1. **Simplified authentication and authorization**
2. **Seamless integration with existing infrastructure**
3. **LDAP/AD, POSIX, PAM, Kerberos, RADIUS and TACACS support**
4. **Support of S/Key, tokens, SecureID and X.509**
5. **Flexible, black-belt engineering team**
6. **Rapid resolution of custom authentication challenges**
7. **Made in EU – 'Clean' code base**

PROXEDO
NETWORK SECURITY

When it comes to dealing with authentication and authorization, a perfect storm is forming of complexity and pain for IT security teams.

NETWORK AUTHENTICATION AND AUTHORIZATION

IT must open the network to a dynamic workforce, but it is also essential to protect critical assets from the unauthorized access that outsourcing and mobility entail. In addition, to comply with industry and governmental regulations, enterprises must prove that they have stringent controls in place to restrict access to credit card information, customer records and other sensitive data.

THE CHALLENGE

Overwhelmed IT teams

Your IT team could face a massive explosion in the number of requests for additional services and applications with the implementation of dynamic options. However, it is likely that your IT budget and headcount hasn't kept pace with the new influx of requirements. This often means that your IT admin needs to decide which of the many user demands takes precedence. Typically, modifying the ACLs (Access Control Lists) is not on the top of the list – the admin staff have other pressing priorities. In addition, the majority of these changes impacts several different systems, which adds to the effort needed and the risk of incorrect access settings.

Compatibility with legacy systems

Authentication is a constant challenge between clients and servers that do not speak the same authentication language. For example, the client might not support authentication based on digital certificates, while the server does not accept password-based authentication.

This scenario is typical in machine-to-machine communication, especially with legacy systems such as AIX, AS400 or HP-UX. Where CLI access, custom scripts or vendor-specific tools may have worked in a less dynamic world, today these encumbering processes are a major bottleneck when it comes to network security. At the same time, it is essential to implement authentication to protect these resources.

Unified authentication

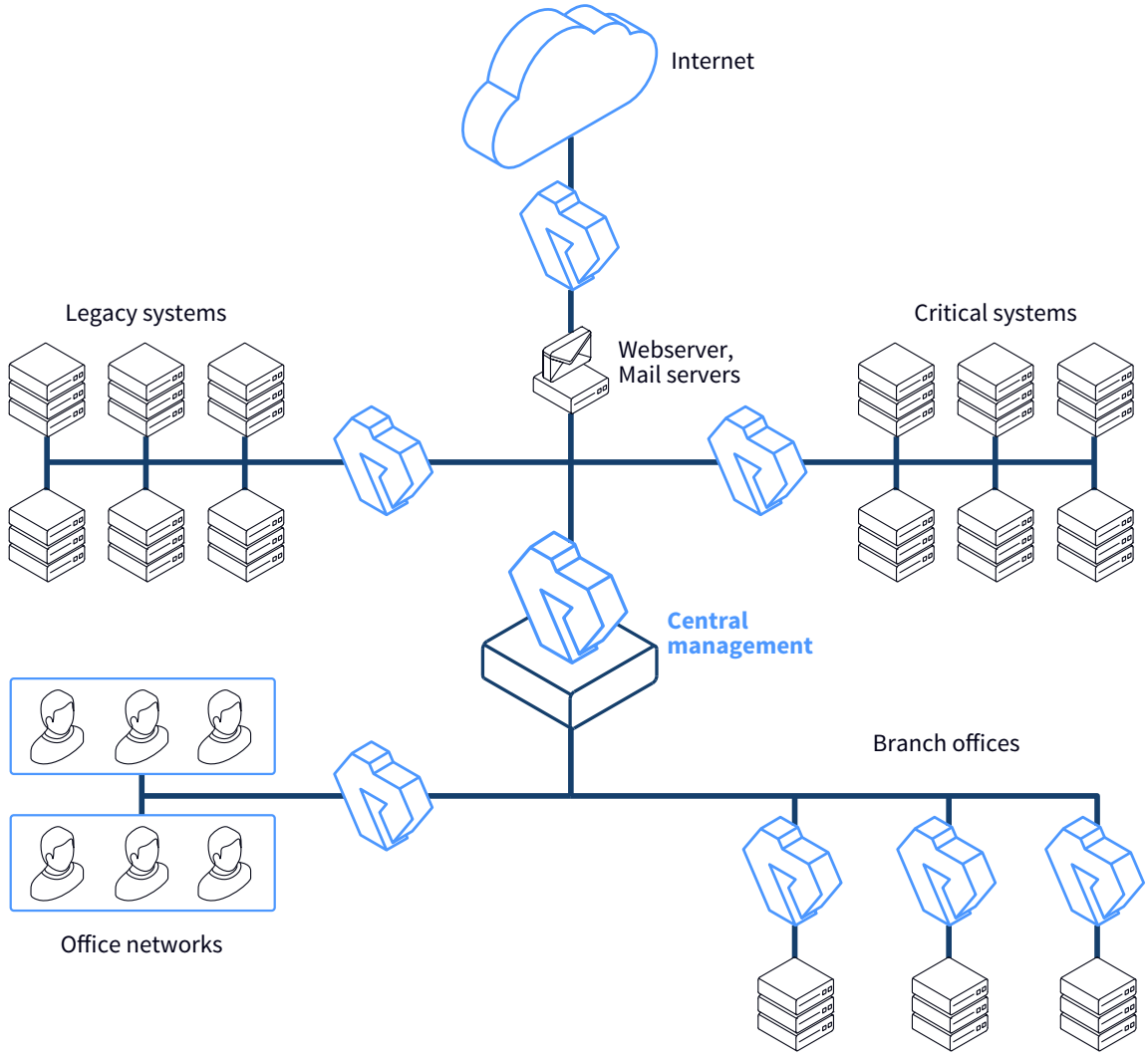
Implementing Single Sign-On (SSO) and integrating it with various authentication backends in a load-balanced architecture could be also a headache for your security team. Not to mention usability questions, such as the fact that HTTP basic authentication will vary from client to client. In such cases, form-based authentication might be beneficial, but after considering the challenges many companies decide to use other, less convenient technologies.

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

Proxedo Authentication Module

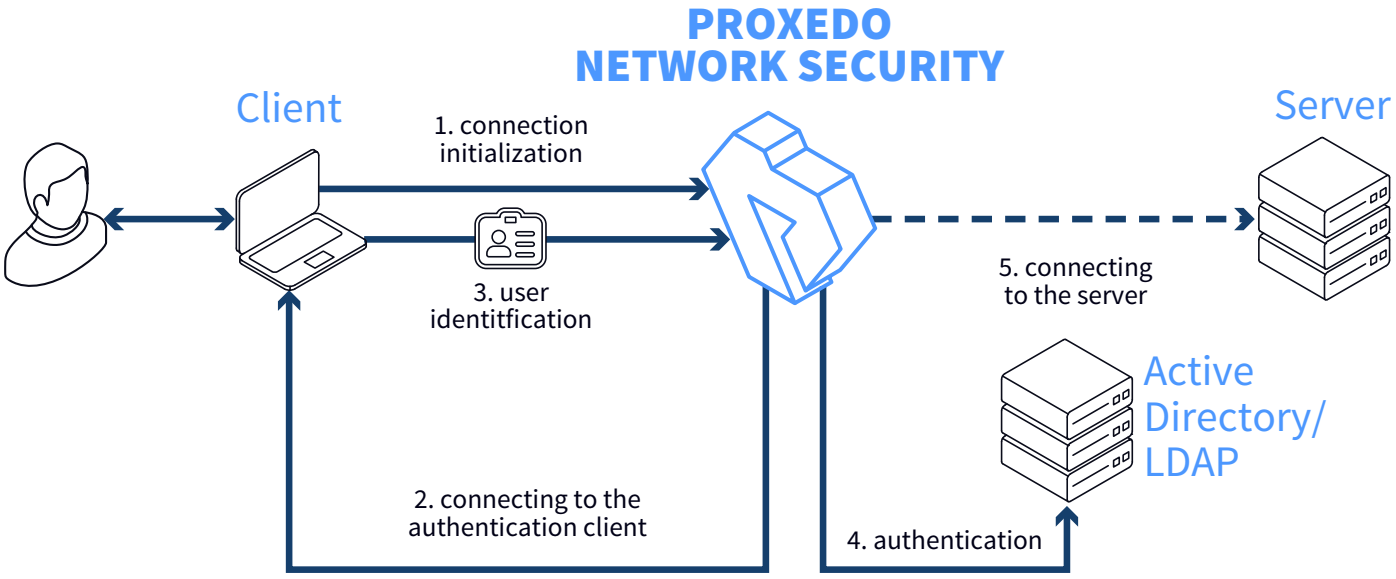
The Proxedo Authentication Module (PAM) is a PNS component that can authenticate all connections passing the security gateway. It aims to authenticate all connections initiated by the user to restrict access of certain services only to the authorized personnel. In contrast with the common practice that identifies the user with the IP address of their computer, PAM identifies and audits the complete network traffic on the user level. Both in-band (authentication within the protocol) and out-of-band (authentication outside the protocol) are supported.

Out-of-band authentication

The advantage of out-of-band authentication is that it can be used with any protocol and authentication method, making it easy to implement a single sign-on that is transparent to the users. A further advantage is that it enables the use of strong authentication methods (e.g. hardware tokens) with protocols that support only weaker methods (e.g. username/password).

BALASYS

info@balasys.eu



The PNS network authentication process

BENEFITS

Proxedo Authentication Module is a middleware that mediates the authentication between Proxedo Network Security and your existing user database. This means that network authentication is easy to implement and integrates smoothly with your existing infrastructure. As a central authentication point, Proxedo Network Security simplifies your network authentication and authorization management. It can take the load off your network operators and developers by handling the authentication challenge in a more efficient way.

Single Sign-On

The Proxedo Authentication Module 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.

Form-based authentication

The Proxedo Authentication Module supports form-based authentication in HTTP(S) protocol. It can be presented to the user with a captive portal to fill in and submit in order to log into a web application or service. You can even integrate it with your existing AD/LDAP database. Form-based authentication is a platform- independent and customizable solution to unify the web-based authentication process across your company, customers and partners.

Public Key Infrastructure

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

Learn more

Proxedo Network Security homepage
Request a trial

BALASYS