Kupní smlouva č. CTU/2018_032

uzavřená ve smyslu ustanovení § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „občanský zákoník“)

I. Smluvní strany

Kupující:	**Česká republika – Český telekomunikační úřad**
Se sídlem:	Sokolovská 58/219, Praha 9 - Vysočany
Doručovací adresa:	poštovní přihrádka 02, 225 02 Praha 025
IČO:	701 06 975
DIČ:	CZ70106975 (osoba identifikovaná k dani)
Bankovní spojení	ČNB – pobočka Praha
Číslo účtu:	xxxxxx/xxxx

Jejímž jménem jedná: Ing. Mgr. Jaromír Novák, předseda Rady ČTÚ

(dále jen **„kupující“**)

a

Prodávající:	**IXPERTA s.r.o.**
Se sídlem:	Lihovarská 1060/12, 190 00 Praha 9
IČO:	275 99 523
DIČ:	CZ27599523
Zastoupena:	Pavlem Šiprem, jednatelem společnosti
Bankovní spojení:	UniCredit Bank Czech Republic and Slovakia, a.s., Želetavská 1525/1, 140 92 Praha 4 - Michle
Číslo účtu:	xxxxxxxx/xxxx

Zapsaná v obchodním rejstříku C117991 vedená u Městského soudu v Praze

(dále jen **„prodávající“**)

II. Úvodní ustanovení

Smluvní strany uzavírají tuto kupní smlouvu (dále jen „smlouva“) na základě výsledků zadávacího řízení v rámci veřejné zakázky na dodávky s názvem „NG Firewall“.

III. Účel a předmět smlouvy, závazky smluvních stran

1. Účelem této smlouvy je stanovení obsahových požadavků, postupů, obchodních podmínek a dalších smluvních ujednání, na jejichž základě dojde k realizaci dodávky NG Firewallu (dále jen „firewall) se servisními službami včetně garance dostupnosti náhradních dílů po dobu účinnosti této smlouvy.
2. Předmětem této smlouvy je závazek prodávajícího dodat kupujícímu do místa plnění podle čl. V odst. 1 této smlouvy nový (tj. nepoužitý, nepoškozený, nerepasovaný a zkompletovaný) firewall s přesnou technickou specifikací uvedenou v příloze č. 1 této smlouvy, poskytnout související plnění podle této smlouvy a převést na kupujícího vlastnické právo k firewallu a na druhé straně závazek kupujícího za řádně a včas dodaný firewall a poskytnuté související plnění zaplatit prodávajícímu sjednanou kupní cenu.

IV. Cena a platební podmínky

1. Prodávající se zavazuje poskytnout kupujícímu plnění podle této smlouvy za kupní cenu ve výši 1 046 040 Kč bez DPH, z toho DPH ve výši 21 % činí 219 668 Kč, tj. 1 265 709 Kč včetně DPH.
2. Ke kupní ceně bude připočtena DPH ve výši platné ke dni uskutečnění zdanitelného plnění. Celková kupní cena uvedená v této smlouvě je sjednána dohodou smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a je stanovena jako konečná, pevná a nepřekročitelná. Kupní cena může být změněna pouze v případě změn sazby daně z přidané hodnoty nebo využití opčního práva kupujícího.
3. Kupní cena zahrnuje veškeré náklady související s plněním této smlouvy.
4. Kupní cena bude uhrazena bezhotovostním převodem na bankovní účet prodávajícího uvedený v záhlaví této smlouvy, a to na základě daňového dokladu – faktury (dále jen „faktura“) vystaveným prodávajícím po převzetí plnění (dodání a implementace firewallu) kupujícím.
5. Prodávající vystaví fakturu ke dni uskutečnění zdanitelného plnění, který je dnem protokolárního předání a převzetí plnění podle čl. VI odst. 5 této smlouvy. Splatnost faktury je 21 dnů ode dne jejího doručení kupujícímu. Faktura musí být doložena dodacím listem o dodání firewallu podle čl. VI odst. 2 této smlouvy, akceptačním protokolem podle čl. VI odst. 5 této smlouvy a dokladu o provedení odborného školení a předání implementační dokumentace podle čl. VI odst. 6 této smlouvy.
6. Faktura musí obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, § 435 občanského zákoníku a současně číslo této smlouvy, včetně uvedení označení „MSEK“.
7. V případě, že faktura nebude obsahovat náležitosti podle platných právních předpisů, popř. bude obsahovat jiné chyby či nedostatky, je kupující oprávněn fakturu vrátit, přičemž nová lhůta splatnosti počíná běžet dnem doručení opravené faktury kupujícímu.

V. Místo a čas plnění, způsob plnění, kontaktní osoby

1. Místem plnění je pracoviště kupujícího – oddělení kontroly datových služeb, Tuřanka 1519/115a, 627 00 Brno.
2. Kontaktní osobou pro převzetí firewallu na straně kupujícího v místě plnění, resp. akceptaci provedené implementace firewallu v určeném datovém centru, provedení odborného školení a předání implementační dokumentace je Ing. xxxxx xxxxxx, tel.: xxx xxx xxx, e-mail: xxxxxxx@ctu.cz.
3. Prodávající se zavazuje, že dodá firewall kupujícímu do místa plnění nejpozději do 30 dnů ode dne účinnosti této smlouvy.
4. Dále se prodávající zavazuje, že provede implementaci firewallu podle části A bod 6 přílohy č. 1 této smlouvy v místě určeném podle odstavce 5 tohoto článku smlouvy, a to nejpozději do 14 dnů ode dne požadovaného termínu zahájení instalace firewallu, který bude uveden v písemné výzvě kupujícího k poskytnutí tohoto plnění podle odstavce 6 tohoto článku smlouvy.
5. Firewall bude prodávajícím instalován na území hlavního města Prahy v prostorech datového centra, určeného a zajištěného kupujícím. Doprava dodaného firewallu do místa implementace v určeném datovém centru bude zajištěna kupujícím. Místo instalace pak bude místem plnění ve vztahu ke sjednané záruce (odstraňování vad firewallu).
6. Dále se prodávající zavazuje, že nejpozději do 14 dnů ode dne potvrzení akceptace implementace firewallu podle čl. VI odst. 5 této smlouvy provede odborné školení pověřených pracovníků kupujícího a předá implementační dokumentaci podle části A bod 6.4 přílohy č. 1 této smlouvy. Školení bude provedeno na náklady prodávajícího v místě

a čase určeném prodávajícím s tím, že přesný čas a místo oznámí prodávající kontaktní osobě kupujícího uvedené v odstavci 2 tohoto článku smlouvy písemně (e-mailem) nejméně 5 pracovních dnů předem. Implementační dokumentace bude předána kontaktní osobě kupujícího v rámci odborného školení.

Písemnou výzvu k poskytnutí plnění podle odstavce 4 tohoto článku smlouvy zašle kupující zástupci prodávajícího (xxxxx xxxxxx, tel.: xxxxxxxxxxxx e-mail: xxxxx.xxxxx@ixperta.com) nejméně 7 dnů před požadovaným termínem zahájení instalace firewallu v určeném datovém centru.

VI. Dodací podmínky

1. Prodávající se zavazuje nejméně tři pracovní dny předem písemně uvědomit kontaktní osobu kupujícího o předpokládaném termínu dodání firewallu podle čl. V odst. 3 této smlouvy.
2. Řádné dodání firewallu podle čl. V odst. 3 této smlouvy potvrdí kupující prodávajícímu formou podpisu dodacího listu kontaktní osobou.
3. Kupující není povinen převzít firewall zejména v případech, kdy firewall, případně jeho obal, vykazuje známky poškození, resp. firewall vykazuje vady, které brání jeho řádnému užívání.
4. Prodávající je povinen společně s firewallem předat kupujícímu doklady, jež jsou nutné k převzetí a užívání firewallu podle občanského zákoníku a předpisů souvisejících, v českém jazyce. Současně je prodávající povinen předat kupujícímu i podrobný původní uživatelský manuál v anglickém jazyce.
5. Řádné poskytnutí plnění v podobě implementace firewallu podle části A bod 6 přílohy č. 1 této smlouvy potvrdí kupující prodávajícímu formou podpisu akceptačního protokolu kontaktní osobou kupujícího.
6. Řádné provedení odborného školení a předání implementační dokumentace podle části A bod 6.4 přílohy č. 1 této smlouvy potvrdí kupující prodávajícímu formou podpisu dokladu o provedení odborného školení kontaktní osobou kupujícího.
7. Kupující je povinen převzít plnění, které je poskytnuto řádně, tj. firewall zejména vykazuje všechny vlastnosti a vyhovuje všem podmínkám uvedeným v této smlouvě či stanoveným kupujícím nebo právními předpisy a technickými normami, a včas.

VII. Zajištění závazků

1. Pro případ prodlení kupujícího s uhrazením kupní ceny ve smyslu čl. IV odst. 5 této smlouvy má prodávající právo požadovat úrok z prodlení v zákonné výši z dlužné částky za každý i započatý den prodlení.
2. V případě prodlení prodávajícího s řádným dodáním firewallu je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,1 % z kupní ceny včetně DPH za každý i započatý den prodlení.
3. V případě prodlení prodávajícího s odstraněním ohlášené vady firewallu v termínu podle čl. IX odst. 4 této smlouvy je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 0,1 % z kupní ceny včetně DPH za každý i započatý den prodlení.
4. V případě porušení jiné povinnosti prodávajícího zakotvené touto smlouvou je prodávající povinen zaplatit kupujícímu smluvní pokutu ve výši 500 Kč za každý i započatý den prodlení.
5. Smluvní pokuta je splatná ve lhůtě 5 dnů ode dne doručení písemné výzvy k její úhradě.
6. Zaplacením smluvní pokuty podle této smlouvy není dotčen nárok smluvní strany na náhradu skutečné škody v celém rozsahu způsobené škody. Žádná ze smluvních stran

neodpovídá za škodu vzniklou jako následek vyšší moci. Uplatněním nároku na smluvní pokutu ani jejím skutečným uhrazením nezaniká povinnost zavázané strany splnit povinnost, jejíž plnění bylo zajištěno smluvní pokutou.

VIII. Nebezpečí škody a nabytí vlastnického práva

Nebezpečí škody a vlastnické právo k firewallu přechází z prodávajícího na kupujícího okamžikem, kdy kupující převezme firewall a potvrdí převzetí firewallu způsobem uvedeným v čl. VI odst. 5 této smlouvy.

IX. Záruka a odpovědnost za vady

1. Na dodaný firewall poskytuje prodávající kupujícímu záruku za jakost v délce 36 měsíců. Záruční doba počíná běžet dnem převzetí firewallu kupujícím. Záruční doba se prodlouží o dobu, po kterou nebude moci kupující užívat firewall z důvodu vad, za něž odpovídá prodávající, a to ode dne oznámení kupujícího o vadě prodávajícímu do dne ukončení servisního zásahu podle odstavce 4 tohoto článku smlouvy.
2. Poskytnutou zárukou se prodávající zavazuje, že po dobu záruční lhůty bude firewall použitelný k dohodnutému nebo obvyklému účelu. Záruka se nevztahuje na opotřebení v rozsahu odpovídajícímu obvyklému způsobu užívání.
3. Zjistí-li kupující vadu v době trvání záruční doby stanovené touto smlouvou, oznámí prokazatelně tuto skutečnost neprodleně prodávajícímu.
4. Prodávající poskytuje kupujícímu záruční servis s garancí ukončení servisního zásahu nejpozději následující pracovní den po nahlášení vady v místě instalace (NBD).
5. Oprávnění k bezplatné záruční opravě firewallu zanikne v případě, kdy k vadě dojde prokazatelným mechanickým poškozením firewallu nebo prokazatelným provozováním firewallu v nevhodném prostředí. Ze záruky jsou vyjmuty též vady způsobené živelnou pohromou a neodbornou manipulací s technikou způsobem nerespektujícím návod k použití firewallu nadměrným opotřebením, neexistencí údržby nebo nedostatečnou či špatnou údržbou.

X. Ukončení smlouvy

1. Tato smlouva může být ukončena splněním, písemnou dohodou obou smluvních stran nebo odstoupením od smlouvy.
2. Kterákoliv ze smluvních stran může odstoupit od smlouvy v případě, že druhá smluvní strana poruší podstatným způsobem své povinnosti vyplývající z této smlouvy.
3. Za podstatné porušení smluvních povinností kupujícím se bude podle této smlouvy považovat prodlení kupujícího s uhrazením kupní ceny o více než 30 dnů.
4. Za podstatné porušení smlouvy prodávajícím se považuje:
   a) nedodržení stanoveného termínu dodání,
   b) neodstranění vady ve sjednané lhůtě,
   c) existence vady bránící naplnění účelu smlouvy a neposkytnutí součinnosti,
   d) uvedení nepravdivých údajů v nabídce ze strany prodávajícího.
5. Stanoví-li oprávněná smluvní strana druhé smluvní straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá smluvní strana v průběhu této lhůty prohlásí, že svůj závazek nesplní.

6. Odstoupení od smlouvy musí být provedeno písemně a doručeno druhé smluvní straně. Právní účinky nastávají dnem doručení odstoupení od smlouvy druhé smluvní straně.
7. V případě, že tato smlouva zanikne odstoupením z viny prodávajícího podle odstavce 2 tohoto článku smlouvy, nemá prodávající nárok na náhradu vynaložených nákladů.

XI. Salvatorské ustanovení

Obě smluvní strany prohlašují, že pokud se kterékoliv ustanovení této smlouvy nebo s ní související ujednání ukáže být neplatným nebo se neplatným stane, že tato skutečnost neovlivní platnost smlouvy jako celku. V takovém případě se obě smluvní strany zavazují nahradit neprodleně neplatné ustanovení ustanovením platným; obdobně se zavazují postupovat v případě ostatních nedostatků smlouvy či souvisejících ujednání.

XII. Závěrečná ustanovení

1. Smluvní strany jsou vázány obsahem této smlouvy.
2. Veškeré změny či doplňky této smlouvy mohou být provedeny pouze písemně, a to formou písemných, vzestupně číslovaných dodatků k této smlouvě potvrzenými oběma smluvními stranami, a to osobami oprávněnými jednat za smluvní strany ve věcech smluvních.
3. Tato smlouva a práva a povinnosti z ní vyplývající se řídí českým právem. Práva a povinnosti smluvních stran, pokud nejsou upraveny touto smlouvou, se řídí občanským zákoníkem a předpisy souvisejícími.
4. Smluvní strany bezvýhradně souhlasí s uveřejněním této smlouvy, případných dodatků uzavřených k této smlouvě, jakož i se zveřejněním dalších aspektů tohoto smluvního vztahu v souladu se zákonem 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. Uveřejnění zajistí kupující.
5. Smluvní strany prohlašují, že smlouvu před jejím podepsáním přečetly, jejímu obsahu rozumí a s jejím obsahem souhlasí. Na důkaz svého souhlasu připojují obě smluvní strany své podpisy.
6. Smlouva byla sepsána ve třech stejnopisech, z nichž prodávající obdrží jeden a kupující dva stejnopisy. Nedílnou součást této smlouvy tvoří příloha č. 1 – Technická specifikace.
7. Tato smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění smlouvy podle zákona o registru smluv.

V Praze dne 13. 7. 2018

za kupujícího:

……
Ing. Mgr. Jaromír Novák
předseda Rady
Českého telekomunikačního úřadu

V Praze dne 20.6.2018

za prodávajícího:

…….
Pavel Šipr
jednatel společnosti

Příloha č. 1 smlouvy

Technická specifikace

Technická specifikace je dělena na 2 části, povinné parametry a volitelné parametry.

Povinné parametry (část A) jsou minimální požadavky na technické vybavení zařízení, které kupující vyžaduje.

Volitelné parametry (B) jsou takové požadavky na technické vybavení zařízení, které svým charakterem zlepšují technické vybavení a zajišťují jeho přidanou hodnotu, přičemž tyto jsou součástí plnění na základě nabídky prodávajícího v rámci zadávacího řízení na příslušnou veřejnou zakázku.

(Poznámka: Dodavatel ve své nabídce v návrhu smlouvy uvede jen ty volitelné parametry, které nabízí v rámci své nabídkové ceny s tím, že ostatní volitelné parametry z návrhu smlouvy vypustí!!!)

Použité zkratky:

3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization and Accounting protocol
AES	Advanced Encryption Standard
AVX	Advanced Vector Extensions
CAS	Column Access Strobe
CPM	Control Processing Module
CPU	Central Processing Unit
CSV	Comma Separated Value
DDoS	Distributed Denial of Service
DDR	Double Data Rate
DLP	Data Lost Prevention
DNS	Domain Name Service
ECC	Error Correction Code
EPS	Event Per Second
FD mód	Full-Duplex Mód
FTP	File Transfer Protocol
HTML	Hyper Text Markup Language
HDD	Hard Disk Drive
HLD	High Level Design
http	Hypertext Transfer Protocol
IF-MAP	Interface for Metadata Access Points
IKE	Internet Key Exchange
IOPS	Input/Output operations Per Second
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
KVM	Kernel Virtual Machine
L2TP	Layer 2 Tuneling Protocol
LDAP	Lightweight Directory Access Protocol
LFF	Large Form Factor (3,5”)
LLD	Low Level Design
MDA	Media Dependent Adapter
MPU	Main Processing Unit
MS AD	Microsoft Active Directory
NGFW	Next Generation Firewall
NIC	Network Interface Card
PDF	Portable Document Format
PIC	Physical Interface Cards
PXE	Pre-boot eXecution Environment
PSU	Power Supply Unit
QoS	Quality of Service
RA	Remote Access
RAM	Random Access Memory
RU	Rack Unit
S2S	Site to Site
SAS	Serial Attached SCSI
SATA	Serial ATA
SFF	Small Form Factor (2,5“)
SLA	Service Level Agreement
SNMP	Simple Network Management Protocol
SPI	State full Packet Inspection
SR-IOV	Single Root I/O Virtualization
SSD	Solid State Drive
SSE	Streaming SIMD Extensions
SSL	Secure Socket Layer
TDP	Thermal Design Power
URL	Uniform Resource Locator
VPN	Virtual Private Network

Parametry NG Firewallu

A. Povinné parametry

1. Hardware NG Firewallu

1.1 Fyzická specifikace

1.1.1	Svislý rozměr	maximálně 2 U
1.1.2	Provedení	umístitelný do racku 19" (RACK MOUNT)
1.1.3	Hmotnost	maximálně 25 kg (plná obsazenost slotů)
1.1.4	Počet slotů pro CPU	minimálně 2
1.1.5	Počet slotů pro PSU	2
1.1.6	Provedení slotů pro PSU	1 + 1 redundance
1.1.7	Počet PCIe slotů	minimálně 3

1.2 Napájecí zdroj (PSU)

1.2.1	Vstupní napětí	2 x AC 230 V (50/60 Hz)

1.3 Chlazení

1.3.1 Vyměnitelné ventilátory (hot-plug)

1.4 Porty/rozhraní pro správu

1.4.1 Lokální konfigurační sériové RS-232 nebo Ethernet RJ-45 rozhraní pro zajištění správy

1.5 Porty/rozhraní pro síťové zapojení NG Firewallu

1.5.1	1 Gbps Ethernet (SFP)	minimálně 4 (včetně možnosti odděleného vzdáleného přístupu pro správu NG Firewallu)
1.5.2	10 Gbps Ethernet (SFP+)	minimálně 4 (postaveno na dvou nezávislých chipsetech s podporou SR-IOV, PXE, IEEE 1588, automatickou negociací 1/10 Gbps a hardwarově akcelerovaný provoz IP: TCP, UDP, IEEE 802

1.6 Výkonnostní parametry

1.6.1	CPU	1 × 8 jádrový procesor s výkonem minimálně 18000 bodů v benchmarkovém testu Passmark) s platností od 13.04.2018 do současnosti (splněno, pokud NG Firewall aktivně využívá všechny instalovaná jádra pro funkce popsané v bodu 2 část A)
1.6.2	RAM	minimálně 48 GB DDR4-2666 CAS-19-19-19 složené minimálně z šesti modulů ECC registered (veškerá RAM dodaná jako součást musí být certifikována výrobcem serveru pro použití v dodaném typu hardware)
1.6.3	Integrovaný diskový řadič	minimální velikost cache 2 GB DDR4, osm 12G SAS kanálů s možností připojení 6G SATA disků, který nebude ubírat PCIe sloty na základní desce a bude zálohovaný pomocí baterie

1.7 Ostatní parametry

1.7.1 SSD disky — 2 × každý s minimální kapacitou 400 GB připojených pomocí 12G SAS rozhraní v Raid 1 s minimálním výkonem 120 000 IOPS při čtení a 80 000 IOPS při zápisu (4k)

1.7.2 PSU — 2 × každý s minimálním výkonem 800 W

1.7.3 Minimální záruka garantovaná výrobcem hardware v režimu 8 x 5 NBD na 3 roky

1.7.4 Systém pro vzdálenou správu mimo přímý komunikační kanál (out of band). Tento systém musí mít vlastní procesor nezávislý na stavu CPU. Musí minimálně nabídnout vzdálenou konzoli na server, schopnost vzdáleně připojit média a provést hromadnou akci na více platformách (například upgrade firmware)

2. Výkonnostní parametry NG Firewallu (všechny parametry musí být splněny současně)

2.1 Minimální prostupnost firewallu (SPI): 20 Gbps

2.2 Minimální prostupnost firewallu + IPS + antivirus + aplikační kontroly + antibot + NAT + QoS + VPN: 3,5 Gbps (každá funkce musí provádět úplnou kontrolu provozu, tzn. každý packet/rámec)

2.3 Minimální celkový počet spojení: 30 miliónů

2.4 Minimální počet nových spojení za vteřinu: 500 tisíc

2.5 Maximální latence http inspektovaného provozu: 2 ms (při 1,7 až 44 KB http response)

V případě nejasností budou hodnoty ověřeny pomocí penetračního testu plně nakonfigurované platformy. Splnění kritérií je nutnou podmínkou akceptace řešení dle bodu 6.3 část A

3. Software NG Firewallu

3.1 Řešení musí být vyhodnoceno v testu NSS Labs Security Value Map pro NGFW 2017 alespoň 85 %

3.2 Základní množina funkcí je:

3.2.1 Firewall (SPI)

3.2.1.1 Obsahuje granulární inspekci, analýzu komunikace a kontroluje síťové toky

3.2.1.2 Řešení musí obsahovat alespoň 150 předdefinovaných služeb a protokolů

3.2.1.3 Každé pravidlo musí nabízet statistiku počtu užití (hit count)

3.2.1.4 Komunikace mezi management platformou a firewallem musí být autentizována a zašifrována

3.2.1.5 Řešení musí podporovat lokální autentizaci či připojení pomocí protokolů Radius

3.2.1.6 Zadavatel požaduje funkci proxy na protokolech http a HTTPS a DHCP server.

3.2.1.7 Základní režimy funkce jsou transparentní L2 a L3

3.2.1.8 Řešení musí podporovat nejméně dvě nezávislé internetové linky a nejméně cluster dvou GW

3.2.1.9 Všechny bezpečnostní funkce kapitoly 3 zejména pak SPI, Antivirus, IPS, apod. musí být organizovatelné do bezpečnostních politik. Tak aby byla administrace co nejjednodušší. Řešení pomocí produktů více výrobců musí také splňovat tuto podmínku

3.2.1.10 Platforma musí být schopna pomocí interní heuristické a signaturní logiky identifikovat útok typu DDoS. Pro útoky hrubou silou musí existovat možnost vytvořit generické politiky, které budou soužit jako

efektivní protiopatření. Nejedná se o požadavek na scrubingové centrum, ale o požadavek na funkci NGF

3.2.1.11 Platforma NGFW musí být schopna poskytnout základní síťové služby:

- 3.2.1.11.1 RFC 1042 VLAN
- 3.2.1.11.2 RFC 4271 Border Gateway Protocol
- 3.2.1.11.3 RFC 2328 Open Shortest Path First
- 3.2.1.11.4 RFC 1035 Domain Name System implementation
- 3.2.1.11.5 RFC 2132 Dynamic Host Configuration Protocol (pro RA VPN uživatele)
- 3.2.1.11.6 Statické směrování provozu
- 3.2.1.11.7 RFC 791 Internet Protocol

3.2.2 Podpora IPv6

- 3.2.2.1 RFC 1981 Path Maximum Transmission Unit Discovery pro IPv6
- 3.2.2.2 RFC 2460 IPv6
- 3.2.2.3 RFC 2464 Transmission of IPv6 Packets over Ethernet Networks
- 3.2.2.4 RFC 3596 DNS Extensions to support IPv6
- 3.2.2.5 RFC 4007 IPv6 Scoped Address Architecture
- 3.2.2.6 RFC 4193 Unique Local IPv6 Unicast Addresses
- 3.2.2.7 RFC 4213 Basic Transition Mechanisms for IPv6 Hosts and Routers
- 3.2.2.8 RFC 4291 IPv6 Addressing Architecture
- 3.2.2.9 RFC 4443 ICMPv6
- 3.2.2.10 RFC 4861 Neighbor Discovery
- 3.2.2.11 RFC 4862 IPv6 Stateless Address Auto-configuration

3.2.3 IPS

- 3.2.3.1 Musí fungovat na principech detekce alespoň: identifikace signatur exploitů, sledování anomálií protokolů, sledování anomálií aplikací a uživatelského chování
- 3.2.3.2 Plná integrace s modulem firewallu
- 3.2.3.3 Musí umožňovat možnost vytvářet politiky pro klientskou, serverovou nebo obě strany současně
- 3.2.3.4 Musí podporovat debug mód s omezením pouze na detekci
- 3.2.3.5 Musí mít centralizovanou funkci pro vytváření událostí
- 3.2.3.6 Konzole pro správu musí administrátorovi umožnit automaticky aktivovat nové politiky na základě konfigurovatelných parametrů. Zejména pak dopadu na výkon, míry rizika, či pravidel pro ochranu klientů nebo serverů
- 3.2.3.7 IPS musí síť chránit proti alespoň zneužití protokolů, komunikaci malware, pokusům o tunelování a generickým typům útoku bez použití předdefinovaných signatur
- 3.2.3.8 IPS musí chránit tzn. detekovat a být schopna blokovat alespoň následující protokoly: DNS, FTP, služby Microsoft Windows, SNMP a peer 2 peer sítě
- 3.2.3.9 IPS musí chránit proti DNS cache poisoning útokům a bránit uživatelům k přístupu k blokovaným doménovým a DNS adresám
- 3.2.3.10 IPS musí být schopna importovat signatury vytvořené pomocí SNORTu
- 3.2.3.11 IPS musí umožnit uživateli blokovat komunikaci podle země původu

3.2.4 Antivirus a antibot

- 3.2.4.1 Musí být schopen blokovat a bránit podezřelou síťovou komunikaci na základě detekce anomálií a na základě aktivního vyhledávání akcí botů
- 3.2.4.2 Řešení musí detekovat systémy typu ransomware pomocí statické či dynamické analýzy (například Cryptolocker, Cryptowall apod.)

3.2.4.3 Řešení musí být schopno se bránit proti pishingovým útokům, vyhledávat command and controll komunikaci, a to včetně komunikace maskované za DNS, IRC, SHH apod.

3.2.4.4 Řešení musí být schopno chránit proti command and controll vzorovým typům komunikace, nikoliv jen reputačním IP/DNS adresám. Zejména metodou detekce domain name generation algoritmů a pomocí integrovaných honeypot pastí pro identifikaci interních hostů

3.2.4.5 Řešení musí být plně integrováno s ostatními moduly firewallu. Tzn. lze vytvořit politiku takovou, která bude obsahovat všechny výše popsané funkce softwarových modulů a společně vyhodnocovat jejich výsledky

3.2.5 Identifikace a kontrola aplikačního provozu

3.2.5.1 Řešení musí být integrovatelné s alespoň těmito zdroji identit: Microsoft Active Directory (bez agenta instalovaného na doménovém kontroléru), na Linuxu postavené LDAP, IF-MAP a Radius

3.2.5.2 Každá bezpečnostní událost musí být logována s ohledem na doménového uživatele, který se komunikace účastní. Identifikace autorizovaných uživatelů musí probíhat na úrovni doménového účtu, nikoliv pouze L2/L3 informací

3.2.5.3 Uživatelé, jejichž identita nebude známa a nebude možné provést autorizaci, musí mít možnost přistoupit k webovému portálu a provést ruční ověření

3.2.5.4 Metoda sběru identity nesmí výrazně ovlivnit výkonnostní parametry systému. Maximální možná zátěž je 5 % výkonu CPU na doménových kontrolérech

3.2.5.5 NG Firewall musí podporovat transparentní autentizaci pomocí Kerberos ticketů

3.2.5.6 NG Firewall musí být schopen identifikovat alespoň 5000 aplikací dle signatury síťového provozu, alespoň 250000 Web 2.0 aplikací

3.2.6 VPN

3.2.6.1 NGFW musí podporovat ověření pomocí vnitřní autority a autority třetí strany (MS AD, LDAP).

3.2.6.2 Řešení musí podporovat alespoň 3DES a AES-256 pro první IKE fázi. Dále pak Diffie-Hellman skipiny: Group 1 (768 bit), Group 2 (1024 bit), Group 5 (1536 bit), Group 14 (2048 bit), Group 19 and Group 20

3.2.6.3 Topologie pro S2S VPN tunely musí být podporována alespoň v režimech full mesh, hvězda a spoke-hub

3.2.6.4 Řešení musí podporovat protokol IPSec, L2TP a bez klientský přístup pro SSL

3.2.6.5 S2S VPN musí podporovat kompresi přenášených dat

3.2.6.6 S2S VPN tunely musí být možné sestavit, když jedna strana nemá veřejnou IP adresu

4. Management NG Firewallu

4.1 Správa

4.1.1 Dedikovaný management má hlavní úkol v poskytnutí jednotné konzole pro správu NGFW, která fyzicky nebude umístěna na stejném hardware. Management musí podporovat běh v prostředí VMware a KVM

4.1.2 Management musí podporovat šifrovanou komunikaci mezi ním samým a NG Firewallem

4.1.3 Všechny akce v management platformě ať už prováděné formou CLI, WebGUI či management aplikace dedikované pro správu na administrátorské stanici musí podléhat principu AAA

4.1.4 Management musí být schopen spravovat všechny popsané funkce v kapitole 3 z jednoho místa
4.1.5 Management musí v případě selhání NGFW podporovat rychlou obnovu na novou instalaci NGFW z interního repositáře
4.1.6 Kromě bezpečnostních logů musí být management schopen zobrazovat také systémové stavy firewallů, a to nejméně stav: CPU, RAM, diskové kapacity a síťových rozhraní

4.2 Sběr logů a jejich korelace

4.2.1 Systém musí být schopen sbírat logy z platformy firewallu, a to alespoň rychlostí 20 000 logů/událostí za vteřinu.
4.2.2 Korelace musí probíhat bud na platformě managementu anebo pomocí dedikovaného SIEM nástroje. Minimální podporovaná kapacita analýzy logů/událostí je 5000 EPS
4.2.3 Úložiště událostí musí být indexováno a na backendu realizováno databází (bez omezení typu). Flat file úložiště událostí není dovoleno z důvodu výkonu. Systém musí být optimalizován pro provoz na SSD discích s tím, že systém (vnitřní organizace dat) musí být schopna využít výkonu SSD disků
4.2.4 Logy musí pocházet z alespoň těchto interní funkcí IPS, Application Control, Anti-Virus, Anti-Bot, Anti-Spam, Uživatelská identita, VPN
4.2.5 Řešení musí být schopno automaticky zachytávat komunikační pakety na základě IPS událostí
4.2.6 Systém musí rozlišovat mezi logy generovanými uživatelskou komunikací a logy generovanými systémovými stavy
4.2.7 Pro každou událost musí existovat možnost automaticky provést následující akce: notifikace, zaslání SNMP trapu nebo spuštění uživatelského skriptu
4.2.8 Veškerá komunikace mezi zdrojem logů (NGFW), management platformou a administrátorskou konzolí musí být zašifrována
4.2.9 Logy musí být z platformy exportovatelné v databázovém formátu
4.2.10 Správa logů a jejich korelace (vyhodnocování) musí být integrována v jedné platformě. V případě použití produktu typu SIEM se nemusí jednat o platformu, která je integrována s managementem. V žádném případě však nemůže běžet management, logy a na platformě firewallu
4.2.11 Korelace logů musí mít grafickou reprezentaci, tj. dash board, ze kterého se administrátor dozví o kritických událostech a je schopen se dostat k detailu události
4.2.12 Korelované události musí být možno exportovat v reportu, a to nejméně ve formátech HTML, PDF či CSV
4.2.13 Reporty musí obsahovat alespoň tyto části:

4.2.13.1 Seznam spojení, která byla blokována pomocí pravidla
4.2.13.2 Nejčastější zdroje komunikace, které byly blokovány pomocí pravidla
4.2.13.3 Pravidla seřazené dle hit count spojení
4.2.13.4 Nejčastější bezpečnostní události podle zdroje a cíle
4.2.13.5 Nejčastější sítové služby dle aplikace nebo protokolu
4.2.13.6 Aktivita uživatelů dle navštívených webových stránek a jejich identit (MS AD nebo LDAP uživatel)
4.2.13.7 Seznam VPN spojení a objem komunikace v návaznosti na typ spojení: pro RA VPN dle uživatelského účtu, pro S2S VPN dle zdrojové a cílové adresy

5. Servisní služby včetně garance dostupnosti náhradních dílů

5.1 Na produkt (hardware a software) musí být garantovaná záruka na 3 roky v režimu 8 x 5 NBD, která bude zahrnovat alespoň tyto služby:

5.1.1 Výměna hardware v přídě selhání do následujícího dne

5.1.2 Garance nových verzí software podobu tří let výrobcem
5.1.3 Technická podpora výrobce po dobu tří let

5.2 Pro bezpečnostní funkce musí být zajištěna aktualizace signatur a všech softwarových funkcí na 3 roky, a to nejméně v tomto rozsahu:

5.2.1 Firewall
5.2.2 IPS
5.2.3 Antivirus a antibot
5.2.4 Identifikace a kontrola aplikačního provozu

5.3 Help desk dodavatele dostupný v režimu non stop 24 x 7 hovořící v českém jazyce, který je možné kontaktovat pomocí webového formuláře, e-mailem či telefonicky

5.4 Bezpečnostní kontaktní osoba dodavatele, která je schopna komunikovat ve smyslu nařízení Regulation (EU) 2016/679 nebo pověřenec ochrany osobních údajů

6. Implementace

6.1 Instalace NG Firewallu. Migrace a konfigurace bezpečnostních politik v předpokládaném rozsahu nejméně 5 člověkodnů na určeném místě

6.2 Instalace managementu platformy, nastavení korelace a reportingu v předpokládaném rozsahu nejméně 5 člověkodnů

6.3 Akceptační testy v předpokládaném rozsahu nejméně 2 člověkodny

6.4 Odborné školení pověřených pracovníků kupujícího v počtu do 5 pracovníků v rozsahu nejméně 3 člověkodny provedené certifikovaným personálem prodávajícího včetně předání implementační dokumentace LLD/HLD NG Firewallu zástupcům kupujícího

6.5 Implementace bude realizována v místě a termínu určeném podle čl. V odst. 4 této smlouvy. Odborné školení pracovníků kupujícího se uskuteční v místě a termínu určeném podle čl. V odst. 6 této smlouvy

B. Volitelné parametry

1. Technické a provozní parametry

1.1. Výkonnostní parametry a možnosti rozšíření

1.1.1 Možnost rozšíření CPU o alespoň 8 jader bez nutnosti provést kompletní výměnu hardware pouze doplněním CPU a případně chladiče
1.1.2 Možnost rozšíření RAM alespoň na 256 GB bez nutnosti provést kompletní výměnu hardware pouze doplněním RAM modulů
1.1.3 Možnost rozšíření NIC na alespoň 8 x 10 Gbps Ethernet (SFP+)
1.1.4 V případě potřeby výměny hardware z pohledu výkonu je žádoucí, aby takový náklad byl co nejnižší. Tento bod je splněn, pokud cena hardware nepřekročí 20 % z celkové ceny zakázky. Uchazeč musí jasně vyjádřit jaká je cena hardware z celkové ceny zakázky
1.1.5 NG Firewall ani management NG Firewallu nejsou licenčně omezeny na počet připojených uživatelů ani množství ukládaných či zpracovávaných logů

1.2 Bezpečnostní parametry a možnosti rozšíření

1.2.1 NG Firewall je licencován na osm aktivních jader a lze jej rozšířit lineárně o další jádra bez nutnosti kupovat větší balíčky licencí
1.2.2 Licence na jádra lze libovolně přidávat či v budoucnu ubírat na roční bázi dle požadavků zadavatele
1.2.3 NG Firewall má možnost rozšíření o emulaci a extrakci síťových hrozeb prováděnou na dedikovaném hardware mimo NG Firewall anebo formou

cloudové služby

1.2.4 NG Firewall je možné rozšířit o řešení DLP a ochranu koncových operačních systémů, která bude integrována do stejného management rozhraní a stejné korelační logiky pro tvorbu bezpečnostních událostí