**TECHNICKÁ SPECIFIKACE**

pro veřejnou zakázku na dodávky v otevřeném nadlimitním řízení

**Rozšíření datového centra statutárního města Karviné (HW a SW infrastruktury)**

**Preambule:** Tato technická specifikace je vypracována ve formě stanovení minimálních požadavků na množství, funkce, vlastnosti, jakost a výkonnostní nebo jiné parametry předmětu plnění veřejné zakázky. Technická specifikace je také součástí obchodních podmínek, ve kterých uchazeči doplní požadované údaje a stávají se tak součástí smlouvy, která bude uzavřena s vítězným dodavatelem.

#### Část 1. – 4 ks Fyzické servery pro virtualizaci desktopů

**Požadované minimální technické parametry a funkcionality**

|  |  |
| --- | --- |
| **Parametr / funkcionalita** | **Minimální hodnota** |
| minimální hodnota PassMark dle cpubenchmark .net | 21800 |
| 2 procesory stejného výrobce jako čipová sada serveru, minimálně 14 jader | ano |
| 1x management karta včetně dedikovaného ethernet portu s odpovídající licencí, umožňující plnou vzdálenou správu serveru s podporou režimu vzdálené obrazovky | ano |
| 19“ rack mount, včetně pohyblivého ramene pro uchycení kabeláže, max. 2U | ano |
| RAM DDR4, 2400MHz | 512GB, rozšiřitelné na min. 1TB |
| bootovací médium na virtualizační OS | interní USB nebo SD karta |
| PCIe 3.0 x16 | 1x |
| PCIe 3.0 x8 | 3x |
| redundantní zdroje a ventilátory adekvátního výkonu, za chodu vyměnitelné, které v budoucnu umožní bezproblémové rozšíření serveru (zejména RAM) | ano |
| 1Gbits LAN port | 8x |
| SAN HBA 16Gbits port | 2x |
| kompatibilita se specifikací IPMI2.0 | ano |
| nabízený server musí být uveden na compatibility listu (http://www.vmware.com/resources/compatibility/search.php?deviceCategory=server) pro VMware minimálně pro verze 5.5. U3 a 6.0 U3 | ano |
| záruku na server musí garantovat výrobce serveru | ano |
| technická podpora v režimu 24/7 s výměnou dílů NBD | 5 let |

#### Část 2. – 1 ks FC diskové pole s SSD disky

**Požadované minimální technické parametry a funkcionality**

|  |  |
| --- | --- |
| **Parametr / funkcionalita** | **Minimální hodnota** |
| duální řadiče diskového pole (upgrade software u řadičů musí být proveditelný za chodu a bez ztráty přístupu hostitelských serverů k datům) | ANO |
| FC 16Gbits port pro každý řadič (zpětná kompatibilita s FC 8 Gbits) | 2x |
| volitelné rozhraní diskového pole (možnost budoucího rozšíření) | 10Gbit iSCSI a/nebo 12Gbit SAS |
| cache pro každý řadič | 8GB |
| 19“ rack mount, max. 2U | ano |
| typ HDD | 1,6TB SSD 12Gbps 2,5“, certifikované pro intenzivní provoz čtení/zápis = 50:50 |
| celková použitelná kapacita při konfiguraci 2x RAID 5 + 2x hotspare disk | 13TB |
| rozšiřitelnost diskového pole na min. | 160ks disků |
| podpora RAID 5, 6, 10 | 5, 6, 10 |
| redundantní, za chodu vyměnitelné zdroje | ano |
| SFP moduly pro připojení do SAN switchů Dell Brocade 300 (8Gb SW) a příslušné optické patch kabely pro každý port v řadiči v délce 5m | ano |
| SW pro plnohodnotnou správu diskového pole a diskových subsystémů s možností ovládání přes CLI a GUI | ano |
| podpora serverových OS | Vmware vSphere 5.5 a vyšší, Windows 2008 a vyšší, Redhat a SLES |
| podpora SnapShotů, klonování a Asynchronního mirroringu | ano |
| nabídka musí obsahovat všechny licence potřebné pro připojení k infrastruktuře zadavatele (min. 6 fyzických serverů) a používání všech požadovaných funkcí, bez časového omezení | ano |
| administrační rozhraní min. v anglickém jazyce | ano |
| technická podpora v režimu 24/7 s výměnou dílů NBD | 5 let |

#### Část 3. – 1 ks SAN switch

**Požadované minimální technické parametry a funkcionality**

|  |  |
| --- | --- |
| **Parametr / funkcionalita** | **Minimální hodnota** |
| počet a typ portů SAN switche | 24portů univerzální (min. E, F, M) |
| full fabric architektura | ano |
| porty - Auto-sensing 2, 4,8, 16 Gbps | ano |
| podpora ISL trunků | ano |
| agregovaná propustnost | 384 Gbps |
| počet aktivních portů včetně licence | 12 |
| všechny aktivní porty osazeny SFP moduly (z toho 2 moduly v provedení „LONG“) | ano |
| redundantní, za chodu vyměnitelné zdroje | ano |
| plně kompatibilní se stávající SAN sítí (Dell Brocade 300) | ano |
| technická podpora v režimu 24/7 s výměnou dílů NBD | 5 let |

#### Část 4. – 1 ks Systém pro sběr a vyhodnocování logů

**Požadované minimální technické parametry a funkcionality**

*A. Obecné*

1. Zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a hardware, mininálně však tyto:

|  |  |  |  |
| --- | --- | --- | --- |
| Apache httpd | Dropbear SSH (mostly Embedded Linux) | Juniper SRX | OpenSSH server |
| Apache Tomcat | Extreme Networks XOS | Kaspersky Endpoint Security | Oracle DB |
| Antivir AVG | FlowMon | Kaspersky Security Center | Palo Alto Networks NGFW |
| Antivir Avast | FortiAuthenticator | Kerio Connect | Shorewall |
| Antivir Eset | FortiDDoS | Kerio Control | SonicWall |
| Antivir Eset Remote administrator | FortiGate (FOS 5.2) | Kernun Clear Web | Sophos |
| Brocade FC switches | FortiMail | Kernun web filter | SpamAssasin |
| ArcSight CEF format all sources | FreeRADIUS | Linux Cron | TrendMicro DeepDiscovery |
| Cisco ASA | Qradar LEEF format all sources | Linux Freeradius | TrendMicro TippingPoint NG-IPS |
| Cisco Firepower | HPE Aruba Networks WLAN | Linux Iptables | UBNT Rocket |
| Cisco IOS | HPE iLo 4 (Server OoB management) | Linux postfix | UBNT UniFI |
| Cisco IronPort | HPE IMC | Mikrotik | VMware |
| Cisco SMB | HPE routers | Microsoft SharePoint | Windows - any logs from Event Viewer |
| Cisco WLC | HPE switches Procurve OS | Microsoft SQL | Windows - any text log from file |
| Dell Force10 | HPE switches Comware OS | Microsoft Windows DHCP log |  |
| Dell iDrac (Server OoB management) | HPE Comware WLAN | Microsoft Windows firewall |  |
| Dell PowerConnect | CheckPoint | Microsoft Windows IIS |  |
| Dell SonicWALL | ISC BIND | MySQL |  |
| Dell W-series WiFi | ISC DHCP | Nginx |  |
| Discard (Special distard rule) | ISC DHCPD | Novell eDirectory |  |

1. možnost dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem nabízeného systému - uživatelsky definované parsery,
2. systém bude standardizovat přijaté logy do jednotného formátu a logy budou parsovány (rozdělovány) do příslušných polí dle jejich typu, nad takto standardizovanými daty systém automaticky vytváří indexy pro rychlejší vyhledávání pro všechna pole standardizovaného logu. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování,
3. systém musí umožnit sběr událostí minimálně ve formátech RAW, Syslog, CEF, JSON RFC7159,
4. systém nesmí umožnit mazání nebo modifikování již uložených logů,
5. systém musí umožnit snadné vyhledávání událostí (ad hoc) bez nutnosti programování,
6. systém musí umožnit grafické znázornění událostí (grafy událostí), včetně možnosti grafického znázornění TOP událostí nad všemi daty za zvolené časové období,
7. systém musí automaticky doplňovat GeoIP informace k událostem a jejich grafické znázornění na mapě, také musí automaticky doplňovat reverzní DNS záznamy k IP adresám,
8. systém musí umožnit unifikované vyhledávání napříč všemi typy dat a zařízení,
9. dodaný systém musí obsahovat předpřipravené základní pohledy na uložená data,
10. dodaný systém musí obsahovat monitoring stavu systému, možnost nastavení alertování při překročení prahových hodnot nebo chybě systému (upozornění pomocí SMTP),
11. systém musí umožnit dotazování externím monitorovacím systémem pro další zpracování alertů a prahových hodnot (minimálně Nagios a PRTG),
12. systém musí obsahovat reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů. Tento nástroj musí být integrován do administrátorské konzole,
13. systém musí obsahovat právě jednu centrální webovou konzoli pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Dále jen „konzole logovacího systému“,
14. systém musí umožnit definovat a přiřazovat uživatelské role definující přístupová práva k uloženým událostem a jednotlivým ovládacím komponentám systému,
15. systém musí umožnit ověření uživatele systému na externím LDAP serveru (Active directory),
16. systém musí umožnit konfiguraci vlastních parserů pomocí vizuálního programovacího jazyka v centrální administrátorské 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. Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy,
17. systém musí umožnit on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat,
18. v centrální administrátorské konzoli je možné přidávat k jednotlivým zdrojům dat, aplikacím, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.,
19. v centrální administrátorské konzoli je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.),
20. všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem,
21. systém musí umožnit na základě zadaných podmínek splněných v přijatých datech vygenerovat alert, text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události,
22. součásti dodávky jsou předpřipravené sety/vzory alertů,
23. konfigurace alertů musí být možná pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku,
24. v alertech je možné využít filtry a značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Karviná). Podmínky a filtry musí být možné řetězit,
25. odesílání alertů musí být možné pomocí SMTP,
26. konfigurační, systémové rozhraní a dokumentace musí být dostupná také v českém jazyce,
27. nabízený systém musí splňovat požadavky normy ISO 27001:2013 na pořizování auditních záznamů. Toto musí být doloženo potvrzením výrobce, nebo dodavatele,
28. 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.

###### *B. HW a SW parametry*

1. Z důvodu zajištění nezávislosti na jiných systémech, musí být systém dodán jako jedna hardwarová appliance o velikosti max. 2U, včetně pohyblivého ramene pro uchycení kabeláže,
2. dodaná HW appliance musí obsahovat veškeré potřebné komponenty (CPU, RAM, diskový prostor) a musí být nezávislá na dalších systémech,
3. min. 2 procesory (min. 10 jader každý), podpora HyperThreadingu,
4. RAM min. 64GB DDR-4,
5. HW 12Gb SAS RAID řadič s podporou RAIDu 0/1/5/6/10/50/60 s cache min. 2GB, která je zálohována baterií nebo flash pamětí,
6. 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,
7. čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data musí být minimálně 40TB s odolností proti výpadku min. 2 disků,
8. minimálně 4x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW,
9. redundantní ventilátory vyměnitelné za chodu systému,
10. redundantní napájecí zdroje vyměnitelné za chodu systému,
11. systém pro vzdálenou správu serveru včetně potřebné licence, pokud je potřeba (obdoba HP iLO, Dell iDRAC apod),
12. dodávaný systém musí podporovat zrcadlení a clustering (při zakoupení dalšího, stejného HW) a možnost rozšiřování kapacity přidáváním dalších nodů do clusteru,
13. aktualizace systému musí být distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální administrátorskou konzoli,
14. systém musí zvládat průměrný příjem min. 6 tis událostí/s, ve špičce až 30 tis událostí/s. V případě vyššího počtu událostí, systém události uloží do vyrovnávací paměti pro pozdější zpracování. Systém nesmí události „zahazovat“,
15. systém nesmí obsahovat žádné licenční omezení počtu zařízení, množství přijatých událostí za sekundu apod.

###### *C. Sběr událostí z Microsoft prostředí*

1. Události z Microsoft prostředí jsou vyčítány agentem, případně jiným způsobem, jak z interních windows logů, tak se souborových logů,
2. systém zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací,
3. systém podporuje nastavení filtrace odesílaných událostí z koncového systému pomocí centrální administrátorské konzole,
4. filtrace odesílaných událostí se konfiguruje pomocí vizuálního programovacího jazyka z centrální administrátorské konzole. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku,
5. sběr událostí z koncového systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému,
6. systém automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.),
7. systém musí zajistit na koncovém zařízení vyrovnávací paměť pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů,
8. komunikace mezi centrálním a koncovým systémem musí být šifrovaná,
9. je vyžadována podpora sběru událostí z koncového systému 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,
10. k odesílaným událostem musí být automaticky doplněn jejich textový popis tak, jak je prezentován v Prohlížeči událostí (Event Viewer) na koncovém systému,
11. v případě použití agenta nesmí být počet instalací licenčně omezen.

###### *D. Sběru událostí z poboček*

1. Systém musí umožnit sběr a správu logů ze vzdálených poboček (12 základních a mateřských škol + 3 příspěvkové organizace města). Vzdálené pobočky jsou k datovému centru připojeny pomocí site-to-site VPN,
2. systém musí zajistit, aby při ztrátě spojení mezi pobočkou a centrálou, nedošlo ke ztrátě událostí (vyrovnávací paměť apod.). Tyto události musí být odeslány do centrálního systému po obnovení spojení.

###### *E. Poskytovaná podpora*

1. Garantované aktualizace systému a parserů výrobcem na dobu minimálně 5 let.
2. Min. 5 letá servisní podpora s opravou v místě instalace a s garantovanou odezvou NBD.

#### Část 5. – 5ks Gb Switch, 24 port PoE+

**Požadované minimální technické parametry a funkcionality**

|  |  |
| --- | --- |
| **Parametr / funkcionalita** | **Minimální hodnota** |
| ***Základní vlastnosti*** | |
| Třída zařízení | L2/L3 switch |
| Velikost zařízení max. 1U | ano |
| Počet metalických portů | 24x10/100/1000Mbit RJ45 |
| Počet optických portů 1Gbit/s s volitelným fyzickým rozhraním | 4x1Gbit SFP nezávislé |
| Podpora PoE+ dle standardu 802.3at | ano |
| Dostupný výkon pro PoE napájení | 370 W |
| Podpora redundantního napájecího zdroje | ano, možno externě |
| Celková propustnost přepínače | 54 Gbps |
| Celkový paketový výkon přepínače | 41 mpps |
| ***Vlastnosti stohování*** | |
| Podporovaný počet přepínačů ve stohu | 4 |
| Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance) | ano |
| Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor) | ano |
| Stoh se chová jako jedno L2 zařízení z pohledu spanning tree | ano |
| Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ano |
| ***Základní funkce a protokoly*** | |
| Podpora "jumbo rámců" do velikosti 9216 Byte | ano |
| Podpora IEEE 802.3ad | ano |
| Podpora VLAN podle IEEE 802.1Q | ano, 1000 aktivních VLAN |
| Počet záznamů v tabulce MAC adres | 8 000 |
| Protokol pro definici šířených VLAN | VTP nebo MVRP |
| IEEE 802.1s - Multiple spanning tree | ano |
| IEEE 802.1w - Rapid spanning tree | ano |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | ano |
| Detekce protilehlého zařízení | CDP nebo LLDP |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano |
| Tunelování 802.1Q v 802.1Q | ano |
| Protokol pro rychlou konvergenci ve specifických L2 kruhových sítích | REP nebo ekvivalentní |
| DHCP server pro IPv4 a IPv6 | ano |
| DHCP relay pro IPv4 a IPv6 | ano |
| DHCP klient pro IPv4 a IPv6 | ano |
| DNS pro IPv4 a IPv6 | ano |
| NTP včetně MD5 autentizace | ano |
| Statické směrování pro IPv4 a IPv6 | ano |
| IGMP Snooping v1/v2/v3 | ano |
| MLD snooping v2 | ano |
| BPDU guard | ano |
| STP root guard nebo ekvivalentní | ano |
| DHCP snooping | ano |
| HW ochrana proti zahlcení (broadcast/multicast/unicast) nastavitelná na % rychlost portu | ano |
| Podpora ověřování 802.1X | ano |
| Podpora ověřování MAC adres | ano |
| Podpora IP source Guard | ano |
| Podpora RA Guard pro IPv6 | ano |
| Podpora IPv4 a IPv6 QoS | ano |
| IEEE 802.1p - Minimální počet front | 4 |
| Hardware podpora IPv4 a IPv6 ACL | ano |
| ***Management*** | |
| CLI formou RJ45 serial konsole port | ano |
| SSHv2 pro IPv4 a IPv6 | ano |
| Omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |
| Podpora SNMPv2c a SNMPv3 | ano |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) | ano |
| Podpora Radius | ano |
| TACACS+ klient | ano |
| Port mirroring | SPAN, RSPAN |
| Podpora IP-SLA nebo alternativního způsobu monitorování provozu a dostupnosti služeb | ano |
| Technická podpora v režimu 24/7 s výměnou dílů NBD v místě instalace | 5 let |
| Výrobcem garantované SW aktualizace min. po dobu | 5 let |

#### Část 6. – 5ks Gb Switch, 48 port

**Požadované minimální technické parametry a funkcionality**

|  |  |
| --- | --- |
| **Parametr / funkcionalita** | **Minimální hodnota** |
| ***Základní vlastnosti*** | |
| Třída zařízení | L2/L3 switch |
| Velikost zařízení max. 1U | ano |
| Počet metalických portů | 48x10/100/1000Mbit RJ45 |
| Počet optických portů 1Gbit/s s volitelným fyzickým rozhraním | 4x1Gbit SFP nezávislé |
| Celková propustnost přepínače | 104 Gbps |
| Celkový paketový výkon přepínače | 77 mpps |
| ***Vlastnosti stohování*** | |
| Podporovaný počet přepínačů ve stohu | 4 |
| Kterýkoli prvek ve stohu může být řídícím prvkem (1:N redundance) | ano |
| Stoh podporuje jednotnou konfiguraci (IP adresa, správa, konfigurační soubor) | ano |
| Stoh se chová jako jedno L2 zařízení z pohledu spanning tree | ano |
| Podpora seskupení portů (IEEE 802.3ad) mezi různými prvky stohu | ano |
| ***Základní funkce a protokoly*** | |
| Podpora "jumbo rámců" do velikosti 9216 Byte | ano |
| Podpora IEEE 802.3ad | ano |
| Podpora VLAN podle IEEE 802.1Q | ano, 1000 aktivních VLAN |
| Počet záznamů v tabulce MAC adres | 8 000 |
| Protokol pro definici šířených VLAN | VTP nebo MVRP |
| IEEE 802.1s - Multiple spanning tree | ano |
| IEEE 802.1w - Rapid spanning tree | ano |
| Per VLAN rapid spanning tree (PVRST+) nebo ekvivalentní | ano |
| Detekce protilehlého zařízení | CDP nebo LLDP |
| Detekce jednosměrnosti optické linky (např. UDLD) | ano |
| Tunelování 802.1Q v 802.1Q | ano |
| Protokol pro rychlou konvergenci ve specifických L2 kruhových sítích | REP nebo ekvivalentní |
| DHCP server pro IPv4 a IPv6 | ano |
| DHCP relay pro IPv4 a IPv6 | ano |
| DHCP klient pro IPv4 a IPv6 | ano |
| DNS pro IPv4 a IPv6 | ano |
| NTP včetně MD5 autentizace | ano |
| Statické směrování pro IPv4 a IPv6 | ano |
| IGMP Snooping v1/v2/v3 | ano |
| MLD snooping v2 | ano |
| BPDU guard | ano |
| STP root guard nebo ekvivalentní | ano |
| DHCP snooping | ano |
| HW ochrana proti zahlcení (broadcast/multicast/unicast) nastavitelná na % rychlost portu | ano |
| Podpora ověřování 802.1X | ano |
| Podpora ověřování MAC adres | ano |
| Podpora IP source Guard | ano |
| Podpora RA Guard pro IPv6 | ano |
| Podpora IPv4 a IPv6 QoS | ano |
| IEEE 802.1p - Minimální počet front | 4 |
| Hardware podpora IPv4 a IPv6 ACL | ano |
| ***Management*** | |
| CLI formou RJ45 serial konsole port | ano |
| SSHv2 pro IPv4 a IPv6 | ano |
| Omezení přístupu k managementu (SSH, SNMP) pomocí ACL | ano |
| Podpora SNMPv2c a SNMPv3 | ano |
| AAA ověřování uživatelů (autentizace, autorizace, accounting) | ano |
| Podpora Radius | ano |
| TACACS+ klient | ano |
| Port mirroring | SPAN, RSPAN |
| Podpora IP-SLA nebo alternativního způsobu monitorování provozu a dostupnosti služeb | ano |
| Technická podpora v režimu 24/7 s výměnou dílů NBD v místě instalace | 5 let |
| Výrobcem garantované SW aktualizace min. po dobu | 5 let |

#### Část 7. – 1 ks SandBox řešení pro odhalení škodlivého kódu

**Požadované minimální technické parametry a funkcionality**

1. Je požadováno řešení ochrany před zero-day škodlivým kódem, viry a malware (založeném na principu tzv. sandbox) ve formě VM appliance (pro VMware Esxi), nebo HW appliance. Dodávané řešení musí být plně integrováno s dodávaným firewallem a řešením ochrany emailové komunikace (antispamem). Plnou integrací se rozumí nativní integrace, umožňující obousměrnou komunikaci mezi firewallem/AS&AV řešením a platformou sandbox (předávání souborů pro kontrolu, předávání detailním informací o kontrole zpět na firewall/AS&AV.
2. Řešení musí poskytovat vícevrstvou ochranu před škodlivým kódem. Vícevrstvou ochranou je myšlena kombinace antivirové kontroly za pomoci signatur, emulace kódu a plnohodnotný sandbox (spuštění v reálném operačním systému). Všechny tyto úrovně musí být integrovány do jednoho zařízení a vzájemně spolupracovat,
3. Všechny prvky ochrany musí být instalovány lokálně v datovém centru zadavatele, nikoliv jako cloud služba.
4. Preferujeme řešení ve formě virtuální appliance pro VMWare ESX/ESXi. Řešení musí umožňovat paralelní běh až 54 operačních systémů, počet je možné upravovat také pomocí licence.
5. Součástí dodávky musí být licence pro min. 4 virtuální systémy a pro min. 1 instalaci MS Office.
6. Všechny části řešení musí být součástí jedné virtuální/HW appliance.
7. Systém musí umožnit integraci v režimu sniffer, on demand scan (předání souborů přes GUI), integrace se síťovým diskem, integrace s firewall a SMTP GW platformou (viz dále), integrace pomocí API (viz dále). Všechny uvedené metody musí být použitelné zároveň a to na jedné virtuální/HW appliance.
8. Je vyžadována plná a obousměrná integrace s platformou firewallu a SMTP brány. Obousměrnou komunikací se rozumí obousměrné předávání informací mezi platformou Sandboxu a firewallem resp SMTP bránou.
9. Řešení musí nabízet otevřené API jak pro možnost získaní informací o prováděných inspekcích a detekovaných hrozbách, tak pro možnost integrace s dalšími produkty. API proto musí umožňovat předat zařízení soubory k inspekci a následně získat informaci o výsledku včetně detailů o inspekci (detekované chování, screenshoty, logy, atd…). Pokud tato funkce vyžaduje samostatnou licenci, tak tato musí být součástí dodávky.
10. Podporované operační systémy: Windows 7, Windows 8.1, Windows 10, Android.
11. Podpora zákaznické konfigurace Windows VM (zákazník si může připravit specifickou konfiguraci OS, využívanou jako standard v prostředí zákazníka).
12. Ochrana proti zjištění běhu v sandbox prostředí (anti evasion techniky).
13. Detekce komunikace s C&C centry.
14. Podpora detekce přístupu na kompromitované URL.
15. Funkce reportingu nalezených problémů (Součástí výsledné informace nesmí být pouze status čistý/škodlivý kód, ale kompletní informací včetně detailního popisu chování, packet capture, a v případě projevu malware v GUI také screenshoty).
16. Podpora kontroly minimálně následujících typů souborů: spustitelné soubory, JAVA, PDF, MS Office dokumenty, běžné multimediální formáty jako např. JPEG, QuickTime, MP3; archívy (ZIP/RAR/7ZIP/TNEF), asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx, ppt, pptx, qt, rm, rtf, swf, tiff, url, vbs, vcf, xls, xlsx, bat, cmd, js, wsf, xml, flv, wav, avi, mpg, midi, vcs, lnk, csv, rm.
17. Podpora reportování ve standardních formátech (minimálně HTML, CSV, PDF, XML).
18. Oddělená LAN konektivita pro systémovou/management komunikaci a pro komunikaci virtuálních strojů do Internetu.
19. Automatická aktualizace signaturových databází minimálně po dobu 5 let.
20. Automatická aktualizace VM zveřejněných výrobcem minimálně po dobu 5 let.
21. Minimálně 5 letá servisní podpora s opravou v místě instalace a s garantovanou odezvou NBD.

#### Část 8. – 2ks HW firewallu v režimu vysoké dostupnosti

**Požadované minimální technické parametry a funkcionality**

1. HW zařízení NGFW/UTM firewallu v režimu vysoké dostupnosti (dvě fyzická zařízení),
2. možnost doplnit druhý napájecí zdroj (interní nebo externí),
3. 19“ Rack mount max. 2Um
4. centralizovaná management konzole (spravuje oba nódy HA clusteru) dostupná přes WEB GUI přímo na zařízení a pro komunikaci je vyžadováno šifrované spojení např. https,
5. min. 4x 1 GE SFP rozhraní na každém firewallu využitelných pro zpracování komunikace,
6. min. 4x 1 GE RJ45 rozhraní na každém firewallu využitelných pro zpracování komunikace,
7. min. 2x 1GE rozhraní pro management,
8. konzolové rozhraní (RS 232 nebo RJ45) pro management,
9. podpora režimu vysoké dostupnosti v režimu active-active (A/A) a active-passive (A/P), pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky. Licence nesmí být žádným způsobem omezená (časově apod.),
10. podpora izolovaných virtuálních kontextů (virtualizace FW na daném HW), součástí dodávky musí být licence na min. 10 takových virtuálních kontextů, včetně licence na kompletní podporu níže uvedených bezpečnostních funkcí v těchto virtuálních kontextech:
    1. Podpora izolovaných administrátorských účtů pro správu jednotlivých virtuálních kontextů,
    2. podpora VLAN (až 1024),
    3. podpora LACP,
    4. podpora L2 (transparetní) a L3 (NAT/router) režimu fungování bezpečnostní brány (včetně podpory HA),
11. dodávané zařízení musí mít certifikace ICSA Labs minimálně pro IPSec VPN, Network Firewall, SSL VPN, Antivirus,
12. celková propustnost firewall min. 8 Gbps (měřeno na UDP paketech o velikosti 64 B až 1518 B),
13. vložená latence firewallu pro nepřesahuje 8 µs (měřeno na malých UDP paketech),
14. kapacita firewallu min. 12 milionů paketu za sekundu,
15. počet nových spojení (setup-rate) min. 200.000 za sekundu,
16. celkový počet konkuretních spojení firewallu 6 milionů,
17. funkce SSL inspekce s udávanou propustností alespoň 1.9 Gbps,
18. funkce antivirové kontroly - deklarovaná propustnost min. 1.5Gbps, signatury automaticky aktualizované výrobcem, možnost rozšíření o inspekci tzv. sandbox technikou (viz dodávané sandbox řešení),
19. funkce detekce aplikací na L7 - propustnost min. 2.5 Gbps (měřeno na http provozu), signatury automaticky aktualizované výrobcem, alespoň 2000 vzorků aplikací, možnost tvorby vlastních signatur,
20. funkce detekce a potlačení narušení (IPS/IDS) - propustnost min. 2.8Gbps (měřeno na http provozu), signatury automaticky aktualizované výrobcem, alespoň 5000 rozpoznávaných hrozeb, možnost tvorby vlastních signatur,
21. funkce IPSEC VPN - propustnost min. 7 Gbps (měřeno při AES 256), podpora site-to-site VPN, podpora klientských VPN,
22. funkce kategorizace webových stránek založená na centrálně spravované databázi výrobce, možnost definice vlastních kategorií, možnost definice vlastních seznamů zakázaných/povolených URL,
23. funkce explicitní web proxy s podporou Kerberos autentizace (autentizace na základě spojení),
24. funkce ochrany před unikem citlivých dat s možností analýzy běžných typů dokumentů a protokolů,
25. funkce SSL VPN pro min. 500 uživatelů, součástí dodávky musí být licence pro VPN klienta v počtu min. 500,
26. funkce transparentního ověřování uživatelů komunikujících skrz NGFW pomocí domény (MS Active Directory),
27. integrované úložiště (např. SSD disk) s kapacitou alespoň 100 GB pro účely ukládání provozních logů.

#### 

#### Část 9. – 1 ks Centrální antispamové řešení

**Požadované minimální technické parametry a funkcionality**

1. podpora VLAN,
2. podpora IPv4 i IPv6,
3. možnost nasazení v režimu gateway/MTA, transparent (včetně licence pro oba režimy, pokud je vyžadována),
4. licence pro neomezený počet uživatelů/IP adres,
5. architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty (dodavatel musí být schopen doložit popis MTA agenta),
6. plnohodnotná správa pomocí web gui (HTTPs) a CLI (SSH) běžícím přímo na virtuální/HW appliance pomocí šifrované komunikace např. https,
7. podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do monitorovacího systému, součástí dodávky musí být i specifický MIB soubor výrobce,
8. podpora archívu (přístup přes protokol IMAP),
9. podpora karantény,
10. podpora externího úložiště (šifrovaná komunikace, např. SFTP),
11. podpora DKIM, SPF a DMARC,
12. požadované AntiSpam funkce (výrobcem spravovaná proprietární AS funkcionalita s možností kategorizace v emailu nalezených URL, ochrana proti outbreak, IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza mailů, podpora systémů třetích stran (blacklisty), kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků) s možností detekce a selekce newsletter emailů, podpora bounce verification,
13. reakce na detekovaný spam minimálně:
    1. přidání tagu,
    2. přidání hlavičky,
    3. přeposlání emailu na jiný SMTP server,
    4. odmítnutí (reject),
    5. zahození (discard),
    6. uložení do karantény,
    7. přepsání adresy příjemce,
14. možnost limitace v rámci SMTP navázané relace (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstranění Received hlavičky),
15. antivirová ochrana aktualizovaná výrobcem s podporou emulace a vyhodnocení chování neznámého kódu a detekcí malware s možností nastavení následně prováděné akce,
16. plná integrace se systémem „sandbox“ - sandbox musí být plně integrován s navrhovaným řešením (email je uchován ve frontě a zpracován na základě výsledku analýzy na sandboxu),
17. ochrana před únikem citlivých informací, filtrování příchozích a odchozích typů souboru v souladu s PCI,
18. podpora funkce ochrany před útoky typu DoS, Antispoofing, rate limiting, vyhodnocování skóre odesílatelů s možností nastavení chování pro různé úrovně,
19. integrované logování a reporting včetně monitoringu,
20. podpora funkce šifrování přenosu mailové komunikace end-to-end bez nutnosti instalovat sw na pracovní stanice s možností vyzvednutí šifrované zprávy bezpečným způsobem přes odkaz na rozhraní zařízení,
21. minimální výkonost při plné AV i AS kontrole 10000 emailů za hodinu,
22. podpora pro minimálně 20 různých domén.

# Část 10. – Instalační práce

Implementační kroky, které jsou součástí dodávky.

**Pro část 1 – 4 ks Fyzický server pro virtualizaci desktopů**

1. Instalace dodaného HW do RACKu v datovém centru zadavatele, úpravy v zapojení napájení, připojení do LAN,
2. instalace Hypervisoru na nový HW – sjednocení verzí se stávajícím prostředím,
3. začlenění nových serverů do stávajícího clusteru VMware VDI,
4. upgrade firmware dodaného HW (na poslední vydaný výrobcem),
5. konfigurace HW managementu a alertingu,
6. konfigurace prostředí SAN přepínačů pro nový HW,
7. definování nových a úpravy stávajících zón,
8. testování nového prostředí na úrovni výpadku a izolace serverů, výpadku spojení SAN a LAN,
9. dokumentace připojení serverů a změn v SAN.

**Pro část 2 – 1 ks Diskové pole s SSD disky**

1. Fyzická instalace diskového pole do RACKu zadavatele,
2. zapojení pole do SAN infrastruktury,
3. konfigurace prostředí diskového pole ,
4. konfigurace pro připojení serverů,
5. konfigurace prostředí SAN přepínačů pro nový HW,
6. definování nových a úpravy stávajících zón,
7. začlenění nového diskového pole do prostředí clusteru VMware VDI,
8. akceptační test - simulovaný výpadek spojení k diskovému poli, výpadek jednoho řadiče,
9. konfigurace managementu, monitoringu a alertů,
10. zaškolení obsluhy,
11. dokumentace připojení diskového pole do infrastruktury zadavatele.

**Pro část 3 - 1 ks SAN switch**

1. Fyzická instalace do RACKu zadavatele,
2. připojení nového switche do stávající SAN sítě,
3. rekonfigurace stávající SAN sítě (přidání/úprava zón),
4. dokumentace k SAN síti.

**Pro část 4 – 1 ks Systém pro management logů kritických systémů**

1. Fyzická instalace do RACKu v datovém centru zadavatele,
2. připojení k síti LAN,
3. konfigurace management rozhraní,
4. nastavení základních reportů a alertů, test alertů,
5. instalace a konfigurace níže uvedených zařízení pro zasílání událostí do systému
   1. 70x windows server,
   2. 10x Linux server,
   3. 30x síťový přepínač (HP a 3COM),
   4. antispam (dodaný v rámci této výzvy),
   5. firewall (dodaný v rámci této výzvy),
   6. sandbox (dodaný v rámci této výzvy),
   7. IPS systém – TippingPoint,
   8. flowmon sonda - Invea FlowMon Probe 4000,
   9. 8x hypervisor VMware ESXi,
6. zaškolení 8 administrátorů systému (předpokládáme školení v rozsahu 8 hodin, obsahem bude minimálně nastavení dashboardů a prohledávání dat, sběr logů z Windows, psaní klasifikátorů a psaní vlastních parserů),
7. implementační dokumentace.

**Pro část 5 – 5ks Gb switch s managementem, 24 port**

1. Fyzická instalace do RACKů zadavatele,
2. zkopírování nastavení konfigurace, včetně konfigurace portů z nahrazovaného switche,
3. přepojení kabeláže z nahrazovaného do nově instalovaného switche.

**Pro část 6 – 5ks Gb Switch s managementem, 48 port**

1. Fyzická instalace do RACKů zadavatele,
2. zkopírování nastavení konfigurace, včetně konfigurace portů z nahrazovaného switche,
3. přepojení kabeláže z nahrazovaného do nově instalovaného switche.

**Pro část 7 – 1 ks SandBox řešení pro odhalení škodlivého kódu**

1. Instalace do infrastruktury zadavatele,
2. integrace s dodaným firewall a antispam řešením,
3. konfigurace virtuálních systémů dle požadavku zadavatele,
4. konfigurace a testování reportů a alertů,
5. implementační dokumentace,
6. zaškolení 8 administrátorů systému (předpokládaný rozsah 8 hodin).

**Pro část 8 – 2 ks HW firewall v režimu vysoké dostupnosti**

1. Fyzická instalace do RACKu zadavatele, připojení k LAN,
2. konfigurace HA clusteru,
3. přenos konfigurace ze stávajícího firewallu (stávající firewall je FortiGate 100D), včetně filtrů, routování, VPN, pravidel apod.,
4. test HA clusteru (automatické převzetí provozu druhým nodem v clusteru),
5. zaškolení 8 administrátorů systému (předpokládaný rozsah max. 8 hodin),
6. implementační dokumentace.

**Pro část 9 – 1 ks Centrální antispamové řešení**

1. Instalace do infrastruktury zadavatele,
2. konfigurace LAN,
3. přenos kompletní konfigurace ze stávajícího antispamového řešení (FortiMail 100C),
4. optimalizace nastavení,
5. test odeslání a příjmu emailu pro všechny domény,
6. nastavení spam reportů a alertů,
7. zaškolení 8 administrátorů systému (předpokládaný rozsah 8 hodin),
8. implementační dokumentace.