

WAC

Web Access Control

Napjainkban az informatikai rendszerek egyik leggyakoribb elérési útvonala a felhasználók számára a web-es felület. Így a legtöbb visszaélés is ezen keresztül történik.

A rengeteg féle böngésző és web szerver, megszámlálhatatlan számú applikáció és töménytelen adat közös és egyen szilárd védelme bonyolult feladatot jelent a rendszergazdák számára.

Erre a komplex problémára jelent kiváló, gyors és igen hatékony megoldást a WebAccessControl (WAC) megoldás. Helyezze el a WAC-ot a web szerver elé oly módon, hogy a kliensek azon keresztül érhék el a rendszert. Mivel a termék teljesen transzparens, így a webkiszolgálón és a klienseken sem kell további beállításokat végezni. A WAC konfigurálása után a rajta keresztül folyó forgalmat elemzi és a visszaéléseket, hibákat kiszűri. Ezzel egyaránt védve a klienseket és a web kiszolgálót a kompromittálódástól.

A WAC leggyakoribb felhasználási területei:

- publikus weboldalak védelme
- interaktív, web 2.0 és SOA alkalmazások védelme
- internet banki alkalmazások védelme
- nagyvállalati intranet rendszerek védelme
- Három rétegű alkalmazások frontend védelme

Protokoll konverzió

A WAC nem csak védelmi, hanem helyesbítési és fordító modulokkal is el van látva. Így ha szükséges, képes http 1.0 és http 1.1 protokollok közti fordításra is. Ha a böngésző szabálytalan kéréssel fordul a kiszolgálóhoz, vagy a kiszolgáló szabálytalan választ adna, azt a WAC korrigálja és képes a kommunikációt az internetes rfc-knek megfelelően lektorálni.

IP verziókezelés

A WAC nem csak a klasszikus IPv4, hanem a folyamatosan terjedő IPv6 protokoll kezelésére is képes. Használható olyan webes rendszerek kezelésére is, melyekben a kiszolgálói hálózat IPv6 protokollt használnak, míg publikus szolgáltatások IPv4 protokollon át érhetőek el.

Webforgalom gyorsítása

A WAC kibővített funkcionalitással képes a statikus web tartalmakat, képeket, szövegeket, videókat a gyorsítótárból kiszolgálni, így csökkentve a web szerver terhelését.

Terheléselosztás

A WAC képes fürtözött web kiszolgálók esetén terhelésmegosztást végezni különböző algoritmusok alapján.

Titkosítás

A WAC képes SSL (Secure Socket Layer) terminálásra. Így a webszerverek más „clear html” kapcsolatot tudnak kezelni.

A projekt az Európai Unió Támogatásával valósult meg



MAGYARORSZÁG MEGÚJUL



Tulajdonságok:

Csoport	Specifikáció
Web Applikációs védelmek	<p>Teljes reverse proxy</p> <p>Monitor mode deployment</p> <p>Buffer overflow</p> <p>HTTP paraméter manipuláció, protokoll megfelelés</p> <p>Null byte blocking</p> <p>Bevitt adat normalizáció</p> <p>Válasz szűrés és felülírás</p> <p>Flexibilis tűzfal akciók</p> <p>Cookie és session befolyásolás</p> <p>Cross-site scripting (XSS)</p> <p>Command injection, SQL injection</p> <p>Titkosítás kikényszerítése</p> <p>Applikáció és szerverhiba üzeneteinek eltakarása</p> <p>Intelligens hibatűró szerverfarm, terheléselosztás</p> <p>Teljes körű URL átírás, átirányítás támogatás</p> <p>Válasz kikényszerítések</p> <p>Pozitív és negatív biztonsági modellek</p>
Adatátviteli biztonság	<p>Teljes SSL v2/3 és TLS támogatás</p> <p>FIPS 140-2 Level 3</p>
Támogatott cryptográfiák	<p>Beépített titkosítás támogatások:</p> <ul style="list-style-type: none"> • Advanced Encryption Standard (AES) • Data Encryption Standard (DES) • Triple DES (3DES) • Blowfish • RSA • Diffie-Helman • Digital Signature Algorithm (DSA) • Secure Hash Algoritmus 1 (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) és Message-Digest 5 (MD5)
Adminisztráció	<p>Vékony kliens alapú multiplatform adminisztrációs felület</p> <p>Command-line interfész (SSH)</p> <p>Simple Network Management Protocol (SNMP)</p> <p>Roles-based access control (RBAC)</p> <p>Központi biztonsági menedzsment támogatás (TCB)</p> <p>Konfigurációk, statisztikák és naplóállományok exportja és importja</p>
Naplózás, monitorozás és audit	<p>Syslog és üzenet és event logs</p> <p>Forgalom és szolgáltatási szint (SLA) monitorozás és riport</p> <p>Riasztások és események monitorozás, statisztika</p>

A gyártó a változtatás jogát fenntartja.

az Ön WAC partnere: