Smlouva o dodání, instalaci a konfiguraci bezpečnostního prvku Firewall, servisu a administrátorského školení obsluhy

Smluvní strany

organizace:	**Fakultní nemocnice Královské Vinohrady**
zřizovatel:	Ministerstvo zdravotnictví ČR
zastoupena:	Doc. MUDr. Robertem Grillem, Ph.D., MHA., ředitelem nemocnice
sídlo:	Šrobárova 1150/50, Praha 10, PSČ 100 34
IČ:	00064173
DIČ:	CZ00064173

(dále jen **„Objednatel“**)

společnost:	Power Systems s.r.o.
obchodní rejstřík:	C 11664 vedená u rejstříkového soudu v Praze
zastoupena:	Pavlem Suchánkem, jednatelem společnosti
sídlo:	V luhu 754/18, 140 00 Praha 4 Nusle
IČ:	45797633
DIČ:	CZ45797633
Bankovní spojení:	[redacted]

(dále jen **„Poskytovatel“**)

uzavírají na základě výsledku podlimitní veřejné zakázky s názvem **„FNKV - Nákup bezpečnostního prvku (Firewall)“,** interní číslo 2019_027_00_00 (dále jen „veřejná zakázka“), zadávané ve zjednodušeném podlimitním řízení dle ustanovení § 53 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“), a podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), tuto smlouvu o dodání, instalaci a konfiguraci bezpečnostního prvku Firewall, servisu a administrátorského školení obsluhy dílo (dále jen „Smlouva“):

Článek 1
Předmět a účel Smlouvy

a) Předmětem této Smlouvy je závazek Poskytovatele dodat Objednateli hardwarové zařízení typu bezpečnostní prvek (dále také jen „Firewall“). Firewall musí splňovat minimálně technické parametry specifikované v bodu 1 Přílohy č. 1 této Smlouvy – Technická specifikace firewallu. Poskytovatel se zavazuje převést na Objednatele vlastnická práva k předmětu dodávky, jakož i poskytnout licence na software, který je součástí Firewallu.

b) Součástí dodávky jsou všechny potřebné transceivery a propojovací kabely:
   - 2x 10Gbit/s tranceiver do FW pro připojení do core boxu ve stejné lokalitě (Short Range) vč. potřebné kabeláže,
   - 2x 10Gbit/s tranceiver do FW pro připojení do core boxu ve vzdálené lokalitě (Long Range) vč. potřebné kabeláže,
   - 2x 10Gbit/s tranceiver do core boxu pro připojení FW ve stejné lokalitě (Short Range) vč. potřebné kabeláže. Tranceiver musí být kompatibilní se stávajícím core boxem (Cisco C6807-XL),
   - 2x 10Gbit/s tranceiver do core boxu pro připojení FW ve vzdálené lokalitě (Long Range) vč. potřebné kabeláže. Tranceiver musí být kompatibilní se stávajícím core boxem (Cisco C6807-XL),
   - 4x 1Gbit/s tranceiver pro propojení FW do HA (High Availability) na delší vzdálenost (Long Range) vč. potřebné kabeláže.

c) Předmětem této Smlouvy je dále závazek Poskytovatele provést instalaci a konfiguraci Firewallu. Instalací se rozumí provedení migrace základní konfigurace ze stávajícího Firewallu na dodaný nový Firewall, uvedení do provozu a provedení administrátorského zaškolení pracovníků Objednatele (dále jen „Implementace“). Podrobnosti ohledně Implementace jsou upraveny v bodu 2 a 3 Přílohy č. 1 této Smlouvy – Technická specifikace Firewallu.

d) Podpora (maintenance) k produktu je sjednána na období 48 měsíců. Podpora (maintenance) zahrnuje nárok na upgrade, update a nové verze Softwaru k produktu a dále technickou podporu po celou dobu platnosti této podpory (maintenance). Konkrétně podpora zahrnuje:
   - Přímý přístup k odborníkům a technickým pracovníkům podpory
   - Správu požadavku (incidentu) podpory: možnost odeslat, aktualizovat, spravovat a kontrolovat stav
   - Online zákaznickou podporu
   - Dokumentaci, přístup k produktovým příručkám, technickým příručkám a často kladeným otázkám (FAQ).
   - Aktualizaci předplatitelských služeb

e) Předmětem této Smlouvy je dále závazek Objednatele uhradit Poskytovateli za řádně a včas poskytnuté plnění dle tohoto článku a čl. 2 Smlouvy cenu dle čl. 3 Smlouvy.

f) Účelem této Smlouvy je zajištění kontrolního bodu k řízení a zabezpečování síťového provozu – Firewall – mezi interní sítí Objednatele a sítí internet, a to formou náhrady stávajícího zařízení s požadavkem, aby tato náhrada proběhla bez výpadku a dopadu na provoz Objednatele.

Článek 2
Místo plnění, předání a převzetí plnění, doba plnění

a) Poskytovatel se zavazuje předat Objednateli Firewall specifikovaný dle čl. 1 odst. 1 této Smlouvy a provést Implementaci dle čl. 1 odst. b) této Smlouvy do 30 kalendářních dnů od nabytí účinnosti této Smlouvy. (dále jen „předání plnění“).

b) Místem plnění je sídlo Objednatele.

c) Předání a převzetí plnění potvrdí Objednatel podpisem předávacího protokolu. Návrh předávacího protokolu vystaví Poskytovatel. Objednatel předávací protokol nepodepíše, pokud nebudou Poskytovatelem splněny všechny náležitosti předání plnění. Obě Smluvní strany obdrží po jednom vyhotovení předávacího protokolu.

d) Předávací protokol bude obsahovat zejména:
   - údaje o Smluvních stranách,
   - popis Firewallu,
   - případné vady a výhrady Objednatele k předanému plnění,
   - případné odůvodnění, proč Objednatel předané plnění nepřevzal,
   - podpis osoby oprávněné jednat za Objednatele.

e) K předání a převzetí Firewallu může Objednatel přizvat další osobu. Na tuto osobu se bude vztahovat povinnost mlčenlivosti dle této Smlouvy.

f) Poskytovatel se zavazuje nahlásit konkrétní termín každého jednotlivého úkonu, které dohromady tvoří předání plnění minimálně 3 pracovní dny předem. V případě zaškolení pracovníků Objednatele nahlásí Poskytovatel termíny školení alespoň 5 dní předem.

g) Objednatel není povinen převzít Firewall zejména v následujících případech:
   - Firewall nevykazuje všechny vlastnosti a nevyhovuje všem podmínkám uvedeným v této Smlouvě,
   - Firewall vykazuje známky poškození,
   - Firewall vykazuje vady, které brání jejímu řádnému užívání a naplnění účelu této Smlouvy,

h) Objednatel je oprávněn převzít i takový Firewall, která vykazuje vady, které nebrání jejímu řádnému užívání nebo naplnění účelu této Smlouvy. Tyto vady se vyznačí v předávacím protokolu. Poskytovatel je povinen tyto vady bezodkladně odstranit. Poskytovatel je však oprávněn vystavit daňový doklad na úplatu za dodání Firewallu až po odstranění těchto vad.

i) Dle dohody Smluvních stran dochází k převodu vlastnického práva k Firewall a oprávnění jej užít podpisem předávacího protokolu Objednatelem.

j) Osobou pověřenou jednat jménem Objednatele ve věcech technických a převzetí plnění je:
[redacted]

k) Osobou pověřenou jednat jménem Poskytovatele ve věcech technických a k předání plnění je:
[redacted]

l) Smluvní strany se vzájemně dohodly, že změna uvedených osob bude oznamována jednostranným písemným sdělením a není potřeba na jejich změnu uzavřít dodatek k této Smlouvě.

Článek 3
Cena a platební podmínky

Celková cena za dodání a Implementaci firewallu (dále jen „Celková cena za dodání“) je stanovena dohodou Smluvních stran takto:

Celková cena za dodání činí 1.877.000,- Kč bez DPH, slovy: jedenmilionosmsetsedmdesátsedmtisíckorunčeských bez DPH, tj. 2.271.170,-Kč včetně DPH, slovy dvamilionydvěstěsedmdesátjednatisícstosedmdesátkorunčeských včetně DPH.

Celková cena za dodání zahrnuje veškeré náklady související s:

- dodáním Firewall dle čl. 1 odst. a) této Smlouvy,
- implementací Firewallu dle čl. 1 odst. b) této Smlouvy,
- předáním plnění dle čl. 2 této Smlouvy.

Celková cena za dodání zahrnuje rovněž náklady na veškeré organizační a koordinační činnosti, manipulaci s předmětem plnění, cla, schvalovací řízení, zabezpečení prohlášení o shodě, certifikátů a atestů, pojištění předmětu plnění apod. Celková cena za dodání rovněž obsahuje poplatek za poskytnutí licence k softwaru, který je součástí Firewall po dobu 48 měsíců od převzetí plnění.
Takto sjednaná Celková cena za dodání je cenou konečnou a nepřekročitelnou. Celkovou cenu za dodání je možno měnit pouze při změně sazby DPH.
Poskytovatel je oprávněn fakturovat Celkovou cenu za dodání na základě daňového dokladu po podpisu předávacího protokolu Objednatele. Jako přílohu daňového dokladu (faktury) na zaplacení Celkové ceny za dodání předloží Poskytovatel prostou kopii předávacího protokolu podepsaného oprávněným zástupcem Objednatele.
Poskytovatelem vystavený daňový doklad (faktura) musí splňovat náležitosti obchodní listiny dle § 435 NOZ a náležitosti daňového dokladu dle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Splatnost daňového dokladu (faktury) musí činit **60 dnů** od vystavení daňového dokladu (faktury). Pokud daňový doklad (faktura) neobsahuje všechny právními předpisy a Smlouvou stanovené náležitosti a podmínky včetně ceny je Objednatel oprávněn jej do data splatnosti vrátit s tím, že Poskytovatel je poté povinen vystavit nový daňový doklad (fakturu).

Článek 4
Technická podpora, odpovědnost za vady, záruka

1. Poskytovatel odpovídá za to, že předmět plnění bude po dobu platnosti smlouvy plně funkční a bude mít vlastnosti uvedené v této Smlouvě, v Příloze č. 1 této Smlouvy – Technické specifikaci a vlastnosti uvedené v nabídce Poskytovatele.

2. Poskytovatel se dále zavazuje, že předmět plnění bude po dobu trvání záruky mít vlastnosti odpovídající právním předpisům, eventuálně dalším technickým požadavkům či normám (zejména doklad o shodě), které má předmět plnění splňovat, a které se na daný předmět plnění vztahují, a bude mít vlastnosti uváděné výrobcem či Poskytovatelem. Poskytnutím záruky se Poskytovatel zavazuje, že poskytne pro Objednatele záruku vyplývající ze záruky výrobce Firewall.

3. V případě uplatnění nároků ze záruky nese Poskytovatel náklady na práci spojenou s odstraněním vad plnění, veškeré náhradní díly, cestovní náklady, jakož i další náklady související s odstraňováním reklamovaných vad plnění.

4. Objednatel má možnost v rámci zakoupené podpory kontaktovat technickou podporu k dodanému řešení telefonicky či elektronicky (e-mail, kontaktní URL) dle níže uvedené tabulky, čímž vznikne požadavek technické podpory. Poskytovatel garantuje při platné technické podpoře

maximální dobu reakce na založený požadavek 1 pracovní den a vyřešení problému (pokud se prokáže vada na produktu) maximálně do 5 pracovních dní.

Kontaktní údaje pro podporu:
[redacted]

Článek 5
Ukončení Smlouvy

1. Tuto Smlouvu lze ukončit pouze některým ze způsobů uvedených v této Smlouvě.

2. Objednatel je oprávněn od této Smlouvy odstoupit v případě podstatného porušení této Smlouvy Poskytovatelem. Za podstatné porušení Smlouvy se považuje situace, kdy:
   a) je Poskytovatel v prodlení s předáním Brány firewall nebo provedením Implementace dle čl. 2 odst. a) této Smlouvy déle než 60 dnů,
   b) Poskytovatel neodstraní vady dle této Smlouvy do 30 pracovních dnů od podpisu předávacího protokolu, ve kterém jsou vady uvedeny Objednatelem,
   c) Poskytovatel při realizaci dodávky postupuje v rozporu se svými povinnostmi a tento závadný stav neodstraní ani na výzvu Objednatele,
   d) dodaná Brána firewall nesplňuje požadavky uvedené v této Smlouvě, v Příloze č. 1 této Smlouvy – Technické specifikaci Brány firewall, požadavky právních předpisů, technických a jiných norem.

3. Každá smluvní strana je oprávněna tuto Smlouvu písemně vypovědět a to i bez udání důvodu. Výpovědní doba činí 2 měsíce následující po měsíci, v němž je výpověď doručena druhé straně.

Článek 6
Povinnost mlčenlivosti

Není-li v konkrétním případě Smluvními stranami sjednáno jinak, je Poskytovatel povinen během plnění této Smlouvy i po jejím ukončení zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od Objednatele v souvislosti s uzavřením a plněním této Smlouvy.

Povinnost mlčenlivosti se nevztahuje na informace, které:

- je Poskytovatel povinen sdělit ze zákona,
- jsou veřejně známé, a to ne v důsledku porušení této povinnosti,
- jsou Objednatelem vysloveně označeny jako nedůvěrné.

Poskytovatel se zavazuje učinit všechna nezbytná opatření, která zajistí, že povinnost mlčenlivosti dodrží i jeho zaměstnanci, spolupracovníci a další osoby podílející se na plnění této Smlouvy.

Povinnost mlčenlivosti trvá i po skončení účinnosti této Smlouvy.

Článek 7
Práva duševního vlastnictví

Poskytovatel se zavazuje, že na Bráně firewall neváznou práva třetích osob, která by narušovala výkon vlastnických práv Objednatele k Bráně firewall.

Poskytovatel se zavazuje, že uzavřením této Smlouvy a předáním plnění Objednateli nedojde k porušení práv třetích osob, zejména práv vycházejících z práva duševního vlastnictví (zejména autorské právo).

Poskytovatel prohlašuje, že je plně oprávněn k dispozici s právy duševního vlastnictví k Bráně firewall a zejména, že je oprávněn poskytnout Objednateli licenci k užití softwaru na Bránu firewall. Na základě těchto oprávnění zajistí Poskytovatel řádné a nerušené užívání Brány firewall Objednatelem včetně zajištění dalších souhlasů a licencí od výrobce, případně jiných nositelů práv duševního vlastnictví, potřebných k užívání Brány firewall Objednatelem.

Článek 8
Další práva a povinnosti Smluvních stran

Poskytovatel se zavazuje, že během plnění této Smlouvy bude maximálně respektovat stávající architekturu Objednatele a aktuální nastavení bezpečnosti sítě Objednatele.

Poskytovatel se zavazuje během plnění této Smlouvy dodržovat veškeré bezpečnostní, zdravotní a požární normy, se kterými bude Objednatelem seznámen.

Objednatel se zavazuje poskytnout Poskytovateli potřebnou součinnost k plnění této Smlouvy, zejména pak k provedení Implementace včetně zaškolení pracovníků Objednatele.

Objednatel je povinen umožnit přístup pověřenému zaměstnanci Poskytovatele do prostor, které budou domluvou určeny v rámci místa plnění za účelem plnění této Smlouvy.

Objednatel je oprávněn při plnění této Smlouvy kontrolovat postup prací Poskytovatele. Zjistí-li Objednatel, že Poskytovatel při plnění této Smlouvy postupuje v rozporu se svými povinnostmi upravenými v této Smlouvě, je Objednatel oprávněn dožadovat se toho, aby Poskytovatel odstranil případné vady a nadále postupoval řádným způsobem.

Článek 9
Závěrečná ustanovení

1. Poskytovatel je povinen mít po celou dobu účinnosti smlouvy uzavřenu pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za škodu způsobenou dodavatelem třetí osobě ve výši min. 3 000 000 Kč (slovy: třimilionykorunčeských) na jednotlivou pojistnou událost. Ověřená kopie pojistné smlouvy nebo pojistného certifikátu je přílohou č. 2 této smlouvy.

2. V případech v této smlouvě výslovně neupravených platí pro obě smluvní strany ustanovení občanského zákoníku.

3. Jakákoliv ústní ujednání při provádění díla jsou právně neúčinná.

4. Veškerá textová dokumentace, kterou při plnění smlouvy předává či předkládá zhotovitel objednateli, musí být předána či předložena v českém jazyce.

5. Tuto Smlouvu lze měnit pouze formou vzestupně číslovaných písemných dodatků podepsaných oprávněnými zástupci obou Smluvních stran.

6. Tato Smlouva se vyhotovuje ve 2 stejnopisech. Každá Smluvní strana obdrží po jednom stejnopise.

7. Písemnosti mezi stranami této smlouvy, s jejichž obsahem je spojen vznik, změna nebo zánik práv a povinností upravených touto smlouvou (zejména odstoupení od smlouvy) se doručují do vlastních rukou. Povinnost smluvní strany doručit písemnost do vlastních rukou druhé smluvní straně je splněna při doručování poštou, jakmile pošta písemnost adresátovi do vlastních rukou doručí. Účinky doručení nastanou i tehdy, jestliže pošta písemnost smluvní straně vrátí jako nedoručitelnou a adresát svým jednáním doručení zmařil, nebo přijetí písemnosti odmítl.

8. Smluvní strany vylučují použití ust. § 1740 občanského zákoníku.

9. Tato smlouva nabývá platnosti dnem podpisu oběma smluvními stranami. Účinnosti tato smlouva nabývá dnem jejího uveřejnění v registru smluv ve smyslu § 6 odst. 1 a § 9 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Smluvní strany se dohodly, že tuto smlouvu uveřejní v registru smluv objednatel.

10. Vztahy Smluvních stran touto Smlouvou blíže neupravené se řídí občanským zákoníkem.

11. Poskytovatel není oprávněn bez výslovného předchozího písemného souhlasu objednatele postoupit jakoukoli pohledávku nebo převést jiná práva či povinnosti, která mu vznikne podle této smlouvy nebo v souvislosti s ní, na třetí osobu.

12. Poskytovatel není oprávněn započíst žádnou svou pohledávku proti pohledávce objednatele z této smlouvy.

13. Tato Smlouva je závazná pro případné právní nástupce obou Smluvních stran.

14. Smluvní strany prohlašují, že tato smlouva neobsahuje žádné obchodní tajemství ve smyslu § 504 občanského zákoníku. Zhotovitel souhlasí se zveřejněním úplného znění této smlouvy v souladu s platnými právními předpisy.

15. Smluvní strany prohlašují, že si tuto Smlouvu přečetly a svobodně souhlasí s jejím obsahem. Na důkaz toho připojují Smluvní strany své podpisy.

Nedílnou součástí této Smlouvy jsou tyto přílohy:
Příloha č. 1 – Technická specifikace
Příloha č. 2 – Ověřená kopie pojistné smlouvy nebo pojistného certifikátu

Za Objednatele:	Za Poskytovatele:
V Praze dne …….	V Praze, dne 3.9.2019
……	……
Doc. MUDr. Robert Grill, Ph.D., MHA. Ředitel nemocnice	Pavel Suchánek jednatel společnosti

1. Technická specifikace Firewallu

Poskytovatel prohlašuje, že jím dodávaný Firewall splňuje veškeré technické požadavky specifikované v tabulce níže:

Požadovaná hodnota parametru	Splněno ANO/NE	Nabízený počet/hodnota
HW architektura		
Všechny parametry propustnosti musí dodavatel uvádět v real world mix paketech, tzv. "application mix"	ANO	
FW musí být typu HW appliance	ANO	
Modul pro zpracování dat musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů (správa zařízení a řídící modul pro podpůrné síťové činnosti), aby nemohlo dojít k jejich vzájemnému ovlivnění	ANO	
FW musí obsahovat jeden dedikovaný port pro správu pomocí konzole pro přístup k CLI	ANO	
FW musí obsahovat minimálně 4 SFP+ datové porty rychlosti 10Gbps	ANO	4
FW musí obsahovat alespoň jeden dedikovaný OOB management port pro plnohodnotnou správu FW	ANO	1
FW musí být schopen ukládat logové údaje na interní SSD storage o velikosti minimálně 220 GB	ANO	2* 240 GB SSD
FW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP)	ANO	
FW musí být rozměrově kompatibilní s 19“ rozvaděčem	ANO	
FW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V	ANO	2

Požadavky na High Availability (HA)		
FW musí podporovat režim HA v módu Active – Active složený alespoň ze dvou zařízení	ANO	
FW musí podporovat režim HA v módu Active – Standby složený alespoň ze dvou zařízení	ANO	
V obou typech HA musejí být veškeré informace o probíhajícím provozu synchronizovány tak, aby při výpadku jednoho z boxů nedošlo ke ztrátě informací NAT a k přerušení aktivních spojení provozu typu TCP i UDP procházejícího přes FW	ANO	
FW musí být schopen provést HA failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy	ANO	

Obecné výkonové parametry		
Propustnost firewallu při plné aplikační kontrole musí dosahovat hodnoty alespoň 4 Gbps	ANO	6 Gbps
Propustnost firewallu při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV musí dosahovat hodnoty alespoň 2 Gbps	ANO	6 Gbps
Minimální počet souběžných spojení musí dosahovat hodnoty alespoň 1.000.000	ANO	20 000 000
Minimální počet nových spojení za sekundu musí dosahovat hodnoty alespoň 55.000	ANO	200 000

Síťová funkcionalita		
FW musí plně podporovat IPv4 i IPv6	ANO	
FW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP	ANO	
FW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64	ANO	
FW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM, IGMP a PBF (Policy Based Forwarding)	ANO	
PBF musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, zóna, IP adresa, uživatel	ANO	

Virtual Private Network (VPN)		
FW musí podporovat Site – To – Site VPN pomocí protokolu IPSec	ANO	
FW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (TLS)	ANO	
Počet současně připojených uživatelů nesmí být licenčně omezený	ANO	
Propustnost IPSec musí být alespoň 2 Gbps	ANO	

Aplikační kontrola		
FW musí podporovat aplikační detekci a kontrolu jako svou nativní funkcionalitu	ANO	
Přiřazení povolené či zakázané aplikace musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Definovaná aplikace musí představovat "match kritérium" při policy lookup	ANO	
FW musí podporovat identifikaci aplikací napříč všemi porty/protokoly	ANO	
FW musí podporovat identifikaci aplikací na nestandardních portech	ANO	
Identifikace aplikace musí probíhat přímo ve FW	ANO	
FW musí detekovat a zabránit aplikaci měnit porty, tzv. port – hopping	ANO	
FW musí podporovat řízení neznámého provozu	ANO	

FW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	

Kontrola na úrovni uživatelských identit		
FW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit	ANO	
Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla	ANO	
Uživatelská identita musí představovat "match kritérium" při policy lookup	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno z Active Directory za pomoci doménového účtu s co nejnižšími možnými právy pro čtení Security logů, bez nutnosti disponovat rizikovými úrovněmi oprávnění (např. Domain Admins)	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog	ANO	
FW musí podporovat získávání vazby IP adresa-uživatelské jméno z terminálových serverů MS (možné za pomoci nainstalovaného agenta)	ANO	

Dekrypce		
FW musí podporovat dekrypci odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům	ANO	
FW musí podporovat dekrypci příchozího SSL/TLS provozu, za pomoci naimportovaného privátního klíče interního serveru	ANO	
FW musí podporovat funkci SSH proxy a kontrolovat tunelované aplikace	ANO	
Dekryptovaný provoz musí být možno definovat na základě URL kategorií, i všech dalších typických parametrů, jako jsou zdrojová a cílová IP adresa, port, uživatelská identita	ANO	
FW musí podporovat dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz	ANO	
FW musí podporovat přeposílání dešifrovaného provozu na jiné skenovací zařízení třetích stran např. DLP, analýza provozu a souborů apod. Zařízení 3 strany následně přepošle čistě přefiltrované data zpět do FW. (tzv. decryption broker)	ANO	

FW musí podporovat přeposílání dešifrovaného provozu na specifický port pro potřeby archivace provozu	ANO	

Sandboxing		
Firewall musí podporovat možnost odeslat do sandboxu k inspekci neznámé vzorky procházející protokolem SMTP, HTTP, FTP, IMAP, POP3 a SMB	ANO	
Sandbox systém musí být od stejného výrobce jako je FW, ale nemusí být HW součástí FW	ANO	
Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro FW, v případě, kdy je testovaný vzorek vyhodnocen jako škodlivý	ANO	
Sandbox musí být schopen automaticky upravit kategorie používané URL databáze, pokud zjistí, že testovaný vzorek je škodlivý a komunikuje na konkrétní URL	ANO	
Sandbox musí poskytovat aktualizace signatur pro AV, Webfiltering, DNS, C&C	ANO	
Sandbox musí podporovat analýzu vzorek na operačním systému instalovaném přímo na hardwaru, tzn. ne ve virtuálním prostředí	ANO	
Sandbox musí podporovat operační systémy Windows, Linux a Android	ANO	
Report z analýzy odeslaného vzorku do sandboxu musí být přístupný přímo z rozhraní FW	ANO	

Bezpečnostní funkcionality		
FW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – whitelisting pouze povolených aplikací a zákaz všeho ostatního, včetně neznámého provozu	ANO	
FW musí obsahovat integrovaný systém ochrany proti zranitelnostem (virtual patching) a síťovým útokům (IPS). Databáze IPS signatur musí být uložena přímo ve FW. Aplikace IPS profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	
FW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
FW musí obsahovat integrovaný systém ochrany proti přítomnosti virů a škodlivého kódu. Databáze AV signatur musí být uložena přímo ve FW. Aplikace AV profilu musí být granulární, na úrovni bezpečnostního pravidla	ANO	
Antivirus musí být schopen kontrolovat provoz v minimálně těchto aplikacích: SMTP, POP3, IMAP, HTTP, HTTPS, FTP a SMB	ANO	
FW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele	ANO	
FW musí podporovat možnost zablokování útoku využívajícího známá	ANO	

C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci		
FW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů	ANO	
FW musí pro přístup ke kritickým aplikacím, poskytovat možnost vynutit více faktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje více faktorovou autentizaci; tato vlastnost musí být konfigurovatelná na úrovní bezpečnostního pravidla	ANO	
FW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu	ANO	
FW musí být schopen automaticky vytvářet C&C signatury a okamžitě je aplikovat do bezpečnostní politiky	ANO	
FW musí poskytovat funkci k ochraně proti tzv. drive-by downloadům; způsob ochrany musí být pro uživatele interaktivní s možností volby akceptace rizika a stažení souboru	ANO	
FW musí podporovat analýzu DNS dotazu tzv. Sinkhole funkcí, která na dotaz malware DNS URL vrátí podvrženou IP adresu pro detailnější analýzu a zároveň se stanice na původní malware stránku nedostane	ANO	
FW musí poskytovat možnost rozšíření o funkcionalitu pokročilé analýzy DNS dotazů proti technikám používajícím DGA (domain generation algorithm) v reálném čase	ANO	

Ochrana proti DoS útokům		
FW musí obsahovat nativní službu pro ochranu proti útoku typu DoS pomocí limitace počtu spojení na úrovni zdrojová a cílová IP adresa, uživatelská identita a aplikace	ANO	

Quality of Services (QoS)		
FW musí poskytovat možnost omezení využívané šířky pásma na základě zdrojové a cílové IP adresy, portu, uživatelské identity, aplikace a času (od – do, den v týdnu + čas apod.)	ANO	
FW musí podporovat prioritizaci provozu na základě DSCP	ANO	
FW musí podporovat prioritizaci provozu na základě Identifikované aplikace	ANO	

URL filtering		
FW musí obsahovat nativní podporu pro využívání databáze URL	ANO	
URL databáze musí být od stejného výrobce jako je FW	ANO	
FW musí být schopen použít URL kategorii v definici bezpečnostního pravidla	ANO	

FW musí podporovat vytváření uživatelsky definovaných kategorií, bez nutnosti využít externí nástroj a bez nutnosti zásahu výrobce/dodavatele	ANO	
URL databáze musí být dynamicky aktualizovaná na základě nově zjištěných URL, vedoucích na škodlivý obsah nebo C&C centra	ANO	
URL databáze musí podporovat možnost zařazení do alespoň dvou kategorií najednou pro jedinou URL	ANO	
Rozhraní URL databáze ve FW musí obsahovat možnost požádat o rekategorizaci nevhodně zařazených URL bez nutnosti otevírání support case	ANO	

Logování		
FW musí obsahovat lokální úložiště logů	ANO	
FW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI	ANO	
FW musí podporovat agregované zobrazení logů na základě jednoho filtrovacího pravidla, napříč jednotlivými typy logů, jako jsou provozní logy, logy bezpečnostních incidentů a logy přístupů na URL	ANO	
FW musí podporovat přeposílání logů na zařízení třetích stran	ANO	
FW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla	ANO	
Přeposílané logy z FW musejí být automaticky rozpoznány nejčastěji používanými typy SIEM (uvedených v Leaders kvadrantu aktuálního Gartner MQ)	ANO	

Management		
Jednotlivé HW appliance musí obsahovat plnohodnotné grafické rozhraní (GUI) pro správu, bez nutnosti používání centrálního management serveru. Připojení ke GUI musí podporovat šifrování	ANO	
Jednotlivé HW appliance musí obsahovat plnohodnotné textové rozhraní (CLI) pro správu, bez nutnosti používání centrálního management serveru. Vzdálené připojení k CLI musí podporovat šifrování. Jednotlivé HW appliance musí umožňovat použití šablon pro bootstraping nových FW použitím USB flash disku	ANO	
FW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikát	ANO	
FW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu	ANO	
FW musí podporovat nativní nástroj pro odchycení provozu	ANO	
FW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem	ANO	

Licence		
FW musí podporovat licenční model nezávislý na počtu ochraňovaných koncových systémů	ANO	

Poskytovatel deklaruje, že předmětem plnění Smlouvy je HW a SW (licence) následujících značek a typů (modelů), které splňuje veškeré požadavky této přílohy:

Předmět plnění (HW, SW,…)	Značka produktu	Model produktu	Platnost licence
HW	Sophos	XG 450	neomezeně
SW	Sophos	XG 450 – EnterpriseGuard Plus, Firewall Central management	4 roky od data aktivace
HW	OEM transceivery	4x 10 Gbit/s tranceiver – SR (Cisco compatible)	neomezeně
HW	OEM transceivery	4x 10 Gbit/s tranceiver – LR	neomezeně
HW	OEM transceivery	4x 1 Gbit/s tranceiver – LR	neomezeně
HW	OEM	All-in-one appliance, add on modul FW/Sandbox/	4 roky
SW	Sophos	iView 500GB (virtual appliance)	4 roky od data aktivace

2. Implementace

Poskytovatel deklaruje, že přechod z aktuálního firewallu na novou Bránu firewall neohrozí provoz ani bezpečnost sítě Objednatele. Při Implementaci bude Poskytovatel maximálně respektovat současnou architekturu a aktuální nastavení bezpečnosti sítě. Veškeré kroky při implementaci budou konzultovány s Odborem ICT ve FNKV.

3. Zaškolení pracovníků Objednatele

Poskytovatel provede zaškolení pracovníků Objednatele minimálně v následujícím rozsahu:

- představení dodané technologie,
- administrátorské školení na základní funkce FW,
- aplikace bezpečnostních politik,
- další rozsah dle potřeb pracovníků Objednatele.

Poskytovatel provede souhrnné zaškolení pracovníků Objednatele v rozsahu 1 školících dnů. Poskytovatel oznámí termín jednotlivých školících dnů alespoň 5 pracovní dnů předem.