

Kupní smlouva č. UKRUK/78872/2018

K níže uvedenému datu uzavřely smluvní strany

Univerzita Karlova

(týká se rektorátu UK)

sídlo: Ovocný trh 560/5, 116 36, Praha 1

IČO: 00216208

DIČ: CZ00216208

bankovní spojení: Česká spořitelna, a.s.

číslo účtu: 909909339/0800

zastoupená: Ing. Miroslavou Oliveriusovou, kvestorkou UK

(dále jen „**kupující**“ nebo též „**UK**“)

a

H-Square ICT Solutions s.r.o.

sídlo: Husova 241/7, 110 00, Praha 1

zapsaná: v obchodním rejstříku vedeném u Městského soudu v Praze pod spisovou značkou C 242583

IČO: 04114574

DIČ: CZ04114574

bankovní spojení: Raiffeisenbank a.s.

číslo účtu: 4114574/5500

zastoupená/

jednající: Ing. Janem Pintou, MBA, jednatelem společnosti

ID datové schránky: r964rup

(dále jen „**prodávající**“)

(dále společně jako „smluvní strany“ nebo „strany“)

v souladu s ustanoveními § 2079 a následujícího zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, tuto smlouvu (dále jen „smlouva“):

I. Úvodní ustanovení

1. Kupující provedl v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, (dále jen „ZZVZ“) výběrové řízení na veřejnou zakázku s názvem „RUK – ÚVT – Dodávka zařízení typu FireWall pro zajištění bezpečnostní ochrany sítě WiFi (eduroam)“, která byla zadávána jako veřejná zakázka malého rozsahu a spolufinancována z prostředků Operačního programu výzkum, vývoj a vzdělávání při realizaci projektu Podpora rozvoje studijního prostředí na Univerzitě Karlově – VRR, č. CZ.02.2.67/0.0/0.0/17_044/0008562.

2. Nabídka prodávajícího byla v souladu s podmínkami veřejné zakázky vybrána jako nejvhodnější.

II. Předmět smlouvy, termíny a místo plnění

1. Předmětem této smlouvy je:
 - a) Závazek prodávajícího dodat 1 ks zařízení typu Next-Generation FireWall vč. licencí příslušného SW dle specifikace uvedené v Příloze č. 2 této smlouvy a splňující minimální technické parametry uvedené v Příloze č. 1 této smlouvy (dále také „zboží“) s dopravou na místo dodání.
 - b) Závazek prodávajícího zajistit odbornou instalaci a konfiguraci zboží v místě plnění dle pokynů kupujícího.
 - c) Závazek prodávajícího zajistit odborné školení konfigurace nabízeného zboží.
(dále písm. a), b) a c) jako „předmět smlouvy“)
 - d) Závazek kupujícího zaplatit prodávajícímu dohodnutou kupní cenu za d předmět smlouvy.
2. Financování předmětu smlouvy je závislé na uvolnění účelové podpory z prostředků Operačního programu Výzkum, vývoj a vzdělávání (výzva č. 02-17-044 - Výzva č. 02_17_044 pro Podpora rozvoje studijního prostředí na VŠ v prioritní ose 2 OP). Konkrétně je kupující řešitelem projektu reg. č. CZ.02.2.67/0.0/0.0/17_044/0008562 s názvem „Podpora rozvoje studijního prostředí na Univerzitě Karlově – VRR“, v rámci kterého je plánováno i financování předmětu smlouvy. Kupující si vyhrazuje právo neodebrat předmět smlouvy a možnost odstoupit od smlouvy v případě, že nedojde k uvolnění finančních prostředků v rámci řešeného projektu. Pokud tato skutečnost nastane, je kupující povinen prodávajícího bez prodlení informovat. Pokud dojde mezi smluvními stranami v této době k plnění, jsou smluvní strany povinny si tato plnění bezodkladně vrátit.
3. Zboží prodávající předá kupujícímu do tří (3) týdnů od data účinnosti smlouvy.
4. Místem dodání zboží je lokalita kupujícího na adrese Ústav výpočetní techniky, Ovocný trh 560/5, 116 36 Praha 1.

III. Předání a převzetí předmětu smlouvy

O dodání zboží na místo plnění bude po provedení úplné a řádné instalace a konfigurace zboží mezi prodávajícím a kupujícím podepsán předávací protokol. Předávací protokol zajistí a kupujícímu předloží prodávající.

IV. Cena a platební podmínky

1. Cena za dodávku předmětu smlouvy byla smluvními stranami stanovena ve výši 1.798.720,- Kč bez DPH (slovy jeden milion sedm set devadesát osm tisíc sedm set dvacet korun českých), DPH ve výši 377.731,20 Kč (slovy tři sta sedmdesát sedm tisíc sedm set třicet jedna korun českých dvacet haléřů), tj. 2.176.451,20 Kč včetně DPH ve výši 21% (slovy dva miliony jedno sto sedmdesát šest tisíc čtyři sta padesát jedna korun českých dvacet haléřů).
2. Cena stanovená v odst. 1 tohoto článku je stanovena jako nejvýše přípustná, přičemž zvýšení této ceny je přípustné pouze v souvislosti se změnou výše DPH.
3. Cena je splatná na základě daňového dokladu – faktury řádně vystavené prodávajícím na základě oboustranně potvrzeného předávacího protokolu dle čl. III. smlouvy. Faktura musí splňovat veškeré náležitosti daňového odkladu, zejm. podle zákona č. 235/2004 Sb., o DPH, v platném znění. Faktura musí obsahovat:
 - a) označení daňového dokladu a jeho pořadové číslo;
 - b) identifikační údaje kupujícího;
 - c) identifikační údaje prodávajícího;

- d) označení banky a čísla účtu, na který má být provedena úhrada kupní ceny;
 - e) popis poskytnutého plnění;
 - f) datum vystavení a datum odeslání faktury;
 - g) datum uskutečnění zdanitelného plnění;
 - h) datum splatnosti;
 - i) rozpad kupní ceny tak, aby byla uvedena výše částky bez DPH, výše sazby DPH a částka za DPH a celková částka s DPH;
 - j) podpis, popřípadě jméno osoby, která fakturu odeslala elektronickou cestou;
 - k) název projektu a registrační číslo projektu: „Podpora rozvoje studijního prostředí na Univerzitě Karlově – VRR, číslo projektu CZ.02.2.67/0.0/0.0/17_044/0008562“;
 - l) přílohou faktury musí být předávací protokol.
4. Lhůta splatnosti faktury je třicet (30) dní ode dne jejího doručení. Kupující je oprávněn ve lhůtě splatnosti vrátit prodávajícímu neúplnou, nesprávně účtovanou nebo nedoloženou fakturu k opravě nebo doplnění, aniž tím bude v prodlení se zaplacením. Kupující musí uvést důvod vrácení. V takovém případě běží nová lhůta splatnosti ode dne doručení opravené faktury kupujícímu.

V. Práva a povinnosti smluvních stran

1. Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků.
2. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob uvedených v Příloze č. 3 smlouvy – Seznam oprávněných osob.
3. Obě strany vyvinou maximální úsilí pro zajištění ochrany informací, které v rámci plnění této smlouvy získá jedna strana od druhé.
4. Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů a k jejich vyřešení zejména prostřednictvím jednání oprávněných osob nebo statutárních zástupců smluvních stran. Nedojde-li k dohodě je každá smluvní strana oprávněna předat spor místně a věcně příslušnému soudu. Rozhodčí řízení je vyloučené.
5. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této smlouvy.
6. Smluvní strany jsou povinny plnit své závazky vyplývající z této smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a splatností jednotlivých peněžních závazků.
7. Prodávající se dále zavazuje:
 - a) Dodat zboží dle technické specifikace uvedené v Příloze č. 2 této smlouvy a zajistit jeho odbornou instalaci a konfiguraci dle pokynů kupujícího v místě plnění.
 - b) Zajistit nejpozději do 1 měsíce po dodání zboží odborné školení konfigurace dodaného zboží v rozsahu min. 2 dny pro celkem 4 osoby (v minimálně 2 termínech). Min. 50% školení musí tvořit praktická cvičení.
 - c) V rámci záruky odstranit hardwarovou závadu zboží výměnou vadného dílu nebo poskytnutím náhradního zařízení. Lhůta pro odstranění hardwarové závady je stanovena takto:

Prodávající je povinen odstranit hardwarovou závadu zařízení (např. formou výměny vadného zařízení na pražské adrese uvedené kupujícím při nahlášení závady) do konce pracovní doby (pracovní dobou se rozumí 8:00 hod. až 17:00 hod.) pracovního dne bezprostředně následujícího po dni, ve kterém byla závada Dodavateli nahlášena.
 - d) Zajistit po dobu záruky upgrade programového vybavení na zboží specifikované v Příloze č. 2 této smlouvy, pokud konfigurace zboží umožní novější verze programového vybavení provozovat.

- e) Zajistit po dobu záruky aktualizaci IPS signatur.
- f) Po dobu záruky zajistit kupujícímu přístup k dokumentaci výrobce zboží a přístup ke znalostní bázi, kterou výrobce v rámci své podpory poskytuje.
- g) Po dobu záruky zajistit odbornou pomoc při řešení konfiguračních a provozních problémů nebo závad dodaného software a vyvinout maximální úsilí (v případě potřeby ve spolupráci se vzdálenou asistenční službou výrobce) vedoucí k vyřešení problému či odstranění závady.

VI. Záruka za zboží

1. Záruční doba zboží činí tři (3) roky od převzetí zboží kupujícím.
2. Reklamací zjevných vad zboží uplatní kupující u prodávajícího nejpozději do sedmi dnů ode dne převzetí zboží, kdy má právo předmět smlouvy odmítnout převzít. Za zjevnou vadu se považuje zejména:
 - záměna zboží (vztahuje se na případy, kdy došlo k dodání jiného zboží, než bylo uvedeno ve smlouvě),
 - množstevní vada (vztahuje se na případ, kdy došlo k dodání jiného množství zboží, než bylo uvedeno ve smlouvě).
3. Kupující má právo reklamovat vady na zboží kdykoliv během záruční doby.
4. Oprava musí být dokončena v souladu s čl. V odst. 7 písm. c) této smlouvy nejpozději pracovní den následující po dni, ve kterém byla závada nahlášena. Oprava bude provedena v místě instalace zařízení (pražské lokality – adresu instalace zařízení specifikuje kupující při hlášení závady), není-li mezi zástupci smluvních stran dohodnuto jinak.
5. Prodávající neodpovídá po předání zboží kupujícímu za poškození zboží živelní událostí nebo mechanickým poškozením ze strany kupujícího nebo třetí osoby, které bylo způsobeno činností v rozporu s návodem k použití.
6. Kupující oznámí prodávajícímu případnou poruchu dodaného zboží telefonicky na linku +420 725 942 320. Prodávající zajistí v pracovní dny v době mezi 8 - 16h obsluhu této telefonické linky určené pro hlášení poruch na zboží. Následně prodávající bez prodlení potvrdí přijetí takového požadavku emailem udaným při hlášení poruchy.

VII. Sankce

1. V případě, že prodávající nesplní lhůtu dle čl. II. odst. 3., je kupující oprávněn účtovat za každý i započatý kalendářní den prodlení smluvní pokutu ve výši 0,5% z celkové ceny bez DPH za každý započatý den prodlení. Maximální výše této smluvní pokuty je omezena 10% celkové ceny bez DPH.
2. V případě, že prodávající nesplní lhůtu pro vyřešení reklamace dle čl. VI. odst. 4. smlouvy, je kupující oprávněn účtovat za každý i započatý kalendářní den prodlení smluvní pokutu ve výši 1% z celkové ceny bez DPH. Maximální výše této smluvní pokuty je omezena 10% celkové ceny bez DPH.
3. V případě, že prodávající bude v prodlení s plněním závazků uvedených v čl. V. odst. 7. písm. b) nebo d)-g), je kupující oprávněn účtovat za každý i započatý kalendářní den prodlení smluvní pokutu ve výši 0,5% z celkové ceny bez DPH. Maximální výše této smluvní pokuty je omezena 10% celkové ceny bez DPH.
4. Uplatní-li kupující svá práva dle odst. 1. až odst. 3. tohoto článku, bude smluvní pokutu fakturovat prodávajícímu s lhůtou splatnosti třicet (30) dnů.
5. Prodávající má právo na smluvní pokutu ve výši 0,5% z celkové ceny bez DPH za každý den prodlení s plněním povinností kupujícího vyplývajících z čl. II. odst. 1. písm. b), přičemž maximální výše této smluvní pokuty je omezena 10% celkové ceny bez DPH.

VIII. Přechod vlastnických práv

1. Vlastnické právo ke zboží, které se podle této smlouvy má stát vlastnictvím kupujícího, přechází na kupujícího dnem jeho předání a převzetí dle čl. III. této smlouvy.
2. Nebezpečí škody na zboží přechází na kupujícího současně s nabytím vlastnického práva ve smyslu odst. 1. tohoto článku.

IX. Řádné plnění

1. Prodávající odpovídá za porušení práv duševního vlastnictví třetích osob.
2. Prodávající odpovídá za právní vady plnění podle této smlouvy.
3. Prodávající se zavazuje, že při plnění této smlouvy nepoškodí práva třetích osob.

X. Platnost a účinnost smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran, přičemž platí datum pozdějšího podpisu a účinnosti dnem registrace smlouvy v registru smluv dle čl. XII. této smlouvy.
2. Tuto smlouvu lze ukončit:
 - a) dohodou smluvních stran, jejíž součástí bude i vypořádání vzájemných závazků a pohledávek,
 - b) odstoupením od smlouvy ze strany kupujícího, pokud mu nebude poskytnuta dotace z prostředků OP VVV na řešení projektu reg. č. CZ.02.2.67/0.0/0.0/17_044/0008562 „Podpora rozvoje studijního prostředí na Univerzitě Karlově – VRR“, nebo mu bude poskytnuta pouze v omezené výši nebo výdaje, které by mu na základě smlouvy měly vzniknout, budou řídicím orgánem OP VVV, popř. jiným kontrolním subjektem, označeny za nezpůsobilé. Dodavatel není v takovém případě oprávněn požadovat jakoukoliv náhradu škody či ušlého zisku.
 - c) odstoupením od smlouvy v případě podstatného porušení smluvních závazků jednou smluvní stranou, zejména v případě prodlení prodávajícího s plněním povinností vyplývajících z čl. II. smlouvy.

XI. Ochrana osobních údajů

1. Smluvní strany prohlašují, že jsou schopny zajistit technické a organizační zabezpečení ochrany osobních údajů uvedených v Příloze č. 3 smlouvy; zejména přijmout veškerá opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům, jejich změně, zničení či ztrátě, jakož i jejich zneužití, včetně opatření týkajících se práce s informačními systémy, v nichž jsou tyto osobní údaje zpracovávány a zajistit mlčenlivosti o údajích, které se v rámci zpracování osobních údajů dozvěděly.
2. Smluvní strany se dále zavazují:
 - a) neužívat osobní údaje k jinému než stanovenému účelu podle této smlouvy;
 - b) učinit s odbornou péčí všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů;
 - c) s odbornou péčí dodržovat všechna kontrolní a ochranná opatření za účelem ochrany osobních údajů;
 - d) veškeré požadavky na opravu osobních údajů, jejich blokování a doplnění se smluvní strany zavazují vzájemně si předávat;
 - e) informovat se vzájemně o všech skutečnostech majících vliv na zpracování osobních údajů;
 - f) oznámit si vzájemně každou pochybnost o dodržování zákona či narušení bezpečnosti osobních údajů;

- g) bude-li to třeba, poskytnout si vzájemně veškerou součinnost při styku a jednáních s Úřadem pro ochranu osobních údajů a se subjekty údajů;
- h) dodržovat všechny ostatní povinnosti stanovené zákonem, i pokud tak není výslovně uvedeno ve smlouvě.

XII. Závěrečná ustanovení

- 3. Prodávající má povinnost poskytnout součinnost a podrobit se kontrole pověřených osob a orgánů (MŠMT, Ministerstvo financí ČR, Evropská komise, Evropský účetní dvůr, Nejvyšší kontrolní úřad, Auditní orgán, Pověřený auditní subjekt, územní finanční orgány, Platební a certifikační orgán a další oprávněné orgány státní správy a kontrolní orgány), a to v souladu s právními předpisy Evropských společenství a Evropské unie a právními předpisy České republiky.
- 4. Prodávající má povinnost spolupůsobit při výkonu finanční kontroly ve smyslu §2 písm. e) a §13 zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, tj. poskytnout kontrolnímu orgánu doklady o plnění dle této smlouvy. Tutéž povinnost jsou povinni splnit i poddodavatelé prodávajícího.
- 5. Smluvní strany berou na vědomí, že tato smlouva vyžaduje uveřejnění v registru smluv podle zákona č. 340/2015 Sb., ve znění pozdějších předpisů a s tímto uveřejněním souhlasí. Uveřejněn bude celý text smlouvy, včetně všech jejích příloh. Zaslání smlouvy do registru smluv zajistí kupující neprodleně po nabytí platnosti smlouvy. Kupující se současně zavazuje informovat prodávajícího o provedení registrace smlouvy tak, že zašle prodávajícímu kopii potvrzení správce registru smluv o uveřejnění smlouvy bez zbytečného odkladu poté, kdy sám potvrzení obdrží, popř. v průvodním formuláři při registraci smlouvy vyplní příslušnou kolonku s ID datové schránky prodávajícího (v takovém případě potvrzení od správce registru smluv o provedení registrace smlouvy obdrží obě smluvní strany zároveň).
- 6. Právní vztahy vzniklé z této smlouvy nebo s touto smlouvou související se řídí zákonem č. 89/2012 Sb., občanským zákoníkem, ve znění pozdějších předpisů.
- 7. Jestliže smluvní strana v případě neplnění či porušení této smlouvy neuplatní všechna svá práva v takovém případě jí náležející, nelze takové jednání v žádném případě vykládat jako vzdání se takových práv pro případ jiného či následného neplnění či porušení sjednaných smluvních povinností.
- 8. Smlouvu lze měnit pouze oboustranně odsouhlasenými číslovanými dodatky podepsanými oprávněnými zástupci kupujícího a prodávajícího. Žádný jiný protokol, dokument, obvyklá praxe nebo zvyk nebudou považovány za dodatek ke smlouvě nebo za její pozměnění.
- 9. Smluvní strany se dohodly, že žádná z nich není oprávněna postoupit svá práva a povinnosti vyplývající z této smlouvy třetí straně bez předchozího písemného souhlasu druhé smluvní strany, s výjimkou peněžitých pohledávek za druhou smluvní stranou.
- 10. Bude-li některé z ustanovení této smlouvy shledáno jako neplatné nebo nevymahatelné, nemá taková skutečnost vliv na platnost nebo vymahatelnost zbývajících ustanovení této smlouvy.
- 11. Tato smlouva je vyhotovena ve čtyřech (4) stejnopisech, z nichž každá smluvní strana obdrží dvě (2) vyhotovení.
- 12. Nedílnou součástí této smlouvy jsou tyto přílohy:
 - Příloha č. 1 – Minimální technické parametry
 - Příloha č. 2 – Technická specifikace
 - Příloha č. 3 – Seznam oprávněných osob

XIII. Podpisy smluvních stran

Smluvní strany prohlašují, že tuto smlouvu prostudovaly, rozumějí jí a souhlasí se závazností jejích podmínek. Toto znění smlouvy vyjadřuje jejich svobodně, vážně, určitě a srozumitelně míněnou vůli.

Dne:

Dne:

Za kupujícího:

Za prodávajícího:

Podpis:

Podpis:

Jméno: Ing. Miroslava Oliveriusová

Jméno: Ing. Jan Pinta, MBA

Funkce: kvestorka UK

Funkce: jednatel společnosti

Příloha č. 1 – Minimální technické parametry

Zařízení musí být jako celek složeno z komponent jednoho výrobce, včetně všech poskytovaných funkcionalit typu IPS (Intrusion Prevention System), AV/AS (Anti-Virus/Anti-Spyware) signatur, databází pro URL kategorizaci, nástroje pro analýzu neznámých hrozeb (sandbox) apod. Zároveň musí být tímto jedním výrobcem zajištěna podpora minimálně po dobu plánované životnosti NGFW.

Celá dodávka musí obsahovat všechny HW komponenty vč. případných licencí. Zadavatel požaduje poskytnutí záruky v min. rozsahu NBD na dobu 3 let. Součástí záruky je možnost bezplatné aktualizace OS veškerých komponent a IPS signatur.

| Požadavek na funkcionalitu | Minimální požadavky |
|--|--|
| Požadavky na HW architekturu | |
| Třída zařízení | HW appliance NGFW firewall |
| Formát zařízení | do racku 19" max 5RU, součástí dodávky je veškeré příslušenství pro montáž do racku |
| Redundantní napájecí zdroje 230V/50Hz s oddělenými přívody | ANO |
| Výměna primárního i záložního zdroje za chodu zařízení | ANO |
| Doložení deklarované propustnosti NGFW | deklarovaná propustnost vybraných níže uvedených výkonnostních parametrů NGFW bude doložena měřicím protokolem. (Měření musí být provedeno při zapnutí všech bezpečnostních funkcí NGFW, včetně SSL/TLS dekrypcie na tzv. real-world vzorku provozu) |
| Modul pro zpracování dat (data plane) musí být v architektuře firewallu hardwarově oddělen od dalších podpůrných modulů pro správu zařízení a modulu řídicí modul pro podpůrné síťové činnosti (control and management plane), aby nemohlo dojít k jejich vzájemnému ovlivnění | ANO |
| NGFW musí obsahovat dedikovaný port typu RJ45 nebo micro-USB pro správu pomocí konzole pro přístup k CLI | ANO |
| FW musí podporovat virtuální kontexty, kterým je možné přidělit oddělené zdroje, a které mohou být spravovány rozdílnými administrátory, bez možnosti vzájemného ovlivnění | min. 20 kontextů |
| Počet portů 10 Gbit/s SFP+ pro zpracování komunikace | 16 |
| Počet portů 40 Gbit/s QSFP+ pro zpracování komunikace | 4 |

| | |
|---|--|
| minimální prostor pro uložení logovaných údajů na interní storage NGFW (uložených v RAID1) | 2TB |
| NGFW musí podporovat agregaci portů pomocí protokolu 802.3ad (LACP) | ANO |
| NGFW musí být rozměrově kompatibilní s 19" rozvaděčem | |
| NGFW musí podporovat dva nezávislé redundantní zdroje napájení AC 230V | |
| Výkonnostní parametry | |
| Propustnost NGFW při plné aplikační kontrole | 18 Gbps |
| Propustnost NGFW při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV, URL filteringu a analýze neznámých hrozeb (sandboxingu) bez zapnutí SSL dekrypce | 9 Gbps (tuto hodnotu požaduje zadavatel doložit testovacím protokolem) |
| Propustnost NGFW při plné aplikační kontrole a zapnutí všech dostupných signatur IPS a AV a URL filteringu se zapnutou SSL/TLS dekrypcí | 3 Gbps (tuto hodnotu požaduje zadavatel doložit testovacím protokolem, přičemž obsah dekryptovaného SSL/TLS provozu při RSA key size 2048 musí být alespoň 50 %.) |
| Minimální počet souběžných spojení | 4 000 000 |
| Minimální počet nových spojení za sekundu | 170 000 |
| Požadavky na High Availability | |
| NGFW musí podporovat režim HA složený alespoň ze dvou zařízení | v módu Active-Active i Active-Standby |
| veškeré informace o probíhajícím provozu musejí být 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 | V obou typech HA |
| NGFW musí být schopen provést failover na základě stavu interface (up/down), nedostupnosti druhého FW v HA, nedostupnosti specifikované IP adresy | ANO |
| Síťová funkcionalita | |
| NGFW musí plně podporovat IPv4 i IPv6. | ANO |
| NGFW musí podporovat zapojení v režimech L2 (s virtuálním L3 rozhraním), L3, transparent a TAP | ANO |
| NGFW musí podporovat překlady adres typu Static NAT, Dynamic NAT, PAT, NAT64. | ANO |
| NGFW musí podporovat směrování typu Static route, RIP, OSPFv2, OSPFv3, BGP, PIM a PBF (Policy Based Forwarding). | ANO |
| PBR musí být možno nakonfigurovat na základě všech dostupných metrik typu interface, IP adresa, uživatel. | ANO |

| Požadavky na VPN | |
|---|-----|
| NGFW musí podporovat site-to-site VPN pomocí protokolu IPSec. | ANO |
| NGFW musí podporovat Remote Access VPN pomocí protokolů IPSec a SSL (TLS). | ANO |
| NGFW musí podporovat Clientless Remote Access VPN. | ANO |
| Počet současně připojených uživatelů nesmí být licenčně omezen. | ANO |
| Propustnost IPSec musí být alespoň 8 Gbps. | ANO |
| NGFW musí podporovat tzv. posture analýzu (kontrolu souladu stavu zařízení s předdefinovanými pravidly) pro připojovaná koncová zařízení. | ANO |
| Požadavky na 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. | ANO |
| Jednotlivé HW appliance musí obsahovat plnohodnotné API rozhraní pro možnost automatizace. | ANO |
| NGFW musí podporovat integraci s managementem virtualizační platformy vCenter pro dynamickou úpravu pravidel v závislosti na aktuálně běžících virtuálních serverech. NGFW musí podporovat centrální management pro hromadnou správu bezpečnostních politik, hromadný upgrade OS a dynamického obsahu (signatury) i správu dalších parametrů. | ANO |
| Centrální management musí umožňovat použití šablon pro bootstrapping nových FW. | ANO |
| NGFW musí pro autentizaci a autorizaci administrátorů podporovat protokoly LDAP, Radius, TACACS+, Kerberos a osobní certifikáty | ANO |
| NGFW musí obsahovat nativní nástroje pro debugging problémových situací v úrovni L2 – L7 ISO/OSI modelu. | ANO |
| NGFW musí podporovat nativní nástroj pro odchyčení provozu. | ANO |

| | |
|---|-----|
| NGFW management musí podporovat práci více administrátorů ve stejném čase, včetně aplikace politik a nastavení vytvořených pouze konkrétním administrátorem. | ANO |
| Aplikační kontrola | |
| NGFW 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 |
| NGFW musí podporovat identifikaci aplikací napříč všemi porty/protokoly. | ANO |
| Identifikace aplikace musí probíhat přímo v NGFW. | ANO |
| NGFW musí podporovat řízení neznámého provozu. | ANO |
| NGFW musí umožňovat tvorbu uživatelsky definovaných aplikací bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele. | ANO |
| Kontrola na úrovni uživatelských identit | |
| NGFW musí podporovat vytváření bezpečnostních pravidel na základě uživatelských identit | ANO |
| Volba uživatelské identity musí být nativní součástí vytváření standardního bezpečnostního pravidla | ANO |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na koncové zařízení | ANO |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace klienta na doménový kontroler | ANO |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno, bez nutnosti instalace dalších komponent mimo samotné HW appliance | ANO |
| NGFW 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, Distributed COM Users) | ANO |
| NGFW musí podporovat získávání vazby IP adresa-uživatelské jméno prostřednictvím načtení informace z logového záznamu, získaného pomocí zabezpečeného protokolu Syslog | ANO |

| | |
|--|-----|
| NGFW musí podporovat získávání vazby IP adresa- uživatelské jméno z terminálových serverů MS a Citrix (možno za pomoci nainstalovaného agenta) | ANO |
| Dekrypce | |
| NGFW musí podporovat dekrypci odchozího SSL/TLS provozu, za pomoci podvržení serverového certifikátu klientům | ANO |
| NGFW musí podporovat dekrypci příchozího SSL/TLS provozu, za pomoci nainportovaného privátního klíče interního serveru | ANO |
| NGFW 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 |
| NGFW musí podporovat dekrypci za pomocí ECC (Elliptical Curve Cryptography), včetně DHE a ECDHE pro příchozí i odchozí provoz | ANO |
| NGFW musí podporovat přeposlání dešifrovaného provozu na specifický port pro potřeby dalšího zpracování | ANO |
| Sandboxing | |
| Firewall musí podporovat možnost odeslat do sandboxu k inspekci vzorky procházející protokolem SMTP, HTTP, FTP, IMAP, POP3, SMB | ANO |
| Sandbox systém musí být podporován v tzv. on-premise umístění | ANO |
| Sandbox systém musí být od stejného výrobce, jako je NGFW, ale nemusí být HW součástí NGFW | ANO |
| Sandbox systém musí být schopen okamžitě automaticky vytvořit IPS/AV signatury pro NGFW, 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 |
| Odpověď ze Sandboxu musí být k dispozici do 5 min. | ANO |
| Bezpečnostní funkcionality | |
| NGFW musí podporovat zavedení tzv. pozitivního bezpečnostního modelu – whitelisting pouze povolených aplikací a zákaz všeho ostatního, včetně neznámého provozu | ANO |

| | |
|---|-----|
| NGFW 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 |
| NGFW musí umožňovat tvorbu uživatelsky definovaných IPS signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele | ANO |
| NGFW 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, SMB | ANO |
| NGFW musí umožňovat tvorbu uživatelsky definovaných spyware signatur bez nutnosti využití externího nástroje nebo zásahu výrobce/dodavatele | ANO |
| NGFW musí podporovat možnost zablokování útoku na známá C&C centra i v případě, že je provoz šifrován a není možné provádět SSL dekrypci | ANO |
| NGFW musí v bezpečnostních pravidlech podporovat použití externích dynamických seznamů; FW musí poskytovat možnost ověřit na základě certifikátů pravost těchto dynamických seznamů | ANO |
| NGFW musí, pro přístup ke kritickým aplikacím, poskytovat možnost vynutit vícefaktorové ověření prostřednictvím webového portálu, bez ohledu na to, jestli cílová aplikace podporuje vícefaktorovou autentizaci; tato vlastnost musí být konfigurovatelná na úrovni bezpečnostního pravidla | ANO |
| NGFW musí poskytovat možnost zabránit odeslání doménových uživatelských přihlašovacích údajů do jiných, než povolených URL kategorií, pro zabránění phishingu | ANO |
| NGFW musí být schopen automaticky vytvářet C&C signatury a okamžitě je aplikovat je do bezpečnostní politiky | ANO |
| NGFW 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 |
| NGFW musí být schopen detekce botnetů na základě behaviorální analýzy | ANO |

| Ochrana proti DoS | |
|---|-----|
| NGFW 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 |
| QoS | |
| NGFW 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 |
| NGFW musí podporovat prioritizaci provozu na základě DSCP | ANO |
| NGFW musí podporovat prioritizaci provozu na základě Identifikované aplikace | ANO |
| URL filtering | |
| NGFW musí podporovat nativní podporu pro využívání databáze URL | ANO |
| URL databáze musí být od stejného výrobce, jako je FW | ANO |
| NGFW musí být schopen použít URL kategorií v definici bezpečnostního pravidla | ANO |
| NGFW 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 |
| Rozhraní URL databáze v NGFW musí obsahovat možnost požádat o rekatégorizaci nevhodně zařazených URL bez nutnosti otevírání support case | ANO |
| Logování | |
| NGFW musí obsahovat lokální úložiště logů | ANO |
| NGFW musí obsahovat nástroj pro analýzu logů bez nutnosti využití dalšího systému mimo GUI | ANO |
| NGFW 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 |
| NGFW musí podporovat přeposílání logů na zařízení třetích stran | ANO |
| NGFW musí umožňovat výběr přeposílaných logů na úrovni bezpečnostního pravidla | ANO |

Příloha č. 2 - Technická specifikace

Příloha č. 3
Seznam oprávněných osob

| Oprávněná osoba | Kupující | Prodávající |
|--|---|--|
| Osoba oprávněná jednat ve věcech smluvních | Ing. Miroslava Oliveriusová miroslava.oliveriusova@ruk.cuni.cz tel. 224 491 316 | Ing. Jan Pinta, MBA jan.pinta@h-square.cz tel. 722 944 414 |
| Osoba oprávněná jednat ve věcech technických | Aleš Houdek ales.houdek@ruk.cuni.cz tel. 224 491 239 | Ing. Jan Linhart jan.linhart@h-square.cz tel. 725 359 924 |