Príloha k Špecifikácii Doplnkovej služby k službe Business CityNET

Rozsah služby Desktop Management

Služba **Desktop Management** poskytuje kompletné riešenie pre monitorovanie dátovej sieťovej komunikácie desktopov (PC, NTB, laptop,...) v centrále sieti VUCNET TTSK využívajúc systém **InveaTech FlowMon**. Tento systém umožňuje:

- Získať detailný prehľad o dátovej komunikácii v monitorovaných bodoch LAN siete TTSK. FlowMon systém je možné "pripojiť" do ľubovoľného bodu siete TTSK a získať prehľad o dátovej komunikácii v tomto uzle.
- Rýchlo identifikovať a riešiť potenciálne problémy v dátovej sieti ako je napríklad momentálne preťaženie siete.
- Sledovať vyťaženie LAN siete TTSK a pripojených organizácii na MPLS sieti.
- Zvýšiť celkovú bezpečnosť siete TTSK (možnosť odhalenia vnútorných aj vonkajších útokov). Systém umožňuje napríklad detekovať infikované pracovné stanice, ktoré vykazujú neprimeranú sieťovú aktivitu.
- Detekovať anomálie dátovej komunikácie v sieti TTSK (musí byť aktivovaný ADS modul).
- Efektívne a podľa reálnej potreby plánovať kapacitu LAN siete a prípojných bodov do siete Internet, Govnet a podobne.
- Monitorovať využívanie siete zo strany užívateľov úradu a pripojených organizácii.

Riešenie FlowMon zahŕňa:

1. Autonómne neinvazívne FlowMon sondy, ktoré generujú štatistické informácie o sieťovej prevádzke
2. FlowMon kolektory pre uchovávanie a ukladanie dát, ich vizualizáciu a následné analýzy týchto informácií
3. Doplnkové moduly pre network behaviorálnu analýzu (ADS) a monitoring výkonnostných parametrov aplikácií (APM).

Výhody FlowMon riešenia

Monitorovanie sietí na základe IP tokov prináša mnoho výhod a zníženie finančných nákladov na správu sietí pre všetkých – malé, stredné a veľké firmy, vládne organizácie, akademické organizácie a i poskytovateľov internetu (ISP). Nasadenie riešenia FlowMon založeného na technológii NetFlow Vám umožní:

- Znalosť o sieti kedykoľvek a na akomkoľvek mieste siete
- Monitorovanie sieťovej prevádzky v reálnom čase
- Zvýšenie bezpečnosti siete a možnosť odhalenia vnútorných aj vonkajších útokov
- Analyzovanie dlhodobých štatistík s rozlíšením na jednotlivé počítače, aplikácie a komunikácie
- Efektívne plánovanie kapacít siete
- Rýchle a presné riešenie problémov na sieti
- Rozpoznanie anomálií ako napr. botnety alebo DDoS útoky
- Získavanie prehľadných výpisov o sieťovej prevádzke
- Jednoduché plánovanie a monitorovanie QoS
- Kontrola peeringu a dohôd o kvalitách služieb (SLA)
- Účtovanie a fakturácie na základe prenesených dát
- Detailné sledovanie užívateľov a služieb

FlowMon vlastnosti

a) Kompletné riešenie pre monitorovanie sieťovej prevádzky, sieťových prvkov a sieťových služieb v reálnom čase
b) Unikátne výhody pre všetky časti organizácie – bezpečnostných inžinierov, sieťových a aplikačných administrátorov, CIO…
c) Vysokorýchlostné spracovanie všetkých dát bez straty paketu pri rýchlostiach od 1Gbps do 100Gbps

d) Najlepší pomer cena/výkon v danom odvetví
e) Jednoduchá neinvazívna implementácia do existujúcej sieťovej infraštruktúry (nezávislá na výrobcovi sieťových prvkov)
f) Jednoduché a intuitívne webové rozhranie pre všetkých – administrátorov, bezpečnostných špecialistov a manažérov
g) Škálovateľná architektúra – vysoko výkonné sondy a kolektory, pluginy pre doplnkové funkcionality
h) Využitie štandardov NefFlow v5/v9 a IPFIX

FlowMon sonda

FlowMon sonda je vysoko výkonné stand-alone fyzické zariadenie, ktoré monitoruje sieťovú prevádzku a generuje štatistiky o IP tokoch (Flows). Tieto štatistiky sú následne exportované na FlowMon kolektor, ktorý ich uchováva a analyzuje prostredníctvom FlowMon monitorovacieho centra, resp. inou kompatibilnou NetFlow/IPFIX aplikáciou. IP toky vytvorené FlowMon sondami obsahujú informácie o tom, kto komunikoval s kým, ako dlho, akým protokolom, koľko preniesol dát a celú radu ďalších informácií zo záhlavia paketu (TCP príznaky, QoS, AS). FlowMon sonda podporuje export dát vo fixnom formáte NetFlow 5, či flexibilných formátoch NetFlow 9 a IPFIX, u ktorých je možné priamo zvoliť, aké informácie sa majú monitorovať a exportovať. FlowMon sondy umožňujú monitorovať aj položky vyšších vrstiev (L5-L7), ako sú HTTP informácie (URL, hostname), VoIP štatistiky (latencia, jitter, straty paketov) či priamo realizovať detekciu aplikácií (NBAR2 štandard) a merať výkonnostné parameter siete (NPM). Vďaka tomu prináša nielen základný prehľad o objemoch sieťovej prevádzky, ale aj detailné informácie o dianí v počítačových sieťach vhodné pre riešenie sieťových problémov (troubleshooting), analýzu výkonu siete (performance monitoring), správu a optimalizáciu siete a v neposlednom rade i zvýšenie jej bezpečnosti.
NetFlow dáta exportované FlowMon sondou sú určené pre spracovanie FlowMon kolektorom . Kolektor poskytuje zber NetFlow dát (i z viacerých zdrojov a sond) a umožňuje používateľovi zobraziť a analyzovať sieťové štatistiky. Každá sonda obsahuje vstavaný kolektor o kapacite 0,5 TB.

FlowMon kolektory (Collectors)

FlowMon kolektor je fyzické jednoúčelové zariadenie určené pre dlhodobé ukladanie, zobrazovanie a analýzu sieťových tokov vo formátoch NetFlow/IPFIX/sFlow a ďalších. FlowMon kolektor umožňuje používateľom presne, rýchlo a efektívne riešiť problémy v sieti, zvýšiť jej bezpečnosť vďaka detekcii vnútorných a vonkajších útokov, predchádzať incidentom, optimalizovať sieť a znižovať prevádzkové náklady. FlowMon kolektor je schopný zbierať NetFlow z iných zariadení v dátovej sieti (routre, switche, sensory, sondy). Odporúčané je použiť zariadenia, ktoré sú schopné generovať plnohodnotné NetFlow 9 / IPFIX a ich funkcionalitu otestovať s riešením FlowMon.
FlowMon kolektor prináša kompletný prehľad o dianí v sieti vo forme dlhodobých grafov s možnosťou voľby perspektív, TOP štatistík o užívateľoch, službách a komunikáciách, užívateľsky definovaných profiloch, možnosti zobrazenia dát až na úroveň jednotlivých komunikácií a mnoho ďalšieho. Poskytuje tak plnú sadu informácií pre monitorovanie a reportovanie o sieťovej prevádzke vrátane notifikácií v prípade definovanej udalosti. Funkčnosť FlowMon kolektoru je možné ďalej rozšíriť o systém FlowMon ADS (technológia NBA/NBAD) pre automatickú detekciu bezpečnostných a prevádzkových anomálií, o FlowMon APM (Application Performance Monitoring) na meranie výkonnostných parametrov aplikácií.

FlowMon Anomaly Detection System (ADS)

FlowMon ADS je riešenie prinášajúce nový rozmer využitia štatistík o prevádzke dátovej siete (NetFlow, IPFIX, jFlow, NetStream). Vďaka unikátnej technológii tzv. behaviorálnej analýzy (Network Behavior Analysis) je možné identifikovať hrozby, ktoré prekonali zabezpečenie do perimetru, boli zavlečené do dátovej siete iným spôsobom, alebo pre ne doposiaľ neexistuje signatúra. Automatická detekcia bezpečnostných incidentov, anomálií prevádzky dátovej siete a konfiguračných problémov výrazne zjednodušuje správu dátovej siete, zvyšuje jej bezpečnosť a umožňuje proaktívne identifikovať príčiny problémov.

Hlavné výhody:

FlowMon ADS automaticky identifikuje rôzne bezpečnostné a prevádzkové problémy, anomálie alebo neočakávané správanie sa používateľov:

- Útoky (scan portov, slovníkové útoky, DoS, Telnet, APT, Zero Day)
- Anomálie prevádzky (DNS, multicast, vysoká variabilita komunikácie, VoIP)
- Anomálie chovania IP adries (zmena profilu chovania)
- Nežiaduca aplikácia (P2P siete, on-line komunikátory, TOR, TeamViewer)

- Malware (víry, spyware, botnety, komunikácie s adresami na blacklistoch)
- Pošta (odchádzajúci SPAM, nelegitímne poštovné servery)
- Prevádzkové problémy (oneskorenie, preťaženie, reverzné DNS záznamy, výpadky služieb)
- Potenciálne úniky dát (upload na verejné servery, webové úložiská)
- Porušenie bezpečnostných politík (obchádzanie proxy serverov, neznáme zariadenia)
- Špecifické metódy (sledovanie senzorovej siete)

FlowMon Application Performance Monitoring (APM)

FlowMon APM je riešenie, ktoré bez inštalácie agentov či rekonfigurácie serverov monitoruje aplikácie z pohľadu ich používateľov. Pre všetkých používateľov, všetky používateľské transakcie a v reálnom čase poskytuje podrobné informácie o skutočnej výkonnosti aplikácií. Vďaka využitiu architektúry riešenia FlowMon je možné APM nasadiť v jednotkách minút a začať transparentne monitorovať kritické podnikové alebo zákaznícke aplikácie na báze HTTP/HTTPS.

Hlavné výhody:

- Detailný pohľad na výkon HTTP/HTTPs aplikácie
- „Správanie sa“ aplikácií jednotlivým užívateľom
- Identifikácia problémov skôr, než ju ohlási používateľ
- Identifikácia príčin výkonnostných problémov
- Meranie reálnej doby odozvy a chovania sa aplikácie
- Poskytovanie „tvrdých dát“ pre upg. HW
- Monitoring užívateľských transakcií v reálnom čase bez nutnosti inštalácie SW, tzv. „AGENTLESS“
- Riešenie zahŕňa inštaláciu, nastavenie a zaškolenie

V rámci zriadenia služby budú dodané nasledovné zariadenia:

Názov	počet
FlowMon Probe 40000 SFP+	1
Gold support 1y: IFP-40000-SFP+	3