

Příloha č. 2 Výzvy k podání nabídky - Závazné minimální obchodní a platební podmínky zadavatele (tj. návrh smlouvy).

Hasičský záchranný sbor Moravskoslezského kraje				
EVIDENCE SMLUV				
HMSK	SML	446	2019	
		poř. číslo	rok	dobu plnění
Ev. číslo v SSD				

## KUPNÍ SMLOUVA

### I. Smluvní strany

**Česká republika - Hasičský záchranný sbor Moravskoslezského kraje**

Sídlo: Výškovická 40, 700 30 Ostrava-Zábřeh

IČO: 70884561

DIČ: CZ 70884561 (není plátcem DPH)

Zastoupený: brig. gen. Ing. Vladimírem Vlčkem, Ph.D., ředitelem HZS Moravskoslezského kraje

Bankovní spojení: ČNB Ostrava, č. účtu: 1933881/0710

(dále jen „kupující“)

a

**VÍTKOVICE IT SOLUTIONS a.s.**

Sídlo: Cihelní 1575/14, 702 00 Ostrava – Moravská Ostrava

IČO: 28606582

DIČ: CZ28606582

Zastoupená:



Bankovní spojení: Česká spořitelna, a.s., č. účtu: 4312807389/0800

zapsána v obchodním rejstříku vedeném Krajským soudem v Ostravě, odd. B, vl. 4229

(dále jen „prodávající“)

### II. Základní ustanovení

1. Smluvní strany uzavírají tuto smlouvu v souladu s ustanoveními § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „OZ“) a dohodly se, že tento závazkový vztah, rozsah a obsah vzájemných práv a povinností z této smlouvy vyplývajících se bude řídit příslušnými ustanoveními citovaného zákoníku, nestanoví-li tato smlouva jinak.
2. Smluvní strany prohlašují, že údaje uvedené v čl. I. této smlouvy a taktéž oprávnění k podnikání jsou v souladu s právní skutečností v době uzavření smlouvy. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení druhé smluvní straně.
3. Smluvní strany prohlašují, že si před uzavřením smlouvy vzájemně sdělily veškeré jim známé skutkové a právní okolnosti, které by mohly být významné ve vztahu k uzavření této smlouvy nebo k plnění z této smlouvy vyplývajícím.
4. Smluvní strany prohlašují, že osoby podepisující tuto smlouvu jsou k tomuto jednání oprávněny.

### III. Předmět smlouvy

1. Předmětem této smlouvy je pořízení 2 ks přístupových VPN firewallů včetně implementace (dále jen „zboží“), které je blíže specifikováno v příloze č. 1 této smlouvy.
2. Prodávající se zavazuje kupujícímu zboží dodat a umožnit mu nabýt vlastnické právo ke zboží. Součástí dodání je i předání dokladů, které se ke zboží vztahují (zejména návody k použití v českém jazyce), a doprava zboží do místa plnění.



3. Vlastnické právo ke zboží přechází na kupujícího okamžikem odevzdání a převzetí zboží kupujícím v místě plnění.
4. Smluvní strany prohlašují, že předmět smlouvy není plněním nemožným a že smlouvu uzavřely po pečlivém zvážení všech možných důsledků.
5. Podkladem pro uzavření této smlouvy je nabídka prodávajícího ze dne 18.10.2019, která byla na základě zadávacího řízení č. 155/2019/VZMR vybrána jako nejvýhodnější.

#### **IV. Kupní cena**

1. Kupující se zavazuje zboží převzít a zaplatit prodávajícímu kupní cenu.
2. Kupní cena je stanovena dohodou smluvních stran a činí:

cena bez DPH	413 223,00 Kč
DPH 21 %	86 776,83 Kč
<b>cena včetně DPH</b>	<b>499 999,83 Kč</b>

3. Podrobná kalkulace celkové kupní ceny tvoří přílohu č. 2 této smlouvy.
4. Sjednaná kupní cena je konečná a zahrnuje veškeré náklady spojené s koupí zboží, a to zejména dopravu zboží do místa plnění podle čl. VI. této smlouvy, instalaci, instruktaž obsluhy, clo, skladování, balné atd..
5. Cena je stanovena jako nejvýše přípustná při sazbě DPH ve výši 21 %, přičemž sazba DPH bude v případě její změny stanovena v souladu s platnými právními předpisy.

#### **V. Čas plnění**

Prodávající je povinen dodat kupujícímu zboží do 60 kalendářních dnů od nabytí účinnosti uzavřené smlouvy.

#### **VI. Místo plnění**

Místem plnění podle této smlouvy je Integrované bezpečnostní centrum Moravskoslezského kraje, Nemocniční 3328/11, Ostrava-Moravská Ostrava.

#### **VII. Způsob dodání zboží**

1. Zboží je dodáno v okamžiku převzetí zboží pověřeným zástupcem kupujícího v místě plnění uvedeném v této smlouvě. Pověřený zástupce kupujícího potvrdí převzetí zboží na dodacím listu, předávacím protokolu nebo jiném obdobném dokladu.
2. Kupující se zavazuje zboží, dodané řádně a včas, převzít a zaplatit za něj kupní cenu.
3. Kupující při převzetí zboží provede kontrolu:
  - a) dodané značky, typu, druhu,
  - b) dodaného množství,
  - c) zjevných jakostních vlastností,
  - d) zda nedošlo k poškození zboží při přepravě,
  - e) dodaných dokladů.
4. V případě zjištěných zjevných vad zboží může kupující odmítnout jeho převzetí, což řádně i s důvody potvrdí na příslušném dokladu. Na následné předání zboží se použijí ustanovení tohoto článku obdobně.

#### **VIII. Jakost, záruka za jakost, vady zboží**

1. Prodávající je povinen dodat zboží v množství, druhu, jakosti, provedení stanovenými touto smlouvou a podle technických parametrů a obchodních podmínek sjednaných

- v této smlouvě. Smluvní strany se dohodly na I. jakosti dodaného zboží. Prodávající je povinen dodat zboží nové, nepoužité, vyrobené v roce 2018 a nebo později.
2. Prodávající není oprávněn dodat větší než sjednané množství zboží, ustanovení § 2093 OZ se nepoužije.
  3. Prodávající prohlašuje, že zboží nemá právní vady podle § 1920 OZ.
  4. Poruší-li prodávající povinnosti stanovené v odst. 1 tohoto článku, jedná se o vady plnění.
  5. V případě dodání vadného plnění se práva a povinnosti smluvních stran řídí ustanoveními § 2099 a násl. OZ.
  6. Smluvní strany se dohodly na záruční době 36 měsíců.
  7. Záruční doba začíná běžet dnem předání zboží kupujícímu bez vad a nedodělků.
  8. Záruční doba neběží po dobu, po kterou nemůže kupující zboží řádně užívat pro vady, které jsou způsobilé založit práva kupujícího z vadného plnění.
  9. Veškeré vady zboží je kupující povinen oznámit prodávajícímu bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení o vadě zaslaného na adresu prodávajícího / telefonicky na tel. č. [REDACTED] / e-mailem na [REDACTED]
  10. Prodávající je povinen kupujícímu písemně potvrdit, kdy bylo právo z vadného plnění uplatněno, způsob provedení opravy a dobu trvání opravy.
  11. Prodávající započne s odstraněním vady nejpozději do 12 hodin od okamžiku doručení oznámení o vadě, pokud se smluvní strany nedohodnou jinak. Po celou dobu opravy zařízení je prodávající povinen zajistit plnou funkčnost náhradním způsobem (např. dodáním náhradního zařízení) tak, aby nebyl ovlivněn standardní provoz.
  12. Vada bude odstraněna nejpozději do 4 pracovních dnů od okamžiku doručení oznámení o vadě, pokud se smluvní strany nedohodnou jinak.
  13. Nebezpečí škody na zboží přechází na kupujícího okamžikem převzetí zboží.
  14. Prodávající je povinen nahradit kupujícímu škodu, která vznikne porušením smluvní povinnosti prodávajícího nebo vadným plněním, a to v plné výši. Prodávající je rovněž povinen kupujícímu nahradit náklady, které kupujícímu vzniknou při uplatňování práv na náhradu škody.

### **IX. Platební podmínky**

1. Smluvní strany nesjednávají zálohy na kupní cenu.
2. Podkladem pro úhradu kupní ceny dodaného zboží bude faktura, která bude mít náležitosti daňového dokladu dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále také „faktura“). Kupující tímto souhlasí s použitím daňového dokladu v elektronické podobě.
3. Faktura musí kromě zákonem stanovených náležitostí obsahovat také:
  - a) označení smlouvy a datum jejího uzavření
  - b) označení banky a čísla účtu, na který musí být zapláceno
  - c) kontaktní údaje prodávajícího pro záležitosti fakturace
  - d) součástí faktury musí být dodací list, předávací protokol nebo jiný obdobný doklad včetně soupisu jednotlivých položek, podepsaný zástupci obou smluvních stran, potvrzující, že zboží podle této smlouvy bylo řádně dodáno.
4. Faktura bude prodávajícím vystavena po odevzdání a převzetí zboží podle této smlouvy. Lhůta splatnosti faktury je dohodou stanovena na 30 kalendářních dnů ode dne doručení faktury kupujícímu. Stejná lhůta splatnosti platí i při placení jiných plateb (např. úroků z prodlení, smluvních pokut, náhrad škody aj.).
5. Prodávající je povinen doručit fakturu do kupujícímu nejpozději do 16.12.2019. Faktura v listinné podobě musí být doručena na adresu kupujícího na ul. Výškovická 40, 700 30



Ostrava-Zábřeh, a faktura v elektronické podobě musí být doručena na e-mailovou adresu: [uctarna@hzsmk.cz](mailto:uctarna@hzsmk.cz).

6. Nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude chybně vyúčtována cena nebo DPH, je kupující oprávněn bez zaplacení fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně k provedení opravy. Ve vrácené faktuře vyznačí důvod vrácení. Prodávající provede opravu vystavením nové faktury. Od doby odeslání vadné faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží opět ode dne doručení nově vyhotovené faktury kupujícímu.
7. Smluvní strany se dohodly, že platba bude provedena bezhotovostním převodem z účtu kupujícího na číslo účtu uvedené prodávajícím na faktuře bez ohledu na číslo účtu uvedené v čl. I. této smlouvy.
8. Povinnost zaplatit cenu zboží je splněna dnem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.
9. Pokud kupující uplatní nárok na odstranění vady zboží ve lhůtě splatnosti faktury, není kupující povinen až do odstranění vady zboží uhradit cenu zboží. Okamžikem odstranění vady zboží začne běžet nová lhůta splatnosti faktury.

#### **X. Podstatné porušení smlouvy**

1. Smluvní strany pokládají za podstatné porušení této smlouvy:
  - a) prodlení prodávajícího se splněním ve sjednaném čase plnění podle čl. V. této smlouvy,
  - b) nedodání zboží v požadované kvalitě nebo množství podle této smlouvy,
  - c) nevyřešení zjištěných vad v souladu s čl. VIII. této smlouvy ve sjednané lhůtě.
2. V případě podstatného porušení smlouvy ze strany prodávajícího je kupující oprávněn od této smlouvy odstoupit podle čl. XII.

#### **XI. Sankční ujednání**

1. V případě prodlení prodávajícího s dodáním zboží je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,2 % z celkové kupní ceny vč. DPH za každý i započatý den prodlení.
2. V případě prodlení kupujícího se zaplacením dohodnuté kupní ceny je kupující povinen zaplatit prodávajícímu úrok z prodlení ve výši 0,05 % z dlužné částky za každý i započatý den prodlení.
3. V případě nedodržení dohodnuté lhůty k odstranění vad dle čl. VIII. této smlouvy, jestliže se tyto vady projeví v záruční době, je prodávající povinen kupujícímu uhradit smluvní pokutu ve výši 1000,- Kč za každý i započatý den prodlení s odstraněním každé vady.
4. Zánik závazku pozdním plněním neznamená zánik nároku na smluvní pokutu za prodlení s plněním.
5. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody, kterou lze vymáhat samostatně.
6. Smluvní pokuty je kupující oprávněn započíst proti pohledávce prodávajícího.
7. Smluvní pokuty sjednané touto smlouvou zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé smluvní straně škoda, kterou lze vymáhat samostatně.

#### **XII. Odstoupení od smlouvy**

1. Odstoupení od smlouvy se řídí ustanovením § 2001 a násl. OZ, pokud není dále stanoveno jinak.

2. Kupující je oprávněn odstoupit od smlouvy, jestliže se prodávající rozhodnutím soudu ocitne v úpadku dle zákona č. 182/2006 Sb., insolvenční zákon, ve znění pozdějších předpisů.
3. Účinky každého odstoupení od smlouvy nastávají okamžikem doručení písemného projevu vůle odstoupit od této smlouvy druhé smluvní straně. Odstoupení od smlouvy se nedotýká zejména nároku na náhradu škody, smluvní pokuty a povinnosti mlčenlivosti.
4. Proávající podpisem této smlouvy prohlašuje, že není veden v registru nespolehlivých plátců DPH vedeném Ministerstvem financí České republiky. V případě, že je toto prohlášení nepravdivé nebo v případě, že bude prodávající dodatečně zapsán v registru nespolehlivých plátců DPH v průběhu plnění této smlouvy a nevyrozumí o tom ihned kupujícího, má kupující právo od smlouvy odstoupit v souladu s odst. 3 tohoto článku.

### **XIII. Závěrečná ujednání**

1. Tato smlouva se řídí právním řádem České republiky. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací smlouvy budou řešeny nejprve smírnou cestou – dohodou. Nedojde-li k dohodě, budou spory řešeny v soudním řízení před příslušnými obecnými soudy České republiky.
2. Proávající není oprávněn bez předchozího písemného souhlasu kupujícího postoupit tuto smlouvu, její část nebo práva a povinnosti z této smlouvy třetí osobě.
3. Proávající bez jakýchkoliv výhrad souhlasí se zveřejněním své identifikace a dalších údajů uvedených ve smlouvě včetně ceny zboží.
4. Změnit nebo doplnit tuto smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této kupní smlouvy a podepsány oprávněnými zástupci obou smluvních stran.
5. Pro případ, že ustanovení této smlouvy oddělitelné od ostatního obsahu se stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečných odkladů nahradit takové ustanovení novým. Případná neplatnost některého z takovýchto ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení.
6. Proávající se zavazuje, že jakékoliv informace, které se dověděl v souvislosti s plněním předmětu smlouvy, neposkytne bez předchozího písemného souhlasu třetím osobám ani je nepoužije v rozporu s účelem této smlouvy, ledaže se jedná o informace, které jsou veřejně přístupné nebo o případ, kdy je zpřístupnění informace vyžadováno zákonem nebo závazným rozhodnutím oprávněného orgánu. Za porušení povinnosti mlčenlivosti osobami, které se budou podílet na dodání zboží dle této smlouvy, odpovídá prodávající, jako by povinnost porušil sám. Povinnost mlčenlivosti trvá i po splnění této smlouvy.
7. Smluvní strany shodně prohlašují, že si tuto smlouvu před jejím podepsáním přečetly, že byla uzavřena po vzájemném projednání, nebyla uzavřena v tísní ani za jednostranně nevýhodných podmínek a že se dohodly o celém jejím obsahu, což stvrzují svými podpisy.
8. Tato smlouva podléhá povinnosti uveřejnění v registru smluv podle 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, přičemž smluvní strany souhlasí s jejím uveřejněním v plném rozsahu. Uveřejnění této smlouvy v registru smluv zajistí kupující.
9. Tato smlouva nabývá účinnosti dnem jejího uveřejnění v registru smluv.
10. Smluvní strany uzavírají tuto smlouvu v souladu s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice



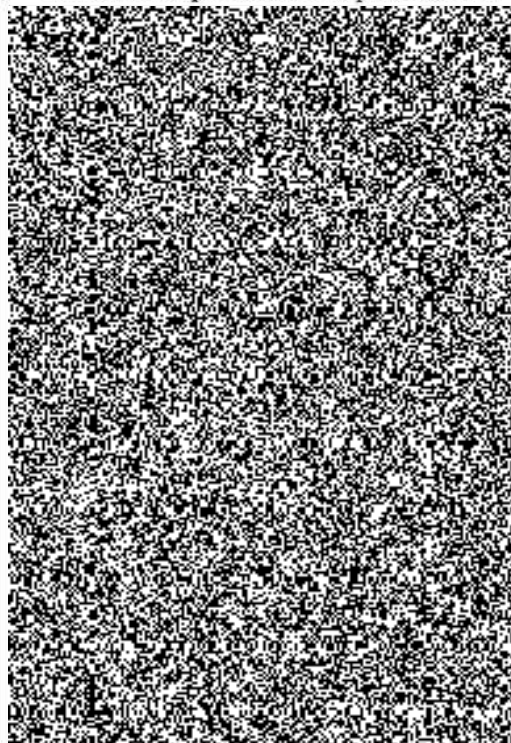
95/46/ES (obecné nařízení o ochraně osobních údajů). Osobní údaje uvedené v této smlouvě budou použity pouze pro účely plnění této smlouvy a při uveřejnění smlouvy budou anonymizovány.

11. Vše, co bylo dohodnuto před uzavřením smlouvy, je právně irelevantní a mezi stranami platí jen to, co je dohodnuto v této smlouvě.
12. Tato smlouva je vyhotovena ve dvou stejnopisech s platností originálu, přičemž každá ze smluvních stran obdrží jeden stejnopis.
13. Nedílnou součástí této smlouvy jsou přílohy č. 1 – technická specifikace a příloha č. 2 – cenová kalkulace.

Ostrava dne..... 5.11.2019

.....  
za k  
brig. gen. I ..... lček, Ph.D.  
H.Z.S. Morav ..... kraje

**Hasičský záchranný sbor**  
Moravskoslezského kraje  
Výškovická 40  
700 30 Ostrava - Zábřeh  
19



**VÍTKOVICE**  
VÍTKOVICE IT SOLUTIONS a.s.  
Cihelní 1575/14  
Moravská Ostrava  
702 00 Ostrava  
IČ: 28606582  
DIČ: CZ28606582

-1-

## Technická specifikace pořízení 2 ks přístupových VPN firewallů

Stávajícím prvkům Cisco ASA 5510 dobíhá technická podpora, je již ukončena výroba a možnost výměny stávajících prvků stejným zařízením. Tyto prvky jsou velmi důležitou součástí síťové infrastruktury IBC, které slouží k oddělení vnitřní sítě Integrovaného bezpečnostního centra Moravskoslezského kraje od neveřejných komunikačních sítí a mimo jiné se pomocí nich vytváří zabezpečené VPN sítě (site-to-site příp. remote access) ve failover modu. Touto technologií jsou připojeny veškerá výjezdová místa jednotek IZS, je jí řízen zabezpečený vzdálený přístup externích firem zabezpečujících servisní služby a také zabezpečený přístup interních pracovníků do IBC z externího prostředí.

### Obecné požadavky:

- 2 nové kusy firewallů
- záruka a podpora 36 měsíců
- firewally musí po pořízení licencí podporovat funkce IPS a anti-mallware, tyto licence nejsou součástí dodávky této veřejné zakázky
- instalace a konfigurace do stávající infrastruktury IBC (včetně integrace do dohledu IBC – CA Spectrum OneClick)

### Technické provedení:

Při dodání komponent bude zhotovitelem zjištěna aktuální verze firmware a konfigurace stávající síťové infrastruktury u zadavatele. Dle těchto zjištění bude na pracovišti zhotovitele proveden update na odpovídající verzi a nastavení nových prvků včetně jejich otestování.

Jakmile budou nové komponenty nastaveny a připraveny k instalaci, bude se zadavatelem dohodnut termín instalace do produkčního prostředí, který bude dle požadavků zadavatele v nočních hodinách (mezi 00:00 a 04:00). Zhotovitel zajistí, aby výpadek netrval déle než 4 hodiny, s tím, že plánovanou dobu výpadku je potřeba minimalizovat.

Dodané zařízení musí splnit (nebo převýšit) všechny technické parametry uvedené v následující tabulce:

Požadovaná funkcionality/vlastnost	Způsob splnění požadované funkcionality/vlastnosti	Doplň dodavatel dle nabízeného zařízení
<b>Výkon a funkcionality firewallu</b>		
Formát zařízení	Appliance, 1RU	Appliance, 1RU
Minimální počet 1Gb 10/100/1000 BaseT Ethernet pro management	1	1
Minimální počet 1Gb 10/100/1000 BaseT datových Ethernet rozhraní, standardně osazených	12	12
Minimální počet 1Gb SFP rozhraní portů pro data, standardně osazených	4	4
Podporovaný počet současně otevřených spojení aplikačního FW	1M	1M
Rychlost vytváření nových spojení aplikačního FW	18K/s	18K/s
Propustnost aplikačního FW (top parametry)	2 Gbps	2.3 Gbps
Propustnost aplikačního FW + IPS (top parametry)	2 Gbps	2.3 Gbps
Propustnost aplikačního FW (transakční profil, 450B průměrná velikost paketu)	500 Mbps	500 Mbps
Propustnost aplikačního FW + IPS (transakční profil, 450B průměrná velikost paketu)	500 Mbps	500 Mbps
Podpora L2 (transparentního) módu s podporou NAT a PAT	Ano	Ano
Podpora L3 (routovaného) módu s podporou NAT a PAT	Ano	Ano
Podporovaný počet VLAN	Min. 400	1024
Podpora stateful failover	active/standby	Active/standby
Podpora zvyšování výkonu pomocí clusterování firewallů – sloučení firewallů do jednoho logického clusteru	Ano	Ano
Cluster firewallů se musí vzhledem k další infrastruktuře tvářit jako jeden prvek s podporou LACP	Ano	Ano
Cluster podporuje stavovou inspekci nesymetrického provozu vstupující do různých firewallů clusteru	Ano	Ano
Možnost sloučení více fyzických rozhraní do jednoho logického s rozkladem zátěže a podporou LACP	Ano	Ano
Dynamické směrování - podpora alespoň RIP, OSPF, BGP	Ano	Ano
Podpora IPv6 dynamického směrování – alespoň OSPFv3, BGP	Ano	Ano
Podpora Policy based Routing	Ano	Ano
Podpora kontroly paketů TCP provozu s ochranou před útoky jejichž cílem je obejít bezpečnostní prvky nestandardním rozkladem dat do paketů, fragmentací, apod.	Ano	Ano
Podpora filtrace IPv4, IPv6	Ano	Ano
Podpora filtrace podle identity uživatele nebo jeho skupiny definované v AD	Ano	Ano
Podpora filtrace podle bezpečnostních skupinových rolí přiřazených na přístupových přepínačích	Ano	Ano
Podpora inspekce IPv6 provozu	Ano	Ano



Možnost filtrace komunikace Botnet sítě s využitím databází o důvěryhodnosti adres v Internetu	Ano	Ano
Podpora NAT64 a DNS64	Ano	Ano
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.	Ano	Ano
Možnost řízení rychlosti datových toků na úrovni pravidel FW	Ano	Ano
Možnost rozšíření o funkce IPS	Ano	Ano
Možnost rozšíření o funkce URL filtrace	Ano	Ano
Možnost rozšíření o funkce antimalware filtrace	Ano	Ano
Bezpečnostní pravidla mohou kromě adres a portů zohlednit i identitu uživatele	Ano	Ano
Zohlednění kontextových informací o koncovém zařízení (typ, stav, spod.) a využití ve filtrech	Ano	Ano
API rozhraní pro sdílení kontextových informací s dalšími systémy	Ano	Ano
Možnost začlenit do SDN řešení – kontrolerem řízená infrastruktura (APIC)	Ano	Ano
<b>Funkce IPS a anti-malware – musí podporovat (není požadováno jako součást dodávky)</b>		
Možnost definovat typ provozu předávaný k inspekci do IPS	Ano	Ano
Podpora také IDS režimu – pasivního monitorování (TAP režim)	Ano	Ano
Možnost definovat režim provozu při zahlcení nebo nedostupnosti IPS funkcí (fail open, fail close)	Ano	Ano
Možnost obejít IPS funkcí při zahlcení nebo nedostupnosti	Ano	Ano
Podpora 802.1Q tagovaných rámců	Ano	Ano
Podpora různých IPS politik pro různé typy provozu	Ano	Ano
Inspekce pro IPv4 i IPv6	Ano	Ano
Podpora funkce Adaptivní konfigurace filtrů, která upozorní, případně vypne filtr, který může způsobit zahlcení systému	Ano	Ano
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	Ano	Ano
Podpora automatické aktualizace filtrů/signatur, geolokační databáze, databáze zranitelností a databáze systémů na internetu s poškozenou reputací	Ano	Ano
Podpora aplikace pro psaní zákaznických filtrů	Ano	Ano
Podpora importu komunitních filtrů/signatur Snort	Ano	Ano
IPS musí umět detekovat a blokovat útoky průzkumných aktivit	Ano	Ano
IPS musí podporovat adaptivní ochranu filtrů proti přetížení či DoS útoku na IPS	Ano	Ano
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	Ano	Ano
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	Ano	Ano



Odkaz na CVE a dokumentaci ke známým bezpečnostním incidentům přímo hyperlinkovým odkazem z dané bezpečnostní události	Ano	Ano
Možnost vyhledávání typu signatury v centrální databázi dodavatele podle typu a závažnosti útoku	Ano	Ano
Funkce pro kontrolu DLP ( např. pomocí Snort preprocesorů)	Ano	Ano
Podpora vrstev IPS politik s možností volit předdefinované politiky v základní vrstvě orientované na bezpečnost nebo naopak minimalizace false-positive	Ano	Ano
Možnost aplikace vrstvy doporučených politik, kterou generuje přímo IPS podle pasivního sledování lokálního prostředí	Ano	Ano
Možnost definice uživatelské vrstvy politik	Ano	Ano
Předefinování pravidel přes vrstvy IPS politik = platí relevantní pravidla v nejvyšší vrstvě IPS politik	Ano	Ano
Různé politiky lze sdílet a aplikovat na různé senzory	Ano	Ano
Podpora aktivní inline ochrany před malware s detekcí známých nebo podezřelých malware nezávislé na aktuálních databázích AV dodavatelů	Ano	Ano
Ochrana před malware typu „zero day attack“ které nelze detekovat tradičními antiviry	Ano	Ano
Retrospektivní ochrana prostředí – pokud SW kód je později detekován jako malware, je na to IPS schopna reagovat	Ano	Ano
Zobrazení trajektorie malware – pohyb, mutace, přenosy v síti mezi stanicemi přímo v GUI centralizované konzole	Ano	Ano
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.	Ano	Při instalaci AMP klienta na koncové zařízení
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	Ano	Ano
Informace o trajektorii malware mezi stanicemi, karanténě, síťových komunikacích získávané a centralizované pro jednotlivé koncové stanice	Ano	Ano
IPS musí být možné nasadit plně transparentně k existujícímu síťovému prostředí a jeho nasazení nesmí být podmíněno rekonfigurací stávajících aktivních prvků	Ano	Ano
Možnost definovat pravidla chování sítě a komponentů, pro automatickou detekci tzv. „compliance violation“	Ano	Ano
Možnost automatické i manuální klasifikace stanice jako „kritické“ se zohledněním v pravidlech, reportech apod.	Ano	Ano
Podpora „remediation“ modulů pomocí nichž lze ovládat další prvky infrastruktury a aplikovat filtry, směrování, apod.	Ano	Ano
Otevřené rozhraní pro uživatelsky vytvářené „remediation“ moduly	Ano	Ano
Podpora databází reputací adres v Internetu (Security Intelligence)	Ano	Ano
<b>Funkce Next-Gen FW</b>		
Možnost definovat různé přístupové politiky pro různé typy provozu, např. podle domén, VLAN, konkrétních FW, apod.	Ano	Ano
Podpora pasivního monitorování (TAP režim)	Ano	Ano

Podpora 802.1Q tagovaných rámců	Ano	Ano
Počet podporovaných aplikací	Min. 3000	4000
Kategorie aplikací (nebezpečné, důležité, apod.)	Ano	Ano
URL kategorií	80	80
Katagorizovaných světových URL	280 milionů	280 milionů
Řízení přístupu k WWW - Web Usage Control (WCU)	Ano	Ano
Filtrace podle typů aplikací webových i ne-webových	Ano	Ano
Filtrace podle reputace serverů	Ano	Ano
SSL inspekce (dekrypce/enkrypce)	Ano	Ano
Security Intelligence database – známé uzly botnet sítě C&C	Ano	Ano
Security Intelligence database – známé adresy anonymních proxy, otevřených mail relay, apod.	Ano	Ano
Security Intelligence database – známé nebezpečné URL adresy a jmenné domény	Ano	Ano
Možnost integrovat vlastní reputační database	Ano	Ano
Podpora komunitních, otevřených standardů popisu aplikací (OpenAppID)	Ano	Ano
Filtry mohou zohlednit roli a identitu uživatele	Ano	Ano
Podpora rozhraní pro sběr informací o síťové komunikaci z prvků infrastruktury – přepínače, směrovače (např. netflow)	Ano	Ano
Využití informací z prvků infrastruktury (např. netflow) pro monitorování a detekci chování sítě	Ano	Ano
Řešení musí být schopné pasivního sběru informací o síťových zařízeních a zobrazení:	Typ zařízení Operační systém Dodavatel OS Použité síť. protokoly Použité síť. služby Otevřené porty síť. služeb Potenciální zranitelnosti	Ano
Přehled o síťových spojení má poskytovat minimálně tyto informace:	Čas startu a konce flow Akce (allow, deny,...) Důvod případného blokování Zdroj. a cíl. adresa Vstupní a výstupní zóna Vstupní a výstupní rozhraní	Ano



	Zdroj, a cíl, port Aplikační protokol IPS událost, pokud vznikne Riziková úroveň IPS události Použitá síťová aplikace Rizikovost aplikace „Business impact“ aplikac e Množství přenesených dat	
<b>Funkce VPN AnyConnect</b>		
Cisco AnyConnect Plus License, 3YR, 25 Users	Ano	Ano
<b>Správa</b>		
Vzdálené správa přes grafické rozhraní bez nutnosti instalace zvláštního SW	Ano	Ano
Přístup ke GUI http/https protokolem	Ano	Ano
Možnost vzdáleného přístupem protokolem ssh přímo do FW	Ano	Ano
Možnost přístupu k textovým logům (syslog) přímo ve FW	Ano	Ano
Možnost centrální správy při nasazení více firewallů	Ano	Ano
Při centrální správě: možnost sdílených bezpečnostních politik	Ano	Ano
Při použití clusteru se spravuje pouze jeden logický prvek	Ano	Ano
Distribuce a správa software firewallu, bezpečnostních update (IPS signatury, databáze zranitelností, Security Intelligence databáze, geolokační databáze, apod.), konfigurací, licencí, atd. z grafického rozhraní managementu	Ano	Ano
Zobrazení logů a událostí v grafickém rozhraní správy	Ano	Ano
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 RADIUS server.	Ano	Ano
Nástroje pro troubleshooting, testování průchodu paketu firewallem, zachytávání provozu pro pozdější vyhodnocování	Ano	Ano
Funkce IPS a Next-Gen FW vyžadující dlouhodobější ukládání dat, korelace, reporty, apod. musí být spravovatelné z centrálního monitorovacího a konfiguračního systému (centrální dohledové konzole)	Ano	Ano
Centrální dohledová konzole musí být schopna dohledovat a spravovat více IPS senzorů a Next-Gen FW funkcí pro možnost korelace, sdílení politik, centrální sledování zdraví boxů, apod.	Ano	Ano
Centrální dohledová konzole musí být schopna poskytovat aktualizaci a distribuci filtrů/signatur automaticky, manuálně a podle časového harmonogramu	Ano	Ano

Trendy, historické přehledy a statistiky z pohledu aplikací, stanic, komunikace, bezpečnostních incidentů jsou graficky a tabulkově zobrazeny v GUI dohledové konzole	Ano	Ano
Přehledy a statistiky na dohledové konzoli lze efektivně filtrovat podle času, typů incidentů, aplikací, koncových stanic	Ano	Ano
Centrální dohledová konzole musí být schopna vytvářet reporty manuálně a podle časového harmonogramu	Ano	Ano
Pro reporty lze definovat template definující formát a obsah reportu	Ano	Ano
Pro template reportů lze definovat proměnné, které se promítnou v aktuálním reportu	Ano	Ano
V grafickém rozhraní dohledové konzole lze definovat uživatelské dashboardy typu top-N	Ano	Ano
Dashboardy použité v GUI dohledové konzole lze rovnou zahrnout i do reportů	Ano	Ano
Centrální dohledová konzole musí být schopna exportovat reporty do formátů, jako jsou PDF, HTML, CSV, apod.	Ano	Ano
Centrální dohledová konzole musí být schopna integrace s Microsoft AD pro vytváření bezpečnostních politik podle uživatele a skupiny uživatelů.	Ano	Ano
Podpora korelace událostí na centralizované dohledové konzoli s definicí odpovídajících akcí, např. zaslání korelované události na SIEM, generování mailu, lokální události, apod.	Ano	Ano
Podpora posílání událostí formou syslog, email, SNMP na externí platformy	Ano	Ano
Podpora Event Streamer API (eStreamer) pro sdílení informací se externími systémy. Minimálně pro tyto SIEM:	ArcSight BMC Remedy Trustwave NetForensics Novell Sentinel Hawk Network Defense Q1Labs-QRadar Log Rhythm SIEM 2.0 LogLogic Splunk	Ano
Pro zprávy odesílané emailem je podpora také autentizovaného SMTP pro komunikaci s mail relay	Ano	Ano
Podpora API pro přístup z externích systémů k databázím centralizovaného managementu	Ano	Ano
Podpora řízeného přístupu podle rolí administrátorů	Ano	Ano
Definice dostupných funkcí v GUI centralizované dohledové konzole podle role administrátora	Ano	Ano
Možnost založit pro daný incident „ticket“ přímo v prostředí GUI managementu	Ano	Ano
Workflow pro předávání „ticketů“ mezi administrátory	Ano	Ano
Konkrétní bezpečnostní incident až na úrovni paketu lze přiložit k danému „tiketu“ pro další analýzu	Ano	Ano



Možnost definice politik pro sledování odpovídajících parametrů „zdraví“ na senzorech a centralizované konzoli (zařízení CPU, obsazení paměti, komunikace s cloudovými službami, apod.)	Ano	Ano
Zákaznický definovatelné limity a akce spojené s jejich překročením při vyhodnocení sledovaných parametrů „zdraví“	Ano	Ano
Různé politiky pro sledování „zdraví“ lze aplikovat na různé senzory nebo centralizovanou konzoli	Ano	Ano
Musí splňovat možnost integrace se stávajícími systémy a Cisco Prime	Ano	Ano

#### Požadavky na kvalifikaci:

Dodavatel v nabídce předloží kopie platných odpovídajících certifikátů techniků pro danou specializaci zabezpečující kvalifikační předpoklady realizace této zakázky .

Dodavatel bude disponovat minimálně 3 pracovníky s platnou certifikací pro oblast síťových technologií, z nichž:

- minimálně jeden splňuje úroveň certifikace Network Professional
- minimálně jeden splňuje úroveň certifikace Design Professional
- minimálně jeden splňuje úroveň certifikace Security

Příloha č. 2 – cenová kalkulace

Jednotlivé položky	cena bez DPH v Kč	21 % DPH	cena s 21 % DPH v Kč
2 ks Cisco Firepower 2110 NGFW appliance, 1U	250 096,00	52 520,16	302 616,16
6 ks PSRT-8X5XNBD Cisco Firepower 2110 NGFW Appliance, 1U	75 000,00	15 750,00	90 750,00
25 ks Cisco AnyConnect Plus License, 3YR, 25-99 Users	3 900,00	819,00	4 719,00
Implementace	84 227,00	17 687,67	101 914,67
<b>Celková cena</b>	<b>413 223,00</b>	<b>86 776,83</b>	<b>499 999,83</b>

