1 Transparent, application proxy gateway

2 Deep inspection and control of network traffic

3 Flexible security enforcement

4 Detailed security and audit logging

5 Integration with antimalware, IDS/IPS, MFA, IAM & SIEM

6 Flexible, black-belt delivery team

7 Made in EU – 'Clean' code base

PROXEDO
NETWORK SECURITY

"According to Intel, 43% of data breaches are attributable to inside attacks."

ZERO TRUST SECURITY ON THE NETWORK

Zero Trust is a security concept centered on the belief that organizations should not automatically trust anything either inside or outside their perimeters. Instead, they must verify everything trying to connect to their systems before granting access. Not surprisingly, organizations will find that implementing the Zero Trust approach is not an overnight accomplishment.

The Challenge

Micro segmentation

Implementing the 'least privilege' principle is the starting point of Zero Trust. The technical challenge lies in identifying sensitive data across all systems to implement least privilege, designing micro segments around different silos of data based on their sensitivity, and monitoring segment access and data flows on a continuous basis. Most systems are not architected to fulfill the micro segmentation requirements of Zero Trust.

Legacy system limitations

Zero Trust requires invulnerable authorization and should give access only to the requested resource. Many legacy systems do not have the capability to provide access control in this manner, including the adoption of the least privilege model.

Peer-to-peer traffic

Many systems use peer-to-peer (P2P) networking, including Windows operating systems and wireless mesh networks. P2P connections could break the Zero Trust and the micro-segmentation model, as systems communicate in a decentralized manner. P2P networks share data with little or no verification, breaking the least privilege model, too.

Digital transformation and DevOps

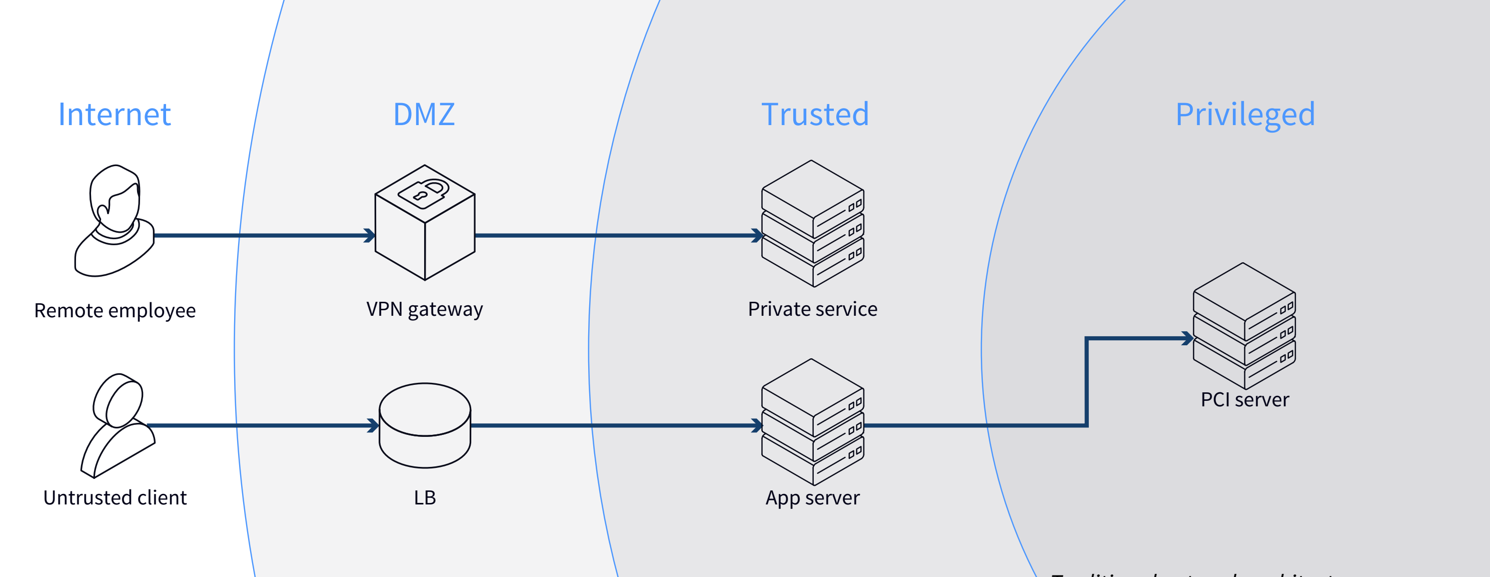
Digital transformation – also known as moving to the cloud, implementing the internet of things and deploying a DevOps culture – does not, by its nature, support Zero Trust. Implementing Zero Trust in a DevOps environment needs additional technology and processes to enforce this paradigm, given that this environment is very dynamic.

Central management challenges

Adopting Zero Trust in distributed networks without central management is a challenging task. Administering custom rules and policies, mitigating security vulnerabilities, implementing network authentication and proper encryption and managing external accesses are all extremely hard to achieve in complex environments.

BALASYS

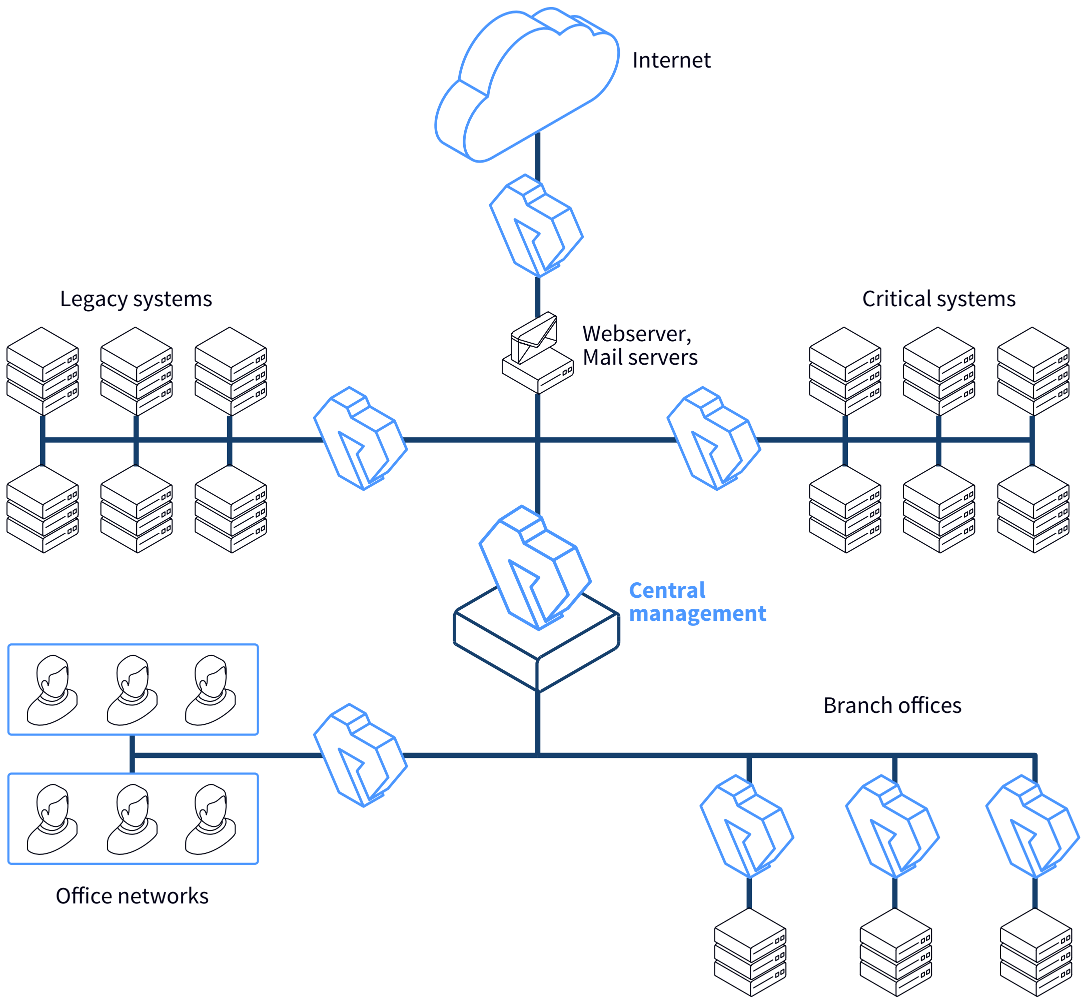
info@balasys.eu



Traditional network architecture

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

BALASYS

info@balasys.eu

Segmentation

Proxedo Network Security supports micro- segmentation by separating any systems from other parts of the network. PNS ensures that those systems are not accessible directly either from the internet or from other segments. It guarantees that any communication with them is restricted and controlled.

BENEFITS

Proxedo Network Security supports high security requirements, including the Zero Trust model. It provides the visibility and controls needed to secure and monitor every device, user and network being used to access business data. You will also be able to monitor device traffic and ensure that every device is authorized. This further minimizes the attack surface of your network.

Your security professionals can create service-based policies for greater efficiency without exposing the system to various vulnerabilities. For example, they can specify a policy where e-banking traffic goes through the firewall but bypasses the threat detection and decryption engine.

Learn more

Proxedo Network Security homepage

Request a trial

BALASYS

Granular protocol control

In contrast with the pattern matching of UTMs, PNS handles network connections on the proxy level. This means that the transferred information is available on the device in its entirety, enabling deep packet inspection and content validation. The gateway can understand the specifications of the network protocols and can reject connections that violate the standards.

Network authentication

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

PNS's 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.

Traffic encryption

Attackers can still perform passive attacks in which they sniff your traffic for sensitive information. In this case, host identification is not enough – strong encryption is required.

PNS offers complete control over SSL/TLS encrypted channels. This capability provides you with full understanding of email and web traffic – even if they arrive in encrypted channels. You can also encrypt non-encrypted or legacy internet protocols.

Robust central management

PNS offers an enterprise-level central management for handling hundreds of firewalls located in different network zones, or even geographically distributed environments. The advanced management GUI provides cost-efficient security operations for enterprises with multiple branch-offices.

Multiple deployment

You can deploy Proxedo Network Security for Zero Trust in two possible ways:

1. **Holistic firewall grid:** In this scenario, you can put small PNS instances in front of each sensitive IT resource. Instances are centrally managed.

2. **Logical deployment:** All network traffic goes through a powerful, central PNS instance which enforces the above security controls separately for each IT resource. Even systems in the same segment can communicate with each other only through the central PNS.