10 Doplnění redundantní Blue Coat proxy

Aktuálně používáme dvojici proxy bran od společnosti BlueCoat. Jedna z těchto bran je již mimo podporu výrobce. Interní informace Očekáváme jeho náhradu za novější model SG-400-20 nebo vyšší model. Licence budou převedeny z původního zařízení Interní informace na nové zařízení SG-400-20. Stávající zařízení Interní informace bude sloužit jako záložní pro případ výpadku nově dodané primární proxy v automatickém HA módu.

Očekáváme nejen fyzickou dodávku zařízení, ale i jeho konfiguraci dle bezpečnostních standardů (vycházejích z požadavků zákona č. 181/2014 Sb., Zákon o kybernetické bezpečnosti a souvisejících předpisů, dále jen ZKB) a „best practice“. Základem nové konfigurace bude nastavení původní brány Interní informace. Konfigurace bude rozšířena o logování do centrálního logovacího nástroje. Zde se očekává taková úroveň logovaní, aby byla v souladu s požadavky dle ZKB. Vlastní implementace musí zajistit redundanci provozu s původní proxy bránou.

Dále se očekává rozšíření stávající konfigurace o řadu vlastností a funkcí, které jsou uvedeny v tabulce níže.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| Blue Coat SG-400-20 nebo vyšší model | 1ks |  |
| Převedení celé konfigurace z původního zařízení | ANO |  |
| Rozšíření stávající konfigurace o dešifrování SSL provozu | ANO |  |
| Rozšíření stávající konfigurace o řízení šířky pásma pro vybraný typ provozu (např. video, zvuk) | ANO |  |
| Rozšíření stávající konfigurace o inspekci veškerého webového provozu koncových zařízení | ANO |  |
| Rozšíření stávající konfigurace o hodnocení typu obsahu (YouTube) | ANO |  |
| Rozšíření stávající konfigurace o inspekce dle typu webové aplikace (např. Google Docs) a použité metody přenosu (GET, POST) | ANO |  |
| Rozšíření stávající konfigurace o integraci se sandbox appliances | ANO |  |
| Rozšíření stávající konfigurace o řízení aplikací a protokolů, které mají povolen internetový provoz. A to i na základě velikosti a typu stahovaného souboru. | ANO |  |
| Konfigurace časové synchronizace vůči NTP | ANO |  |
| Konfigurace SNMP pro monitoring z PRTG dohledu | ANO |  |
| Vytvoření politik pro zavedení výjimek k definovaným pravidlům pro všechny uživatele, určitou skupinu AD, konkrétní uživatele apod. | ANO |  |
| Vyžadujeme od nasazeného řešení možnost trasování provozu konkrétního uživatele | ANO |  |
| Požadujeme samostatné fyzické porty pro provoz a pro „out of band“ management | ANO |  |
| Zajištění přenosu nastavených pravidel na záložní zařízení | ANO |  |
| PoC pro nově konfigurované vlastnosti | ANO |  |
| Zahoření a hardening zařízení dle „best practice“ | ANO |  |
| Low level a high level design řešení | ANO |  |
| Fyzická instalace | ANO |  |
| Vytvoření konfigurace pro zajištění vysoké dostupnosti | ANO |  |
| Nastavit logování do centrálního logovacího nástroje, pro zaznamenávání KBU a KBI v souladu s aktuálními požadavky VKB. | ANO |  |
| Počet zdojů AC pro jedno zařízení | 2 |  |
| Podpora výrobce na HW a SW komponenty | 5 let |  |
| Nasazení reportovacího nástroje pro analýzu provozu s daty za poslední týden a možností zobrazení archivu 6 měsíců | ANO |  |

# Centrální management pro bezpečnostní prvky Symantec

Nástroj pro správu a inventarizaci Symantec Proxy SG appliancí a Sandbox appliancí. Hlavním cílem je zajištění kompletní synchronizace konfigurací mezi dvojící Symantec Proxy SG a dvojící SandBox zařízení.

Očekáváme nejen fyzickou dodávku softwaru, ale i jeho konfiguraci dle bezpečnostních standardů (vycházejících z aktuální verze VKB) a „best practice“. Implementací je míněno vytvoření low level, high level designu, vlastní konfigurace, provozu v testovacím režimu a akceptačních testů.

Podpora aplikací a i veškeré potřebné licence v rámci dodávky musí být minimálně na 5 let.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| Požadujeme licenci minimálně pro 10 spravovaných zařízení | ANO |  |
| Návrh a provedení akceptačních testů | ANO |  |
| Low level a high level design řešení | ANO |  |
| Fyzická instalace | ANO |  |
| Provedení formou virtuální appliance do VMware ESX 6.0 nebo vyšší | ANO |  |
| Inventarizace a management zařízení | ANO |  |
| Kontrola stavu a monitoring spravovaných zařízení | ANO |  |
| Výkonové statistiky | ANO |  |
| Zálohování a obnova | ANO |  |
| Management licencí | ANO |  |
| Řízení politik a jejich aplikace | ANO |  |
| Konfigurace a synchronizace zařízení | ANO |  |
| SW podpora včetně updatu a upgrade a licence minimálně na 5 let | ANO |  |
| Integrace Centrálního Managementu se stávajícími emailovou branou Symantec Interní informace | ANO |  |
| Integrace se Symantec Proxy SG, vytvoření potřebné konfigurace, nastavení synchronizace konfigurace mezi Proxy SG | ANO |  |
| Integrace se SandBox zařízeními, vytvoření potřebné konfigurace, nastavení synchronizace konfigurace mezi SandBoxy | ANO |  |
| SW podpora včetně implementace a veškeré potřebné licence musí být minimálně na 5 let | ANO |  |