# 11 Doplnění SandBox funkcionality k webovým, mailovým branám Symantec a k Symantec EndPoint Protection

Aktuálně používáme dvojici proxy bran od společnosti Symantec. Tyto zařízení běží dle těchto požadavků:

* Licence pro 400 uživatelů
* Inspekce webového provozu na základě pravidel definovaných v administraci systému
* Antivirová kontrola Interní informace
* Vysoká dostupnost řešení
* Používá reputační databáze
* Propustnost mají minimálně 150 Mbps

Stávající web proxy brány chceme rozšířit o dvojici zařízení, které zajistí SandBox funkcionalitu pro webovou, mailovou komunikaci a u koncových stanic. Dodaná zařízení musí být plně kompatibilní se stávajícími Symantec proxy branami. Interní informace

Očekáváme nejen fyzickou dodávku zařízení, ale i jeho konfiguraci dle bezpečnostních standardů (vycházejích z aktuální verze VKB) a „best practice“. Implementací je míněno vytvoření low level, high level designu, vlastní konfigurace, začlenění do infrastruktury, provoz v testovacím režimu a akceptační testy.

Podpora fyzických zařízení, SW komponent a i veškeré potřebné licence v rámci dodávky musí být minimálně na 5 let.

| *Požadavek na funkcionalitu* | *Minimální požadavky* | *Splněno: ANO / NE / Hodnota* |
| --- | --- | --- |
| *Zahoření a hardening zařízení dle „best practice“* | *ANO* |  |
| *Návrh a provedení akceptačních testů* | *ANO* |  |
| *Low level a high level design řešení* | *ANO* |  |
| *Fyzická instalace* | *ANO* |  |
| *Minimální počet malware vzorků za 24 hodin: 12000* | *ANO* |  |
| *Plnou kompatibilitu se stávajím řešením Symantec* Interní informace | *ANO* |  |
| *Podpora výrobce na 5 let* | *ANO* |  |
| *Licence na veškeré potřebné funkce na 5 let* | *ANO* |  |
| *Lokální SandBox bez nutnosti odesílání vzorků do cloudu* | *ANO* |  |
| *Vysokou dostupnost řešení (dvojice zařízení)* | *ANO* |  |
| *Minimálně 2ks 500 GB harddisků* | *ANO* |  |
| *Dva redundantní hot swap AC zdroje* | *ANO* |  |
| *Minimálně jeden management metalický port 1000Base-T* | *ANO* |  |
| *Minimálně jeden metalický port 1000Base-T pro kontrolovaný provoz* | *ANO* |  |
| *Licence na Malware Analýzu na 5 let* | *ANO* |  |
| *HW a SW podpora včetně updatu a upgrade na 5 let včetně implementace* | *ANO* |  |
| *Microsoft licence pro provoz v SandBoxu* | *ANO* |  |
| *Emulační SandBox - emulace prostředí OS Windows a detekci malware v něm* | *ANO* |  |
| *Virtualizační SandBox - konfigurovatelné profily, v kterém je provede replikace prostředí zákazníka.* | *ANO* |  |
| *SandBox pro prostředí OS Android* | *ANO* |  |
| *Kombinace statické a dynamických technik pro analýzu malware* | *ANO* |  |
| *Reputační filtry pro detekci malware* | *ANO* |  |
| *Automatická aktualizace nových hrozeb z globální databáze výrobce minimálně 1x za 24 hodin* | *ANO* |  |
| *Realtime sandboxing pro detekci a blokování malware* | *ANO* |  |
| *Generování verdiktů, včetně analytických artefaktů* | *ANO* |  |
| *Detekce generických exploitů* | *ANO* |  |
| *Podpora libovolných PC formátů* | *ANO* |  |
| *Detekce jedinečných i polyformní URL, které odkazují na cílové hrozby* | *ANO* |  |
| Interní informace | *ANO* |  |
| *Integrace SandBox bran se stávajícími emailovou bránou Symantec* Interní informace | *ANO* |  |
| *Přímá integrace SandBox bran se Symantec Endpoint Protection Manager* | *ANO* |  |
| *Přímá integrace SandBox bran se Symantec Proxy SG* | *ANO* |  |
| *Přímá integrace s centrálním managementem Symantec Management Center* | *ANO* |  |