1. **Authentication and granular traffic control**
2. **Detailed security & audit logging**
3. **Enforced data encryption**
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

According to the 2019 Cost of a Data Breach Report, compliance failures were one of the biggest contributors to the costs incurred by data breaches.

NETWORK SECURITY COMPLIANCE AND AUDIT

The Challenge

Compliance pressure is increasing. IT security regulations, policies and related audit requirements vary greatly in terms of wording and technical details, which means you need flexible solutions to fulfill them. Nevertheless, all have one key requirement in common: regulated companies must protect customer data at rest and in transit. If data leakage occurs, it can lead to serious consequences, including penalties, loss of customer trust, future sales, compliance costs and even bankruptcy.

PCI DSS

Unlike other industry standards, such as the ISO 27001, PCI-DSS requirements are far more technical than you may be accustomed to. Strong authentication and access control to card data, regular monitoring of networks, installation and maintaining firewalls, encryption of data transmission and complete malware protection are just a few areas that financial providers need to address.

PSD2

PSD2 is the second edition of the European Union's Financial Services Directive, which has turned the entire industry upside down in the EU and beyond. It requires banks to grant access to customer account data for retailers and fintech providers. PSD2 consists of many indefinite requirements, such as the need to 'log all data' transmitted or to operate a secure communication channel to partners. Becoming PSD2 compliant causes a lot of headaches, even for security pros.

GDPR

For most businesses, implementing security controls will probably account for the biggest share of future spending on GDPR. Both data controller and processor companies may gather, process and share personal information. With GDPR, gaining control over these data is mandatory. To maintain robust data security, companies must adopt best practices in areas such as encryption, data anonymization or pseudonymization, and access management.

Other regulations

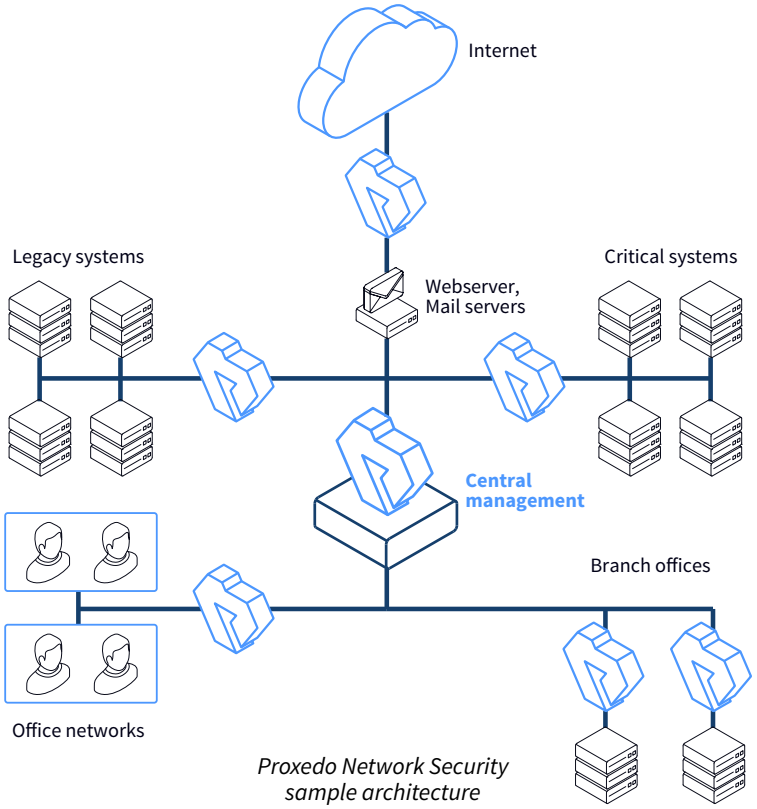
In addition to the above, we could continue the list with HIPAA, FISMA, ISO:27001, ETSI, etc. Not to mention the technical requirements detailed in NIST 800-52, whose cryptography-related guidelines have been adopted by many of the above frameworks. The regulatory pressure on financial institutions is particularly onerous, as they must deal not only with the above international directives, but also MiFID II and local legislation too.

BALASYS

info@balasys.eu

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

BENEFITS

Proxedo Network Security helps streamline your compliance efforts through its comprehensive access control, encryption and logging capabilities. Thanks to its highly flexible and detailed configuration, you can easily adapt to diverse network security related compliance needs.

Network authentication

You can implement an extra authentication layer to identify which user is accessing the resource and, if required, integrate with multi-factor authentication (MFA).

PNS' single sign on solution offers a simple way to integrate with Active Directory/LDAP and other authentication services. Linking all network connections to a single authentication greatly simplifies your user access management and system audit.

Encryption

PNS offers complete control over SSL/TLS (the secure layer of HTTP and many others) channels. The gateway can handle the TLS protocol in the traffic to ensure a consistent implementation of encryption in front of your sensitive systems, which don't necessarily support TLS. It allows flexible configuration of encryption policies towards various communicating parties. You can also encrypt non-encrypted or legacy internet protocols.

Data masking

PNS' data manipulation capability enables the anonymization of sensitive data that supports compliance with various privacy standards such as the GDPR. Data can be transferred anonymously to your external partners.

Security and audit logging

Most IT security regulations have strict expectations regarding the logging of sensitive data communication. PNS offers highly customizable, application-level log generation capabilities. Among other features, it can log who accessed what and when. The gateway can also log encrypted traffic and cryptographic settings. You can set up high log verbosity for higher quality auditing. It can even forward security logs to your SIEM or SOC to improve your security monitoring posture.

Learn more

Proxedo Network Security homepage
Request a trial

BALASYS