1. **Transzparens, alkalmazásszintű proxy átjáró**
2. **Rugalmas és professzionális mérnöki támogatás**
3. **Gyors megoldás az egyedi hálózatbiztonsági problémák kezelésére**
4. **Rendkívül szigorú biztonsági szabványok bevezetése**
5. **Egyedi, proxy alapú technológia**
6. **Magyar fejlesztésű kódbázis – „Clean code"**
7. **Kiemelkedő biztonság**

PROXEDO
NETWORK
SECURITY

„...az a feltételezés, hogy a biztonság tűzfal megvásárlásával kezdődik és ezzel be is fejeződik, egyszerűen téves."

– Art Wittmann

PROXEDO NETWORK SECURITY

Nagyvállalati hálózatok rugalmas védelme

- Kritikus rendszerek elkülönítése és védelme
- Hálózati autentikáció
- Hálózat monitorozása és hibakeresés
- Többrétegű fenyegetésérzékelés
- Zero Trust biztonsági modell
- Hálózati adatvédelem és titkosítás
- Megfelelőség & audit

A hálózatbiztonsághoz nem elég néhány tűzfal

A felhőben futó alkalmazások, a távoli munkavégzés elterjedése és a felhasználók saját eszközeinek vállalati használata (BYOD) miatt elmosódtak a korábban élesen körülhatárolt hálózati végpontok, amelyek ezelőtt még jól védhetőek voltak egy vállalati tűzfallal. A hagyományos határvédelmi megoldásokat azonban ma már egy átlagosnál kicsit jobban képzett támadó is könnyedén megkerüli.

A digitalizációs kényszer hatására a vállalati rendszereknek több száz kritikus fontosságú alkalmazást kell folyamatosan kiszolgálniuk, miközben rugalmasan alkalmazkodniuk kell a folyamatosan változó üzleti követelményekhez hogy támogassák az innovációt. Mindezt úgy, hogy közben megelőzzék az egyre kifinomultabb kibertámadásokat és megfeleljenek az egyre komplexebb iparági és megfelelőségi szabványoknak. Emiatt az egyes vállalatok IT-biztonsági szabályzatai is egyre bonyolultabbá válnak, amelyek már rendkívüli mértékű rugalmasságot követelnek meg a hálózatbiztonsági megoldásoktól.

Egyedi biztonsági követelmények teljesítése

A hagyományos tűzfalak és UTM-ek csak korlátozottan tudnak megfelelni a vállalatok egyedi IT-biztonsági szabályzatainak. Ha egy vállalat kizárólag egy újgenerációs tűzfal szolgáltatásaira hagyatkozik, rugalmatlanná válik és mivel nem tudja kellő gyorsasággal kiszolgálni a speciális üzleti igényeket, lemarad a piaci versenyben. Az IT-biztonsági szakembereknek további, egyedi hálózatbiztonsági követelményeknek is meg kell felelniük, annak érdekében hogy megfelelően támogassák mind az üzleti folyamatokat, mind az elvárt biztonsági szintet.
Van olyan megoldás, amely minderre képes.

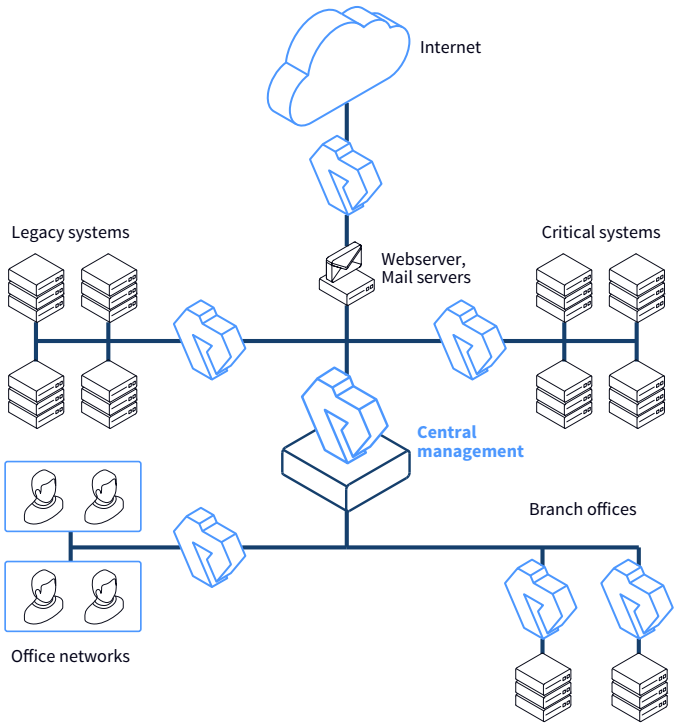
Proxedo Network Security

A PNS egy rendkívül rugalmas, többcélú biztonsági átjáró, amellyel a legapróbb részletekig ellenőrizhető a vállalati hálózati forgalom, így védelmet nyújt a legkifinomultabb belső és külső támadások ellen is. A PNS minden részletre kiterjedő mély csomagvizsgálatot (Deep Packet Inspection - DPI) biztosít a normál és a titkosított hálózati kommunikációban is, továbbá a forgalom szűrésére és a tartalom módosítására is képes. A PNS olyan rugalmas architektúrával és szkriptelhető konfigurációval rendelkezik, amellyel bármilyen szigorú IT-biztonsági szabályzattal rendelkező vállaltnál alkalmazható, a Zero Trust alapelveit is beleértve.

A PNS-t használó ügyfeleink olyan egyedi hálózatbiztonsági problémák megoldására képesek, amelyeket a tűzfalak nem képesek kezelni.

BALASYS

info@balasys.hu



A Proxedo Network Security architektúrája

TECHNIKAI ELŐNYÖK

- Több mint 15 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
- WAF és threat intelligence
- AV, sandboxing és URL-szűrés
- IDS/IPS, DLP, MFA és SIEM integráció

Bővebb információ

A PNS weboldala
Próbaverzió igénylése
Árajánlat kérése

BALASYS

Vállalati hálózatok egyszerű modellezése

A PNS használatával modulárisan, mintegy építőkockaszerűen modellezheti le a hálózatát, így nem kell kitérnie a hálózat minden apró részletére a biztonsági szabályzatban. Ezáltal a PNS-sel - egyedülálló módon - jelentősen leegyszerűsíthető a szabályzat adminisztrációja, valamint a hálózati módosítások és migrálási projektek végrehajtása.

Minden részletre kiterjedő protokoll ellenőrzés

A PNS proxy szinten kezeli a hálózati kapcsolatokat, ellentétben például a UTM-ekkel, amelyek kizárólag az előre definiált, már meglévő mintákat képesek felismerni. A hálózati kapcsolaton átmenő információk teljes egészében elérhetők az eszközön, amelyen részletes protokollvizsgálat és -validálás végezhető. Az átjáró felismeri az egyes protokollok tulajdonságait, és megszakítja a kapcsolatot azokkal, amelyek nem felelnek meg a sztenderd előírásoknak.

Átfogó titkosítás

A PNS teljes körű kontrollt biztosít az SSL/TLS-titkosítású csatornák felett. A gyakorlatban ez azt jelenti, hogy a PNS-t használó ügyfeleink még a titkosított csatornákon keresztül zajló email- és webes forgalmat is ellenőrízni tudják. Emellett a PNS támogatja a nem titkosított és a legacy kriptográfiai protokollok korrekt titkosítását is.

A forgalom módosítása

A PNS 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 PNS 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 PNS 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 PNS elősegíti, hogy minden fontos eseményről - ez testreszabható - készüljön naplófájl, akár az alkalmazások szintjén is. Az átjáró még a titkosított forgalom naplózására is képes. A PNS-sel a hálózati hibaelhárításhoz (debugging) és forenzikus vizsgálatokhoz rendkívül részletes naplózást is beállíthat.