

■ Websense Web Security Gateway



Az internet gyors fejlődésével a **Web 2.0 technológiák** drámaian megváltoztatták az emberek web használati szokásait. Ezen új technológiák egyrészt új lehetőségeket hoznak magukkal, másrészt eddig ismeretlen biztonsági kockázatok felbukkanásához vezetnek.

A kihívás

A múltban az internetes oldalak tartalma többnyire statikus volt és megjósolható. Nagyrészt webmesterek szabályozták a tartalmat, így a biztonsági termékek fejlesztői megbízhatóan el tudták különíteni a „biztonságos” oldalakat a „veszélyesektől”.

Manapság a **webtartalom dinamikus**: a végfelhasználók folyamatosan frissítik azok tartalmát, alkalmazásokat osztanak meg, és valós időben, összetett csatornákon kommunikálnak.

A **káros, rosszindulatú tartalom bárhol felbukkanhat - még az eddig megbízhatónak vélt oldalakon is**. Ezek a veszélyforrások új, eddig ismeretlen fenyegetésnek teszik ki a hálózatot, ezzel együtt pedig a céges információkat is.

A megoldás

A **Websense Web Security Gateway biztonságos web használatot** nyújt, miközben szabályozza a legújabb web-alapú eszközöket és alkalmazásokat.

A Websense Web Security Gateway **valós időben elemzi a web forgalmat, azonnal kategorizálja az új oldalakat és a dinamikus tartalmakat, felfedi a biztonsági kockázatokat, és blokkolja a veszélyes tartalmakat**, ide értve a távoli proxykat, a hacker oldalakat, felnőtt tartalmat, botneteket, keyloggereket, rejtett támadásokat, kémprogramokat és sok egyéb veszélyes tartalmat.

A Websense Web Security Gateway **betömi az új webtartalmak által generált biztonsági réseket**, képes terminálni a titkosítást, és ellenőrizni az SSL forgalmat, mielőtt a letöltött adatok elérik a belső hálózatot.

- A Websense Web Security Gateway valós időben azonosítja és blokkolja a rosszindulatú web tartalmat, mialatt a legitim tartalmat felismeri és hozzáférhetővé teszi
- Képesé tesz a Web 2.0 technológia biztonságos használatára
- Több, mint 120 protokoll figyelése és korlátozása, IM protokollok esetén akár küldött fájlok blokkolása is
- Tisztán látás: Webtartalom elemzése akár az SSL csatorna terminálásával, valós fájl típusok felismerésével
- Egyszerű kezelés: Egy intuitív felületen keresztül lehetséges az összes beállítás megadása és ellenőrzése, adatok riportolása

Technikai részletek:

- High Availability - támogatott a magas rendelkezésre állás
- Transzparens és explicit proxy működési mód
- Teljes értékű SSL proxy komplett tanúsítvány management rendszerrel
- Autentikáció: Active Directory, LDAP, RADIUS, Novell, NTLM v2

Rendszerkövetelmények:

- Operációs rendszer: Red Hat Linux v4, update 5* vagy Windows Server 2003
- CPU: 2 x Dual-core 2.8GHz processor
- RAM: 4GBHDD: 2 db: 100GB az op. rendszernek és az adatoknak, 100GB a cache-nek (RAID-1 javasolt)
- NIC: 2 db 10/100/1000 Mb/s