PODROBNÁ TECHNICKÁ SPECIFIKACE

k veřejné zakázce zadávané podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění

Multifunkční informační a komunikační systém Nemocnice Prachatice a.s.

část 8 - Filtrace webového provozu pro bezpečný a efektivní Internet

Zadavatel:	Nemocnice Prachatice, a.s.	IČO:	260 95 165
Spisová značka:	B 1461 vedená u Krajského soudu v Českých Budějovicích	Den zápisu:	30. září 2005
Sídlo:	Prachatice, Nebahovská 1015, PSČ 383 01		
Zastoupený:	Ing.Michalem Čarvašem, MBA, předseda představenstva MUDr. Františkem Stráským, členem představenstva		

Termín plnění této části veřejné zakázky – 30 dní

Dodávané řešení pro filtraci webového provozu musí splňovat následující technické specifikace:

SHRNUTÍ

- řešení řadící se do kategorie Internet Security Gateway
- kontrola webového provozu pro cca 250 uživatelů doménové sítě
- nastavení bezpečného a efektivního přístupu na internet pro uživatele
- nastavení firemních procesů (kdo kam může) a nastavení bezpečnostní politiky podle šablon skupin pracovního zařazení uživatele
- kategorizace nově navštívených webů dodavatelem řešení a jejich následná implementace do filtrování - aktualizace webového filtru
- kategorizace uživatelů – uživatel, skupina, team, stanice, typ zařízení, síť apod.
- nastavení prevence proti zavlečení škodlivého kódu
- omezení zneužívání internetu k nepracovním aktivitám uživatelů
- detailní reporting a statistiky pro manažerské řízení
- centrální správa a kontrola webového provozu
- inspekce protokolů http, https, ftp
- možnost provozu jako virtuální appliance na Microsoft Hyper-V 2012 R2 a vyšší

PODROBNÝ POPIS

1. POŽADOVANÉ ŘEŠENÍ

Řešení ve formě hw nebo sw appliance aplikované na výstupu z LAN do Internetu. Nastavení webového filtru porovná zařazení uživatele, který vysílá požadavek na internetový provoz (např. dle jeho pracovní pozice, která má přiřazené skupiny a k nim přiřazená firemní pravidla co je povolené) a podle toho internetový požadavek povolí nebo zakáže. Zamezí se tím zneužívání internetu k nepracovním aktivitám uživatelů, zbytečného vytěžování šířky pásma a několika násobně se zvýší ochrana před zavlečením škodlivého kódu do firemní LAN. Bude poskytovat monitoring a reporting internetového provozu v reálném čase s možností kategorizace vyžadovaných webů, služeb apod.

2. SPRÁVA PROVOZNÍCH DAT A MONITOROVÁNÍ

V hlavní správě dodávaného řešení se budou vytvářet a spravovat jednotliví uživatelé (propojení LDAP), skupiny uživatelů, skupiny dle pracovního zařazení a šablony webů. Centrální správa (dashboard) bude poskytovat detailní přehled o veškeré komunikaci interní sítě LAN s internetem. Řešení bude možné administrovat ze systémů Windows i Linux. Součástí budou i statistiky přístupů a veškeré logy komunikace. Budou podporovány autentizační mechanizmy jako jsou Active Directory, Kerberos, LDAP, RADIUS, Basic, atd. Veškerá pravidla nastavení budou vázána na konkrétního uživatele nebo skupinu uživatelů. Pro jednotlivé pracovní týmy nebo pozice bude možné stanovit různé politiky přístupů.

3. WEBOVÝ FILTR A FILTRACE

Přístup uživatelů na internet bude efektivně řízen webovým filtrem. Ten bude pracovat na základě katalogu www stránek, které uživatelé skutečně navštěvují. Databáze bude neustále aktualizovaná o uživateli nově navštěvované stránky. Dodavatel řešení, bude v rámci licence nové záznamy v databázi třídit a kategorizovat do příslušných skupin. Systém tak umožní s vysokou přesností blokovat stránky s nebezpečným či nevhodným obsahem a nastavit účinná pravidla bezpečného přístupu na internet. Bude možné vytvořit např. kategorie povolené, s upozorněním a zakázané. Těmto kategoriím bude možné přiřadit jednotlivé weby nebo skupiny / druhy webů. A následně křížově k těmto kategoriím přiřadit uživatele, skupinu uživatelů, zařízení, typ zařízení, síť apod.

4. REPORTING A MANAŽERSKÉ ROZHRANÍ

Bude možné generovat statistiky - detailní reporting včetně přehledných výstupů pro manažery. Reporting bude možné třídit a zobrazovat tak pouze záznamy, které bude potřeba skutečně analyzovat. Výsledky – reporting bude možné využít pro manažerské řízení - například při definici bezpečnostních politik i samotném řízení webového provozu.