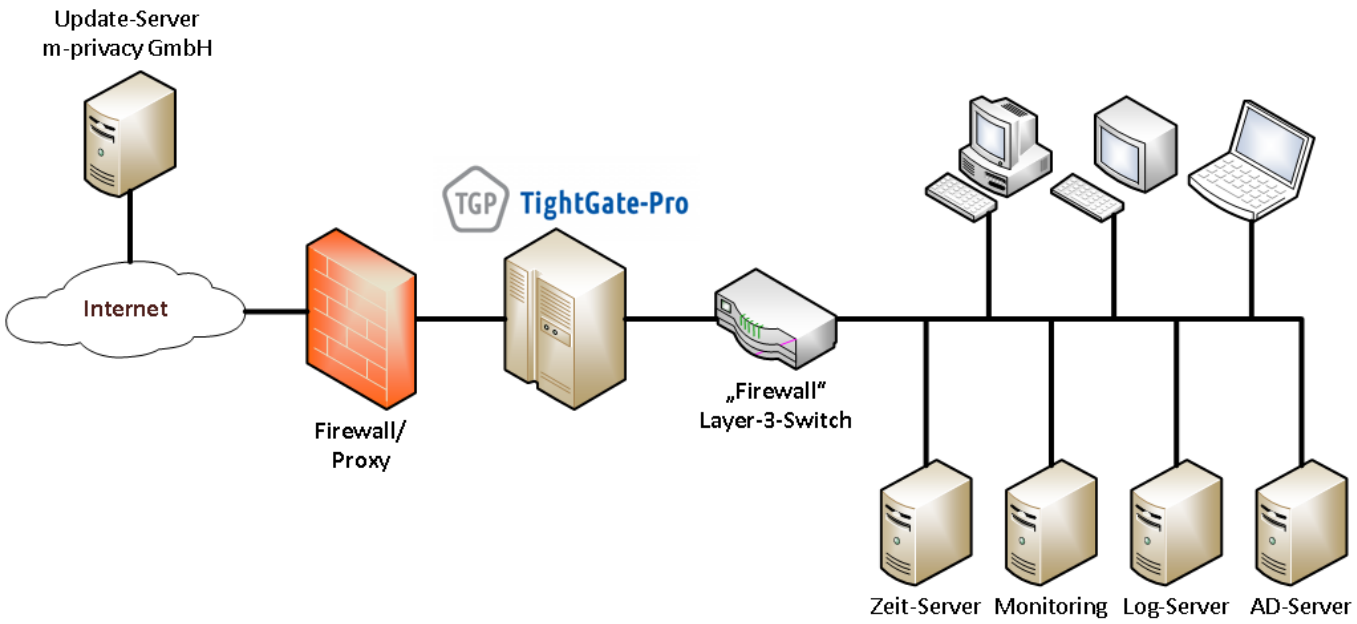
Introduction

The dedicated Remote-Controlled Browser System (ReCoBS) TightGate-Pro provides preventive protection against attacks from the Internet and thus regularly proves to be more effective than classic filter systems such as malware scanners, firewalls or intrusion detection systems (IDS). TightGate-Pro is a specially developed ReCoBS protection system that is installed as an appliance upstream of the company or authority network. The programmes for free Internet access (Internet browser) no longer run on the workstation computer, but centrally on TightGate-Pro.

The Internet is accessed exclusively via TightGate-Pro. Only the screen output of the browser is transferred to the internal network and displayed on the workstation PCs.

At the same time, the user's mouse and keyboard entries are sent to TightGate-Pro for remote control of the browser. A VNC protocol optimised for security is used for communication between the workstation computer and TightGate-Pro.

Network planning



TightGate-Pro is typically integrated into the organisational infrastructure directly behind the first firewall. TightGate-Pro is isolated from the internal network (LAN) by a layer 3 switch with packet filtering. This ensures that only defined connections from workstations (via TightGate-Viewer and, if applicable, TightGate-Schleuse) to TightGate-Pro are authorised. The layer 3 switch also regularly prevents connections from TightGate-Pro to the internal network. Exceptions are only permitted if TightGate-Pro has to use services that are only available in the internal network (see diagram).

Alternatively, TightGate-Pro can be operated in a DMZ. However, it should be noted that the network throughput in the direction of the internal network increases significantly, especially when playing multimedia content. The available bandwidth must be sufficiently high to ensure that the display remains smooth. The m-privacy GmbH therefore strongly recommends that the protection in the direction of the LAN is realised via a dedicated layer 3 switch, which guarantees an appropriate data

throughput for each TightGate-Pro server.

Environmental measures

The secure operation of TightGate-Pro and the protection it provides for workstation computers and the surrounding network are also influenced by the IT environment of the TightGate-Pro server and the client computers.

Securing the workstation computers (client computers)

Workstation computers from which the Internet is accessed via TightGate-Pro must not have any other access to the Internet. Their network connections must be completely sealed off from the Internet using appropriate packet filters or firewalls. If a risk analysis makes this necessary, suitable malware protection must be set up in the internal network and on the client computers.

Users should only use client computers with restricted rights. The system administration must ensure that TightGate-Viewer cannot be started with administrative authorisations in order to prevent permanent or unauthorised changes to configuration settings.

The use of TightGate-Pro is only possible with TightGate-Viewer. Other VNC viewers are either unable to establish a connection due to a lack of functionality (e.g. encryption methods) or do not fulfil the security requirements. The system administrator must ensure that the installation and operation of alternative VNC viewers is prevented on the workstation computers.

Warning

TightGate-Pro does not offer any system-related protection against attacks that affect client computers or the internal network via other shared network channels. Basic protective measures for the operating environment of TightGate-Pro must therefore be ensured by the system administrator.

Intrinsic security of TightGate-Pro

TightGate-Pro has comprehensive mechanisms for its own protection to ensure stable and safe continuous operation.

Server operating system and communication protocol

The operating system only contains the components required for operation. Consistent encapsulation of all programs and processes prevents the uncontrolled execution of unauthorised software and manipulation of installed components. A function-specific communication protocol between TightGate-Pro and TightGate-Viewer reliably prevents uncontrolled access to and from the internal network.

Isolation of user accounts

All user accounts and sessions initiated by VNC users are completely isolated from each other. Mutual

access or interference is excluded. VNC users only have authorisations for their respective user role and have no administrative rights.

Secure starting conditions

Every user session on TightGate-Pro starts in a defined, secure initial state. Central security options are predefined on the server side and are automatically reset at the start of each session. Changes made by the user therefore do not have a permanent effect and do not open up any security gaps.

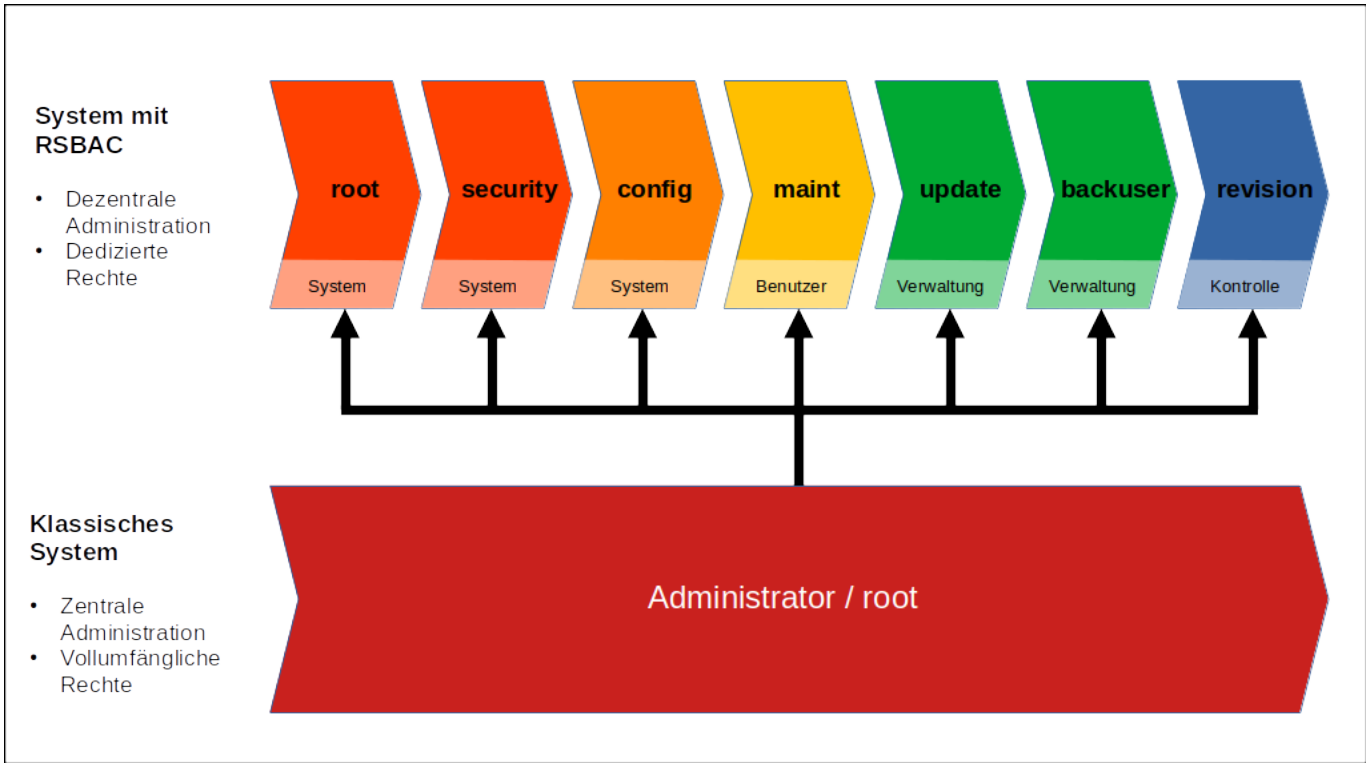
At the end of an Internet session, no active content remains on TightGate-Pro. All programmes and applications started in the user context are automatically closed when the user logs off.

The complete encapsulation of all software components in strictly separate authorisation spheres reliably prevents applications from influencing each other - particularly with regard to the Internet browser used.

Multi-dimensional system hardening and error resistance

The combination of various hardening and encapsulation measures as well as the specialised communication protocol result in a high level of security robustness - even under the assumption that individual software components may have inadequacies in logic or implementation.

The administration concept of TightGate-Pro



TightGate-Pro has predefined administrator roles that replace the conventional administrator (root). None of these administrator roles has comprehensive access rights to the entire system (superuser privileges). The advantages of this decentralised administration concept are, on the one hand, the protection of the system and the user data from a functionally inappropriate omnipotence [1]. On the other hand, mapping individual administration processes to several roles enables tasks to be delegated. The specific authorisations of the respective roles are summarised in a table in the

appendix to this administration manual.

System-related administration

For system and security administration, the account ***config*** account is available for system and security administration. It manages network settings and system-wide specifications, such as for user accounts. There is no access to user directories or user settings, which means that the majority of maintenance tasks can be delegated in compliance with data protection regulations.

Personal area

The account ***maint*** account is responsible for user administration. Users can be created, access authorisations adjusted and passwords changed. In addition ***maint*** can also restart individual services and enable remote maintenance access if required. However, this role is not able to view user directories or data.

Maintenance area

The following roles exist for maintenance tasks ***backuser*** and ***update***. Both have very limited rights. ***backuser*** is only responsible for creating and managing backups, while ***update*** performs system maintenance tasks. Neither role has access to network settings or user directories.

Security area

Central system security is guaranteed by the RSBAC access rights protection. The associated configuration is fully set up on delivery and must not be changed as a rule. To customise the RSBAC security parameters, the administrators ***root*** and ***security*** administrators are available.

[1)]
The conventional concentration of all administration tasks and system rights in a central account puts this account at particular risk with regard to intrusion attempts. Unauthorised persons who gain access to such a user account gain access to the entire system