Příloha B výzvy

OBCHODNÍ PODMÍNKY

veřejné zakázky malého rozsahu

Dodávka technologie FIREWALL

STAREZ – SPORT, a.s.

se sídlem Křídlovická 34, 603 00 Brno, IČO: 269 32 211

PŘEDLOHA KUPNÍ SMLOUVY

Veškeré technické, obchodní a jiné smluvní podmínky, které jsou zadavatelem zpracovány ve formě předlohy smlouvy, **musí být vybraným dodavatelem plně respektovány**.

Zadavatel **nevyžaduje, aby byl návrh smlouvy předložen** v nabídce.

KUPNÍ SMLOUVA

mezi těmito smluvními stranami

STAREZ – SPORT, a.s.

se sídlem:	Křídlovická 911/34, 603 00 Brno	
IČO:	26932211	
DIČ:	CZ26932211	
plátce DPH		
společnost zapsaná	v obchodním rejstříku vedeném Krajským soudem v Brně pod sp. zn. B 4174	
bankovní spojení:	Komerční banka a.s., číslo účtu: 35-1393300227/0100, ověřený bankovní účet	
společnost zastoupená:	Mgr. Martinem Mikšem, generálním ředitelem společnosti	
kontaktní osoba:	……., správce IT	
	telefon:	+420 …….
	e-mail:	.....@starezsport.cz

dále jen „***kupující***"

a

[Obchodní firma]

se sídlem:	……..	
IČO:	……..	
DIČ:	……..	
[ne/plátce] DPH		
společnost zapsaná	v obchodním rejstříku vedeném …….. soudem v …… pod sp. zn. ……..	
bankovní spojení:	……..	
zastoupená	……..	
kontaktní osoba:	……..	
	Telefon:	+420 ……..
	E-mail:	……..

dále jen „***prodávající***"

uzavírají tuto smlouvu:

I. Základní ustanovení a účel smlouvy, definice a výklad pojmů

1. Tato smlouva je uzavřena dle ust. §§ 2079 a násl. zákona č. 89/2012, občanský zákoník, ve znění pozdějších předpisů (dále jen „*občanský zákoník*") a podle zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „*autorský zákon*").
2. Prodávající prohlašuje, že bankovní účet uvedený v záhlaví této smlouvy je bankovním účtem zveřejněným ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „*zákon o DPH*"). V případě změny tohoto účtu je prodávající povinen doložit vlastnictví k novému účtu, a to kopií příslušné smlouvy nebo potvrzením peněžního ústavu; nový účet však musí být zveřejněným účtem ve smyslu předchozí věty.
3. Účelem této smlouvy je získat síťové bezpečnostní technologie s cílem vytvořit robustní a bezpečné prostředí pro zpracování a přenos dat s minimálním rizikem kybernetických hrozeb a zajištěním integrity a dostupnosti informačních systémů.

II. Předmět smlouvy

1. Předmětem smlouvy je dodávka síťových bezpečnostních technologií (Firewall), technologií pro logování bezpečnostních událostí, autentizaci uživatelů umožňující MFA (multi-factor authentication), správa a podpora v oblasti kybernetické bezpečnosti. Prodávající se touto smlouvou zavazuje na místo plnění dodat a kupujícímu odevzdat předmět smlouvy podle technických podmínek zadavatele a nabídky dodavatele podané do výběrového řízení Dodávka technologie FIREWALL, a to vše dle specifikace, která je přílohou č. 1 této smlouvy (dále též společně jen „*věc*" nebo „*zboží*"), včetně dokladů a písemností ke zboží se vztahující, zejména záruční list, návod k obsluze, prohlášení o shodě. Prodávající umožní nabýt kupujícímu ke zboží vlastnické právo.
2. Prodávající se zavazuje dodat zboží nové, dříve nepoužívané, které není zatíženo právy třetích osob.
3. Prodávající se zavazuje kupujícímu poskytnout veškeré potřebné licence, které jsou potřeba k řádnému užívání zboží (dále jen „*licence*"), a to jako nevýhradní, časově neomezené, s celosvětovou působností, přičemž kupující není povinen licenci / licence využít. Licence je součástí zboží.
4. Kupující se zavazuje zboží převzít a zaplatit prodávajícímu kupní cenu sjednanou v článku III. této smlouvy, a to za podmínek sjednaných touto smlouvou.
5. Prodávající se dále zavazuje provádět záruční opravy po dobu záruky sjednané v článku VI. této smlouvy a její příloze č. 1. Záruční opravy bude provádět k tomu řádně proškolená a oprávněná osoba.

III. Cena

1. Celková cena díla byla sjednána ve výši **..... Kč** bez DPH.
2. Ke sjednané ceně bude připočtena DPH podle účinných obecně závazných právních předpisů. V případě, že jedná o přenesenou daňovou povinnost dle § 92e zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, kód CZ-CPA kód 41-43, daň odvede objednatel.

3. Sjednaná cena zahrnuje též odměnu za poskytnutí licence dle čl. II. odst. 3., je-li taková licence potřebná k řádnému užívání zboží.
4. Sjednaná cena je cena nejvýše přípustná, přičemž obsahuje veškeré náklady prodávajícího na plnění dle této smlouvy, vč. nákladů na dopravu a dalších (např. náklady na přepravu, převod práv, pojištění, daně, cla, provádění předepsaných zkoušek, zabezpečení prohlášení o shodě a dále vedlejší náklady např. předpokládaná rizika spojená s obecným vývojem cen, inflací a kurzovými vlivy) a jakékoliv další výdaje spojené s realizací dodávky při zohlednění veškerých rizik a vlivů. Cena obsahuje i náklady na předepsané servisní kontroly a na záruční opravy sjednané v čl. VI. této smlouvy.

IV. Platební podmínky

1. Podkladem pro úhradu ceny bude faktura, která bude mít náležitosti daňového dokladu dle zákona o č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a náležitosti stanovené ust. § 435 občanského zákoníku (dále jen „*faktura*"). Přílohou faktury bude předávací protokol o převzetí zboží kupujícím.
2. Fakturu je prodávající povinen vystavit a doručit kupujícímu do 10 dní od řádného předání a převzetí zboží a poskytnutí licence. Veškeré cenové údaje budou uváděny v korunách českých.
3. Zálohy na platby nejsou sjednány.
4. Lhůta splatnosti faktury je s ohledem na povahu závazku dohodou stanovena na 21 kalendářních dnů ode dne jejich doručení kupujícímu. Daňový doklad – faktura bude doručena jedním z těchto způsobů:
   - osobně nebo poštou do sídla kupujícího nebo
   - elektronicky e-mailem na adresu e-podatelna@starezsport.cz
5. Kupující je oprávněn vadnou fakturu před uplynutím lhůty splatnosti vrátit druhé smluvní straně bez zaplacení k provedení opravy v těchto případech:
   a) nebude-li faktura obsahovat některou povinnou nebo dohodnutou náležitost nebo bude-li chybně vyúčtována cena,
   b) budou-li vyúčtovány práce, které nebyly provedeny či nebyly potvrzeny oprávněným zástupcem kupujícího.
6. Ve vrácené faktuře kupující vyznačí důvod vrácení. Prodávající provede opravu vystavením nové faktury. Vrátí-li kupující vadnou fakturu prodávajícímu, přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží opět ode dne doručení nově vyhotovené faktury kupujícímu. Prodávající je povinen doručit kupujícímu opravenou fakturu do 3 dnů po obdržení vrácené vadné faktury.

V. Místo a doba plnění. Doprava, umístění či montáž. Předání a převzetí zboží

1. **Místem plnění** je STAREZ – SPORT, a.s., Ponávka 808/3a, 602 00 Brno-město.
2. Prodávající se zavazuje dodat zboží v době **do jednoho měsíce od nabytí účinnosti této smlouvy.**
3. O předání a převzetí zboží bude sepsán předávací protokol, který podepíše prodávající i kupující. V případě, kdy kupující nepřevezme zboží předávané mu prodávajícím,

uvede tuto skutečnost do předávacího protokolu i s důvody, které ho k nepřevzetí zboží vedou.

4. Kupující nabude vlastnické právo ke zboží jeho převzetím. Licenci je kupující oprávněn využívat od nabytí vlastnického práva ke zboží.
5. Kupující se zavazuje umožnit prodávajícímu vstup na místo plnění tak, aby mohla být řádně provedena dodávka zboží. Taktéž se zavazuje umožnit prodávajícímu nebo osobám pověřeným prodávajícím k poskytování plnění dle této smlouvy vstup na místo plnění v případech záručních oprav zboží.
6. Prodávající se zavazuje dopravit věc na místo plnění, přičemž o konkrétním termínu dopravy věci prodávající informuje kupujícího alespoň 3 pracovní dny předem, nebude-li mezi kupujícím a prodávajícím dohodnuto jinak. Prodávající po dopravení věc rovněž vybalí a zkontroluje, je-li povinen provést umístění či montáž věci.
7. Prodávající se zavazuje obstarat a předat kupujícímu ke dni odevzdání věci veškeré atesty, certifikáty, prohlášení o vlastnostech či prohlášení o shodě věci s požadavky příslušných právních předpisů či technických norem.
8. Prodávající se zavazuje zpracovat či jinak obstarat písemné doklady a dokumenty, které jsou nutné k převzetí či užívání věci, zejména instrukce a návody k obsluze, provozu a údržbě věci, dokumentace skutečného stavu zapojení, jakož i ostatní dokumenty nezbytné pro provoz věci, a příp. další doklady a dokumenty, které se k věci jinak vztahují, a to v českém, příp. anglickém jazyce.
9. Převzetím věci přechází na kupujícího vlastnické právo k věci, jakož i nebezpečí škody na věci. Tím není omezena odpovědnost prodávajícího za škody, které vzniknou jeho zaviněním po převzetí věci kupujícím.

VI. Práva a povinnosti z vadného plnění, záruka za jakost, záruční servis

1. Prodávající garantuje kupujícímu, že zboží bude způsobilé ke smluvenému účelu užívání v souladu s předanými doklady a podmínkami této smlouvy.
2. Prodávající se zavazuje poskytnout plnou záruku na zboží po dobu minimálně 2 let ode dne jeho převzetí kupujícím, není-li stanovena doba delší.
3. Prodávající se zavazuje provést záruční opravy bezplatně.
4. Vady zboží, které se projeví v průběhu záruční doby, budou prodávajícím odstraněny bezplatně nebo prodávající poskytne kupujícímu náhradní zboží stejných nebo lepších parametrů.
5. Veškeré vady zboží je kupující povinen uplatnit u prodávajícího bez zbytečného odkladu poté, kdy vadu zjistil, a to formou písemného oznámení (za písemné oznámení se považuje i oznámení e-mailem), obsahujícího specifikaci zjištěné vady.
6. Prodávající započne s odstraněním vady bez zbytečného odkladu po doručení oznámení o vadě prodávajícímu, pokud se smluvní strany nedohodnou písemně jinak. Vada bude odstraněna nejpozději **do dvacátého pracovního dne** od okamžiku doručení oznámení o vadě, nedohodnou-li se strany písemně jinak.
7. Nezapočne-li prodávající s odstraněním vady ve stanovené lhůtě, nebo pokud prodávající vadu ve sjednané lhůtě neodstraní je kupující oprávněn zajistit odstranění vady na náklady prodávajícího u jiné odborné osoby.
8. Provedenou opravu vady prodávající předá kupujícímu písemným protokolem. Na provedenou opravu poskytne prodávající záruku za jakost v délce dle odst. 2.

9. Místem plnění opravárenských úkonů je místo plnění dle této smlouvy. Opravy vyžadující technické zázemí specializovaného pracoviště budou prováděny v autorizovaném servisu prodávajícího.

VII. Sankční ujednání, odstoupení od smlouvy

1. Pokud bude kupující v prodlení s úhradou sjednané ceny proti sjednané lhůtě, je povinen zaplatit prodávajícímu úrok z prodlení ve výši 0,1 % z dlužné částky za každý i započatý den prodlení.
2. Kupující je oprávněn po prodávajícím požadovat a prodávající je povinen zaplatit kupujícímu:
   a) smluvní pokutu ve výši 0,1 % z kupní ceny plnění bez DPH za každý i započatý den prodlení s předáním zboží a/nebo poskytnutí licence kupujícímu;
   b) v případě prodlení se zahájením servisního zásahu bude prodávajícímu účtována smluvní pokuta ve výši Kč 1 000,- Kč za každý den prodlení.
3. Zánik závazku pozdním splněním neznamená zánik nároku na smluvní pokutu za prodlení s plněním.
4. Sjednané smluvní pokuty zaplatí povinná strana nezávisle na zavinění a na tom, zda a v jaké výši vznikne druhé straně škoda.
5. Smluvní pokuty budou hrazeny na základě vystavených faktur se lhůtou splatnosti 14 kalendářních dnů ode dne jejich doručení.
6. Smluvní pokuty se nezapočítávají na náhradu případně vzniklé škody. Náhradu škody lze vymáhat samostatně vedle smluvní pokuty v plné výši.
7. Ustanovení v odst. 6 zavazuje smluvní strany i po odstoupení od smlouvy.
8. V případě podstatného porušení smlouvy může smluvní strana od smlouvy odstoupit. Smluvní strany kromě zákonem vymezeného podstatného porušení smlouvy pokládají za podstatné porušení smlouvy:
   a) na straně prodávajícího:
      - nedodání zboží ani **do jednoho měsíce** po uplynutí sjednané lhůty,
      - bylo-li příslušným soudem rozhodnuto o tom, že prodávající je v úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů (a to bez ohledu na právní moc tohoto rozhodnutí);
      - bylo-li zahájeno insolvenční řízení na základě dlužnického návrhu prodávajícího,
   b) na straně kupujícího:
      - kupující je v prodlení s úhradou daňového dokladu – faktury ve lhůtě delší než 30 kalendářních dnů po splatnosti.
9. Odstoupení od smlouvy musí být písemné, jinak je neplatné. Odstoupení je účinné ode dne, kdy bylo doručeno druhé smluvní straně. V pochybnostech se má za to, že odstoupení od smlouvy bylo doručeno třetím kalendářním dnem od jeho odeslání oprávněnou stranou poštovní zásilkou s dodejkou.

VIII. Ochrana osobních údajů

1. Smluvní strany tímto společně prohlašují, že jsou si vědomy vzájemných práv a povinností dle zákona č. 110/2019 Sb., o zpracování osobních údajů, ve znění pozdějších předpisů (dále také jen „ZZOÚ") a Nařízení Evropského parlamentu a Rady (EU) č. 2016/679, obecné nařízení o ochraně osobních údajů (dále také jen „GDPR"), zejména pak povinností stíhající jak správce osobních údajů, tak i zpracovatele osobních údajů, zejména povinnost zpracovávat osobní údaje korektně a zákonným a transparentním způsobem. Smluvní strany se zavazují osobní údaje zpracovávat takovým způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.
2. V případě, že jedna ze smluvních stran zjistí, že došlo či je důvodné podezření, že by mohlo dojít k porušení z povinnosti či povinností plynoucí z GDPR nebo ZZOÚ je tato strana bez zbytečného odkladu povinna vyrozumět o této skutečnosti druhou smluvní stranu.
3. Nad rámec povinností stanovených ZZOÚ a GDPR se smluvní strany navzájem zavazují postupovat při nakládání s osobními údaji ohleduplně a eticky tak, aby nevznikla ani jedné ze smluvních stran či třetí osobě v souvislosti se zpracováním osobních údajů újma.

IX. Ostatní ujednání

1. Kupující si vyhrazuje právo uplatnit institut zvláštního způsobu zajištění daně z přidané hodnoty ve smyslu § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění (dále jen „ZDPH"), pokud prodávající bude požadovat úhradu za zdanitelné plnění na bankovní účet, který nebude nejpozději ke dni splatnosti příslušné faktury zveřejněn správcem daně v příslušném registru plátců daně (tj. způsobem umožňujícím dálkový přístup). Obdobný postup je kupující oprávněn uplatnit i v případě, že v okamžiku uskutečnění zdanitelného plnění bude o prodávajícím zveřejněna v příslušném registru plátců daně skutečnost, že je nespolehlivým plátcem. V případě, že nastanou okolnosti umožňující kupujícímu uplatnit zvláštní způsob zajištění daně podle § 109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění, bude kupující o této skutečnosti prodávajícího informovat. Při použití zvláštního způsobu zajištění daně bude příslušná výše DPH zaplacena na účet prodávajícího vedený u jeho místně příslušného správce daně, a to v původním termínu splatnosti. V případě, že kupující institut zvláštního způsobu zajištění daně z přidané hodnoty ve shodě s tímto ujednáním uplatní, a zaplatí částku odpovídající výši daně z přidané hodnoty uvedené na daňovém dokladu vystaveném prodávajícím na účet prodávajícího vedený u jeho místně příslušného správce daně, bude tato úhrada považována za splnění části závazku kupujícího odpovídajícího příslušné výši DPH sjednané jako součást sjednané ceny za zdanitelné plnění.
2. Závazky stanovené k ochraně informací kupujícího nebo prodávajícího, které jsou předmětem obchodního tajemství či důvěrnými informacemi kupujícího, platí i po zániku ostatních závazků z této smlouvy.
3. Změnit nebo doplnit smlouvu mohou smluvní strany pouze formou písemných dodatků, které budou vzestupně číslovány, výslovně prohlášeny za dodatek této smlouvy a podepsány oprávněnými zástupci smluvních stran.
4. Není-li stanoveno ve smlouvě výslovně jinak, řídí se vzájemná práva a povinnosti smluvních stran ust. § 2079 a násl. občanského zákoníku a autorským zákonem.

5. Pokud se jakékoli ustanovení smlouvy stane neplatným či nevymahatelným, nebude to mít vliv na platnost a vymahatelnost ostatních ustanovení smlouvy. Smluvní strany se zavazují nahradit neplatné nebo nevymahatelné ustanovení novým ustanovením, jehož znění bude odpovídat úmyslu vyjádřenému původním ustanovením a smlouvou jako celkem.
6. Smlouva je vyhotovena ve dvou stejnopisech s platností originálu podepsaných oprávněnými zástupci smluvních stran, přičemž kupující i prodávající obdrží každý jedno z nich.
7. Prodávající není oprávněn bez souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.
8. Vzhledem k veřejnoprávnímu charakteru kupujícího se smluvní strany dohodly, že prodávající výslovně souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů. Prodávající prohlašuje, že umožní kontrolnímu orgánu v případě kontroly hospodaření s veřejnými prostředky u kupujícího prověřit své účetnictví a účetní doklady v rozsahu nezbytném ke splnění účelu kontroly.
9. Smluvní strany potvrzují, že si smlouvu před jejím podpisem přečetly a s jejím obsahem souhlasí. Na důkaz toho připojují své podpisy.
10. Smlouva nabude platnosti dnem jejího podpisu oběma smluvními stranami a účinností uveřejněním v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů. Prodávající s uveřejněním smlouvy v registru smluv podle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů, souhlasí.
11. Součástí smlouvy jsou tyto přílohy:

    Příloha č. 1: technická specifikace předmětu plnění

V Brně dne

V Brně dne

Za kupujícího:

Mgr. Martin Mikš, generální ředitel

STAREZ-SPORT, a.s.

Za prodávajícího:

……

……..

Příloha č. 1: technická specifikace předmětu plnění

a) **počet a obchodní název/typ nabízených HW zařízení** *Bude doplněno podle vítězné nabídky*

b) **typ a počet licencí** *Bude doplněno podle vítězné nabídky*

Základní technické požadavky požadovaného řešení

- Zadavatel požaduje platformu postavenou na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí (firewall, SSL dekrypce, porovnávání se signaturovou databází).
- Celá dodávka musí obsahovat všechny HW komponenty a licence na dobu alespoň **2 let**.
- Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.
- Zadavatel požaduje dodání zařízení ve formátu HW appliance o velikosti 1RU.
- Zadavatel požaduje veškeré příslušenství (montážní prvky) pro montáž do RACKu.
- Možnost rozšíření platformy o další prvek typu NGFW jehož cílem bude zajišťování sdílení telemetrických informací, vizualizace stavu sítě, zařízení a klientů, přičemž celé řešení musí být podporováno výrobcem.
- Možnost o rozšíření platformy pro sběr logů a grafického reportingu včetně oboustranné komunikace (tím se rozumí minimálně odeslání a zpětné načítání logů pro účel vizualizace), přičemž zde musí existovat garantovaná podpora funkcionality.
- Součástí nabídky musí být také řešení pro logování síťových a bezpečnostních událostí detekovaných firewally a řešení umožňující autentizaci doménových uživatelů rozšířenou o druhý faktor provozované odděleně formou fyzické nebo virtuální appliance v prostředí zákazníka.
- Řešení musí zahrnovat dodávku FW ve vysoké dostupnosti v režimu minimálně 1+1.
- Možnost přístupu na webový portál výrobce HW s možností zadávat servisní požadavky a stahovat aktualizace firmwaru a softwaru.

HW parametry

- Počet síťových rozhraní copper, RJ45 10/100/1000 - min 16x;
- Počet GE SFP – min 8x ;
- Počet 10 GE SFP – min 4x (včetně min. 2x SFP+ fiber transceiverů s dosahem min. 250m);
- Konzolový port pro management;
- Dedikovaný port RJ45 pro management;
- Dedikovaný port RJ45 pro HA konfiguraci;
- USB 3.0 port pro zálohu konfigurace, případně pro připojení USB 4G modemu;
- Redundantní napájecí zdroj.

Výkonnostní parametry

- Propustnost FW (stavové filtrování, UDP paket) paket o velikosti 1518 B, 512 B, 64 B- min 26000 Mbps, 26000 Mbps, 10000 Mbps;
- Latence firewallu (64 B UDP paket) - max 5 mikro sec;
- Počet naráz otevřených spojení – min 2,7 M;
- Počet nových spojení za sekundu - min. 260 000;
- Počet firewall pravidel až 10 000;
- Podpora virtualizace (min 10 virtuálních kontextů);
- Podpora funkce bezdrátový kontrolér - 128 AP;

- Podpora funkce integrovaný switch controller – podpora až 64 switchů.

Funkce

Síťování a vysoká dostupnost

- Podpora režimu vysoké dostupnosti, L2, Active Active, Active Passive, full mesh HA, VRRP, synchronizace stavové tabulky a IPsec SAs mezi nódy v clusteru;
- Režim fungování L2 – transparentní režim, L3 – NAT/Router;
- Podpora VLAN;
- Podopora multicast, vytváření politiky pro multicast routování;
- Podpora 802.3ad link aggregation;
- Funkce Load Balancing – možnost rozdělování zátěže směrující na virtuální IP na reálně servery, podpora health check funkcí, podpora SSL offloading;
- Podpora centrální NATovací tabulky, stavová inspekce SCTP komunikace;
- Podpora dynamických routovacích protokolů BGP, OSPF, ISIS, RIP;
- Policy-based routing;
- Funkce SD WAN – možnost rozkládání provozu mezi více linek na základě aplikačních signatur, IP adres a portů u známých aplikací, kvality linky včetně automatické detekce nefunkčnosti linky.

VPN

- **Funkce SSL VPN**
  - Podpora klientského i bezklientského (portálového) režimu;
  - Minimální počet současně navázaných SSL VPN tunelů: 450;
  - Minimální propustnost SSL VPN: 1900Mbps.
- **Funkce IPSEC VPN**
  - podpora site-to-site VPN;
  - podpora klientských VPN;
  - dostupnost VPN klienta pro koncové stanice (Windows, MacOS);
  - funkce klientských IPSec VPN nesmí být licencovaná na počet uživatel. V opačném případě Zadavatel požaduje dodání neomezené licence;
  - Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1900;
  - Minimální počet klientských IPSEC VPN tunelů: 15000;
  - propustnost IPSec VPN min. 12,5 Gbps (měřeno při AES256-SHA256);
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování;
  - podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování;
  - podpora funkce dynamického navazování IPsec tunelů dle potřeby komunikace;
- Podpora VXLAN;
- Podpora L2TP, PPTP, GRE;
- podpora dynamických routovacích protokolů OSPF, BGP ve VPN IPsec.

Bezpečnostní funkce

- **Funkce detekce aplikací na L7 (Application Control)**
  - Detekce známých aplikací na základě signatur;
  - Signaturové databáze automaticky aktualizované výrobcem;
  - Propustnost funkce Application Control (HTTP 64K) minimálně 12000 Mbps;
  - alespoň 4000 podporovaných aplikací pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) Zadavatel požaduje pokročilé akce typu

blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci);
  - možnost tvorby vlastních signatur;
  - detekované aplikace je možné: povolit, monitorovat, blokovat;
  - na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci;
  - funkce AppCtr se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně Zadavatel požaduje možnost využití v rámci tzv. NGFW pravidel popsaných výše.
- **Funkce detekce a potlačení narušení (IPS/IDS)**
  - signatury automaticky aktualizované výrobcem;
  - alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem;
  - možnost tvorby vlastních signatur;
  - funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům;
  - propustnost funkce IPS včetně logování min. 4800Mbps (měřeno na komunikaci typu mix aplikací).
- **Funkce antivirové kontroly**
  - Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem;
  - Signatury automaticky aktualizované výrobcem;
  - Zadavatel požaduje AV kontrolu rozšířenou o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky);
  - možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce;
  - deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2900 Mbps;
  - funkce AV kontroly se konfiguruje v rámci profilů, které jsou následně přiřazeny konkrétním FW pravidlům;
  - Podpora služby výrobce, která umožní detekovat malware, který byl objevený v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů;
  - Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu/bezpečnostní emailové bráně v reálném čase odstraní aktivní obsah z dokumentu, Dokument zůstává v původním formátu, jsou z něj odstraněny všechny aktivní prvky. Upravený dokument jde k původnímu příjemci, originální dokument se odešle do Sandboxu.
- **Funkce kategorizace webových stránek**
  - založená na centrálně spravované databázi výrobce;
  - minimálně 50 filtračních kategorií;
  - možnost definice vlastních kategorií;
  - možnost definice vlastních seznamů zakázaných URL;
  - kategorizace musí zahrnovat I české a slovenské internetové stránky.
- **Funkce DNS filtru**
  - Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u předchozího bodu);
  - Možnost definovat vlastní tzv. blacklist domén;
  - Možnost přesměrovat komunikace se zakázanými doménami na vlastní portal/URL;
  - Možnost importu seznamu blokovaných domén do DNS filtru;
  - Detekce a blokování komunikace do botnet sítí.
- **Funkce ochrany před únikem citlivých informací (DLP)**
  - možností analýzy běžných typů dokumentů a protokolů;

    - možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum;
- Email filter – jednoduchá antispamová a antivirová inspekce elektronické pošty;
- Podpora SSL dekrypce/SSL inspekce s minimální propustností 3900Mbps;
- DoS Policy prevence proti základním útokům typu DoS;
- Firewall musí být vybaven bezpečnostním modulem pro ukládání citlivých informací založeným na bázi HW (TPM).

Firewall

- Možnost nastavovat firewall politiku na základě geografických údajů;
- Aplikace firewall policy na známé internetové služby, kde databáze těchto služeb je pravidelně aktualizována výrobcem;
- Možnost snadné integrace cloudové služby. Minimálně na: MS Azure, Amazon Web Services, Google Cloud;
- Podpora Identity based policy – nastavení bezpečnosti uživateli na základě členství ve skupině na doménovém kontroléru;
- Viditelnost do provozu na aplikační úrovni;
- Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace (definované v rámci funkce application control, nikoliv pouhý TCP/UDP port) resp. kategorie URL filteringu (nikoliv jako AppCtrl resp URL filtering profil aplikovaný na dané pravidlo);
- Ověřování uživatelů LDAP, Active Directory, Single Sign On, Radius, TACACS+, Ověřování na základě certifikátu;
- Dynamické profily – možnost přiřadit konkrétní profil uživateli na základě jeho ověření;
- Traffic Shaping, QoS s podporou prioritizace provozu na základě DSCP markování a ToS, aplikace traffic shaping na konkrétní aplikaci nebo webovou kategorii;
- Podpora VoIP, SIP včetně zabezpečení, rate limitingu, analýzy protokolu
- Podpora funkce reverzní proxy;
- Podpora silné autentizace uživatelů – integrovaná podpora generátor jednorázových hesel (OTP) – pro dvoufaktorovou autentizaci, podpora certifikátů pro ověření uživatelů;
- **Explicit proxy**
    - podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP);
    - podpora transparentního ověřování uživatel proti MS AD protokolem Kerberos;
    - funkce transparentní proxy, kdy dochází k automatickému přesměrování provozu na proxy server bez nutnosti konfigurovat klienta;
    - Funkce transparentního ověřování uživatelů pomocí domény (MS Active Directory) včetně podpory autentizace uživatel na terminálovém serveru.

Integrovaný kontrolér bezdrátových (Wifi) sítí

- Wifi controller integrovaný do NGFW platformy;
- Každá bezdrátová síť (SSID) bude reprezentována virtuálním síťovým rozhraním;
- podpora bezpečnostních profilů (AV, AppControl, Webfilter, DLP) přímo na wifi controlleru;
- podpora SSL dekrypce uživatelského provozu přímo na wifi controlleru;
- Podpora wifi přístupových bodů stejného výrobce s výrobcem FW řešení;
- Možnost volby z různých modelů (např. 802.11abgn, 802.11ac, 802.11ac wave2, indoor, outdoor);

- On-wire rogue AP detekce a mitigace;
- Podpora fast-roamingu (802.11 k,v,r);
- podpora více PSK u jednoho SSID;
- podpora IPSEC tunelu pro šifrování data plane (uživatelských dat);
- podpora WPA3 šifrování;
- podpora WiFi 6 standardu;
- podpora BSS coloring (WiFi 6);
- podpora diagnostických WiFi nástrojů, například pro analýzu spektra.

Virtualiazce

- Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné řešení včetně odděleného GUI, management účtů, atp.;
- Součástí dodávky musí být licence na min. 10 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech);
- Každý virtuální kontext je zároveň samostatným wifi kontrolerem;
- Podporou izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů).

Management

- FW cluster musí být možné plnohodnotně spravovat pomocí lokálního GUI a CLI, provozovaného přímo na FW platformě bez nutnosti instalovat klienta na koncovou (management) stanici;
- Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě;
- Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury).

Logování

Systém musí být plně kompatibilní s dodávanými zařízeními, musí podporovat analýzu logů nad provozem. Dále musí být schopné poskytovat reporty nad logy a informovat správce systému o hrozbách, které byly v síti odhaleny.

Celá dodávka musí obsahovat všechny HW a SW komponenty a licence na dobu **2 let**. Žádné z nabízených řešení nesmí být v době podání nabídky v režimu end of sales/end of support. Všechny požadované funkce musí být v době podání nabídky součástí stabilní verze operačního systému/firmware, funkce zařazené na tzv. roadmapu nebudou akceptovány.

Hlavní požadavky:

- Musí se jednat o virtuální appliance s podporou minimálně VMware, KVM a Hyper-V stejného výrobce jako současného NGFW;
- Minimální limit pro množství přijatých logů za jeden den: 10GB;
- Možnost kontroly logů vůči databázi kompromitovaných zdrojů (IoC) minimálně pro stejné množství zdrojů jako je minimální limit;
- Podpora minimálně 4 virtuálních interface;
- Možnost škálovatelného navýšení kapacity úložiště na základě licence;
- Možnost provozovat appliance pouze jako dočasné úložiště logů z důvodu šetření datového pásma;
- Mít možnost specifikovat typ logů, které budou na hlavní analyzační nástroj odeslány okamžitě.

Multitenantnost

- Možnost rozdělení zařízení na oddělené administrativní sekce (každý virtuální kontext firewallu může být v jiném administrativním kontextu centrálního logovacího zařízení);
- Každý administrativní celek musí mít možnost mít vlastního administrátora, který nebude mít přístup do jiných administrativních celků.

Logovací funkce

- Musí se jedna o centrální logovací prvek pro všechny firewally;
- Musí umět ukládat jakkoliv Syslog zprávy;
- Funkce zpětné kontroly logů o přístupu na web (až 7 dní) z důvodu „zero-day" malicious websites;
- Vizualizace provozu nad všemi firewally;
- Možnost dostat se z vizuálního zobrazení proklikem na konkrétní logy;
- Realtime a historický náhled do logů;
- Korelace logů;
- Samostatná sekce týkající se hrozeb v síti;
- Podpora prohlížení statistických údajů nad logy;
- Funkce zpětné kontroly logů až 7 dnů zpět a zjištění, jestli systém nebyl napaden při přístupu na škodlivou webovou stránku. Logy jsou kontrolovány oproti pravidelně aktualizované databázi podezřelých IP adres, domén nebo webových URL adres.

Reporting

- Podpora reportů nad logy ve formátu HTML/CSV/XML/PDF;
- Generování reportů v pravidelných intervalech;
- Předefinované vzory pro reporty na nejčastější použití;
- Možnost vytváření vlastních reportů na základě konkrétních SELECT dotazů do databáze;
- Možnost úpravy reportů do vlastního designu – vlastní loga, texty, úprava hlavičky.

Další funkce

- Event Management – upozorňování na důležité informace z logů – emailem a snmp trapy, syslog zprávou;
- Předvytvořený dashboard pro využití dohledovým centrem;
- Možnost rozšíření o funkce SOC – parsování, analýza a korelace logů. Následná automatizovaná odpověď na incidenty za účelem blokace dané hrozby na NGFW stejného výrobce, případně karanténa klienta. Automatizované odpovědi mohou být definovány administrátorem, případně je možno využít vzorové scénáře.
    - Možnost customizace rozhraní pro NOC/SOC;
    - Incident Management – management incidentů vytvořených ze vzniklých eventů v SOC rozhraní;
    - PlayBook Automatizace – automatizované odpovědi na incidenty dle vzorových scénářů;
- Outbreak služba – v případě rychle šířící se kybernetické hrozby vyhodnocené výrobcem systému může administrátor tohoto systému zobrazit varování a k tomu odpovídající event handlery a předdefinované reporty. Administrátor následně může prohledat pomocí daných reportů stávající logy na zařízení za účelem identifikace daného malwaru.

Možnosti správy a komunikace

- Podpora SNMPv2, SNMPv3;
- Podpora REST API;

- Správa přes webové rozhraní HTTPS;
- Administrátorské účty musí být možné konfigurovat lokálně nebo na vzdáleném serveru (LDAP, RADIUS, Tacacs+);
- Podpora statického routování;
- Možnost zašifrování spojení mezi zařízením, které odesílá logy a analyzačním nástrojem, který je předmětem této zadávací dokumentace.

Autentizace

Systém musí být kompatibilní s dodanými technologiemi a podporovat několik druhů autentizace uživatelů popsaných níže. Zároveň musí umožňovat zavedení second faktor authentication (2FA) a vše s podporou výrobce alespoň 2 roky.

Hlavní požadavky

- Autentizaci min. pro **100 uživatelů**;
- Podpora alespoň. 200 mobilních tokenů;
- Podpora virtualizace, pakliže se jedná o virtuální appliance min.: VMware ESXi/ ESX 6/ 7/ 8, Microsoft Hyper-V Server 2010, 2012 R2, and 2016, Microsoft Azure, AWS;
- Podpora vysoké dostupnosti v režimu: Active-Passive;
- Podpora Single Sign-On;
- Secure Multifactor/OTP autentizace;
- Podpora Radius, LDAP, AD, SAML SP/IdP, FIDO 2;

Požadavky na mobilní token

- Minimálně pro **10 uživatelů**;
- Mobilního klíč ve formě aplikace na mobilní telefon s podporou platforem: iOS, Android, Windows;
- OTP splňující alespoň normy: RFC 6238, RFC 4226;
- Podpora PUSH notifikací s podporou zobrazení přihlašovacích informací;
- Ochrana aplikace pomoci PIN, Fingerprint a Facial recognition;
- Ochrana proti brute-force útoku.