1. **Customizable security policy**
2. **Comprehensive TLS and VPN support**
3. **Data masking**
4. **Highly flexible & skilled delivery team**
5. **Implementation of high security standards**
6. **Pioneers in proxy technology**
7. **Made in EU – 'clean' codebase**

PROXEDO
NETWORK SECURITY

"Global privacy spending on compliance tooling will rise to USD 8 Billion through 2022."

– 2019 Gartner Security and Risk Survey

NETWORK PRIVACY AND ENCRYPTION

The Challenge

TLS encryption – a double-edged sword

Encryption is the only way to keep your data safe while it is in transit on the network. The Transport Layer Security (TLS) protocol is one of the few methods that can be used not only to protect privacy and confidentiality, but also used to hide malicious activities. Indeed, attackers are moving more and more to encryption to hide their activities. Data exfiltration, malicious communication with Command and Control (C&C) and malicious downloads all utilize SSL/TLS encrypted traffic. There's no shortage of high-profile exploits with attackers hiding in HTTPS traffic. Just think of the Magecart breach of British Airways, where HTTPS traffic was used to obfuscate the credit card information exfiltrated from various payment pages. The breach affected 380,000 customers.

Application servers lack proper encryption

Application servers, including most mail, file and remote access servers, either can't provide satisfactory TLS settings or don't have TLS support at all. Even Apache and NGINX, the most common web servers, have difficulties with supporting important TLS features. From an encryption perspective, significant vulnerabilities in these servers can be found in the cryptographic libraries. This calls for a dedicated TLS device that takes over the role of traffic security and encryption.

Insecure SSL/TLS versions

There are six protocols in the SSL/TLS family: SSL v2, SSL v3, TLS v1.0, TLS v1.1, TLS v1.2, and TLS v1.3. Except for the last two, all the other versions are outdated, insecure (in many cases) and shouldn't be used. However, they are still needed in practice, leaving huge security gaps in many web servers and business applications.

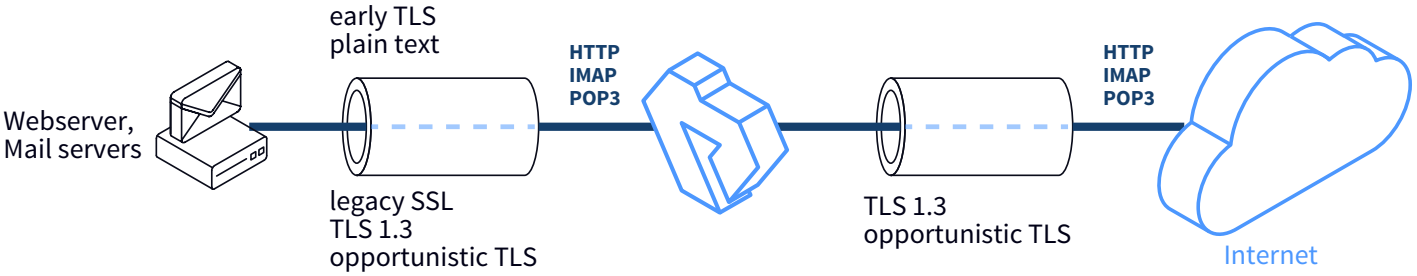
Human factor – the greatest privacy risk

Many security analysts claim that human error is the biggest challenge in data privacy and security. Not to mention human curiosity, misuse and intentional leakage of personal data. On the other hand, for an IT security administrator it can become overwhelming to manage literally thousands of patches released each year, which means that the efforts required to maintain privacy is constantly growing.

BALASYS

info@balasys.eu

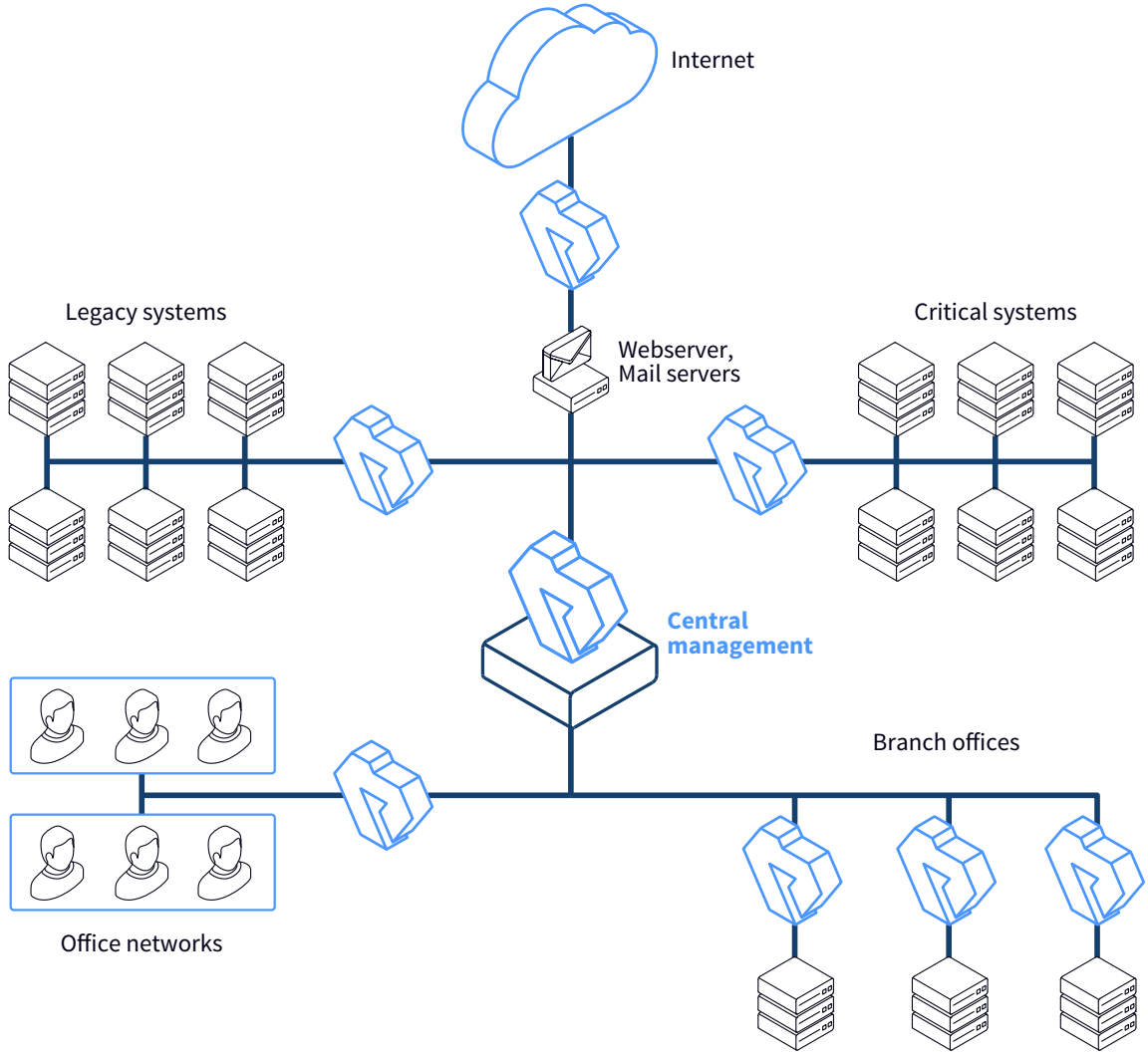
Copyright Balasys IT Kft. All rights reserved.



Flexible TLS configuration with PNS

SOLUTION

Proxedo Network Security (PNS) is a highly flexible, multipurpose network security suite that can granularly control traffic to protect enterprises from advanced internal and external threats. PNS provides deep packet inspection (DPI) of regular and encrypted network communication and has the capability to filter and modify its content. Thanks to its flexible architecture and scriptable configuration, your organization can implement ANY security policy, including the Zero Trust model. With PNS, you are able to manage custom security problems which your firewalls or UTMs are unable to solve.



Proxedo Network Security sample architecture

info@balasys.eu

Copyright Balasys IT Kft. All rights reserved.

BENEFITS

Proxedo Network Security helps you comply with the most recent privacy and encryption requirements. It ensures proper TLS settings for your business, including:

- the enforcement of secure protocols and the latest cipher suites
- the implementation of complete certification chains
- the protection of private keys
- the mitigation of other known problems.

You can implement security measures centrally to simplify the process compared to installing the right cryptography on all servers or clients.

Beyond in-depth inspection of HTTPS traffic, PNS takes over security tasks from your application servers so they can focus on their primary functions. This greatly increases the reliability and security of your web servers, thus increasing customer satisfaction.

Learn more

Proxedo Network Security homepage
Request a trial

BALASYS

Traffic Encryption

PNS offers complete control over TLS (the secure layer of HTTP, IMAP, SMTP, FTP, etc.) channels. PNS was one of the first IT security products to support the latest TLS 1.3 protocol.

The gateway can ensure a consistent implementation of encryption in front of sensitive systems that don't necessarily support TLS. The gateway allows flexible configuration of encryption policies towards communicating parties which enhances interoperability further. You can also encrypt non-encrypted or legacy internet protocols. Different security policies can be applied on connections from diverse hosts. This means that the need to apply settings generally supporting the 'weakest link' is obsolete, and you can implement the highest security standards while excluding the wobbly ones.

Comprehensive VPN support

PNS supports IPSec (both IKEv1 and IKEv2) and OpenVPN solutions, which use different methods to tunnel private traffic over the internet. Site-to-site and road warrior VPNs are also supported to secure the communication between remote branches/users and your company's central systems.

Selective TLS-offloading

In certain privacy scenarios, TLS-inspection is forbidden. In these cases, PNS can ensure the desired communication remains encrypted and no one inspects that traffic. For example, traffic related to your users' online banking activity would never be inspected.

Data masking

PNS's data manipulation capability enables the anonymization of sensitive data that supports compliance with various privacy standards, such as GDPR. Data can be transferred anonymously to your external partners, including your cloud- based service providers.

This also makes it possible to hide information about security risks and treat the vulnerabilities of your legacy applications. For example, you can remove banners or other information specific to the applications in order to hide sensitive information about your infrastructure.

Public Key Infrastructure

PNS offers a PKI system to provide a convenient and efficient way of managing certificates and keys required for secure communication between parties. The solution can be set to perform the regular distribution of certificates and CRLs (Certificate Revocation Lists) automatically, ensuring that no invalid or revoked certificate can be used. The PKI system can manage private keys, client certificates and sign requests for TLS and VPN connections as well. In fact, it helps you act as a trusted CA (Certificate Authority).