1. **Transparent, application proxy gateway**
2. **Implementation of high security standards**
3. **Pioneers in proxy technology**
4. **Flexible, black-belt delivery team**
5. **Made in EU – 'Clean' code base**

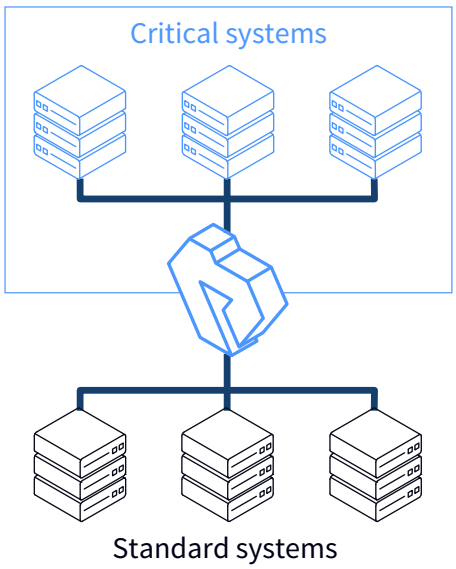
PROXEDO
NETWORK SECURITY

"When a cyber-criminal gains unauthorized access to a network, segmentation or 'zoning' can provide effective controls to limit further movement across the network."

– Wikipedia

SEPARATION AND PROTECTION OF CRITICAL SYSTEMS

We define critical IT infrastructure as systems and data required for the continued operation of a business. This includes, but is not limited to, payment card processing systems, accounting systems, ERP and supply chain distribution systems, intellectual property and customer databases.



In-depth protection of business-critical servers

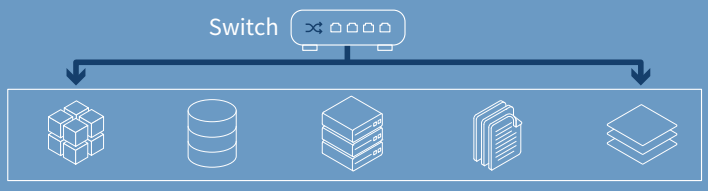
The Challenge

No segmentation – Great risk

Most organizations have not taken appropriate steps to protect critical infrastructure, such as implementing segmentation, prevention and detection controls. Implementing demilitarized zones and gateways between networks with different security requirements are always challenging.
Figure A displays a flat network with both administrative and critical infrastructures in the same segment. Information flows to and from critical systems with little or no control. Users of critical systems have access to the internet and attackers can potentially see these systems during scanning and enumeration steps.

Attackers love flat networks

If an attacker has initially compromised a workstation, he may seek to create a remote connection to a server, map a network resource or use legitimate network administration tools to access sensitive information or execute malicious code on that server. Properly planned and implemented network segmentation and segregation is a key security measure to assist in preventing such threats.



Flat network without segmentation

Regulations and standards require separation

PCI-DSS and similar standards provide guidance on creating clear separation of data within the network, for example by separating the network for payment card authorizations from those for Point-of-Service or customer Wi-Fi traffic. A sound security policy entails segmenting the network into multiple zones and rigorously enforcing the policy on what is allowed to move from zone to zone.

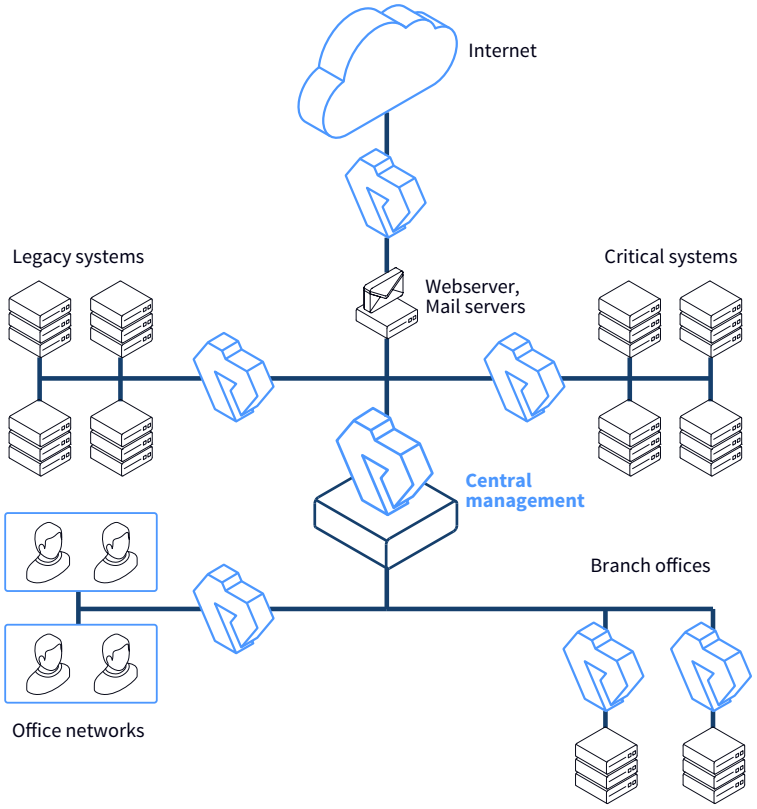
BALASYS

info@balasys.eu

SOLUTION

A proxy gateway for network separation

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

PNS can help you create a mature and segregated IT environment, allowing you to better focus your security strategy on prioritized systems. Additionally, it can provide a way to isolate compromised hosts or networks in a timely manner following a network intrusion.

1. **Enhanced Security** – Network traffic can be isolated to prevent communication between network segments.
2. **Improved Access Control** – Allow users to access only specific network resources.
3. **Improved Monitoring** – Enable the detection of suspicious IT events and help mitigate them.
4. **Improved Performance** – Fewer hosts per subnet means local traffic is minimized. A local subnet can isolate broadcast traffic.
5. **Improved Containment** – If a network breach occurs, its effect is limited to the local subnet.

Learn more

Proxedo Network Security homepage
Request a trial

BALASYS

Segregation

Proxedo Network Security can segregate critical systems from other systems. PNS ensures that those systems are not directly accessible from the internet and guarantees that any communication with them is restricted and controlled.

Granular protocol control

PNS handles network connections on the proxy level. This means that the transferred information is available on the device in its entirety, enabling deep protocol inspection and validation. The gateway can understand the specifications of the protocols and can reject connections that violate the standards. In-depth content filtering can be also added.

Comprehensive encryption support

PNS offers complete control over TLS (formerly SSL) encrypted channels. This capability provides your critical systems with protection against dangerous traffic – even if they arrive in encrypted channels. You can also encrypt non-encrypted or legacy network protocols.

Traffic manipulation

PNS can modify certain elements of the traffic. This makes it possible to hide sensitive information about your critical infrastructure and treat the vulnerabilities of your applications. For example, you can remove error messages, banners in order to hide faulty configuration or mask personal data (e.g. credit card numbers) for compliance or privacy purposes.