

Smlouva o dodávce zařízení NGIPS

(dále jen „Smlouva“)

Č. smlouvy prodávajícího: 233/2019

uzavřená ve smyslu ustanovení § 2079 a následujících (kupní smlouva) zák. č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „občanský zákoník“), mezi

kupujícím:

Název / firma: **CESNET, zájmové sdružení právnických osob**
Zapsané ve: spolkovém rejstříku, vedeném Městským soudem v Praze, pod spisovou značkou L 58848
Sídlo: Zikova 1903/4, 160 00 Praha 6
IČO: 63839172
DIČ: CZ63839172
Bankovní spojení: Komerční banka, a. s., pobočka Praha 6
č. účtu: 19-8482200297/0100
Zastoupené: Ing. Janem Gruntorádem, CSc., ředitelem

a

prodávajícím:

Název / firma: **CompuNet s. r. o.**
Zapsané v: OR u Městského soudu v Praze, pod spisovou značkou C 118594
Sídlo: Zubatého 295/5, 150 00 Praha 5
IČO: 27608514
DIČ: CZ27608514
Bankovní spojení: Komerční banka a. s.
č. účtu: 51-1998450287/0100
Zastoupené: Ing. Pavlem Pikhartem, jednatelem

1. Úvodní ustanovení

- 1.1. Tato Smlouva stanoví obsah právního vztahu mezi výše uvedenými smluvními stranami. Ustanovení této Smlouvy je třeba v případě nejasností vykládat v souladu se zadávacími podmínkami stanovenými v zadávací dokumentaci včetně příloh na plnění veřejné zakázky s názvem „Dodávka zařízení NGIPS“, č. j. 1031/2019 (dále také jen „Veřejná zakázka“), která je zveřejněna na profilu kupujícího na adrese: <https://zakazky.cesnet.cz/vz00000245>, jakož i v souladu s nabídkou prodávajícího podanou na plnění této Veřejné zakázky, jejíž technická a cenová část tvoří jako nedílná součást této Smlouvy přílohu č. 1 této Smlouvy.
- 1.2. Plnění na základě této Smlouvy jsou kupujícím pořizovány za účelem nahrazení a upgrade stávajícího zařízení IPS, jehož doba životnosti uplynula. Toto zařízení musí jednak zajistit ochranu vybraných lokálních sítí zadavatele a jednak se stát součástí systému iABU (inteligentní analýza bezpečnostních událostí), do kterého bude dodávat data o bezpečnostních anomáliích v zabezpečených sítích. Zařízení musí s minimální latencí provádět inspekci komunikace až na úroveň aplikace a automaticky blokovat závadný síťový provoz v reálném čase. Nezávadný provoz bude zařízením procházet bez zjiitelného omezení či modifikace komunikace. Informace o provozu bude zařízení přehledným způsobem předávat bezpečnostním analytikům správy počítačové sítě zejména prostřednictvím Security Information and Event Management (SIEM) systému. Prodávající je povinen k tomuto účelu při dodávce a plnění vždy přihlížet.

2. Předmět plnění smlouvy

2.1. Předmětem plnění této Smlouvy je závazek prodávajícího dodat/poskytnout kupujícímu následující plnění:

2.1.1. Dodávky

Dodávka 1 ks zařízení Next-Generation Intrusion Prevention System (NGIPS) s minimální agregovanou inspekční kapacitou 10 000 Mbit/s při plném zatížení se všemi zapnutými filtry v reálném provozu se síťovými moduly, a to na základě specifikace a požadavků zadavatele uvedených v zadávací dokumentaci Veřejné zakázky, zejména v její části 3 – Předmět veřejné zakázky a na základě nabídky prodávajícího podané na plnění Veřejné zakázky.

Prodávající kupujícímu dodá hardware (dále jen „HW“) a případně i nezbytný software/ firmware (dále jen „SW“), uvedené v nabídce prodávajícího na plnění Veřejné zakázky, která tvoří přílohu č. 1 této Smlouvy.

Prodávající garantuje, že dodávané SW produkty získal v souladu s právními předpisy a že je oprávněn je dodávat.

2.1.2. Záruka a technická podpora

Součástí dodávky bude i poskytnutí záruky za jakost a řádnou funkčnost dodaných zařízení podle ustanovení § 2113 a násl. zákona č. 89/2012 Sb., občanského zákoníku (dále jen „občanský zákoník“), jejíž součástí bude i odborná technická podpora, na dobu 36 měsíců (dále jen „technická podpora“). Technická podpora mj. zahrnuje aktualizace softwarového a firmwarového vybavení dodaného zařízení a je poskytována v rozsahu 24*7*365 a dále dle specifikace uvedené v příloze č. 1.

2.2. Kupující se zavazuje za řádně poskytnuté plnění uhradit prodávajícímu níže stanovenou cenu.

3. Cena za předmět plnění

3.1. Celková cena za plnění této Smlouvy činí **2 993 122,- Kč bez DPH**.

3.2. Detailní specifikace ceny je uvedena v příloze č. 1 této smlouvy.

3.3. Cena za plnění této Smlouvy byla stanovena na základě nabídky prodávajícího předložené do zadávacího řízení na zadání Veřejné zakázky, jsou v ní započteny veškeré poplatky a veškeré další náklady související s plněním předmětu Smlouvy a je cenou nejvýše přípustnou. Cena zahrnuje i poskytnutí záruky a technické podpory.

3.4. DPH bude účtováno v zákonné výši podle platných a účinných právních předpisů.

4. Platební podmínky

4.1. Cena za plnění této Smlouvy bude kupujícím prodávajícímu uhrazena jednorázově na základě daňového dokladu - faktury (dále jen „faktura“) prodávajícího, kterou je prodávající povinen vystavit po řádně poskytnutém plnění (viz odst. 6.1. a 6.2.).

4.2. Přílohou faktury musí být příslušný akceptační protokol podepsaný oprávněnou osobou kupujícího, jinak nezakládá povinnost kupujícího platit.

4.3. Splatnost faktury je 30 dnů ode dne jejího doručení kupujícímu. Faktura musí obsahovat všechny náležitosti řádného účetního a daňového dokladu ve smyslu příslušných zákonných ustanovení. Faktura musí dále obsahovat odkaz na tuto smlouvu (č. 233/2019). V případě, že faktura nebude mít odpovídající náležitosti, je kupující oprávněn zaslat ji ve lhůtě splatnosti zpět prodávajícímu k doplnění či opravě, aniž se tak dostane do prodlení se splatností; lhůta splatnosti počíná běžet znovu od opětovného doručení náležitě doplněného či opraveného dokladu.

4.4. Cena za plnění této Smlouvy bude kupujícím prodávajícímu uhrazena bezhotovostním převodem na účet prodávajícího uvedený na titulní stránce této smlouvy, popřípadě na účet sdělený na faktuře.

4.5. Kupující neposkytuje zálohy.

4.6. V případě, že prodávající bude v okamžiku plnění předmětu této smlouvy uveden správcem daně jako „nespolehlivý plátc“ dle § 106a zákona 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“) nebo že účet prodávajícího, který prodávající uvedl

na jím vystaveném daňovém dokladu, nebude zveřejněn správcem daně podle § 98 písm. d) zákona o DPH, nebo že účet prodávajícího, který prodávající uvedl na jím vystaveném daňovém dokladu, bude účtem vedeným poskytovatelem platebních služeb mimo tuzemsko (ČR), bude plnění dle této smlouvy považováno za uhrazené i tak, že kupující uhradí prodávajícímu pouze cenu bez DPH a DPH uhradí přímo na účet příslušného finančního úřadu.

5. Doba a místo plnění

5.1. Doba plnění je stanovena následovně:

5.1.1. dodávku HW a SW podle odst. 2.1.1. provede prodávající nejpozději do 31. prosince 2019;

5.1.2. záruku a technickou podporu podle ustanovení odst. 2.1.2. bude prodávající poskytovat nejméně ve lhůtách a po dobu v tomto ustanovení uvedenou počínaje dnem podpisu akceptačního protokolu (viz odst. 6.1. a 6.2.).

5.2. Místem plnění je sídlo kupujícího. na adrese Zikova 1903/4, Praha 6.

6. Způsob předání a práva a povinnosti smluvních stran při plnění smlouvy

6.1. K předání plnění předmětu veřejné zakázky dojde na základě akceptační procedury – po ukončení zkušebního provozu, v jehož průběhu bude ověřováno splnění technických parametrů, které uchazeč uvede v nabídce, a řádná funkčnost a bezvadnost dodaných zařízení. Zkušební provoz bude zahájen ihned po dodávce zařízení a jeho délka bude maximálně 30 dnů od jeho zahájení. V případě prokazatelných nedostatků vzniklých v době zkušebního provozu je uchazeč povinen je neprodleně odstranit, a to nejpozději do 5 pracovních dní od okamžiku, kdy tyto nedostatky vyjdou najevo. V případě nedostatků, které budou prokazatelně v zásadním rozporu s požadavky objednatele uvedenými v zadávací dokumentaci, resp. s údaji uvedenými uchazečem v jeho nabídce, a které prokazatelně nemohou být v přiměřené době odstraněny, platí, že dodavatel uvedl mylné informace ve své nabídce a bude postupováno podle čl. 9 této Smlouvy. Zkušební provoz bude v případě úspěchu zakončen podpisem akceptačního protokolu oběma stranami, který bude podkladem pro fakturaci. Tento protokol podepsaný zadavatelem bude tvořit přílohu daňového dokladu – faktury. Řádně dodaným plněním se v případě dodávek rozumí řádně ukončená dodávka, provedení zkušebního provozu a uvedení do řádného provozu plnění v rozsahu a způsobem stanoveným v zadávací dokumentaci.

6.2. V případě záruky a technické podpory se řádně poskytnutým plněním rozumí řádné a včasné poskytnutí těchto plnění v souladu s podmínkami stanovenými v zadávací dokumentaci Veřejné zakázky, resp. v této Smlouvě.

6.3. Záruka a technická podpora počíná běžet dnem podpisu akceptačního protokolu (viz odst. 6.1.).

6.4. Poruchy / vady / nefunkčnost bude kupující v rámci záruky podpory oznamovat:

- na tel. čísle: 226 776 664
- na e-mail: help@compunet.cz
- v zákaznickém portále, ke kterému prodávající poskytne kupujícímu přístup nejpozději v den podpisu akceptačního protokolu

Prodávající se zavazuje nahlásit neprodleně kupujícímu případnou změnu kontaktních údajů pro ohlašování poruch, a to nejpozději 48 hodin před započatím užívání nových kontaktů.

6.5. Práva z vadného plnění se řídí ustanovením § 2099 a násl. občanského zákoníku, pokud v této smlouvě není stanoveno jinak.

6.6. Akceptační protokol podepsaný oběma stranami bude tvořit přílohu daňového dokladu – faktury.

6.7. Kupující se zavazuje poskytnout prodávajícímu řádnou součinnost při dodávce HW a SW. V případě neposkytnutí součinnosti kupujícím se prodlužují lhůty plnění o dobu, kdy prodávající nemohl v důsledku neposkytnutí součinnosti plnit své závazky.

6.8. Prodávající je povinen dodat pouze originální a nové HW a SW produkty, přičemž jejich původ je povinen na požádání kupujícího kdykoliv prokázat. Prodávající je dále povinen na výzvu kupujícího bezodkladně doložit příslušné certifikáty a osvědčení k dodávanému HW a SW, například (ale

nikoliv pouze), že dodávaný HW a SW splňuje příslušné technické normy a právní předpisy platné v ČR.

- 6.9. Kupující a prodávající budou při dodávkách zařízení postupovat v úzké součinnosti tak, aby bylo zajištěno, že plněním Veřejné zakázky nedojde k závažným zásahům do činnosti kupujícího či třetích stran.
- 6.10. Proávající se zavazuje poskytnout kupujícímu servisní služby i v případě, kdy poruchy (závady) komponent vzniknou nevhodným skladováním či umístěním, neodborným zásahem či manipulací, mechanickým poškozením ze strany kupujícího, resp. aplikací zařízení v rozporu s technickými podmínkami výrobce nebo v důsledku živelné pohromy; cena za servisní zásahy v uvedených případech není součástí ceny za plnění této smlouvy a bude dohodnuta smluvními stranami předem, pokud to situace dovolí.
- 6.11. Proávající se dále podpisem této smlouvy zavazuje:
 - 6.11.1. zachovat mlčenlivost o všech skutečnostech, které se dozví při plnění Veřejné zakázky nebo v souvislosti s ním;
 - 6.11.2. nepostoupit jeho práva či povinnosti jakékoliv třetí osobě bez písemného souhlasu kupujícího;
 - 6.11.3. nahradit kupujícímu škodu způsobenou případným subdodavatelem;
 - 6.11.4. zajistit maximální flexibilitu při plnění předmětu veřejné zakázky, zejména při řešení odůvodněných potřeb kupujícího, které vyplynou v průběhu plnění smlouvy;
 - 6.11.5. zajistit archivaci dokumentů o plnění Veřejné zakázky po dobu nejméně do konce roku 2028;
 - 6.11.6. zajistit ochranu osobních údajů v souladu s právními předpisy.

7. Vlastnické právo, nebezpečí škody na věci a úprava práv vyplývajících z duševního vlastnictví

- 7.1. Vlastnické právo přejde na kupujícího v okamžiku podpisu akceptačního protokolu.
- 7.2. Nebezpečí škody přechází na kupujícího v okamžiku, kdy na kupujícího přejde vlastnické právo.
- 7.3. Pokud plněním prodávajícího na základě této smlouvy bude poskytnutí jakéhokoliv SW třetích osob, je prodávající povinen zajistit, aby na kupujícího přešla veškerá nezbytná práva (licence) k užívání takového SW, aby mohl být naplněn účel této smlouvy, a to za následujících podmínek:
 - 7.3.1. kupující bude oprávněn k výkonu práva veškerý SW užít v rozsahu potřebném pro řádné užívání předmětu plnění;
 - 7.3.2. oprávnění (licence) musí být poskytnuto na dobu neurčitou (i po skončení účinnosti této smlouvy);
 - 7.3.3. cena licence je zahrnuta v celkové ceně plnění dle čl. 3 této Smlouvy.

8. Odpovědnost

- 8.1. Každá ze smluvních stran této smlouvy nese odpovědnost za prodlení, za vady a způsobenou škodu. Podmínky a následky odpovědnosti vyplývají z této smlouvy a z obecně závazných právních předpisů, zejména občanského zákoníku. Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení škodám a k minimalizaci vzniklých škod.
- 8.2. Žádná ze stran této smlouvy není odpovědná za škodu způsobenou v důsledku okolností vylučujících odpovědnost ve smyslu občanského zákoníku. Smluvní strany se zavazují upozornit druhou stranu bez zbytečného odkladu na vzniklé okolnosti vylučující odpovědnost bránící řádnému plnění smlouvy a zavazují se k maximálnímu úsilí k jejich odvrácení a překonání.
- 8.3. Proávající nese odpovědnost za to, že zboží dodané a předané podle této smlouvy bude ke dni dodání nepoužité (nové), plně funkční a bude splňovat požadavky, stanovené v zadávací dokumentaci veřejné zakázky.
- 8.4. Proávající odpovídá za to, že byl oprávněn poskytnout licenci k SW v požadovaném rozsahu podle odst. 7.3. této smlouvy.

9. Náhrada škody, smluvní sankce a odstoupení od smlouvy

- 9.1. Náhrada škody vzniklé jedné ze smluvních stran druhou smluvní stranou se řídí ustanoveními občanského zákoníku.
- 9.2. Kupující má právo na smluvní pokutu ve výši 0,1 % z celkové ceny plnění bez DPH za každý i jen započatý den prodlení s předáním v termínu plnění dle odst. 5.1.1, nejvýše však 10 % z celkové ceny plnění podle čl. 3 této Smlouvy, čímž není dotčeno právo na náhradu případné škody, která může spočívat mj. v tom, že kupující nebude oprávněn čerpat dotaci určenou na financování

Veřejné zakázky. Kupující bude oprávněn si případný nárok na smluvní pokutu podle tohoto odstavce započítat oproti ceně, kterou bude povinen zaplatit na základě této smlouvy. Kupující má právo odstoupit od této smlouvy či jí vypovědět s okamžitou účinností v případě prodlení prodávajícího s dodáním plnění po dobu delší 15 dnů.

- 9.3. V případě, že v průběhu realizace plnění vyjde najevo, že vlastnosti (zejm. technické vlastnosti) dodávek a/nebo služeb jsou prokazatelně v rozporu s informacemi, které prodávající uvedl v nabídce v rámci zadávacího řízení na zadání této Veřejné zakázky, bude mít kupující právo na smluvní pokutu ve výši 300.000,- Kč. Současně bude kupující mít právo odstoupit od této smlouvy; takové odstoupení od smlouvy však nebude mít vliv na právo kupujícího na zaplacení smluvní pokuty a nároku na náhradu škody.
- 9.4. V případě, že v průběhu realizace plnění vyjde najevo, že prodávající poskytl kupujícímu SW, jehož autorem či majitelem práv je třetí osoba, přičemž prodávající nebyl k takovému poskytnutí oprávněn, má kupující právo na smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení této povinnosti a nárok na náhradu škody. Kupující bude též v takovém případě oprávněn vyzvat prodávajícího k zajištění licence v potřebném rozsahu (bez dodatečných plateb ze strany kupujícího), přičemž pokud taková povinnost nebude ze strany prodávajícího splněna do 30 dnů ode dne obdržení výzvy, bude mít kupující právo odstoupit od smlouvy. Právo kupujícího na náhradu škody a smluvní pokutu uvedenou v tomto odstavci však zůstává nedotčeno.
- 9.5. Bude-li kupující v prodlení se zaplacením jakékoliv faktury řádně vystavené na základě této smlouvy prodávajícím k datu její splatnosti, má prodávající právo na úrok z prodlení ve výši 0,1 % z nezaplacené částky za každý započatý den prodlení platby. Prodávající je oprávněn odstoupit od této smlouvy, pokud bude kupující v prodlení se zaplacením kupní ceny (její částí) delším než 15 dní.
- 9.6. Obě smluvní strany mají právo odstoupit od této smlouvy v případě opakovaného prodlení druhé smluvní strany s plněním jakékoliv povinnosti podle této smlouvy. Nárok na náhradu škody a smluvní pokutu do dne odstoupení od smlouvy zůstane nedotčen (škoda může spočívat mimo jiné i v nákladech vynaložených kupujícím na realizaci nového výběrového/zadávacího řízení).
- 9.7. Výše náhrady škody v souladu s touto smlouvou v jakémkoliv směru a jakékoliv smluvní strany není omezena. Žádným ujednáním o smluvní pokutě, ani jejím skutečným zaplacením, nebude dotčen nárok smluvních stran na náhradu škody.
- 9.8. Jakákoliv ze smluvních stran této smlouvy může za podmínek v této smlouvě uvedených odstoupit pouze od části smlouvy, pokud to není vyloučeno povahou plnění.
- 9.9. Účinky odstoupení od smlouvy nastanou okamžikem doručení písemného projevu vůle vyjadřujícího odstoupení od smlouvy druhé smluvní straně.
- 9.10. Kupující má právo odstoupit od této smlouvy, pokud mu nebude poskytnuta dotace ze státního rozpočtu České republiky a nebude mít zajištěno financování z jiných zdrojů. Prodávající není v takovém případě oprávněn požadovat jakoukoliv náhradu škody či ušlého zisku.
- 9.11. S ohledem na podmínky financování plnění, které je předmětem této smlouvy, má kupující dále právo odstoupit od této smlouvy v případě, že výdaje, které mu na základě této smlouvy vzniknou, budou poskytovatelem dotace, případně jiným kontrolním subjektem, označeny za nezpůsobilé.

10. Závěrečná ustanovení

- 10.1. Smluvní strany budou vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které budou, jsou nebo mohou být důležité pro řádné plnění smlouvy.
- 10.2. Smluvní strany se budou navzájem informovat o každé organizační změně (např. změna tel. čísel, změna adresy, bankovního spojení atd.) bez zbytečného odkladu.
- 10.3. Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo ke zbytečnému prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.
- 10.4. Všechna oznámení mezi smluvními stranami, která se budou vztahovat ke smlouvě, nebo která mají být učiněna na základě smlouvy, musí být učiněna v písemné podobě a prokazatelně doručena druhé smluvní straně na adresu uvedenou ve smlouvě, nebude-li stanoveno nebo mezi smluvními stranami dohodnuto jinak.
- 10.5. Prodávající podpisem této smlouvy bere na vědomí a souhlasí s tím, že:

- 10.5.1. se stává v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě, v platném znění, osobou povinnou spolupůsobit při výkonu finanční kontroly; v rámci této kontroly je prodávající povinen umožnit kontrolu v souladu s podmínkami stanovenými uvedeným zákonem a je povinen umožnit oprávněným kontrolním orgánům přístup i k těm částem nabídky, smlouvy a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. jako obchodní tajemství, utajované skutečnosti) za předpokladu, že budou splněny požadavky kladené právními předpisy (např. zákonem č. 255/2012 Sb., o kontrole, v platném znění);
- 10.5.2. je povinen smluvně zajistit, aby zástupci poskytovatele dotace a případně další oprávněné osoby byli oprávněni obdobným způsobem kontrolovat i jeho případné subdodavatele;
- 10.5.3. se na zadávací řízení, na plnění zakázky a na následnou kontrolu vztahují mimo zákon č. 134/2016 Sb., o zadávání veřejných zakázek, i další právní předpisy (např. zák. č. 320/2001 Sb., o finanční kontrole ve veřejné správě a zák. č. 130/2002 Sb. o podpoře výzkumu, experimentálního vývoje a inovací z veřejných prostředků a o změně některých souvisejících zákonů).
- 10.6. Prodávající bere na vědomí, že podle ustanovení § 219 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, je kupující povinen zveřejnit tuto smlouvu na svém profilu zadavatele.
- 10.7. Závazkový vztah založený touto Smlouvou se řídí občanským zákoníkem.
- 10.8. Smlouva nabývá platnosti a účinnosti dnem podpisu poslední ze smluvních stran.
- 10.9. Tato smlouva byla sepsána ve 2 vyhotoveních s platností originálu, z nichž jedno obdrží kupující a jedno prodávající.
- 10.10. Smluvní strany prohlašují, že smlouva byla sepsána podle jejich skutečné a svobodné vůle, smlouvu si přečetly, s jejím obsahem souhlasí a na důkaz toho připojují podpisy svých odpovědných zástupců.

Za kupujícího:
V Praze dne 17.12.2019



Ing. Jan Gruntorád, C.Sc.
ředitel

cesnet
.....

CESNET z. s. p. o.
Žitkova 4
160 00 Praha 6
IČ: 63839172
DIČ: CZ63839172

Za prodávajícího: 18.12.2019
V Praze dne



Ing. Pavel Pikhart
jednatel

CompuNet s.r.o.
Zubatého 295/5
150 00 Praha 5
IČ: 27608514, DIČ: CZ27608514

Seznam příloh smlouvy:

Příloha č. 1: Specifikace dodávky zařízení - technická a cenová část nabídky prodávajícího

Příloha č. 1 smlouvy
Specifikace dodávky zařízení - Technická a cenová část nabídky prodávajícího

TECHNICKÉ A CENOVÉ ŘEŠENÍ

Navrhované zařízení Next-Generation Intrusion Prevention System (NGIPS) TippingPoint 8400TX, disponuje minimální agregovanou inspekční kapacitou 10 000 Mbit/s při plném zatížení se všemi zapnutými filtry v reálném provozu se síťovými moduly, součástí je i dohledová konzole a licence polížebné k jejímu provozu The TippingPoint Security Management System (SMS) pro správu a monitoring zařízení (HW či SW řešení včetně příslušných licencí, vše zahrnuto v ceně dodávky), dále síťovým modulem se dvěma segmenty 10GbE s SR/LR fiber bypass porty s ochranou proti přerušení síťové linky v případě výpadku napájení. K tomuto zařízení bude dodána záruka s odbornou technickou podporou 24 x 7 x 365 po dobu 36 měsíců, včetně dopravy, odborné montáže zařízení a školení v rozsahu minimálně osm hodin.

Na dodávané řešení poskytujeme odbornou technickou podporu po dobu tří let od dodání v režimu 24 x 7 x 365 v rozsahu dle přílohy č. 1 zadávací dokumentace veřejné zakázky: „Dodávka zařízení NGIPS“. Nahlášení problému je možné telefonicky +420 226 776 664 či e-mailem help@compunet.cz, přičemž je reakční doba výrobcem certifikovaného experta pro servis a konfiguraci 2 hodiny od nahlášení. V případě závady celého zařízení a nutnosti jeho nahrazení je možné zapůjčení náhradního, kompatibilního IPS se stejným, nebo vyšším síťovým i inspekčním výkonem včetně jeho instalace, bezúplatné odstranění HW a SW závad včetně výměny vadného dílu v místě plnění servisním technikem do druhého pracovního dne. Součástí jsou rovněž konzultační služby v případě konfiguračních a SW problémů, dále pak zprostředkování komunikace s výrobcem zařízení v případě chybné funkce zařízení, či požadavku na jeho funkční vylepšení, také s vývojovým týmem filtrů a pravidel výrobce, aktualizace a výměny HW. Disponujeme téměř výrobcem certifikovanými pracovníky pro odbornou a technickou podporu nabízeného systému.

Datasheet je uveden v samostatném dokumentu.

POPIS	PRODUKT. OZN.	POČET	CENA ZA KS	CELKEM
TippingPoint 8400TX HW + Support 3 roky				
TippingPoint 8400TX HW + Support 1Yr	TPNN0091	1	589 079 Kč	589 079 Kč
TippingPoint 8400TX HW Support Renewal 1Yr	TPRM0082	2	102 547 Kč	205 094 Kč
TippingPoint 10Gbps TPS Inspection License + Support + DV 1Yr	TPNN0277	1	1 236 763 Kč	1 236 763 Kč
TippingPoint 10Gbps TPS Inspection License Support DV 1Yr Renewal	TPRN0156	2	262 698 Kč	525 396 Kč
TippingPoint 10Gbps TPS ThreatDV Subscription Service 1Yr	TPNN0287	1	145 930 Kč	145 930 Kč
TippingPoint 10Gbps TPS ThreatDV Subscription Service 1Yr Renewal	TPRN0166	2	145 930 Kč	291 860 Kč
TrendMicro NX IPS 2-sgml 10G Fiber LR Bypass Module*	TPNN0074 (JC881A)	1	0 Kč	0 Kč
TIPPINGPOINT 8400TX HW + SUPPORT 3 ROKY – CELKOVÁ CENA POLOŽKU				2 993 122 Kč

*Zadavatel disponuje síťovým modulem, který je plně kompatibilní s nabídnutým zařízením a bude využit ve vlastnictví zadavatele. Cena tohoto modulu není součástí cenové nabídky.

	Cena v Kč bez DPH	Sazba DPH v %	Cena v Kč vč. DPH
Celková nabídková cena, plnění celého předmětu veřejné zakázky	2 993 122,-	21	3 621 678,-



Trend Micro™

TIPPINGPOINT™ THREAT PROTECTION SYSTEM FAMILY

Real-time detection, enforcement, and remediation without compromising security or performance

Organizations today are in the constant shadow of evolving and sophisticated cyber threats. In some cases, these threats are not only more complex than those of the past, but they are also targeted and rely on newly discovered vulnerabilities or exploits. In other cases, threats take advantage of older vulnerabilities that you thought were long forgotten. Safeguarding your network assets and data from such threats requires detailed visibility into all your network layers and resources. It requires comprehensive, up-to-date security intelligence, and a dynamic approach that uses awareness and automation to adapt to new threats, new vulnerabilities, and everyday network changes.

These vastly different threats require a multi-pronged approach to security. Organizations need robust security solutions at the edge of and inside their networks to prevent malicious attacks from getting to critical resources. They also need comprehensive threat intelligence to protect against known, unknown, and undisclosed vulnerabilities.

Trend Micro™ TippingPoint™ Threat Protection System (TPS) is a powerful network security platform that offers comprehensive threat protection against known and undisclosed vulnerabilities with high accuracy. TPS provides industry-leading coverage across different threat vectors from advanced threats, malware and phishing, etc. with extreme flexibility and high performance. The TPS uses a combination of technologies, including deep packet inspection, threat reputation, URL reputation and advanced malware analysis on a flow-by-flow basis—to detect and prevent attacks on the network. The TPS enables enterprises to take a proactive approach to security, providing comprehensive contextual awareness and deeper analysis of network traffic. This complete contextual awareness, combined with the threat intelligence from Trend Micro™ TippingPoint™ Digital Vaccine™ Labs (DVLabs) provides the visibility and agility necessary to keep pace with today's dynamic, evolving enterprise and data center networks.

"Trend Micro's Deep Discovery™ was a no brainer. It outperformed all competitors and was well-respected by Gartner". When Trend Micro purchased TippingPoint, we knew we had the best of both worlds."

Frank Bunton,
Vice President and CISO,
MedImpact



KEY FEATURES

TippingPoint Threat Protection Extended to the Cloud: Trend Micro® Cloud Network Protection, powered by Trend Micro® TippingPoint™, is a powerful inline security solution that allows enterprises to extend their existing TippingPoint network protection to their hybrid cloud environments. Offering comprehensive threat protection—including virtual patching, shielding against vulnerabilities, blocking exploits, and defending against known and zero-day attacks with high accuracy—it provides industry-leading coverages across multiple threat vectors. Apply your TippingPoint security controls and policies to your cloud environments via your existing Security Management System (SMS).

On-Box SSL Inspection: Sophisticated and targeted attacks are increasingly using encryption to evade detection. TPS reduces security blind spots created by encrypted traffic with on-box SSL inspection.

Performance Scalability: The increase in data center consolidation and proliferation of cloud environments requires security solutions that can scale as network demands increase. TPS delivers unprecedented security and performance for high-capacity networks with a scalable deployment model that includes the industry's first 40Gbps NGIPS in a 1U form factor with the ability to scale up to 120 Gbps aggregate in a 3U form factor.

Flexible Licensing Model: Easily scale performance and security requirements with pay-as-you-grow approach and flexible licenses that can be reassigned across TPS deployments without changing network infrastructure.

Real-Time Machine Learning: Many security threats are short-lived and constantly evolving, at times limiting the effectiveness of traditional signature and hash-based detection mechanisms. TPS uses statistical models developed with machine learning techniques deliver the ability to detect and mitigate threats in real time.

Enterprise Vulnerability Remediation (eVR): Quickly remediate vulnerabilities by integrating third-party vulnerability assessments with the TippingPoint product portfolio. Customers can pull in information from various vulnerability management and incident response vendors (Rapid7, Qualys, Tenable), map Common Vulnerabilities and Exposures (CVEs) to TippingPoint Digital Vaccine™ filters, and take action accordingly.

Advanced Threat Analysis: Extend protection from unknown threats through integration with Trend Micro® Deep Discovery™ Analyzer. TPS pre-filters known threats, forwards potential threats for automatic sandbox analysis, and remediates in real time upon confirmation of malicious content.

High Availability: Ideal for inline deployment, TPS has multiple fault-tolerant features including hot-swappable power supplies, watchdog timers to continuously monitor security and management engines, built-in inspection bypass, and zero power high availability (ZPHA). In addition, TPS can be provisioned using redundant links in a transparent active-active or active-passive high availability (HA) mode.

Integrated Advanced Threat Prevention: TPS integrates with Trend Micro® Deep Discovery™ advanced threat detection solutions, rated as the most effective and "Recommended" breach detection system by NSS Labs.

Asymmetric Traffic Inspection: Traffic asymmetry is widespread and pervasive throughout enterprise and data center networks. Enterprises must overcome challenges from both flow and routing asymmetry to be able to fully protect their networks. TPS by default inspects all types of traffic, including asymmetric traffic, and applies security policies to ensure comprehensive protection.

Agility and Flexibility: TPS embraces software-defined network protection by deploying IPS as a service. TPS also protects virtualized applications from within your virtualized infrastructure (VMware®, KVM).

Best-in-Class Threat Intelligence: Digital Vaccine Labs (DVLabs) provide cutting-edge threat analysis and security filters that cover an entire vulnerability to protect against all potential attack permutations, not just specific exploits. In addition to DVLabs, exclusive access to vulnerability information from the Zero Day Initiative (ZDI) protects customers from undisclosed and zero-day threats. ZDI is the largest vendor-agnostic bug bounty program, with 700 vulnerabilities published in 2016. In 2016, Trend Micro TippingPoint customers were protected an average of 57 days ahead of a vulnerability being patched by affected vendors.

Virtual Patching: Virtual patching provides a powerful and scalable frontline defense mechanism that protects networks from known threats and relies on vulnerability-based filters to provide an effective barrier from all attempts to exploit a particular vulnerability at the network level rather than the end-user level. This helps enterprises gain control of their patch management strategy with pre-emptive coverage between the discovery of a vulnerability and the availability of a patch, as well as added protection for legacy, out-of-support software.

Support for a Broad Set of Traffic Types: TPS platform supports a wide variety of traffic types and protocols. It provides uncompromising IPv6/v4 simultaneous payload inspection and support for related tunneling variants (4in6, 6in4, and 6in6). It also supports inspection of IPv6/v4 traffic with VLAN and MPLS tags, mobile IPv4 traffic, GRE and GTP (GPRS tunneling), and jumbo frames. This breadth of coverage gives IT and security administrators the flexibility to deploy its protection wherever it is needed.

Centralized Management: The TippingPoint Security Management System (SMS) delivers a unified policy and element management graphical user interface that provides a single mechanism for monitoring operational information, editing network security policies, configuring elements and deploying network security policy across the entire infrastructure whether its physical or virtual.

Key Benefits

Pre-emptive threat prevention

TPS deployed inline has the ability to inspect and block all directions of traffic (inbound, outbound, and lateral) in real time to protect against known, unknown and undisclosed vulnerabilities.

Threat insight and prioritization

Visibility and insight is crucial to making the best security policy decisions. TPS delivers complete visibility across your network and provides the insight and context needed to measure and drive threat prioritization.

Real-time enforcement and remediation

Defend the network from the edge, to the data center, and to the cloud with real-time, inline enforcement and automated remediation of vulnerable systems. TPS achieves a new level of inline, real-time protection, providing proactive network security for today's and tomorrow's real-world network traffic and data centers. The Threat Suppression Engine (TSE) architecture performs high-speed inline deep packet traffic inspection, and the purpose-built appliance's modular design enables the convergence of additional security services.

Operational simplicity

With flexible deployment options that are easy to set up and manage through a centralized management interface, TPS provides immediate and ongoing threat protection with out-of-the-box recommended settings.

TPS TECHNICAL SPECIFICATIONS



Features	440T (TPNN0291)	2200T (TPNN0292)	8200TX (TPNN0090)	8400TX (TPNN0091)
Supported IPS Inspection Throughput	250 Mbps/500 Mbps/1 Gbps	1 Gbps/2 Gbps	3/5/10/15/20/30/40 Gbps	3/5/10/15/20/30/40 Gbps
SSL Inspection	Not available	500 Mbps	2 Gbps (2K keys SHA256)	2 Gbps (2K keys SHA256)
Latency	<100 microseconds	<100 microseconds	<40 microseconds	<40 microseconds
Concurrent Sessions	1,000,000	10,000,000	120,000,000	120,000,000
New connections per second	70,000	115,000	650,000	650,000
MTBF (Mean Time Between Failures)	39,694 hours @ 25C ambient	34,837 hours @ 25C ambient	88,706 hours @ 25C ambient	88,706 hours @ 25C ambient
Form Factor	1U	2U	1U	2U
Weight	15.28 lb (6.93 Kg)	26.26 lb (11.91 Kg)	32 lb (max including IOMs) 29 lbs (w/ blank IOMs)	50 lb (max including IOMs) 41.5 lb (w/ blank IOMs)
Dimensions (W x D x H)	16.78 in.(W) x 17.3 in.(D) x 1.72 in.(H) 42.62 cm x 45.00 cm x 4.40cm	16.77 in (W) x 18.70 in (D) x 3.46 in (H) 42.60 cm x 47.50 cm x 8.80 cm	16.78 in (W) x 17.3 in (D) x 1.72 in (H) 42.62 cm x 45.00 cm x 4.40 cm	16.77 in (W) x 18.70 in (D) x 3.46 in (H) 42.60 cm x 47.50 cm x 8.80 cm
Management Ports	One out-of-band 10/100/1000 RJ-45 one RJ-45 serial manageable			
Management Interface	Security management system (SMS), local web console, command-line, SNMPv2c, SNMPv3 (TippingPoint MIB available)			
Network Connectivity	Eight 10/100/1000 RJ-45 ports and integrated bypass support one 10/100/1000 RJ-45 high availability ports	Eight 10/100/1000 RJ-45 ports with integrated bypass support 8 x 1 G SFP 4 x 10 G SFP+ one 10/100/1000 RJ-45 high availability ports support for external ZPHA for SFP/SFP+	2x IOM slots, mix/match: 6-segment 1 GE copper 6-segment 1 GE SFP 4-segment 10 GE SFP+ 1-segment 40 GE QSFP+ 4-segment 1 GE copper bypass 2-segment 1 GE SR/LR fiber bypass 2-segment 10 GE SR/LR fiber bypass	4x IOM slots, mix/match: 6-segment 1 GE copper IOM 6-segment 1 GE SFP IOM 4-segment 10 GE SFP+ 1-segment 40 GE QSFP+ 4-segment 1 GE copper bypass 2-segment 1 GE SR/LR fiber bypass 2-segment 10 GE SR/LR fiber bypass
On-Box Storage	8 GB hot-swappable CFast drive		32 GB hot-swappable 1.8" SSD module	
Voltage	100-240 VAC, 50-60 Hz		100 to 240 VAC/-40 to -60 VDC	
Current (Max. Fused Power)	4-2 A	12-6 A	12/6 Amps AC, 24/16 Amps DC	
Max Power Consumption	250 W (853 BTU/hour)	493 W (1,682 BTU/hour)	750 W (2,557 BTU/hour)	
Power Supply	Single fixed	Dual/redundant hot-swappable	Dual/redundant hot-swappable	
Operating Temperature	32°F to 104°F (0°C to 40°C)			
Operating Relative Humidity	5% to 95% non-condensing			
Non-Operating/Storage Temperature	-4°F to 158°F (-20°C to 70°C)			
Non-Operating/Storage Relative Humidity	5% to 95% non-condensing			
Altitude	Up to 10,000 feet (3,048 m)			
Safety	UL 60950-1, IEC 60950-1/EN 60950-1, CSA 22.2 60950-1/RoHS compliance			
EMC	Class A, FCC, VCCI, KC EN55022, CISPR 22, EN55024 CISPR 24, EN61000-3-2 EN61000-3-3, CE marking			

CLOUD NETWORK IPS TECHNICAL SPECIFICATIONS

Features	Cloud Network Protection
AWS Instance Type	C5.2xlarge
IPS Inspection Throughput*	Up to 3.5 Gbps
Latency	<100 microseconds
Concurrent Connections	7.5M
New Connections Per Second	75,000

*undergoing performance testing final numbers may vary

vTPS TECHNICAL SPECIFICATIONS

Features	vTPS Standard	
Supported IPS Inspection Throughput	250 Mbps/500 Mbps/ 1 Gbps/2 Gbps	250Mbps/500Mbps/ 1Gbps/2 Gbps
SSL Inspection	NA	Yes
Number of Logical Cores	2 or 3	4
Memory	8 GB	16 GB
Disk Space	16 GB	16 GB
IPS Concurrent Connections	1,000,000	
New Connections per Second	Up to 120 K VMware Up to 60 K KVM	
Virtual Platform Support	VMWare ESXi 5.5, 6.0, 6.5 (NSX is not required for transparent inspection and enforcement) & KVM - Redhat Enterprise Linux™ 6, 7	
Network Drivers	VMWare- VMNet3; KVM- virtIO	
Number of Network Segments	1	
Number of Virtual Segments	No limit	
Dedicated Management vNIC	Yes	



Securing Your Connected World

TIPPINGPOINT I/O MODULES

TippingPoint IO Module Description	Product SKU
TippingPoint IO Module: 6-segment Gig-T	TPNN0059
TippingPoint IO Module: 6-segment GbE SFP	TPNN0068
TippingPoint IO Module: 4-segment 10GbE SFP+	TPNN0060
TippingPoint IO Module: 1-segment 40GbE QSFP+	TPNN0069
TippingPoint IO Module: 4-segment Gig-T Bypass	TPNN0070
TippingPoint IO Module: 2-segment 1G Fiber SR Bypass	TPNN0071
TippingPoint IO Module: 2-segment 1G Fiber LR Bypass	TPNN0072
TippingPoint IO Module: 2-segment 10G Fiber SR Bypass	TPNN0073
TippingPoint IO Module: 2-segment 10G Fiber LR Bypass	TPNN0074

© 2019 Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro logo, and the white globe logo are trademarks and registered trademarks of Trend Micro Corporation. All other trademarks are the property of their respective owners. This document is for informational purposes only and does not constitute an offer of any product or service. Trend Micro and its affiliates assume no responsibility for the use of the information contained herein. For more information, please contact your local Trend Micro representative.

For details about what personal information we collect and why, please see our Privacy Notice on our website at <https://www.trendmicro.com/privacy>