Introduction

The dedicated Remote-Controlled Browser System (ReCoBS) TightGate-Pro provides preventive protection against attacks from the Internet. This makes it regularly more effective than any filtering system such as malware scanners, firewalls or intrusion detection systems (IDS). TightGate-Pro is a dedicated ReCoBS protection system that is deployed as an appliance upstream of the corporate or government network. The programs for free Internet access (Internet browser) are no longer executed on the workstation PC, but on TightGate-Pro.

Access to the Internet is exclusively from 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, mouse and keyboard information is transferred from the workstation PCs to TightGate-Pro for remote control of the browser. A VNC protocol optimized for security is used for communication between the workstation PC and TightGate-Pro.

TightGate-Pro and TightGate-Pro (CC) version 1.4

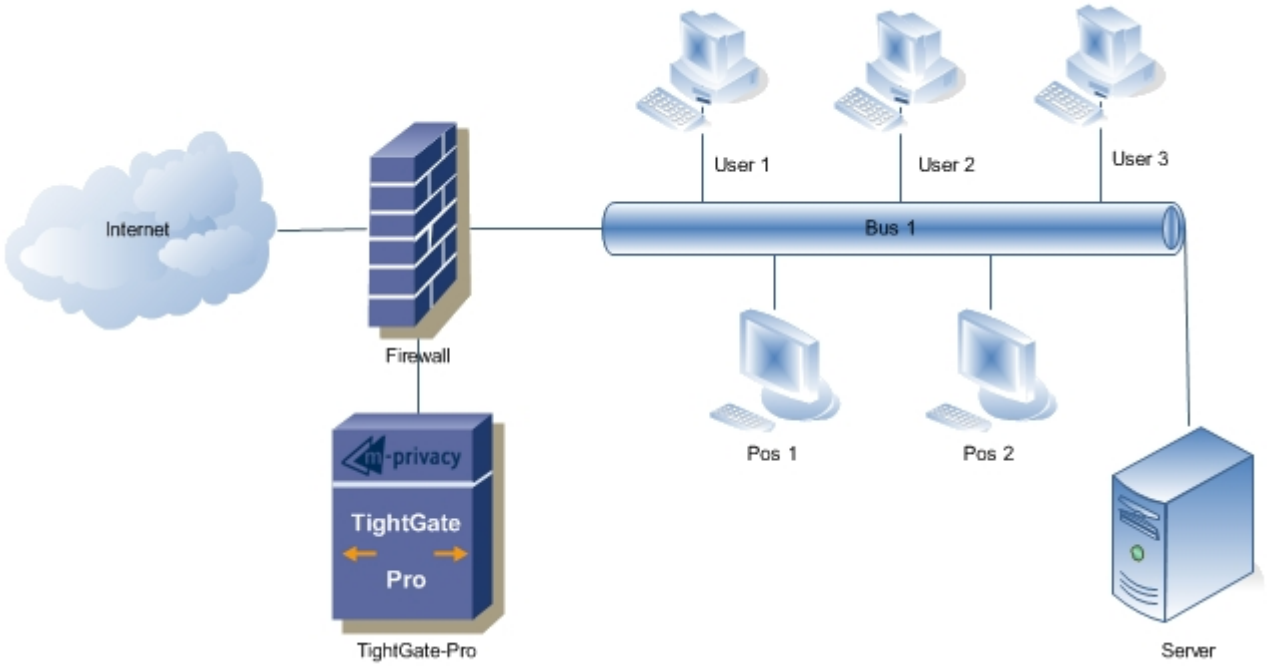
The ReCoB system TightGate-Pro is available in two variants. These is TightGate-Pro for standard environments (hereinafter referred to as "TightGate-Pro") and TightGate-Pro (CC) version 1.4 for CC-compliant environments. TightGate-Pro (CC) version 1.4 differs significantly from TightGate-Pro for standard environments in a number of pre-settings and the handling of file exchange between the server and the client computer:

- TightGate-Pro (CC) Version 1.4 server ships with factory deactivated text exchange via clipboard. This setting can be changed by the administrator ***config***. The viewer program TightGate-Pro (CC) Version 1.4 client is delivered with the default setting for individual confirmation of each text transfer.
- The administration roles ***root*** and ***security*** are also available in TightGate-Pro (CC) Version 1.4 Server, but can only log on in so-called soft mode (with RSBAC control deactivated). At the same time, the VNC server is deactivated for security reasons so that clients cannot log on via the Viewer.

Notice: Further differences in detail are explained in the respective setting options.

Caution: TightGate-Pro server and TightGate-Pro (CC) version 1.4 Servers may only be used with TightGate-Viewer from m-privacy GmbH. TightGate-Pro client or TightGate-Pro (CC) version 1.4 client are therefore mandatory, alternative viewer programs cannot be used. The system administrator must ensure that the installation and operation of alternative client programs (VNC Viewer) on the workstation computers (client computers) is not possible. A CC-compliant overall system is only possible with the combination of TightGate-Pro (CC) version 1.4 Server and TightGate-Pro (CC) Version 1.4 client.

Network planning



TightGate-Pro is regularly integrated into the organizational infrastructure in the Demilitarized Zone (DMZ) immediately behind the first firewall. Should this not be possible for technical or organizational reasons, there is nothing to prevent a direct connection of the protection system to the Internet from a security point of view. The strong self-protection of the ReCoBS server prevents negative influences on the level of protection as far as possible.

Workstation computers from the internal network can use the secure services of TightGate-Pro. At the same time, suitable packet filters must be installed upstream to ensure that the workstations or the Internet-bound applications installed on them (Internet browsers, e-mail programs, etc.) can no longer connect directly to the Internet outside the internal network. The transition to the Internet is made exclusively via TightGate-Pro. If necessary, direct connections to trustworthy remote stations (online banking, VPN, etc.) can be permitted by the administration, provided that attacks on the internal network via these connections can be excluded with sufficient security.

Environment

The secure operation of TightGate-Pro and the resulting protective effect on workstation computers and the surrounding network can be influenced by the IT environment of TightGate-Pro Server and the client computers (workstation stations).

Protection of workstations (client computers)

Workstations (client computers) from which the Internet can be accessed via TightGate-Pro are not allowed to have any other connection to the Internet. The network connection of the client computers must be isolated from the Internet using appropriately configured packet filters or firewalls. If necessary, adequate malware protection must be provided in the internal network and on the client computers if a threat analysis reveals a corresponding need.

Users should only use the client computers with limited user rights. The system administrator must

ensure that the TightGate-Viewer is not started by the user with administrative rights in order to prevent permanent anchoring of unintentional or unauthorized changes to configuration settings on the TightGate-Viewer. TightGate-Pro can only be used with the TightGate-Viewer. Other VNC viewers either cannot connect to TightGate-Pro due to a lack of functionality (e.g. encryption methods) or do not meet the requirements with regard to certain security precautions or procedures. The system administration must ensure that the installation and operation of alternative VNC viewers on the workstations is not possible.

Warning: TightGate-Pro does not offer any protection against attacks that affect the client computers or the internal network via network channels that have been released elsewhere. Basic measures to protect the operating environment of TightGate-Pro must be taken by the system administrator.

Self-protection of TightGate-Pro

TightGate-Pro has extensive self-protection mechanisms to ensure stable and secure continuous operation.

Operating system and communication protocol of the server

The TightGate-Pro operating system has only those program components that are indispensable for its operation. Comprehensive encapsulation of all programs and processes effectively prevents the uncontrolled execution of unauthorized software and the manipulation of installed program components on TightGate-Pro. A function-specific communication protocol between TightGate-Pro and TightGate-Viewer reliably prevents uncontrolled access to and from the internal network.

Encapsulation of user accounts

All user accounts and user sessions initiated by logged in users (VNC users) are completely isolated on TightGate-Pro. There is no mutual access or influence. VNC users are not equipped with administrative permissions that open up options for action beyond the user role.

Secure launch conditions

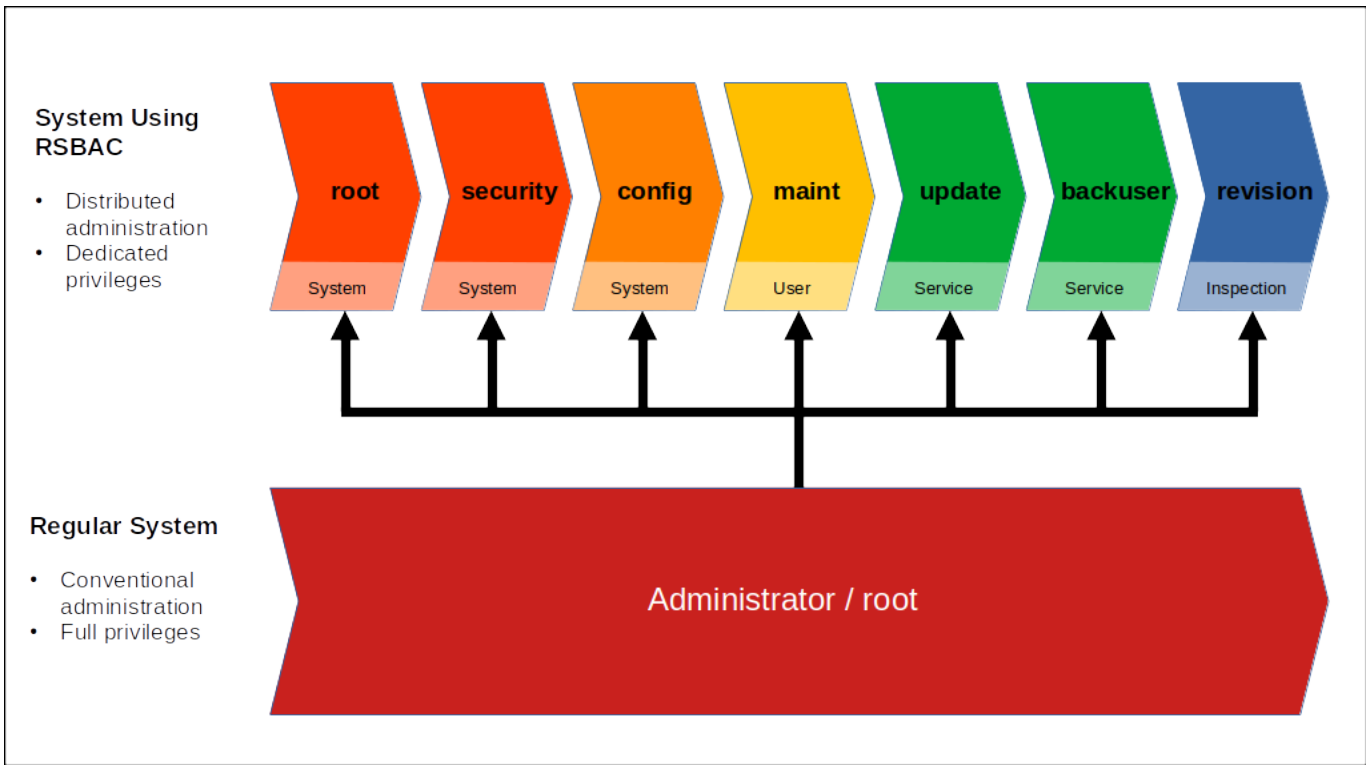
Each user session on TightGate-Pro starts in a secure initial state. Essential security options are fixed on the server side. Subsequent configuration changes, such as settings in the program menu of the TightGate Viewer, are not stored permanently in the user context and are reset to the default values when the user session ends. Furthermore, TightGate-Pro does not retain any active content from an Internet session after it has ended. All programs and applications started on TightGate-Pro in the user context are automatically terminated when TightGate-Pro is logged off. A mutual influence of applications on TightGate-Pro, in particular with regard to the Internet browser used, is excluded by complete encapsulation of all software components in separate authorization spheres.

Multidimensional system hardening and error resistance

The combination of different hardening and encapsulation measures for the self-protection of TightGate-Pro according to the state of the art in connection with a function-specific protocol for communication with the client computers results in an extraordinary degree of security robustness. This applies in particular under the a priori assumption that individual program components of TightGate-Pro may be afflicted with inadequacies with regard to program logic or implementation.

In the course of the installation of TightGate-Pro, therefore, none of the measures described in Section 1.4 are necessary to achieve the intended level of protection.

The administration concept of TightGate-Pro



TightGate-Pro has factory default administrator roles that replace the traditional administrator (root). None of these administrator roles have comprehensive access rights to the entire system (superuser privileges). The advantages of this decentralized administration concept are on the one hand the protection of the system and the user data against a functionally inappropriate omnipotence[1]. On the other hand, by mapping individual administration processes to several roles, it is possible to delegate tasks. The concrete authorizations of the respective roles are summarized in a table in the appendix to this administration manual.

Warning: Generally it should be noted that the administration of TightGate-Pro or TightGate-Pro (CC) version 1.4 is to be performed exclusively by trustworthy and adequately trained, security-conscious specialists. TightGate-Pro or TightGate-Pro (CC) version 1.4 cannot or only to a very limited extent counter a security risk caused by operating errors or incorrect configuration. Against this background, the passages of this documentation marked with the keyword ***Warning*** must also be observed.

System related administration

The administrator account ***config*** was created for the system and security administration of

TightGate-Pro. This is responsible for network settings and system-wide defaults, e.g. for user accounts. However, this administration role has no access to user directories and user settings. Most maintenance tasks can thus be delegated without hesitation under data protection law.

User administration

The administration account ***maint*** is responsible for the user administration of TightGate-Pro. Users can be created, access rights and restrictions can be set and passwords can be changed. This administrator also has the option of restarting individual services and, if necessary, activating remote maintenance access. A content control of user directories and data by ***maint*** is excluded.

Maintenance

The administrator accounts ***backuser*** and ***update*** were provided for maintenance tasks of TightGate-Pro. They have only a very limited range of functions and specially defined rights. The ***backuser*** is exclusively responsible for creating and managing backups and the necessary settings. The same applies to the ***update*** role when maintaining the system. Both roles have neither access to the network settings nor are they allowed to view user directories.

Security

The central security of TightGate-Pro is guaranteed by the RSBAC access right protection. The RSBAC configuration is completely configured on delivery and must not be changed by administrators on a regular basis. The administrators ***root*** and ***security*** are available for editing the RSBAC security settings. Both are disabled by default.

Note: In TightGate-Pro (CC) version 1.4 servers for CC-compliant environments, the ***root*** and ***security*** administration roles are only available when the system is started in soft mode.

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