# Kupní smlouva č. 11/2019/VZFAF

uzavřená dle ust. § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „***OZ***")

## I.
## Smluvní strany

**Univerzita Karlova, Farmaceutická fakulta v Hradci Králové**
se sídlem: Akademika Heyrovského 1203/8, 500 05 Hradec Králové
zastoupena: prof. PharmDr. Tomášem Šimůnkem, Ph.D., děkanem
IČO: 00216208
DIČ: CZ00216208
Bankovní spojení: ČSOB, a.s.
Číslo účtu: 153149586/0300
(dále jen „**Kupující**")

*a*
**DATASYS s.r.o.**
se sídlem **Jeseniova 2829/20, 130 00 Praha 3**
zapsán do obchodního rejstříku, živnostenského rejstříku, jiného veřejného rejstříku, nebo jiné evidence **C 28862 u Městského soudu v Praze**
zastoupená **XXX**, **prokuristou**
Číslo účtu (u plátců DPH takové číslo, které bylo správcem daně zveřejněno v registru plátců DPH): **27-9647490267/0100, Komerční banka, a.s.**
IČO: **61249157**
DIČ: **CZ61249157**
(dále jen „**Prodávající**")

(Kupující a Prodávající dále společně jen „**Smluvní strany**", nebo každý z nich samostatně jen „**Smluvní strana**"),

uzavírají dnešního dne, měsíce a roku tuto kupní smlouvu (dále jen „**Smlouva**").

## II.
## Předmět koupě a místo plnění

1. Předmětem koupě dle Smlouvy je dodávka **centrálního řešeni zabezpečení bezdrátové sítě (firewall) a systému na centralizovanou správu logů do Farmaceutické fakulty v Hradci Králové** včetně instalace a konfigurace do infrastruktury Kupujícího. Přesná specifikace předmětu koupě je uvedena v příloze č. 1 Smlouvy, která je její nedílnou součásti (dále jen „**Předmět koupě**"). Místem plnění je sídlo Kupujícího.

2. Prodávající bere na vědomí, že předmět plnění dle Smlouvy je součástí dotačního projektu „Modernizace výukových prostor na FaF UK za účelem zvýšení kvality vzdělávání", registrační č. CZ.02.2.67/0.0/0.0/16_016/0002529 v rámci Operačního programu Výzkum, vývoj a vzdělávání (dále jen „**OP VVV**").

3. Prodávající bere na vědomí, že jelikož je kupní cena financována z prostředků dotace, může mít nesplnění jakékoliv povinnosti Prodávajícího dopad na financování. Konstatování výdajů jako nezpůsobilých, případné udělení odvodu či správních sankcí v důsledku porušení této povinnosti bude představovat škodu, která Kupujícímu vznikla.

## III.
## Termín plnění

1. Prodávající se zavazuje odevzdat Předmět koupě Kupujícímu nejpozději **do 28 dnů** ode dne nabytí účinnosti Smlouvy.

## IV.
## Kupní cena

1. Kupní cena za Předmět koupě se sjednává dohodou Smluvních stran a činí:

| | |
|---|---|
| Cena bez daně z přidané hodnoty (dále jen „**DPH**") celkem: | 1 695 735,54 Kč |
| DPH 21 %: | 356 104,46 Kč |
| Cena vč. 21% DPH celkem: | 2 051 840,00 Kč |

2. Kupující se zavazuje zaplatit Prodávajícímu sjednanou kupní cenu. Výsledná cena s DPH je zaokrouhlena na celé koruny.

3. Kupní cena za Předmět koupě je cenou konečnou a nejvýše přípustnou a zahrnuje veškeré náklady a poplatky spojené s plněním Smlouvy. Tímto ustanovením není dotčen odst. 4.

4. Kupní cenu je možné změnit pouze v případě, že dojde v průběhu realizace Smlouvy ke změnám daňových předpisů upravující výši DPH, o čemž jsou Smluvní strany povinny uzavřít dodatek ke Smlouvě.

## V.
## Platební podmínky

1. Kupní cena bude vyúčtována daňovým dokladem (fakturou), který Prodávající vystaví do 14 kalendářních dnů po odevzdání Předmětu koupě Kupujícímu.

2. Kupní cena bude vyúčtována daňovým dokladem, který Prodávající vystaví do 14 kalendářních dnů po odevzdání Předmětu koupě kupujícímu.

3. Pokud daňový doklad dle odst. 1. nebude obsahovat všechny náležitosti dle ust. § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a náležitosti stanovené Smlouvou, je Kupující oprávněn jej do data splatnosti vrátit zpět k doplnění či opravě, aniž se tak dostane do prodlení. Doba splatnosti počíná běžet znovu od opětovného vystavení řádně doplněného či opraveného daňového dokladu.

4. Faktura musí obsahovat název veřejné zakázky „FaF UK – Centrální řešení zabezpečení sítě – Firewall II", a dále název a registrační číslo příslušného dotačního projektu, z něhož je kupní cena hrazena, tj. „Modernizace výukových prostor na FaF UK za účelem zvýšení kvality vzdělávání", registrační č. CZ.02.2.67/0.0/0.0/16_016/0002529.

5. Veškeré platby dle Smlouvy budou probíhat výhradně v českých korunách a rovněž veškeré cenové údaje budou v této měně.

## VI.
## Povinnosti Kupujícího

1. Kupující se zavazuje poskytnout Prodávajícímu nezbytnou součinnost, která je třeba k tomu, aby Prodávající mohl odevzdat Předmět koupě v dohodnutém termínu a na sjednaném místě. Kupující je povinen Předmět koupě převzít.

## VII.
## Vady předmětu koupě, záruka za jakost

1. Prodávající odpovídá za to, že Předmět koupě bude mít ke dni předání všechny vlastnosti vyplývající ze Smlouvy. Za vadu se považuje i skutečnost, že funkční vlastnosti Předmětu koupě nebudou odpovídat povinným funkčním vlastnostem, jak vyplývají z technických norem, pokud se takové technické normy na Předmět koupě plnění vztahuji. Za vadu se dále považují i právní vady.
2. Prodávající se zavazuje poskytnout záruční dobu v délce trvání 24 měsíců. Záruční doba běží od odevzdání Předmětu koupě Kupujícímu.
3. Záruka se neposkytuje na vady způsobené konfigurací Předmětu koupě, která je v rozporu s požadavky uvedenými v technické dokumentaci Předmětu koupě (dále jen „Technická dokumentace"), umístěním Předmětu koupě do prostor nesplňujících podmínky specifikované v Technické dokumentaci, pochybením obsluhy a užíváním Předmětu koupě v rozporu s pokyny uvedenými v Technické dokumentaci, chybami v programovém kódu, hardware a v dalších komponentách třetích stran, které nebyly Kupujícímu předány dle Smlouvy. Za shora uvedené vady odpovídá Kupující.

## VIII.
## Personální zajištění

1. Na základě ujednání této Smlouvy jsou odpovědnými osobami:

za Kupujícího:

ve věcech organizačních a technických:
**Ing. Ladislav Rudišar**, vedoucí Centra informačních technologií kupujícího,
tel: XXX, e-mail: XXX

ve věcech smluvních:
**JUDr. Jana Župčanová**, právnička kupujícího,
tel: XXX, e-mail: XXX

za Prodávajícího: -

- ve věcech smluvních: XXX XXX@datasys.cz, +420 XXX
- ve věcech organizačních: XXX: XXX@datasys.cz, +420 XXX
- ve věcech technických: XXX: XXX@datasys.cz, +420 XXX

## IX.
## Ostatní závazky Prodávajícího a Kupujícího

1. Smluvní strany se zavazují během plnění Smlouvy i po jejím ukončeni zachovávat mlčenlivost o všech skutečnostech, které se dozví od druhé Smluvní strany v souvislosti s plněním Smlouvy.
2. Prodávající je povinen zavázat výše uvedenými povinnostmi mlčenlivosti i své případné poddodavatele.
3. Prodávající prohlašuje, že má uzavřenou pojistnou smlouvu, jejímž předmětem je pojištění povinnosti nahradit majetkovou i nemajetkovou újmu způsobenou Prodávajícím třetí osobě, přičemž pojistná částka činí minimálně hodnotu kupní ceny včetně DPH dle čl. IV. odst. 1.
4. Prodávající prohlašuje, že Předmět koupě není zatížen právy třetích osob, ze kterých by pro Kupujícího vyplynuly jakékoli další finanční nebo jiné povinnosti vůči třetím osobám.

## X.
## Smluvní pokuty

1. V případě prodlení Prodávajícího se splněním povinnosti odevzdat Předmět koupě Kupujícímu a provést instalaci a implementaci Předmětu koupě do stávajícího systému Kupujícího je Prodávající povinen zaplatit Kupujícímu smluvní pokutu ve výši 0,1 % z celkové kupní ceny bez DPH za každý den prodlení.
2. V případě prodlení Kupujícího s úhradou kupní ceny je Kupující povinen zaplatit Prodávajícímu smluvní pokutu ve výši 0,05 % z celkové kupní ceny bez DPH za každý den prodlení.
3. V případě porušení povinnosti mlčenlivosti dle čl. IX. odst. 1. je Smluvní strana, která povinnost mlčenlivosti porušila, povinna uhradit druhé Smluvní straně smluvní pokutu ve výši 50.000,- Kč, a to za každý jednotlivý případ porušení této povinnosti.
4. Ujednáními o smluvních pokutách v tomto článku není dotčena vzájemná povinnost Smluvních stran k náhradě majetkové i nemajetkové újmy, a to i v rozsahu smluvní pokutu převyšujícím.
5. Splatnost smluvních pokut je do 10 dnů ode dne doručení výzvy k jejich úhradě druhé Smluvní straně.

## XI.
## Zvláštní ujednání

1. Prodávající si tímto vyhrazuje k Předmětu koupě dle Smlouvy vlastnické právo ve smyslu ust. § 2132 a násl. OZ. Kupující se stane vlastníkem Předmětu koupě až úplným zaplacením kupní ceny. Nebezpečí škody na věci však na Kupujícího přechází již jejím převzetím.
2. Kupující není oprávněn postoupit či převést kterýkoli ze svých závazků či práv ze Smlouvy ani Smlouvu jako celek na třetí osobu bez předchozího písemného souhlasu Prodávajícího.
3. Kupující podpisem Smlouvy přebírá na sebe nebezpečí změny okolností ve smyslu ust. § 1765 OZ.

## XII.
## Závěrečná ustanovení

1. Tato Smlouva a práva a povinnosti z ní vzniklé, včetně práv a povinností z porušení Smlouvy, ke kterému eventuálně dojde, se řídí platnými právními předpisy, především příslušnými ustanoveními OZ a pravidly OP VVV.
2. Vzhledem k charakteru organizace Kupujícího se Smluvní strany dohodly, že prodávající výslovně souhlasí se zveřejněním Smlouvy v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů (dále jen „**zákon o registru smluv**"), zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů. Zároveň Smluvní strany navzájem prohlašují, že Smlouva neobsahuje žádné obchodní tajemství.
3. Tato Smlouva nabývá platnosti dnem podpisu poslední ze Smluvních stran a účinnosti uveřejněním v registru smluv podle zákona o registru smluv.
4. Změny nebo dodatky smlouvy, včetně změny nebo dodatku tohoto ustanovení, musí být provedeny písemně a musí být odsouhlaseny oběma smluvními stranami.
5. Prodávající je povinen archivovat veškeré písemnosti zhotovené pro plnění Smlouvy a umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je plnění dle Smlouvy hrazeno, provést kontrolu dokladů souvisejících s tímto plněním, a to po celou dobu archivace projektu, minimálně však do konce roku 2033. Kupující je oprávněn po uplynutí 10 let od ukončení plnění podle Smlouvy od Prodávajícího výše uvedené dokumenty bezplatně převzít.
6. Prodávající bere na vědomí, že je jako osoba povinná dle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, povinen spolupůsobit při výkonu finanční kontroly, mj. umožnit všem subjektům oprávněným k výkonu kontroly přístup ke všem dokumentům, tedy i k těm částem nabídek, smluv a souvisejících dokumentů, které podléhají ochraně podle zvláštních právních předpisů (např. obchodní tajemství), a to za předpokladu, že budou splněny požadavky kladené právními předpisy; tuto povinnost rovněž zajistí Prodávající u případných jeho poddodavatelů.
7. Kupující prohlašuje, že při jednání o uzavření Smlouvy mu byly sděleny všechny pro něj relevantní skutkové a právní okolnosti k posouzení možnosti uzavřít Smlouvu a další související

smlouvy dle § 1728 OZ a že neočekává ani nepožaduje od Prodávajícího žádné další informace v této věci.

8. Nedílnou součástí Smlouvy je příloha č. 1 — Technická specifikace - část 1 a část 2.

9. Tato Smlouva je sepsána v českém jazyce. Pokud je Smlouva uzavírána elektronickými prostředky, je vyhotovena v jednom originále. Pokud je Smlouva uzavírána v listinné podobě, je vyhotovena ve dvou stejnopisech s platností originálu, z nichž každá Smluvní strana obdrží po jednom.

## XIII.
## Podpisy smluvních stran

1. Smluvní strany prohlašují, že jsou s obsahem Smlouvy srozuměny a že je výrazem jejich svobodné a vážné vůle, není uzavřena v tísni a za nápadně nevýhodných podmínek, na důkaz čehož pod Smlouvu připojují své podpisy.

V Hradci Králové dne _____

V Praze dne _____

Za Kupujícího:

Za Prodávajícího:

Univerzita Karlova,
Farmaceutická fakulta v Hradci Králové

DATASYS s.r.o.

_____
prof. PharmDr. Tomáš Šimůnek, Ph.D.
děkan

prof. PharmDr. Tomáš Šimůnek, Ph.D.
Digitally signed by prof. PharmDr. Tomáš Šimůnek, Ph.D.
Date: 2019.06.07 11:04:44 +02'00'

_____
Jméno: XXX Funkce:
prokurista

Digitally signed by XXX
Date: 2019.05.29 4:35:17 +02'00'

## Technická specifikace

Příloha č. 1 Technická specifikace - část 1

Požadujeme dodání řešení typu Next Generation FireWall (NGFW), který bude splňovat níže uvedené minimální požadované parametry

Celá dodávka musí obsahovat všechny HW komponenty a požadované licence. 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

| Číslo | Popis: **Fortinet Fortigate FG300E, typ bundle FG-300E-BDL-950-60** | Splňuje |
|---|---|---|
| | **Základní technické požadavky** | |
| 1 | HW appliance NGFW/UTM firewallu s vysokou dostupností (2ks v zapojení 1+1) | Ano |
| 2 | Platforma postavená na HW akcelerované architektuře (tj. zařízení vybavené kombinací CPU + specializované obvody FPGA/ASIC pro zpracování komunikace a vybraných výpočetně náročných funkcí jako firewall, SSL dekrypce, porovnávání se signaturovou databází atd.) | Ano |
| 3 | zařízení ve formátu HW appliance o velikosti 1RU | Ano |
| 4 | veškeré příslušenství (montážní prvky) pro montáž do RACKu součástí | Ano |
| 5 | možnost doplnit druhý napájecí zdroj (interní nebo externí), nebo zařízení vybavené dvěma zdroji | Možnost doplnit druhý napájecí zdroj |
| 6 | Min. 16x 1 GE SFP rozhraní firewallu využitelných pro zpracování komunikace | 16 univerzálních SFP šachet |
| 7 | Min. 16x 1 GE RJ45 rozhraní firewallu využitelných pro zpracování komunikace | Ano |
| 8 | 2 x samostatné 1GE rozhraní pro management | Ano |
| 9 | konzolový port pro management | Ano |
| 10 | Podpora režimu vysoké dostupnost (režim L2 cluster, tedy využití virtuálních MAC adres; celý cluster se tváří z pohledu L3 jako jedno zařízení) v režimu active-active (A/A) a active-passive (A/P). Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky. | Ano |
| 11 | Zařízení bude dodáno s bezplatnou podporou dodavatele po dobu 5 let s odstraněním závady druhý pracovní den po dni jejího nahlášení a po celou tuto dobu budou k dispozici aktualizace systému a firmware hardwarových komponent | Ano |
| 12 | **Požadované síťové a bezpečnostní funkce, součástí dodávky musí být i příslušná licence (je-li výrobcem požadována). Požadované výkonnostní pramatery musí být oficiálně deklarovány výrobcem firewallu.** | |
| 13 | Podpora VLAN, min. 2 000 | 8192 |
| 14 | Podpora LACP | Ano |
| 15 | Počet FW pravidel min. 5.000 | 10000 |
| 16 | Možnost definice FW pravidel v tzv. NGFW režimu (tj. součástí základní definice FW pravidla je kromě zdroje/cíle také typ aplikace nikoliv pouhý TCP/UDP port | Ano |
| 17 | Celková propustnost firewall min. 20 Gbps (měřeno na UDP paketech o velikosti 64B) | 20 Gbps |
| 18 | Vložená latence firewallu nepřesahuje 5 µs (měřeno na malých UDP paketech (64B)) | 3 µs |
| 19 | Počet nově navázaných TCP spojení (setup rate) min. 200.000 za sekundu | 300 tis/s |
| 20 | Celkový počet konkuretních TCP spojení firewallu 2 miliony | 4 mil |
| 21 | **Funkce detekce aplikací na L7 (Application Control)** | |
| 22 | Detekce známých aplikací na základě signatur | Ano |
| 23 | Signaturové databáze automaticky aktualizované výrobcem | Ano |
| 24 | Alespoň 3.000 podporovaných aplikací | Ano |
| 25 | Pro populární cloudové aplikace (minimálně Facebook, Dropbox, Evernote, Flickr, Google Apps, iCloud, LinkedIn) požadujeme pokročilé akce typu blokování upload/download souborů, blokování her v rámci aplikace, blokování login, atd. (relevantní k dané aplikaci) | Ano |
| 26 | Možnost tvorby vlastních signatur | Ano |
| 27 | Detekované aplikace je možné: povolit, monitorovat, blokovat | Ano |
| 28 | Na základě typu aplikace musí být možné omezit šířku pásma pro danou aplikaci | Ano |
| 29 | Propustnost funkce Application Control včetně logování minimálně 6 Gbps | 7 Gbps |
| 30 | Funkce Application Control se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům. Alternativně požadujeme možnost využití v rámci tzv. NGFW pravidel popsaných výše. | Ano |
| 31 | **Funkce detekce a potlačení narušení (IPS/IDS)** | Ano |
| 32 | Signatury automaticky aktualizované výrobcem | Ano |
| 33 | Alespoň 11.000 rozpoznávaných hrozeb (signatur) definovaných výrobcem | Ano |
| 34 | Možnost tvorby vlastních signatur | Ano |
| 35 | Funkce IPS se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům | Ano |
| 36 | Propustnost funkce IPS včetně logování min. 4 Gbps (měřeno na komunikaci typu mix aplikací) | Ano |
| 37 | **Funkce antivirové kontroly** | Ano |
| 38 | Ochrana před škodlivým kódem (malware, trojské koně, atp.), včetně ochrany před polymorfním kódem | Ano |
| 39 | Signatury automaticky aktualizované výrobcem | Ano |

| | | |
|---|---|---|
| 40 | AV kontrola rozšířená o inspekci tzv. sandbox technikou, poskytovanou formou služby dodávané výrobcem FW (licence musí být součástí dodávky) | Ano |
| 41 | Možnost rozšíření o inspekci tzv. sandbox technikou formou lokální HW appliance stejného výrobce | Ano |
| 42 | Deklarovaná propustnost AV kontroly, v kombinaci s IPS, Application Control a zapnutým logováním min. 2,5 Gbps | 3 Gbps |
| 43 | Funkce AV kontroly se konfiguruje v rámci IPS profilů, které jsou následně přiřazeny konkrétním FW pravidlům | Ano |
| 44 | Podpora služby výrobce, která umožní detekovat malware, který byl objeven v době od poslední aktualizace AV signaturové databáze pomocí globální a rychle se aktualizující databáze hashů | Ano |
| 45 | Funkce odstranění aktivního obsahu z dokumentů kancelářských aplikací – AV engine na firewallu v reálném čase odstraní aktivní obsah z dokumentu. Dokument zůstává v původním formátu , jsou z něj odstraněny všechny aktivní prvky a je doručen příjemci. Originální dokument je odeslán ke kontrole do Sandboxu. | Ano |
| 46 | Podpora SSL dekrypce/SSL inspekce s minimální propustností 3,5 Gbps (TLS 1.2AES 256-SHA, měřeno v kombinaci s IPS kontrolou) | 3,9 Gbps |
| 47 | **Funkce IPSEC VPN** | |
| 48 | Podpora site-to-site VPN | Ano |
| 49 | Podpora klientských VPN | Ano |
| 50 | Dostupnost VPN klienta pro koncové stanice (Windows, MacOS) | Ano |
| 51 | Funkce klientských IPSec VPN nesmí být licencovaná na počet uživatelů, v opačném případě bude součástí dodávky neomezené licence. | Ano |
| 52 | Minimální počet IPSEC VPN tunelů typu lokalita-lokalita: 1.000 | 50 tis. |
| 53 | Propustnost IPSec VPN min. 20 Gbps (měřeno při AES 256) | 20 Gbps |
| 54 | Podpora konfigurace redundatních IPSec VPN tunelů za pomoci statického směrování | Ano |
| 55 | Podpora konfigurace redundatních IPSec VPN tunelů za pomoci dynamického směrování | Ano |
| 56 | **Funkce SSL VPN** | |
| 57 | Podpora klientského i bezklientského (portálového) režimu | Ano |
| 58 | Minimální počet současně navázaných SSL VPN tunelů: 500 | 500 |
| 59 | Minimální propustnost SSL VPN: 2,5 Gbps | 2,5 Gbps |
| 60 | **Funkce kategorizace webových stránek** | |
| 61 | Založená na centrálně spravované databázi výrobce | Ano |
| 62 | Minimálně 50 filtračních kategorií | Ano |
| 63 | Možnost definice vlastních kategorií | Ano |
| 64 | Možnost definice vlastních seznamů zakázaných URL | Ano |
| 65 | Kategorizace musí zahrnovat i české a slovenské internetové stránky | Ano |
| 66 | **Funkce DNS filtru** | |
| 67 | Možnost blokovat DNS dotazy na základě příslušnosti k URL kategorii (obdobné kategorie jako u kategorizace webových stránek) | Ano |
| 68 | Možnost definovat vlastní tzv. blacklist domén | Ano |
| 69 | Možnost přesměrovat komunikace se zakázanými doménami na vlastní portál/URL | Ano |
| 70 | **Funkce ochrany před únikem citlivých informací (DLP)** | |
| 71 | Možnost analýzy běžných typů dokumentů a protokolů | Ano |
| 72 | Možnost definice pravidel min. na základě regulárních výrazů, watermarkovacího nástroje a typu kontroly typu file checksum | Ano |
| 73 | **Podpora funkce explicit proxy** | |
| 74 | Podpora všech požadovaných ochranných profilů (AV, IPS, AppCtrl, DLP) | Ano |
| 75 | Funkce transparentního ověřování uživatelů pomocí domény MS Active Directory včetně podpory autentizace uživatelů na terminálovém serveru | Ano |
| 76 | **Virtualizace** | |
| 77 | Podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW). Každý virtuální kontext musí být plnohodnotné FW řešení včetně odděleného GUI, managementu účtů, atp. | Ano |
| 78 | Součásti dodávky musí být licence na min. 5 virtuálních kontextů (včetně licence na kompletní podporu požadovaných bezpečnostních funkcí v těchto virtuálních kontextech) | Ano |
| 79 | Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů (samostatný administrátor pro jeden či více virtuálních kontextů) | Ano |
| 80 | **Management** | |
| 81 | Podpora SNMP včetně SMPB MIB souboru dodávaného výrobcem, možnost začlenění do stávajícího systému dohledu sítě | Ano |
| 82 | Podpora otevřeného API (možnost integrace vybraných funkcí do stávající management infrastruktury | Ano |
| 83 | **Certifikace** | |
| 84 | Certifikace ICSA Labs minimálně pro Firewall, IPSec VPN, IPS, Antivirus, SSL VPN | Ano |

*Zadavatel si vyhrazuje právo otestování schody udávaných parametrů propustnosti jednotlivých bezpečnostních funkcí s reálným měřením/chováním zařízení v testovacím prostředí.*

Ve sloupci "splňuje" uchazeč vyplní zda splňuje požadovaný parametr popř. uvede konkrétní hodnotu daného parametru nabízeného řešení

**Příloha č. 1 Technická specifikace - část 2**

Požadujeme dodání systému na cetralizovanou správu logu, který bude splňovat níže uvedené minimální požadované paratmetry.

| Číslo | Popis:<br>Centrální úložiště logů DATASYS ELISA Security Manager, HW appliance ESM-10K-40T (2019b) | Splňuje |
|---|---|---|
| | **Obecné požadavky na systém pro centralizovanou správu logů, událostí a strojových dat** | |
| 1 | Systém pracuje jako appliance s jedním uceleným rozhraním pro všechny administrátorské i operátorské činnosti. Nevyžaduje instalaci dalších systémů a aplikací vyjma podpory sběru na pobočkách a agenta pro sběr Windows logů. | Ano |
| 2 | Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware. | Ano |
| 3 | Systém umožňuje dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce. | Ano |
| 4 | Zařízení bude dodáno s bezplatnou podporou dodavatele po dobu 5 let s odstraněním závady druhý pracovní den po dni jejího nahlášení a po celou tuto dobu budou k dispozici aktualizace systému a firmware hardwarových komponent. | Ano |
| 5 | Parsery a alerty musí umožňovat použití matematických operací. | Ano |
| 6 | Parsery a alerty musí podporovat dekódování URL. | Ano |
| 7 | Systém přijímá a zpracovává logy, události a další strojově generovaná data prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožnovat příjem logů i na uživatelsky definovaných UDP a TPC portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv. | Ano |
| 8 | Systém zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje ji a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí. | Ano |
| 9 | Všechny pole a položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem. | Ano |
| 10 | Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159. | Ano |
| 11 | Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci. | Ano |
| 12 | Systém musí umožňovat přijatou zprávu zahodit na základě konfigurace nebo parseru. | Ano |
| 13 | Systém provádí konsolidaci logů na centrálním místě. | Ano |
| 14 | Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce. | Ano |
| 15 | Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí). Vizualizace musí být dynamická, tj volbou v jednom grafu se ostatní příslušné grafy v pohledu na data upraví dle požadované volby automaticky. | Ano |
| 16 | Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období. | Ano |
| 17 | Systém provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě bez nutnosti využívat služeb třetích stran či externí aplikace. | Ano |
| 18 | Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám. | Ano |
| 19 | V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB. | Ano |
| 20 | Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení. | Ano |
| 21 | Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ČSN/ISO 27001:2013 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením. | Ano |
| 22 | Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování. | Ano |
| 23 | Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. | Ano |
| 24 | Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění. | Ano |
| 25 | Systém podporuje výrobcem průběžně aktualizované reporty a pohledy. | Ano |
| 26 | Konfigurační a systémové rozhraní a dokumentace musí být identické v anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce. | Ano |
| 27 | Systém nabízí kapacitní i výkonovou škálovatelnost. | Ano |
| 28 | Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB. | Ano |

| | | |
|---|---|---|
| 29 | Požadujeme, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště. | Ano |
| 30 | Monitoring stavu systému a notifikace pomocí SMTP nebo Syslog při překročení prahových hodnot nebo chybě. | Ano |
| 31 | Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (HP iMC, Zabbix, Nagios, MRTG a další) a umožnoval autorizovaný přístup ke strukturované databázi logů. | Ano |
| 32 | Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 316 / 2014 ze dne 15. prosince 2014 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)" k Zákonu 181 / 2014 „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti" ze dne 23. července 2014. | Ano |
| 33 | Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému. | Ano |
| 34 | Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému. | Ano |
| 35 | Systém musí provádět parsování a normalizaci přijatých událostí bez nutnosti instalovat externí aplikace nebo systémy, a to přímo ve svém rozhraní. Jedinou přípustnou vyjímkou je monitorování systémů Windows, které přes WMI protokol neumožňuje monitorovat textové logy. | Ano |
| 36 | Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze. | Ano |
| 37 | **Minimální HW parametry požadovaného systému** | |
| 38 | Jedna hardwarová appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. | Ano |
| 39 | HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech. | Ano |
| 40 | 2 procesory (min. 10 jader každý), podpora HyperThreadingu. | Ano |
| 41 | Min. 64GB DDR-4. | Ano |
| 42 | Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí. | Ano až 42 TB |
| 43 | Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček/s. | Ano |
| 44 | Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW. | Ano |
| 45 | Větráky v systému musí být vyměnitelné za provozu a redundatní. | Ano |
| 46 | 2x napájecí zdroje s redundancí napájení 1+1. | Ano |
| 47 | Virtuální KVM (tj. převzetí textové i grafické konsole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače. | Ano |
| 48 | Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod). | Ano |
| 49 | **Výkonnostní a SW parametry systému** | |
| 50 | Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správcovské konzoli, není nutné editovat žádné konfigurační soubory). | Ano |
| 51 | Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správcovskou konzoli. | Ano |
| 52 | Systém musí podporovat downgrade, pro případ problémů s novou verzí systému po upgrade. | Ano |
| 53 | Průměrný trvalý příjem min. 2500 událostí/s. s možností navýšení na minimálně 6000 událostí/s. prostřednictvím licence nebo rozšíření hardware. | Ano |
| 54 | Špičkový příjem 10 tis. událostí/s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. | Ano |
| 55 | Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčne neomezený počet událostí v GB za den nebo licence na minimálně 200 GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat. | Ano až 42 TB licenčně bez limitu |
| 56 | Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli. Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| 57 | Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy. | Ano |
| 58 | Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat a případná chybová hlášení. | Ano |

| | | |
|---|---|---|
| 59 | V centrální správcovské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod. | Ano |
| 60 | V centrální správcovské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.). | Ano |
| 61 | Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem. | Ano |
| 62 | Podpora zrcadlení a clusteru – 2 nody v režimu active / active. | Ano |
| 63 | Dvounodový cluster se chová jako 1 celek. | Ano |
| 64 | V případě využití dvou nodů v clusteru se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru. | Ano |
| 65 | V případě rozšíření systému na cluster (2 nody) musejí zařízení odesílající události, odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi nody. | Ano |
| 66 | Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém. | Ano |
| 67 | **Alerty** | |
| 68 | Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert. | Ano |
| 69 | Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozpársované události. | Ano |
| 70 | Předpřipravené sety/vzory alertů výrobcem. | Ano |
| 71 | Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| 72 | Jako výstupní pravidlo Alertu musí systém umět odeslat událost, která alert vyvolala na externí systém minimálně prostřednictvím SMTP nebo Syslogu přes TCP protokol. | Ano |
| 73 | V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha). | Ano |
| 74 | Systém podporuje základní funkce SIEM - funkce pro korelace událostí a upozornění s hraničními limity. | Ano |
| 75 | **Sběr událostí z Microsoft prostředí** | |
| 76 | Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring textových souborových logů. | Ano |
| 77 | Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací. | Ano |
| 78 | Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole. | Ano |
| 79 | Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku. | Ano |
| 80 | Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému. Správa a aktualizace Windows agenta se neprovádí z Group Policy. | Ano |
| 81 | Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.). | Ano |
| 82 | Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů. | Ano |
| 83 | Komunikace Windows agenta a centrálního systému musí být šifrovaná. | Ano |
| 84 | Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb. | Ano |
| 85 | Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému. | Ano |
| 86 | Počet instalací Windows agenta nesmí být licenčně omezen. Případně požadujeme licenci na 800 systémů. | Ano |
| 87 | **Podpora pro sběr událostí z poboček** | |
| 88 | Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat. | Ano |
| 89 | Systém musí podporovat centralizovanou správu pro sběr událostí přímo z centrálního úložiště dat. | Ano |
| 90 | Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit. | Ano |
| 91 | Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí. | Ano |
| 92 | Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100 GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem. | Ano |
| 93 | Řešení pro sběr dat z poboček musí mít výkon minimálně 5000 událostí /s. a to i v trvalé zátěži. | Ano |
| 94 | Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů. | Ano |
| 95 | Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V. | Ano |
| 96 | Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT). | Ano |

Ve sloupci "splňuje" uchazeč vyplní zda splňuje požadovaný parametr popř. uvede konkrétní hodnotu daného parametru nabízeného řešení

# Zabezpečení sítě firewall - FortiGate 300E

Podnikové firewallové řešení společnosti Fortinet poskytuje komplexní zabezpečení sítě na jedné platformě, s jedním bezpečnostním operačním systémem a jednotnou správou pravidel z jednoho uživatelského rozhraní. Nabízí bezkonkurenčně nejvyšší míru ochrany proti nejpokročilejším bezpečnostním hrozbám a cíleným útokům.

## Integrace pomocí architektury Security Fabric

Zařízení FortiGate, propojená pomocí architektury Fortinet Security Fabric, tvoří páteř uceleného podnikového řešení společnosti Fortinet.

## Založené na bezpečnostním procesoru

- Spojuje procesor architektury RISC a specializované obsahové a síťové bezpečnostní procesory společnosti Fortinet, což zaručuje bezkonkurenční výkon
- Zjednodušuje konstrukci zařízení a umožňuje špičkový výkon u sítí menšího rozsahu
- Podporuje firewallovou akceleraci u paketů všech velikostí a maximalizuje tím propustnost
- Poskytuje zrychlené zpracování obsahu v rámci jednotného řízení hrozeb (UTM), což zvyšuje výkon a zkvalitňuje ochranu
- Zvyšuje výkon VPN pro bezpečný vysokorychlostní vzdálený přístup

## Obsahový procesor

Nový, přelomový obsahový procesor SPU CP9 pracuje mimo přímý tok síťových dat a urychluje inspekci pomocí výpočetně náročných bezpečnostních funkcí:

- Vyšší výkon detekce průniku (IPS) díky jedinečné schopnosti úplného porovnávání signatur ve specializovaných proprietárních obvodech
- Schopnost inspekce SSL provozu na základě nejnověji vydaných sad šifer
- Přebírá úlohy šifrování a dešifrování

## Síťový procesor

Síťový procesor SPU NP6Lite pracuje sériově s firewallovými a VPN funkcemi a poskytuje:

- Firewall o rychlosti síťového připojení pro pakety všech velikostí
- Akceleraci VPN
- Prevenci průniku založenou na detekci anomálií, výpočet kontrolních součtů a defragmentaci paketů
- Tvarování provozu a řazení do front podle priorit

## FortiOS

Veškeré bezpečnostní a síťové funkce platformy FortiGate lze řídit a spravovat pomocí jediného intuitivního operačního systému. Snižte si provozní náklady a ušetřete čas díky skutečně konsolidované bezpečnostní platformě příští generace.

- Skutečně konsolidovaná platforma s jedním operačním systémem pro veškeré bezpečnostní a síťové služby všech řešení FortiGate.
- Špičková ochrana: ověřená kvalita zabezpečení a výkon v testech NSS Labs, VB100, AV Comparatives a ICSA.

- Řízení tisíců aplikací, blokace zneužití nejnovějších zranitelností a filtrování internetového provozu za základě milionů hodnocení URL v reálném čase.
- Automaticky detekuje, blokuje a neutralizuje útoky v řádu minut pomocí integrovaného systému ochrany proti pokročilým hrozbám.
- Řeší veškeré síťové potřeby díky širokému spektru funkcí včetně směrování, přepínání, WiFi, LAN a WAN.
- Nejrychlejší firewallová platforma na trhu založená na proprietárních bezpečnostních procesorech.

## Bezpečnostní služby FortiGuard™

FortiGuard Labs poskytuje informace o vývoji hrozeb v reálném čase a komplexní bezpečnostní aktualizace pro všechna řešení společnosti Fortinet. Tým sestává z bezpečnostních výzkumníků, techniků a forenzních specialistů a spolupracuje s předními světovými organizacemi, které sledují vývoj hrozeb, s dalšími dodavateli síťových a bezpečnostních řešení i národními bezpečnostními složkami:

- Aktualizace v reálném čase — nepřetržitý výzkum celosvětově poskytuje bezpečnostní zpravodajství pro všechny platformy Fortinet v režimu 24x7x365 prostřednictvím sítě Fortinet Distributed Network.
- Bezpečnostní výzkum — Laboratoře FortiGuard dosud odhalily přes 170 unikátních zranitelností nultého dne a měsíčně poskytují miliony automatizovaných aktualizací signatur.
- Ověřená efektivita bezpečnostního zpravodajství — účinnost síťové bezpečnostní platformy využívající FortiGuard ověřily přední mezinárodní nezávislé laboratoře i spotřebitelé na celém světě.

## Podpůrné služby FortiCare™

Náš tým zákaznické podpory FortiCare poskytuje globální technickou podporu pro veškeré produkty Fortinet. Centra podpory jsou umístěná v Severní a Jižní Americe, Evropě, Asii a na Blízkém východě. FortiCare nabízí služby, které vyhoví potřebám podniků všech velikostí:

- Rozšířená podpora — pro zákazníky, kteří potřebují podporu pouze během běžné pracovní doby.
- Komplexní podpora — pro zákazníky, kteří potřebují nepřetržitou podporu kvůli zajištění kriticky důležitého provozu včetně rozšířených možností výměny hardwaru.
- Pokročilé služby — pro globální nebo regionální zákazníky, kteří potřebují mít přiděleného vlastního manažera technické podpory, vyšší zaručené parametry úrovně služeb, rozšířenou podporu softwaru, prioritní řešení problémů, návštěvy na místě a další služby.
- Profesionální služby — pro zákazníky s rozsáhlejšími a složitějšími bezpečnostními implementacemi, kteří vyžadují architektonické služby, návrh, implementaci a zprovoznění řešení, provozní služby apod.

# Specifikace zařízení:

| | |
|---|---|
| **Interfaces and Modules** | |
| GE RJ45 Interfaces | |
| GE SFP Slots | |
| GE RJ45 Management Ports | |
| USB Ports | |
| RJ45 Console Port | |
| Local Storage | |
| Included Transceivers | |
| **System Performance — Enterprise Traffic Mix** | |
| IPS Throughput | |
| NGFW Throughput | |
| Threat Protection Throughput | |
| **System Performance and Capacity** | |
| IPv4 Firewall Throughput (1518 / 512 / 64 byte, UDP) | |
| IPv6 Firewall Throughput (1518 / 512 / 64 byte, UDP) | |
| Firewall Latency (64 byte, UDP) | |
| Firewall Throughput (Packet per Second) | |
| Concurrent Sessions (TCP) | |
| New Sessions/Second (TCP) | |
| Firewall Policies | |
| IPsec VPN Throughput (512 byte) | |
| Gateway-to-Gateway IPsec VPN Tunnels | |
| Client-to-Gateway IPsec VPN Tunnels | |
| SSL-VPN Throughput | |
| Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode) | |
| SSL Inspection Throughput (IPS, avg. HTTPS) | |
| SSL Inspection CPS (IPS, avg. HTTPS) | |
| SSL Inspection Concurrent Session (IPS, avg. HTTPS) | |
| Application Control Throughput (HTTP 64K) | |
| CAPWAP Throughput (1444 byte, UDP) | |
| Virtual Domains (Default / Maximum) | |
| Maximum Number of Switches Supported | |
| Maximum Number of FortiAPs (Total / Tunnel) | |
| Maximum Number of FortiTokens | |
| Maximum Number of Registered Endpoints | |
| High Availability Configurations | |

| | |
|---|---|
| **Dimensions and Power** | |
| Height x Width x Length (inches) | |
| Height x Width x Length (mm) | |
| Weight | |
| Form Factor | |
| Power Consumption (Average / Maximum) | |
| Power Source | |
| Current (Maximum) | |
| Heat Dissipation | |
| Redundant Power Supplies (Hot Swappable) | |
| **Operating Environment and Certifications** | |
| Operating Temperature | |
| Storage Temperature | |
| Humidity | |
| Noise Level | |
| Operating Altitude | |
| Compliance | |
| Certifications | |

# Integrovaný bezpečnostní a provozní dohled nástrojem DATASYS ELISA Security Manager

## Technická specifikace centrálního úložiště logů HW appliance ESM-10K-40T

# Specifikace DATASYS ELISA HW appliance ESM-10K-40T

Appliance ESM-10K-42T je kompletní ELISA Security Manager systém v podobě předinstalovaného fyzického serveru DELL s "On-Site Service" hardwaru „následující pracovní den“ na 5 let. Jedná se model optimalizovaný pro trvalé zpracování až 10000 EPS a krátkodobě pro příjem až 30000 EPS. Základní přehled výkonových parametrů:

- CPU 2x 2,4 GHz [10C/20T]
- RAM 64 GB
- HDD 40 TB [RAID 6] + SSD 4 TB [RAID 6]
- redundantní napájení

Detailní technická specifikace HW appliance:

| Komponenta HW appliace | Ks |
|---|---|
| DELL PowerEdge R740XD Server EMEA Shipping | 1 |
| Chassis with up to 12x3.5" HDD, 4 x3.5" HDDs on MP and 4x2.5" HDDs on Flexbay for 2CPU | 1 |
| Intel® Xeon® Silver 4114 2.2G, 10C/20T, 9.6GT/s, 14M Cache, Turbo, HT (85W) DDR4-2400 | 2 |
| 16GB RDIMM, 2666MT/s, Dual Rank | 4 |
| PERC H730P RAID Controller, 2Gb NV Cache, Minicard | 1 |
| 4TB 7.2K RPM SATA 6Gbps 512n 3.5in Hard Drive | 12 |
| 1.92TB SSD SATA Mix Use 6Gbps 512 2.5in Flex Bay AG Drive, 3 DWPD, 10512 TBW | 4 |
| 6 Performance Fans forR740/740XD | 1 |
| Dual, Hot-plug, Redundant Power Supply (1+1), 750W | 1 |
| Broadcom 57416 2 Port 10Gb Base-T + 5720 2 Port 1Gb Base-T, rNDC | 1 |
| Rack Power Cord 2M (C13/C14 10A) | 2 |
| Riser Config 2, 3 x8, 1 x16 slots | 1 |
| iDRAC9 Enterprise with OME Server Configuration Management | 1 |
| PowerEdge 2U Standard Bezel | 1 |
| ReadyRails™ Sliding Rails With Cable Management Arm | 1 |
| 5Yr ProSupport and 4hr Mission Critical | 1 |

## Vlastnosti nástroje ELISA

DATASYS ELISA je robustní a výkonné řešení typu SIEM pro sběr, korelace a analýzu logů. Jádrem systému je extrémně rychlá „noSQL" analytická databáze ***Elasticsearch*** s vylepšeným uživatelským rozhraním ***Kibana***, které poskytuje vysoký komfort při analýze detekovaných bezpečnostních incidentů a relevantních logů. Elasticsearch databázi je možné distribuovat na více serverů za účelem rozdělení zátěže a vysoké dostupnosti indexovaných dat.

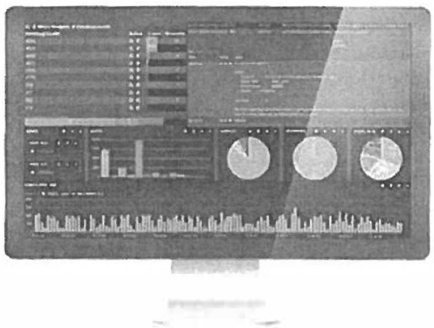
Uživatelským prostředím je webový prohlížeč. Vyhledávání v databázi událostí je podobné s vyhledáváním v internetovém vyhledávači – prováděno jednoduše zadáním klíčových slov. Po krátkém zaškolení dokáže ale i nezkušený uživatel formulovat též komplexní filtry, které široce přesahují možnosti vyhledávání v relačních databázích. Definice filtrů lze ukládat pro opakované použití.

ELISA poskytuje díky své architektuře bleskové odezvy i v případě objemných indexů/databází. Uživateli je v základu zobrazen histogram počtu výskytů vyhovujících záznamů za zvolený časový interval a jejich tabulkový stránkovaný přehled. V odladěné konfiguraci našeho řešení ***ELISA*** jsou události přenášeny do analytické databáze v původní, strukturu záznamu zachovávající podobě, s bezproblémovou podporou diakritiky.

Označením konkrétní události získá uživatel přehled o všech jejích atributech a možnost drill-down analýzy. Výběrem některého z atributů totiž uživatel ihned získá statistický přehled výskytu jeho různých hodnot s možností rychlého (i negativního) filtrování dle dané hodnoty.

***Bezpečnostní události jsou v systému ELISA vyhodnocovány na dvou úrovních:***

- na vstupu při prvotním zpracování události
  - detekce výskytu konkrétních událostí
  - korelace mezi událostmi
    - opakované výskyty
    - relace mezi různými událostmi
    - kontextové korelace
    - „first" události apod.
- definovanými periodickými dotazy do databáze
  - statistické anomálie



***Hlavními vstupními kanály systému ELISA jsou:***

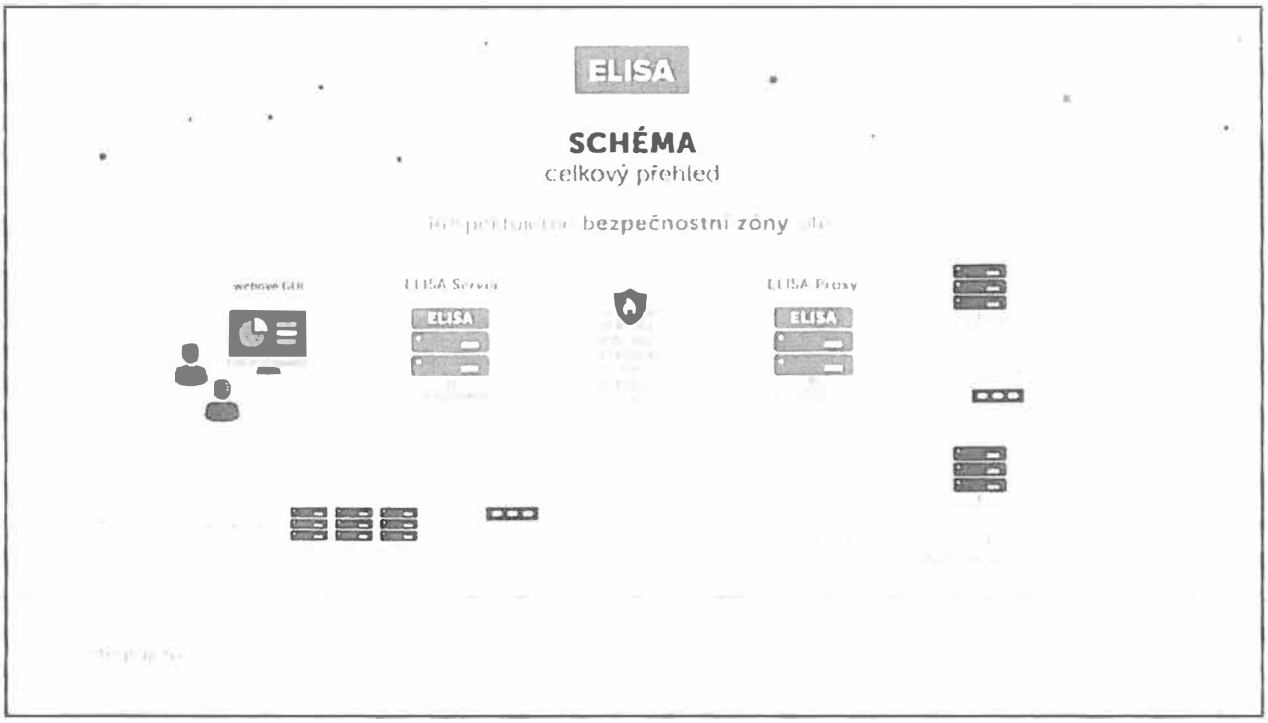
- binární protokol s podporou TLS šifrování pro přenos strukturovaných událostí (NXlog agent)
- syslog (udp i tcp)
- SNMP trapy
- netflow

Doprovodný nástroj ***NXlog*** nebo jeho klon ***DATASYS DSlog*** je určen k instalaci na monitorované systémy, které nedokáží záznamy z logů zpracovat a odeslat autonomně. Agent podporuje sběr událostí z textových logů, windows eventlogů, různých typů strukturovaných logů (CSV, j2log a dalších) a z tabulek relačních databází.

***Význačné vlastnosti agenta NXlog[1]:***

- multiplatformní a nenáročný na zdroje
- vytváří buffer událostí v případě nedostupnosti centrálního systému ELISA
- pamatuje si pozici již zpracovaných událostí i po restartu
- podporuje rotované log soubory, různé typy kódování a víceřádkové záznamy
- umožňuje filtrování a korelace událostí už na monitorovaném systému
- podporuje přenos strukturovaných záznamů v binárním formátu a šifrovaný přenos (SSL)

Pro získání přehledu o logické architektuře sběru dat v ELISA doporučujeme shlédnout produktové video https://youtu.be/fRpc9fgWdiw .




[1] Součástí dodávky licence produktů „ELISA Security Manager" a „ELISA Log Manager" je neomezená licence pro užívání programového vybavení „NXlog Enterprise Edition". Detailní popis zde: http://nxlog.co/products/nxlog-enterprise-edition .

Bezpečnostní dohled je v systému ELISA, realizován těmito komponentami:

- **ELISA Log Manager**
  - Zajišťuje sběr logů zejména těmito mechanismy:
    - Příjem událostí ze síťových zařízení protokoly syslog, SNMP Trap, netflow
    - Načítání událostí z windows eventlogů a různě formátovaných textových logů pomocí multiplatformního agenta nebo i vzdáleně bez agenta[2]
    - Získávání logů přes http/s, ftp/s, sftp, scp, ssh, nfs, cifs, atd.
    - Načítání logů z databázových[3] tabulek, CheckPoint LEA, VMware API apod.
  - Provádí zpracování logů a jejich uložení v prokazatelně nezměněné podobě
    - Filtrování, parsování, transformace a normalizace atributů
    - Kryptografická signatura RAW formátu logu

- **ELISA Security Manager**
  - Zajišťuje obohacování logů o související informace z dalších zdrojů
  - Vykonává persistentní korelace událostí v časovém okně i několika měsíců pro automatickou alarmování potenciálních bezpečnostních incidentů
  - Provádí výpočet „Risc Score" formulí ASSET_VALUE*SEVERITY*RELIABILITY s výslednými hodnotami v rozsahu 0 až 100, přičemž hodnotu aktiva lze definovat na úrovni zařízení
  - Poskytuje přednastavená korelační pravidla, která řeší klasické hrozby a bezpečnostní rizika a pracují s generalizovanou víceúrovňovou kategorizací, takže při správné konfiguraci parserů dat zůstávají detekční pravidla funkční i po výměně firewallu, AV systému apod.

- **ELISA Change Auditor**
  - Detekce a protokolování změn v konfiguracích serverů a zařízení
    - File Integrity Monitoring
    - Registry Integrity Monitoring
    - Protokolování rozdílů v různých exportech konfigurací
    - Protokolování změn provedených ve VMware vCenter

Nástroj ELISA podporuje[4] integraci i s dalšími v ČR rozšířenými bezpečnostními nástroji, například:

- FLOWMON pro detekci anomálií v síťové komunikaci
- NetSHIELD pro detekci a blokování neautorizovaných zařízení v síti
- OpenVAS nebo Greenbone Security Manager pro aktivní nalézání zranitelností v síti

[2] Podpora „Microsoft EventLog API" a „Microsoft Windows Event Forwarding". Podpora formátů CEF, SDEE apod.

[3] Obecně podporujeme jakoukoli DB přístupnou přes ODBC.

[4] Uvádíme jen vzorové příklady pokročilejších integrací, díky podpoře standardních protokolů a průmyslových standardů podporuje ELISA na úrovni zpracování bezpečnostních alarmů integraci prakticky jakéhokoli nástroje.

DATA SYS

*Jako v IT odvětví rodinné společnosti. DATASYS je jedničkou mezi IT firmami na trhu působíme od roku 1994 a přinášíme spolehlivá řešení v následujících oblastech.*

## BEZPEČNOST

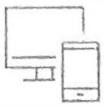
Jsme dodavatelem bezpečnostních řešení, nástrojů a služeb. Naší specializací je sledování vzdálených přístupů. Umíme však zabezpečit a monitorovat informační systémy na mnoha úrovních, náš přístup je pragmaticky vyvážený, realizace důsledná.

## VÝVOJ A INOVACE

Pokrokové nápady převádíme v realitu. Dodáváme serverové back-end aplikace, klient/server řešení, webové aplikace i aplikace pro mobilní telefony. Dokážeme integrovat oddělené systémy i navrhovat zcela nová řešení.

## INFRASTRUKTURA

Informační systémy nemohou fungovat bez pevných základů. Infrastruktura představuje páteř každého informačního systému a my se zaměřujeme na komplexní implementační a integrační služby.



## IT AS A SERVICE

Umíme se postarat o všechny vaše IT. Vyřešíme vaše problémy se softwarem i hardwarem, jsme na příjmu 24 hodin denně, 7 dní v týdnu. Budeme vaším opravdovým partnerem pro inovace a IT vám doručíme jako spolehlivou službu.

## NAŠI KLIENTI




**80+**

klíčových zaměstnanců

**415**
**mil. Kč**

obrát v roce 2018

**5000+**

realizovaných projektů

**25**
**let**

zkušeností

*Pojďme se potkat a společně najít vhodné řešení.*