ÚSTAV
VÝPOČETNÍ
TECHNIKY

Název veřejné zakázky: **„Bezpečnostní sondy pro páteřní síť“**

TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

1. KOLEKTOR

Hardware:

- x86-64 server, velikost max. 2U
- Minimálně 2 procesory, minimálně 8 jader na procesor
- SPECint2006 Rate Baseline min. 620 (pro celý systém)
- Minimálně 64 GB RAM
- Ethernet 2 x 1 gbit/s
- Subsystém vzdálené správy s vyhrazeným Ethernet portem a plnou a časově neomezenou podporou přístupu na grafickou konzoli serveru. Subsystém vzdálené správy musí být funkční bez ohledu na stav operačního systému serveru. Je požadována kompatibilita s IPMI 2.0
- Duální napájení
- Diskový řadič (HW) s podporou RAID 0, 1, 5, 10
- Pevné disky typu SSD o celkové kapacitě minimálně 9,6 TB, hot swap

Vlastnosti aplikace:

- Bezztrátové uložení flow statistik multigigabitových linek (až 100 Gbit/s)
- Možnost dohledání libovolné komunikace až na úroveň jednotlivých flow záznamů, průběžné grafy provozu, top statistiky, reporty, alerty, databáze aktivních zařízení na síti vč. identifikace zařízení.
- Zabezpečená vzdálená správa, dohled a konfigurace – výhradně zabezpečenými protokoly SSH, HTTPS.
- Základní správa prostřednictvím příkazové řádky.
- Webové uživatelské rozhraní v českém jazyce. Uživatelsky definovatelný dashboard s podporou více záložek (konfigurace per uživatel).
- Správa uživatelů a přístupových práv na zařízení prostřednictvím uživatelských rolí. Separace dat s omezením přístupu pro jednotlivé role/uživatele.
- Podpora autentizace vůči LDAP (Active Directory), TACACS+, Cisco ISE, otevřená pro další potenciální zdroje uživatelských identit.
- Časová synchronizace zařízení proti centrálnímu zdroji času na síti.
- Použití lokální DNS cache.
- Podpora standardů Cisco AVC (vč. položek HTTP hostname a URL), Cisco NEL, Cisco NSEL, Cisco NBAR2.
- Podpora položek IPFIX proměnlivé délky.
- Podpora rozšíření VMware NSX a Gigamon IPFIX Extensions.
- Sběr a analýza RTT, SRT, delay, jitter, retransmise, out-of-order pakety pro monitoring výkonu sítě.

- Podpora monitoringu aplikační vrstvy pro protokoly HTTP, VoIP SIP, DNS, SMB/CIFS, DHCP.
- Podpora pro monitorování rozšířených informací vyšších vrstev (L3/L4) – minimálně TTL (Time to live), TCP Window size, TCP SYN packet size, umožňujících identifikaci NATů.
- Možnost přeposílání přijímaných flow statistik ke zpracování na další kolektory včetně možnosti samplování na úrovni datových toků.
- Přijímání a přeposílání IPFIX dat pomocí spolehlivého TCP spojení s možností šifrování (TCP/TLS) dle standardu RFC 5153.
- Identifikace zdroje flow dat.
- Flow statistiky je možné (i automaticky) zálohovat na externí síťové úložiště pro dlouhodobou archivaci a zpětně obnovit uživatelem do kolektoru.
- Vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělenými do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH), včetně plné konfigurace grafů a pohledů uživatelem.
- Vizualizace výkonnostních metrik sítě.
- Generování statistik a podrobných výpisů nad volitelnými časovými intervaly s volitelnými filtry. Různé formáty výstupů, minimálně PDF, CSV.
- Předdefinovaná sada reportů s možností plné konfigurace uživatelem. Reporty dostupné prostřednictvím webového uživatelského rozhraní, ve formátu PDF nebo CSV. Automatická distribuce reportů e-mailem nebo na na externí síťové úložiště.
- Pro přizpůsobení výstupů je možno filtrovat data s využitím libovolných atributů flow statistik vč. L7 rozšíření nebo výkonnostních parametrů sítě. Filtry je možné kombinovat prostřednictvím logických spojek AND, OR, NOT. Výstupy je možné formátovat, zejména zahrnovat do zobrazení jednotlivé atributy flow záznamů nebo používat řazení (např. dle objemu přenesených dat, dle času nebo dle výkonnostních parametrů datové komunikace).
- Automatická notifikace v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, překročení definované relativní nebo absolutní prahové hodnoty, atd.) prostřednictvím emailu, SNMP trapu a syslogu, možnost automatického spuštění uživatelem definovaného skriptu.
- Možnost definovat si vlastní perzistentní pohledy na data, které budou systémem kontinuálně aktualizovány. K definici pohledu je možné použít libovolný filtr.
- Možnost dohledat každý jednotlivý datový tok (flow záznam).
- Podpora geolokace, možnost filtrovat na základě dané geografické lokality (státu/země).
- Dokumentované RESTful API pro získávání a zpracování dat, včetně úprav konfigurace (např. definice vlastních pohledů, reportů, apod.).
- Aplikace pro mobilní zařízení platformy Android a iOS, pro zobrazování základních informací v podobě grafů a statistik per jednotlivý uživatel.
- Monitorování dostupnosti zdroje flow dat pomocí SNMP.
- Součástí je agent SNMP pro možnost monitoringu funkce samotného kolektoru.

2. SESTAVA MODULÁRNÍ BEZPEČNOSTNÍ SONDA:

- 1 ks Modul **Sonda Netflow** (požadované vlastnosti jsou popsány níže)
- 2 ks Modul **Optický rack mount TAP** (požadované vlastnosti jsou popsány níže)
- 4 ks Modul Optický převodník SFP+, 10Gbase-LR, singlemode, 1310 nm, 10 km, LC
- 4 ks Modul Optický propojovací kabel, singlemode 09/125, duplex, délka 2 m, konektory SC-LC
- 2 ks Modul Optický propojovací kabel, singlemode 09/125, duplex, délka 5 m, konektory SC-SC

VLASTNOSTI MODULŮ:

Sonda Netflow

Sonda NetFlow je zařízení, které generuje statistiky o provozu na počítačové síti. Je nezbytné, aby sonda jako zdroj NetFlow dat byla nezávislá na použité síťové infrastruktuře a svou funkcí nijak neovlivňovala sledovanou síť. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Vytváření síťových statistik musí být prováděno autonomními, nezávislými a k tomuto účelu navrženými zařízeními.

Požadované parametry:

- 1U rack mount zařízení, snadná instalace do stávající síťové infrastruktury, nezávislost na stávající síťové infrastruktuře, pasivní zařízení – neviditelné z pohledu vrstev L2,L3
- dva plnohodnotné administrativní porty 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- vzdálená správa výhradně přes zabezpečené protokoly SSH, HTTPS,
- 4x monitorovací rozhraní 10Gb/s SFP+,
- výkon minimálně 5 miliónů paketů za sekundu na každém portu,
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik, podpora monitorování MAC adres,
- podpora vzorkování na úrovni paketů i toků,
- podpora filtrování a export datových toků na základě AS,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- subsystém vzdálené správy s vyhrazeným Ethernet portem a plnou a časově neomezenou podporou přístupu na grafickou konzoli serveru. Subsystém vzdálené správy musí být funkční bez ohledu na stav operačního systému serveru. Je požadována kompatibilita s IPMI 2.0.
- vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance),
- podpora standardů NEL a NSEL, monitorování MAC adres,
- podpora pro příjem a analýzu informací o detekovaných aplikacích dle NBAR2 standardu,
- podpora pro příjem a analýzu HTTP provozu – včetně položek typu URL, hostname,
- podpora pro příjem a analýzu provozu DNS,
- podpora pro příjem a analýzu VoIP statistik (jitter, latence, ztrátovost),
- podpora pro příjem a analýzu SMB provozu,
- podpora pro příjem a analýzu DHCP provozu,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky. Základní správa prostřednictvím příkazové řádky.
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- podpora autentizace vůči LDAP (Active Directory)
- monitorování výkonových parametrů sítě (Network Performance Monitoring – NPM)

Schopnosti sondy z pohledu vyhodnocení dat:

- podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace,
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami,
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD,
- podpora geolokace na základě IP adresy,
- top N statistiky, vytvářeni profilů, pokročilý reporting (online, email, pdf, csv…), grafy, dashboardy
- pokročilý alerting definovaných událostí (email, SNMP Trap, syslog),
- řízení uživatelského přístupu.

Specifikace monitorovacího systému:

- ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5, NetFlow v9, IPFIX),
- specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9, IPFIX) včetně pokročilých funkcí filtrování exportů, rozpoznávání aplikací, extrakce informací o http a SIP provozu a sledování performance metrik (server response time, jiter, round trip time, delay)
- možnost ukládání statistik IP toků na vestavěném kolektoru v rámci sondy,
- plná zákaznická podpora v českém jazyce a české uživatelské rozhraní,
- podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s
- monitorování rozšířených informací L3/L4, umožňujících detekci NATů (TTL, TCP Window size, TCP SYN packet size).
- sonda umožňuje rozšíření o funkcionalitu záznamu provozu v plném rozsahu na základě uživatelem definovaného pravidla záchytu. Rozšíření je řešeno formou licence/instalace SW bez nutnosti změny HW konfigurace.

Optický rack mount TAP

Optický TAP je rozbočovačem sítě, který je pasivní a nepředstavuje žádnou hrozbu pro stabilitu provozu. Je snadno instalovatelný, bezchybový a neviditelný v síti. Je pasivní a bez elektrického napájení nepředstavuje bod selhání.

TAP musí směřovat část signálu z linky do nástrojů pro monitoring provozu při maximálních rychlostech. Musí kopírovat všech 7 vrstev ISO/OSI. Musí nabízet kvalitní a cenově efektivní řešení pro rozbočení sítě pro IDS (bezpečnost), SNMP (řízení), RMON (vzdálená správa) a analýzu protokolu.

Požadované parametry:

- Architektura: rack mount TAP
- Konektory: SC
- Režim provozu: Single mode
- Single Mode: vlnové délky 850/1300 nm 1310/1550 nm
- Maximální průchozí ztráty (dB): 2.0/6.1
- Dělicí poměr: 70:30
- Dělící poměr se může měnit maximálně o: 3-4%
- Maximální velikost zařízení: 113 x 88 x 30 mm