systému
- Podpora VPN připojení na úrovni virtuálních kontextů
- podpora VPN clustering a load balancing
- Podpora autentizačních mechanizmů: lokální databáze na FW, RADIUS, Windows NT LAN Manager (NTLM), Active Directory Kerberos, RSA softID, RSA securID, Lightweight Directory Access Protocol (LDAP), digitální certifikáty (X.509), smartcards
- Podpora veřejných CA
- Možnost současné autentizace AAA a certifikátem
- Podpora CRL a OCSP pro kontrolu revokace certifikátu
- Podpora SSO metod: KCD, Netegrity, ClearTrust, SAML, NTLM/FTP/CIFS pass-through, HTTP pass-through pomocí formuláře; HTTP-POST pomocí substitucí proměnných
- Podpora IPv6 adresních rozsahů a přiřazení IPv6 adres klientům v případě dual-stack přístupu přes IPv4 infrastrukturu
- Podpora čistého IPv6 přístupu na VPN koncentrátor
- Možnost jednotné správy přístupu uživatelů přes VPN ale i lokálně na LAN a WiFi

Management

- Vzdálená správa konfigurace přes grafické rozhraní bez nutnosti instalace zvláštního SW
- Možnost přístupu přes IPv6: SSHv2, Telnet, HTTP/HTTPS a ICMP
- Možnost centrální správy při nasazení více firewallů
- Při centrální správě: možnost sdílených bezpečnostních politik
- Distribuce a správa SW firewallu, dalších modulů (např. pro VPN), konfigurací, licencí z grafického rozhraní managementu
- Zobrazení logů a událostí v grafickém rozhraní správy s mapováním na konfiguraci bezpečnostních politik
- Centrální dashboard musí umožnovat nakonfigurovat systém tak, aby zobrazoval události malwaru detekované kompatibilním klientem na koncovém zařízení, přímo v dohledu centrálního managementu, spolu s událostmi detekovanými na NGFW
- Řešení v rámci komunikace s kompatibilním Anti-Malware klientem na koncovém bodu musí umět vyžádat aktivní blokaci škodlivých souborů na koncovém bodu prostřednictvím klienta, přímo z centrální managementu pro NGFW
- Systém musí umožňovat integraci se systémem pro správu identit (ISE) a přístupu do sítě přes rozhraní pxGrid pro získání doplňujících informací. Získané informace musí umět využít v rámci bezpečnostních pravidel nebo aktivaci obranných opatření v síti.
- Systém musí umožňovat propustit či zablokovat ICMP/TFTP provoz na základě SGT z ISE
- Možnost zaslání informace o TCP nebo UDP toku procházejícím firewallem (start a konec spojení, identifikovaný uživatel, přenesený objem dat, typ služby, délka trvání spojení) na TACACS nebo RADIUS server.
- Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování
- Podpora SNMPv3, privátní MIB, Syslog, SNMP Trap
- Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního sytému (centrální dohledové konzole)
- Centrální dohledová konzole musí být schopna sledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů apod.
- Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu
- Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole
- Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic
- Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu
- Pro reporty lze definovat template definující formát a obsah reportu
- Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu
- V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N
- Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů

- Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV apod.
- Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.
- Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události apod.
- Podpora posílání událostí formou syslog, email, SNMP na externí platformy
- Podpora přenosu informací ohledně hostů, discovery, napadení, aktivitě uživatelů, přenášených souborů a zjištěného malware do SIEM systému IBM QRadar
- Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay
- Podpora JDBC API pro přístup z externích systémů k databázím centralizovaného managementu
- Podpora řízeného přístupu podle rolí administrátorů
- Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora
- Možnost definice politik pro sledování odpovídajících parametrů „zdraví" na senzorech a centralizované konzoli (zatížení CPU, obsazení paměti, komunikace s cloudovými službami apod.)
- Zákaznicky definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví"
- Různé politiky pro sledování „zdraví" lze aplikovat na různé senzory nebo centralizovanou konzoli

Správa HW

- Centrální dohledová konzole ve formě HW platformy (1RU) s podporou až 50 senzorů
- Centrální dohledová konzole musí být schopna zpracovat min. 30 milionů IPS událostí
- Centrální dohledová konzole musí disponovat alespoň 32 GB operační paměti
- Centrální dohledová konzole musí disponovat úložištěm min. 900 GB
- Podpora min. RAID 1 hot swappable
- Síťová rozhraní min. 2x 1Gbps, 1x 1Gbps rozhraní pro správu

Požadavky na propojovací prvky (shrnutí pro všechny lokality)
Všechny níže sepsané moduly a pasivní/aktivní DAC kabely musí být od stejného výrobce jako je výrobce firewallů. Není možno nabídnout moduly a pasivní/aktivní DAC kabely výrobců třetích stran. Následující tabulka popisuje požadované množství a typy kabelů/modulů.

Typ prvku	Počet kusů
10GBASE SFP+ modul pro sigle-mode trasu alespoň 10 km dlouhou	8
10GBASE SFP+ modul pro multi-mode trasu do 300 m	4
1000BASE-LH SFP modul pro sigle-mode trasu alespoň 10 km dlouhou	28
1000BASE-T Copper SFP modul pro metalické rozvody	8

Testování nabízených zařízení Firewall
Zadavatel si vyhrazuje právo otestování shody udávaných parametrů propustnosti jednotlivých bezpečnostních funkcí s reálným měřením/chováním zařízení v testovacím prostředí a testování funkčnosti vybraných pravidel včetně pravidel založených na identitě uživatele z AD. S ohledem na požadavky zadávací dokumentace budou testovány zejména tyto funkce:

- Test kapacity firewallu (UDP PPS (Packets per Second) test, test propustnosti UDP packetů o velikosti 512 a 1518 bytes)
- Test počtu konkurenčních spojení (TCP)
- Test počtu nově navazovaných spojení
- Test propustnosti NGFW
- Test funkčnosti zavedených vybraných pravidel

Dodavatel se podáním nabídky zavazuje na žádost Zadavatele k zapůjčení testovací platformy pro výše uvedené testy.
Součástí zapůjčení musí být také migrace Zadavatelem vybraných pravidel ze stávajících firewallů včetně navázání těchto pravidel na AD Zadavatele za účelem ověření funkčnosti testovaného řešení.
V případě, že Zadavatel při testech zjistí, že zařízení nesplňují požadované parametry, bude toto Zadavatelem hodnoceno jako nesplnění zadávacích podmínek a Účastník bude vyloučen z výběrového řízení.
Dodavatel se podáním nabídky zavazuje k dodání MIB (Management Information Base) k zapůjčené testovací platformě, ze které bude možné vyčítat protokolem SNMP minimálně následující parametry:

- Vytížení procesoru (včetně jednotlivých jader), paměti a jednotlivých interface
- Počet celkových navázaných spojení, a průměrnou dobu potřebnou k navázání spojení

- Stavy hlavních systémových front

Implementace

Přípravné práce
Dodavatel řešení připraví migrační scénář pro migraci provozovaných firewallů na nové prostředí. Migrace musí zachovat plnou funkcionalitu v rozsahu stávajících pravidel firewallů provozovaných Zadavatelem na vrstvách L3-L7 modelu OSI včetně vazby pravidel na skupiny uživatelů a zařízení v Active Directory a sytému pro správu identit ISE. Zároveň musí být zachován centralizovaný monitoring ve stávajícím rozsahu.

Migrace musí zachovat režim vysoké dostupnosti v lokalitách FNO a LDN Klokočov tak, aby v případě výpadku jednoho zařízení nebo ISP došlo k automatickému failoveru a zachování konektivity v plném rozsahu.

Scénář musí zohlednit roli Zadavatele jako provozovatele základní služby podle vyhlášky č. 437/2017 Sb., musí mít minimální dopad na provoz Zadavatele a podléhá jeho schválení.

Migrační scénář podléhá schválení oddělení Infrastruktury ÚNIT FNO.

Implementační práce hardware
Zadavatel požaduje fyzickou kompletaci a instalaci do rozvaděčů připravených Zadavatelem ve všech třech lokalitách. Dále požaduje zahoření dodaného hardware včetně aktualizace firmwarů a obslužných softwarů na Zadavatelem odsouhlasené verze.

Před nasazením firewallů do produkčního prostředí Zadavatele zprovozní Dodavatel laboratorní segment v síti Zadavatele, ve kterém otestuje v součinnosti se Zadavatelem připravená pravidla a politiky, ověřování uživatelů a skupin vůči AD a systému pro správu identit ISE, odolnost systému proti výpadkům (failover mechanizmy) apod.

Implementační práce software
Dodavatel ve spolupráci se Zadavatelem připraví instalační balíčky klientů pro endpointy, které budou nasaditelné pomocí nástroje Microsoft SCCM provozovaným Zadavatelem. Systém pro zabezpečení koncových bodu pak bude v rámci pilotního nasazení nainstalován na 100 vybraných zařízení (stolních počítačů, notebooků) s operačním systémem Windows 10, na kterých bude ověřena funkčnost klientů, spolupráce s firewally a jejich centrální správa. Nasazení na zbývající koncové stanice ve správě zadavatele bude provedeno Zadavatelem po ukončení pilotního provozu.

Nasazení do produkce
Náhrada stávajících firewallů za dodávaný systém bude probíhat za plného provozu nemocnice a musí probíhat tak, aby měla minimální dopad na její provoz. Maximální doba akceptovatelného výpadku síťových služeb poskytovaných firewally v jedné lokalitě během jejich náhrady je 1 hodina. Vlastní výměna firewallů bude po předchozí dohodě se Zadavatelem probíhat ve večerních hodinách (18–24 h). Součástí implementace musí být integrace do sytému Prime Infrastructure a ISE, stejně jako i případné související konfigurace síťových prvků nebo management nástrojů v síti zadavatele a nastavení automatického zálohování konfigurace, ke kterému je možné využít stávající nástroje Zadavatele (Prime Infrastructure).

Součástí fyzické instalace je odpojení patch kabelů, demontáž stávajících zařízení, montáž nových zařízení (Hardware), zapojení patch kabelů, kabelový management, kontrola zapojení a zapojení na centrální management. Součástí nasazení firewallů musí být také migrace příslušných pravidel ze stávajících firewallů, jejich optimalizace z pohledu správy i výkonu, propojení na zdroje identit (AD, ISE) a kontrola funkčnosti řešení a jednotlivých pravidel.

Servisní služby
Účastník musí zajistit minimálně následující podmínky servisních služeb:

- Účastník poskytne Zadavateli po dobu trvání záručního a rozšířeného servisu všechny relevantní verze SW, aktualizace geolokačních databází, signatur malware a IDS (Intrusion Detection System), databází IP adres a URL, nabízených výrobcem tak, aby dodané řešení vyhovovalo zadání Zadavatele a fungovalo bez závad.
- Zadavatel musí mít možnost se sám zaregistrovat na stránkách výrobce a musí mít možnost samostatného stahování nových verzí SW a registrace k odběru automatických mailových zpráv týkajících se dodávaných zařízení a upozorňující na tyto skutečnosti:
    - bezpečnostní incidenty, které vyžadují od Zadavatele povýšení operačního systému/firmware či aplikování změny konfigurace či opravy (záplaty),
    - konec prodeje či podpory,
    - nové verze operačního systému/firmware
    - známé chyby operačního systému/firmware

- Servisní zásahy v rámci záruky budou přednostně prováděny v místě plnění. Závada, jejíž odstranění z jakýchkoliv důvodů nebude na místě možné, nebo vhodné, bude řešena výměnným způsobem za nové zařízení odpovídající minimálně všem technickým, funkčním a kvalitativním parametrům jako původní zařízení. Jestliže dojde k opravě vyměněného zařízení, může být toto po opravě instalováno zpět. Veškeré související náklady případných servisních, konfiguračních a implementačních prací hradí Dodavatel. Veškerá manipulace s opravovanou komponentou bude protokolárně zaznamenána. V případě, že oprava vadné komponenty nebude možná, bude předmětná komponenta nahrazena novou stejných nebo lepších parametrů, na níž bude možno provozovat stejný SW jako na původní.
- Systém musí zahrnovat standardní záruční (servisní) podporu výrobce zařízení, software a Dodavatele systému po dobu 2 let s možností rozšíření na celkovou dobu 5 let.
- Požadovaná úroveň podpory na celé řešení je 7 x 24 s reakční dobou 4 hodiny po celé období 5 let a dobou vyřešení 14 dnů, pokud se smluvní strany nedohodnou jinak. V případě závad nebo problémů, které závažně ovlivňují služby poskytované dodaným systémem, musí Dodavatel, do doby finální opravy, zajistit do 8 hodin od nahlášení zjištěné závady funkcionalitu náhradním řešením.
- Na dodaný HW je požadovaná úroveň podpory 7 x 24 s garantovanou dobou opravy 8 hodin po celé období 5 let.
- Dodavatel je povinen po celou dobu 5 let v případě dostupnosti nových verzí software/firmware nebo jejich oprav (tzv. patche), které řeší závažné bezpečnostní problémy nebo novou funkcionalitu řešení, po předchozím schválení Zadavatele tyto aktualizace či opravy aplikovat, a to minimálně jednou ročně.
-

Zaškolení
Zaškolení v rozsahu nutném pro zvládnutí každodenní správy systému v minimálním rozsahu 16 hodin pro 5 lidí, školení bude probíhat v prostorách FNO a v termínech stanovených FNO.

Dokumentace
Vyhotovení technickoprovozní dokumentace. V rámci realizace řešení služeb bude Dodavatelem zpracována a předána dokumentace řešení minimálně v tomto rozsahu:

- Provozně-technická dokumentace v rozsahu požadovaném vyhláškou č. 529/2006 Sb. § 10 a § 11.
- Plán zálohování a obnovy včetně doporučení pravidel pro pravidelné ověřování jednotlivých postupů.
- Relevantní bezpečnostní dokumentace vzhledem k dodávce dle zákona 181/2014 Sb. o kybernetické bezpečnosti, včetně jeho novel a jeho prováděcích právních předpisů:
  - hodnocení rizik souvisejících s plněním předmětu výběrového řízení,
  - topologie infrastruktury,
  - přehled síťových zařízení,
  - doplnění bezpečnostních politik
- Schéma zapojení a síťové nastavení protilehlých zařízení.
-

Akceptační testy
Předpokladem pro předání řešení do provozu bude splnění akceptačních testů, které Dodavatel připraví pro ověření následujících funkcionalit:

- Byly dodány fyzické zařízení dle požadované technické specifikace
- Všechny HW i SW komponenty systému jsou nainstalovány a napojeny na infrastrukturu FNO
- Veškeré komponenty systému jsou řádně licencované
- Dochází k automatické aktualizaci filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů dostupných na internetu s poškozenou reputací.
- Zajištění vysoké dostupnosti zajišťuje vysokou dostupnost systému v případě výpadku jednoho ze zařízení v dané lokalitě nebo některého z ISP.
- Klientský SW pro zabezpečení koncových zařízení je nainstalovaný na 100 zařízeních, je plně funkční a řízený systémem centrální správy.
- Jsou zachyceny pokusy o přenesení malware a pokusy o komunikaci se systémy s poškozenou reputací, a to na firewallech i koncových zařízeních, je viditelná trajektorie pohybu přenášeného malware.
- Jsou plně funkční pravidla migrovaná z původních firewallů, jsou funkční pravidla pracující s identitou uživatele/zařízení spravovanou v systému Active Directory nebo ISE.
- Konfigurace jednotlivých částí řešení je pravidelně zálohována.

Příloha č. 2

Položkový rozpočet předmětu plnění

Položka č.	Plnění	Nabídková cena v Kč bez DPH	DPH v %	DPH v Kč	Nabídková cena v Kč vč. DPH
1.	Dodávka infrastruktury firewallů, včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů včetně příslušných licencí a záručního servisu v rámci standardu záruky za jakost na období 1.-2. roku	14 264 749,88 Kč	21,00%	2 995 597,47 Kč	17 260 347,35 Kč
2.	Instalace a implementace systému do prostředí Zadavatele	2 248 469,00 Kč	21,00%	472 178,49 Kč	2 720 647,49 Kč
3.	Zaškolení a zhotovení dokumentace	420 000,00 Kč	21,00%	88 200,00 Kč	508 200,00 Kč
4.	Rozšířené servisní služby na období 3.-5. roku	1 404 000,00 Kč	21,00%	294 840,00 Kč	1 698 840,00 Kč
Celková nabídková cena za realizaci předmětu plnění veřejné zakázky v Kč *(bude uvedeno na Krycím listě nabídky a v bodě IV.3 Smlouvy)*		18 337 218,88 Kč	21,00%	3 850 815,96 Kč	22 188 034,84 Kč

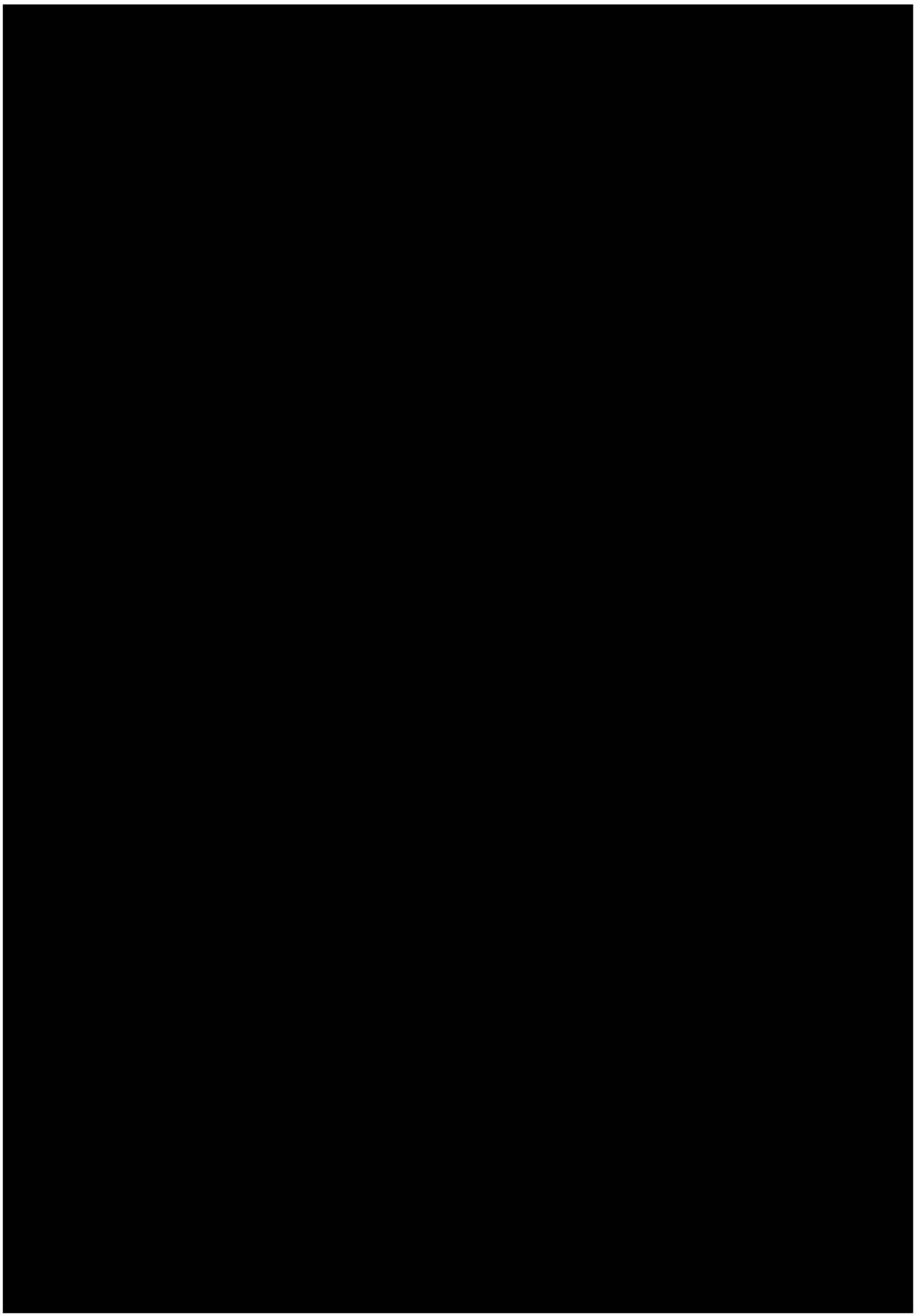
A/	Náklady, které budou spolufinancovány z IROP - dodávka, instalace a implementace infrastruktury firewallů, včetně nástroje pro jejich centrální správu a zabezpečení koncových bodů, příslušné licence, zaškolení a zhotovení dokumentace, záručního servisu v rámci standardu záruky za jakost na období 1. – 2. roku - částka, která bude uvedena v bodě IV.3.A/ smlouvy	16 933 218,88 Kč	21,00%	3 555 975,96 Kč	20 489 194,84 Kč
B/	Náklady, které budou hrazeny z vlastních zdrojů zadavatele - zajištění technické (servisní) podpory po ukončení záruky po dobu následujících 3 let - částka, která bude uvedena v bodě IV.3.B/ smlouvy	1 404 000,00 Kč	21,00%	294 840,00 Kč	1 698 840,00 Kč

V Praze dne 18.08..2021

Ing. Milan Zinek

Digitally signed by Ing. Milan Zinek
Date: 2021.08.18 13:35:35 +02'00'

ALEF NULA,a.s.
Ing. Milan Zinek
Předseda představenstva



Příloha č. 3

Realizační tým Dodavatele

Označení role	Jméno a příjmení	Kontaktní údaje (telefon, e-mail)
[redacted]		

V Praze dne 18.8.2021

Ing. Milan Zinek

Digitally signed by Ing. Milan Zinek
Date: 2021.08.18 13:35:57 +02'00'

ALEF NULA,a.s.
Ing. Milan Zinek
Předseda představenstva