1. **Transparent, application proxy gateway**
2. **Flexible, black-belt engineering team**
3. **Rapid resolution of custom security challenges**
4. **Implementation of high security standards**
5. **Pioneers in proxy technology**
6. **Made in EU – 'clean' code base**

PROXEDO
NETWORK SECURITY

"Remaining secure depends on many factors but defenders who will see the most success will be those who are able to identify and mitigate threats at a more granular level."

– Sarah Chandley

MULTILAYER THREAT DETECTION AND PREVENTION

In order to adequately protect your network, you need access to tools and techniques that provide advanced multi-layered threat protection. Automated mitigation in real-time is also necessary in order to remediate security incidents. It is also important to add fast collection and analysis of incident related information for accurate forensic investigations. However, while all of this may be easy to map out at an enterprise level, it is extremely hard to implement in practice.

THE CHALLENGE

Application Layer Threats

The application layer in the OSI (Open Systems Interconnection) model is the hardest to defend. The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define. This layer is also the most exposed to the outside world. Applications must be accessible over port 80 (HTTP) or 443 (HTTPS) or over other ports depending on the protocol (SSH, FTP, IMAP, etc.) being used.

Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting and parameter tampering. Other possible exploits include viruses, worms, phishing, keyloggers, backdoors, program logic flaws, bugs and trojans.

Network Layer Threats

The most common network layer threats are router-related, including information gathering, sniffing, spoofing, and DDoS attacks in which multiple hosts bombard a target router with requests. Other incidents at this level are unauthorized retrieval of endpoint identity and unauthorized access to internal systems.

Presentation Layer Threats

At this layer, the most widespread threats are malformed SSL/TLS (Secure Sockets Layer/ Transport Layer Security) requests. Considering how resource intensive the inspection of TLS packets can be, attackers typically use TLS to hide attacks against web servers on HTTP.

Mitigation of these attacks is challenging as you must offload the TLS from the origin infrastructure and inspect the application traffic for signs of attack or violation of policy. A good solution should also ensure that your traffic is then re-encrypted and forwarded back to the origin infrastructure.

Session and Transport Layer Threats

Session layer threats include session hijacking (stealing tokens), SYN flood and man-in-the-middle attacks. You should prevent unauthorized password usage and data access, which are common attacks at these layers, by using encryption and authentication methods.

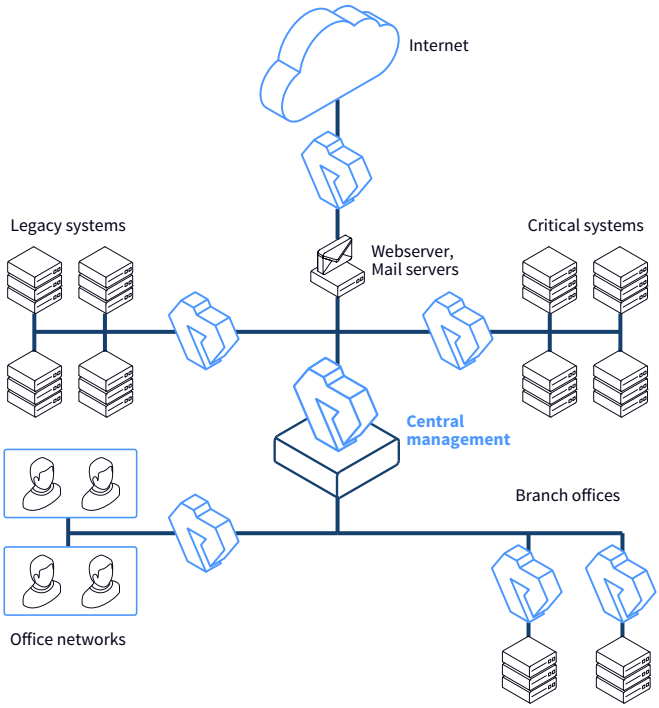
If you don't use the latest TLS or other encryption protocol with proper settings to secure all your internet communications, you put your data at risk of eavesdropping, tampering or message forgery.

BALASYS

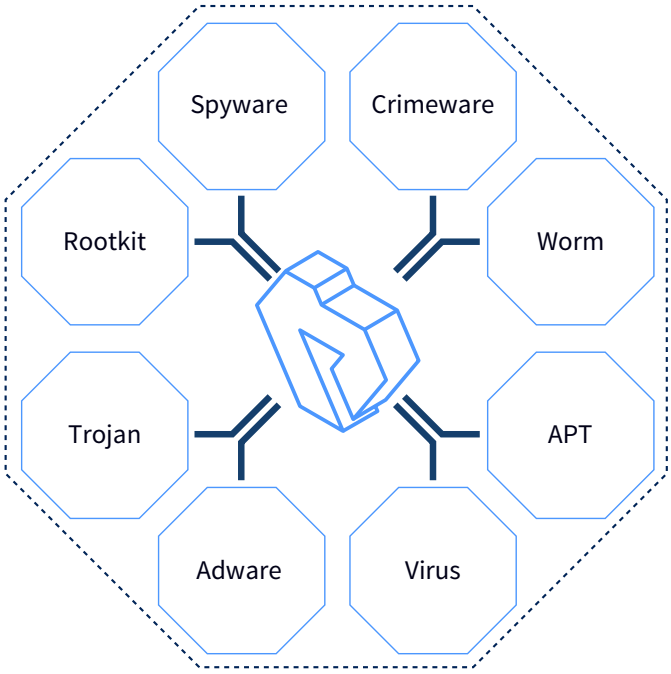
info@balasys.eu

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



Integrated content filtering& dynamic malware analysis

Application layer

Granular protocol control

Thanks to the proxy technology, PNS handles network connections on the application layer. 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. PNS can control 100% of the commands and attributes of the protocols.

Presentation, Session and Transport layers

Comprehensive encryption support

PNS offers complete control over 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. Proper TLS settings ensure that no compromised or outdated TLS ciphers or key exchange algorithms are being used.

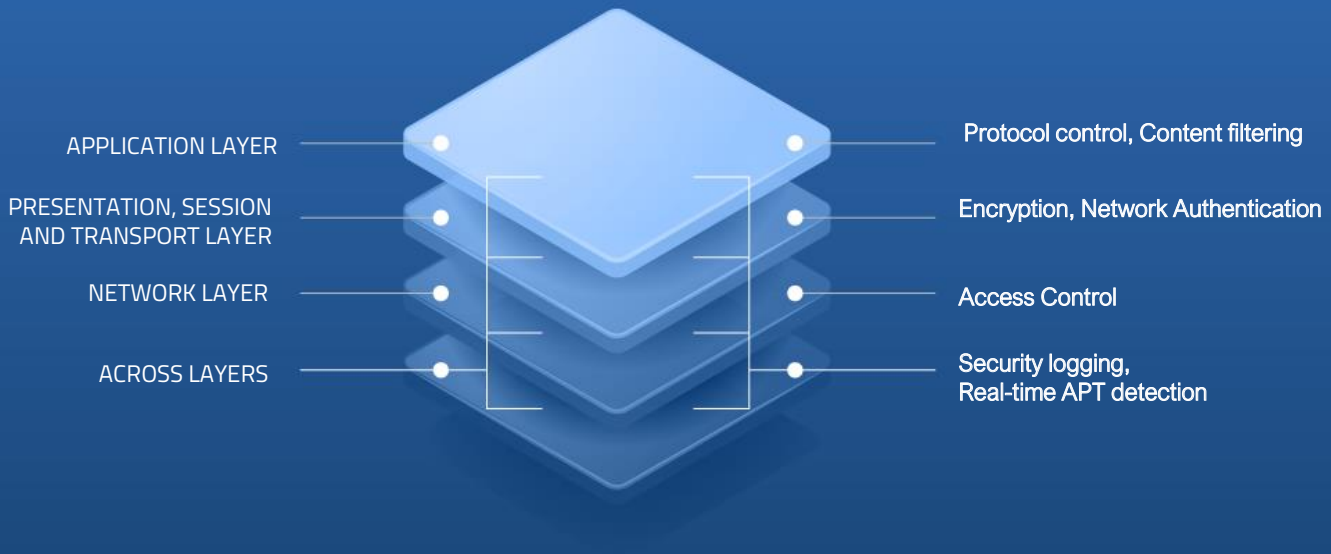
Network Authentication

The Proxedo Authentication Module can authenticate all connections passing the network gateway. It authenticates all sessions initiated by the user to restrict access of certain services only to the authorized personnel. Authentication and authorization implement an additional layer of threat prevention.

BALASYS

info@balasys.eu

Multi-layer threat management with Proxedo Network Security



BENEFITS

Layered security strategies are reactions to today's cyber threat landscape. Rather than simply waiting for attacks to hit endpoints, layered security takes a holistic view of defense, accounting for the multitude of vectors by which modern malware is delivered and recognizing the importance of network and end user-level security.

Advantages of this strategy include:

- A strategy for guarding against increasing polymorphic malware
- Protection from attacks via email attachment, files, adware, links, apps, and more
- DNS-level security to defend against threats originating at the network level

Learn more

Proxedo Network Security homepage
Request a trial

BALASYS

Network layer

Access Control

With PNS's packet filtering functionality, you can implement Access Control Lists (ACLs) to control access based not just on IP subnetworks but also on domain names. You can even shape IP subnetworks and domain names to the administrative hierarchy of network zones to control ACLs, where lower levels of the hierarchy can inherit the rules applied to the higher levels.

Across layers

Detailed security logging

PNS offers highly customizable log generation capabilities on each of the OSI layers described above. The gateway can even log encrypted traffic and the parameters of the encrypted channel. You can set up high log verbosity for better network debugging and forensics investigations. You can feed your SIEM with reliable, relevant logs to improve your security monitoring and alerting capabilities.

New approach for real time APT defense

Proxedo's malware detection module is a multilayer malware analysis tool for detecting emails and shared files infected with malicious payloads. Beyond detecting viruses in attachments, it can also provide you with protection against targeted APT attacks by setting an unparalleled level of defense. The multilayer detection system enables the integration of multiple antivirus engines for filtering known malicious codes, as well as dynamic, behavior-based analytics to identify unknown (zero-day) attacks.