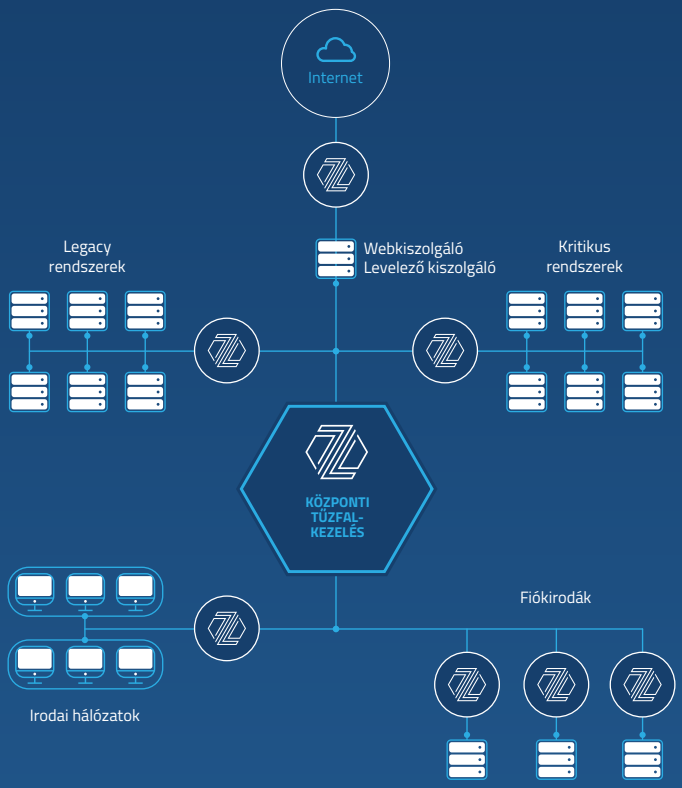
BALASYS

Zorp Gateway

Rugalmas védelem vállalati hálózatok számára

„...téves elképzelés azt feltételezni, hogy a biztonság egy egyszerű tűzfal megvásárlásával garantálható."
— Art Wittmann



A hálózat mélységi védelme a Zorp Gateway használatával

A hálózatbiztonság a tűzfalaknál sokkal többet jelent

A felhőalapú alkalmazások, a mobilitás és a saját eszközök használata (BYOD) miatt a hálózati határpontok (a vállalati tűzfalak eredeti helye) nehezen behatárolható területté váltak. A fejlettebb támadások ma már könnyedén megkerülik a hagyományos határvédelmet.

A mai vállalati hálózatoknak több száz kritikus fontosságú alkalmazást kell kiszolgálniuk, valamint megfelelően rugalmasnak kell lenniük, hogy a gyorsan változó üzleti fejlesztéseket támogassák – mindeközben meg kell akadályozniuk a kibertámadásokat, továbbá biztosítaniuk kell a megfelelőséget. Ennek eredményeként az ilyen rendszereket szabályozó biztonsági házirendek soha nem látott méretűvé és bonyolultságúvá váltak, ezért egyre nagyobb szükség van rugalmas hálózatbiztonsági megoldásokra.

Megfelelés az egyedi biztonsági követelményeknek

Az előkonfigurált tűzfalak és UTM-ek a testreszabott házirendek terén meglehetősen korlátozottak. Ha kizárólag egy újgenerációs tűzfal szolgáltatásaira hagyatkozik, vállalata lemaradhat a versenytársaitól, mivel nem tudja megfelelő gyorsasággal kiszolgálni a speciális üzleti igényeket. Biztonsági vezetőként egyéni hálózatbiztonsági követelményeknek is meg kell felelnie, ellenkező esetben rossz kompromisszumokat kell kötnie a hatékony üzleti folyamatok és az elvárt biztonsági szint között. Szerencsére azonban van megoldás.

Zorp Gateway

A Zorp Gateway olyan kiemelten rugalmas, többcélú biztonsági átjáró, amellyel precízen szabályozható a vállalati hálózatok forgalma a belső és külső támadások elleni védelem érdekében. A Zorp Gateway lehetővé teszi a normál és a titkosított hálózati kommunikáció részletes vizsgálatát, továbbá a forgalom szűrésére és módosítására is képes. Rugalmas architektúrájának és szkriptelhető konfigurációjának köszönhetően vállalata speciális hálózatbiztonsági problémákkal is megbirkózhat, illetve képes lesz BÁRMILYEN biztonsági házirend implementálására.

Mire alkalmas?

- Kritikus rendszerek szeparálása
- Legacy rendszerekkel való kompatibilitás biztosítása
- Vállalati tűzfal
- Webalkalmazás tűzfal (WAF)
- Mélységi védelem – Holisztikus tűzfal grid
- Malware-észlelés
- Forgalomtitkosítás és -visszafejtés
- Speciális hálózatbiztonsági projektek

Technikai előnyök

- Több mint 20 protokoll és azok csatornáinak felügyelete
- „Best match" alapú szabály-kiértékelés
- LDAP/AD, Kerberos és RADIUS támogatás
- Erős hitelesítés (S/Key, SecurID, X.509 stb.)
- Licenc- és tanúsítványkezelés
- TLS 1.3 támogatás
- IPSec és OpenVPN
- AV/sandbox, IDS/IPS, DLP és SIEM integráció

*A **Zorp Gateway** egy transzparens, alkalmazásszintű proxy átjáró, amely a világ első, moduláris proxy-technológiájára, a 20 éves fejlesztői múlttal rendelkező Zorp hálózatbiztonsági keretrendszer képességeire épül.*

Funkciók

VÁLLALATI HÁLÓZATOK EGYSZERŰ MODELLEZÉSE

A Zorp Gateway használatával építőkocka szerűen modellezheti le a hálózatát, így nem kell rögzítenie a hálózat minden apró részletét a biztonsági szabályrendszerben. Ezzel az egyedi képességgel nagy mértékben leegyszerűsíthető a szabályok adminisztrációja, valamint a hálózati módosítások és migrálási projektek végrehajtása.

RÉSZLETES PROTOKOLLVIZSGÁLAT

Az UTM-ek mintázat megfeleltetésével ellentétben a Zorp Gateway az alkalmazásproxy szintjén kezeli a hálózati kapcsolatokat. Ez azt jelenti, hogy az átvitt információk teljes egészében elérhetők az eszközön, amely részletes protokollvizsgálatot és -validálást tesz lehetővé. Az átjáró ismeri a protokollok tulajdonságait, és elutasítja azokat, amelyek nem felelnek meg az előírásoknak.

ÁTFOGÓ TITKOSÍTÁS

A Zorp Gateway teljes körű felügyeletet biztosít a TLS-titkosítású (korábban SSL) csatornák felett. Ez a képesség védettséget biztosít a veszélyes webhelyek és e-mailek ellen akkor is, ha azok titkosított csatornán keresztül érkeznek. Emellett a nem titkosított vagy legacy internetprotokollok titkosítását is támogatja.

A FORGALOM MÓDOSÍTÁSA

A Zorp Gateway képes a forgalom bizonyos elemeinek módosítására. Ezáltal lehetősége van az ügyféladatok vagy az érzékeny infrastruktúra információk elrejtésére, és a legacy alkalmazások biztonsági réseinek kezelésére. Például eltávolíthatja a forgalomból a hibás konfigurációból adódó hibaüzeneteket és bannereket, vagy a személyes adatokat (pl. bankkártyaszámok) az adatvédelmi előírásoknak való megfelelés érdekében.

SINGLE SIGN-ON

A Zorp Gateway single sign-on megoldásával egyszerűen integrálódhat az LDAP- és más hitelesítési szolgáltatásokkal. Az összes hálózati kapcsolat egyetlen hitelesítési szolgáltatáshoz kapcsolása nagy mértékben leegyszerűsíti a felhasználói hozzáférések kezelését, valamint a rendszerauditokat.

ROBOSZTUS KÖZPONTI FELÜGYELET

A Zorp Gateway vállalati szintű központi felügyeletet kínál a különböző hálózati zónákban vagy akár eltérő földrajzi helyeken található tűzfalak százainak kezeléséhez. A fejlett menedzsment GUI költséghatékony biztonságfelügyeletet biztosít a több fiókirodával rendelkező vállalatok számára.

RÉSZLETES AUDITNAPLÓZÁS

A Zorp Gateway jól testre szabható, alkalmazásszintű naplólétrehozási képességekkel rendlekezik. Az átjáró akár a titkosított forgalom naplózására is képes. A hálózati hibaelhárítás (debugging) és forenzikus vizsgálatok érdekében rendkívül részletes naplózást is beállíthat.

A Zorp Gateway előnyei

- Gyors alkalmazkodás a speciális üzleti igényekhez
- Könnyebb jogszabályi megfelelőség és adatvédelem
- Rugalmas és professzionális mérnöki csapat
- Egyedi hálózatbiztonsági problémák megoldása
- Rendkívül szigorú biztonsági követelmények implementálása
- Forradalmi proxytechnológia
- Magyar fejlesztés – „Tiszta” kódbázis
- Kedvező ár-érték arány

Bővebb információ

- A Zorp Gateway honlapja
- Próbaverzió igénylése
- Árajánlat kérése

BALASYS