Excellence in Digital Security.

genua.

genubox

High-Security Remote Maintenance Solution

Technical Information

Table of Contents

1. A Remote Maintenance Solution with a Wide Range of Applications

This information brochure is aimed at people and companies who are involved in the remote maintenance of all kinds of systems, like operating technicians, mechanical engineers and system integrators.

It gives a concise overview of how genubox can help you to provide a comprehensive remote maintenance service, while protecting the network of the equipment operator.

1.1. The Challenge

Whether you are dealing with a work stoppage at the plant or travel expenses incurred by a maintenance team – time is money. A machine breakdown in production, or an outage of server systems has to be avoided at all cost. By using industry-standard protocols like S7 by Siemens for example, industrial plants can be monitored around the clock. Problems can thus be swiftly detected and solved to avoid or reduce down times.

Manufacturers who sell their high-maintenance industrial machinery, manufacturing equipment, or drive systems all around the world usually employ remote maintenance options via the Internet for precisely this reason. This enables them to access information on the equipment's condition on a 24/7 basis, and, in principle, they can access the equipment remotely via their service center at any time.

For remote maintenance purposes, however, the customer's IT network needs to be partially opened to the maintenance provider. In general, this opening cannot be avoided, but should be restricted as much as possible for security reasons. This is where the usual methods of implementing remote maintenance access often cause misgivings on the part of the customer, because they expose an unnecessarily large part of the IT network. In addition, the solutions for identifying and authenticating the remote service provider are usually inadequate.

Another critical aspect is that remote maintenance service customers often cannot reproduce every detail of the work carried out by the service provider.

Last but not least, companies worry that remotely maintained production processes will add additional complications and require specialized IT personnel to support the solution.

1.2. Possibilities and Limitations of Traditional Remote Maintenance Methods

In this section, we consider the various solutions for creating an opening in an IT network for third-party access, and we examine the advantages and disadvantages of each solution.

1.2.1. Opening the Firewall, or Access via Modem/ISDN

In order to enable remote maintenance access, the customer opens his firewall for the remote maintenance provider's sender IP address and the target IP address of the equipment undergoing maintenance. Or, similarly, another access path can be set up via modem or ISDN, which bypasses the firewall.

This standard solution has the following risk factors:

1. There is no authentication of the service provider and no access authorization.
2. This means there is a danger of third parties gaining access, especially if the opening in the firewall inadvertently remains longer than necessary after the completion of the work.
3. In addition, a hacker could intercept and possibly take control of the access established for remote maintenance purposes.
4. Furthermore, if there are any implementation errors in the firewall, this may enable direct access to other areas in the customer's network.
5. There is no separation at network level.
6. Due to the lack of recording or insufficient logging of the access, the maintenance process and possible problems cannot be traced afterwards.
7. Without the option of only enabling dial-in after consultation, there is a permanent risk to network security if the main firewall malfunctions.

1.2.2. Access via VPN

The use of the IPsec VPN protocol is sometimes suggested for protecting remote maintenance access. This method does, indeed, eliminate the first and second risk factors.

However, this method harbors another risk: because IPsec implements fully transparent and routed access to the network, there is now a possibility that the IT networks of different customers, which are accessed for maintenance purposes at the same time via IPsec, could unintentionally communicate with one another. Given that the maintenance providers are specialists, dealing with systems that are typical for an industry, there is a very real danger that the networks of competing companies could come into contact this way and could thereby grant unauthorized persons access to the maintenance objects. For this reason, it is important to ensure that network coupling does not occur with remote maintenance solutions.

2. The Solution: Secure Access for Remote Maintenance with genubox

genubox uses the flexible and very secure OpenBSD operating system, which comes with a TCP/IP stack optimized for security, routing functions, a packet filter, authentication methods as well as comprehensive cryptographic functions. In the following, you will discover how these can be used effectively to protect remote maintenance access.

The Remote Maintenance Solution genubox

2.1. genubox as Rendezvous Server and Application Level Gateway

The first and second risk factors can be eliminated by using SSH with its reliable encryption and authentication features. Compared with the IPsec method mentioned above, it offers the advantage of more flexible and more personalized identification of the remote maintenance provider. This eliminates the risk of connecting different customer networks, as SSH only connects the required applications, not entire networks (elimination of risk factor 4).

An additional filter function serves to divide the customer's network into two areas. One area contains the equipment undergoing maintenance, which is accessible to the remote maintenance provider, while the other network area cannot be accessed. It is a considerable advantage that filtering can also take place at OSI layer 2 (in bridging mode). If, as usual, the filtering takes place at OSI layer 3 (routing mode), it would also be necessary to restructure the customer's network into two self-contained subnetworks – this can be avoided in bridging mode. A filter function at OSI layer 3 is possible at any time, though.

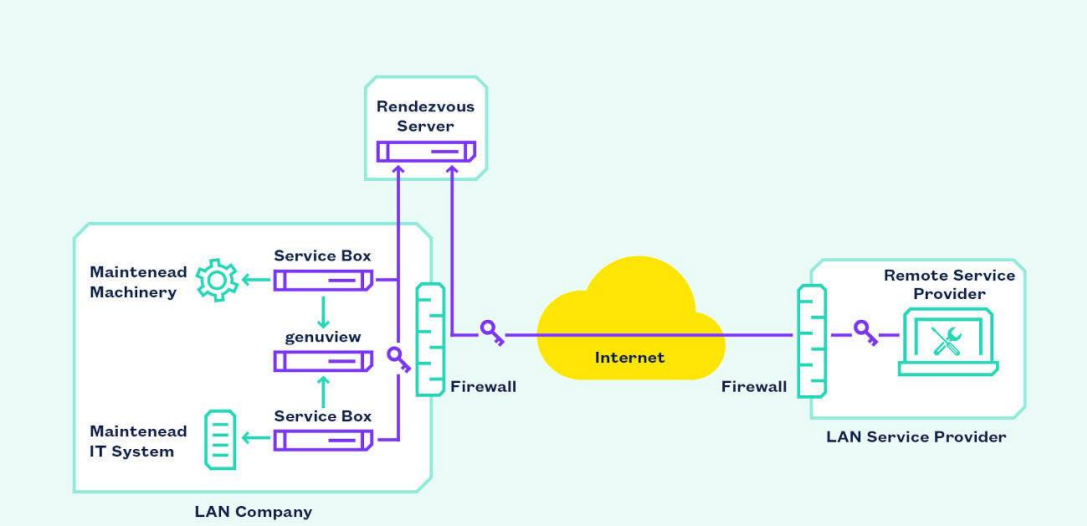
The remote maintenance provider first creates a SSH tunnel to genubox where he is authenticated. Through the tunnel, he can then access the equipment undergoing maintenance with any TCP-based applications.

Furthermore, genubox offers the services of a complete Industrial firewall system. The packet filter function of which is configured to not compromise the ability of other customer systems to access the equipment undergoing maintenance. On the other hand, the filter prevents any unauthorized connections that the remote maintenance provider may, intentionally or unintentionally, try to establish between the equipment undergoing maintenance and other customer systems. This restricts any risk associated with remote maintenance access to the network of the equipment undergoing maintenance (elimination risk factor 3).

genua follows the BSI recommendation for secure remote maintenance and offers an application level gateway for remote desktop and SSH target system access on the service box. As a result, this prevents a continuous data connection from the remote maintenance provider to the target system at the application level. The application level gateway acts as an intermediary to the target system.

2.2. Setting up a Rendezvous Solution

The only remaining threat to the customer's network is a potential fault in the main firewall. This can be avoided by preventing the remote maintenance provider from directly dialing up the customer's network (elimination risk factor 6).



Rendezvous in the DMZ as a secure solution

Instead, the maintenance provider is only allowed to connect to a rendezvous server located in the cloud or a demilitarized zone (DMZ) next to the main firewall. Thus

- -the operator decides, whether remote maintenance is permitted and
- -the complete supervision of the remote maintenance procedure is possible.

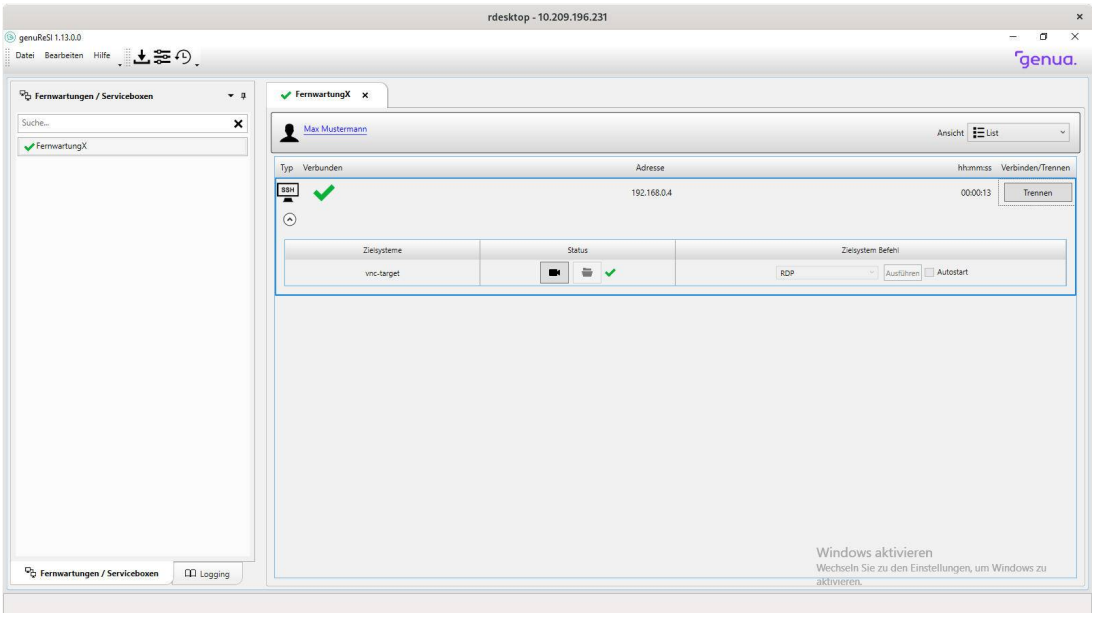
In addition, the remote access is logged. genubox also offers the option of video recording and live transmission of the maintenance process (elimination of risk factor 5).

In summary: genubox, used in combination with a rendezvous server, offers maximum control and security for remote maintenance solutions. No adjustments need to be made to the firewall or other systems in the customer's network.

2.3. More Comfort with the Remote Maintenance Application

The Remote Maintenance App makes high security remote maintenance access simpler and more comfortable than previously possible: The Remote Maintenance App is a MS Windows application that makes it possible for both the remote maintenance provider and the customer (machine operator/administrator) to administer the remote maintenance configuration with only a few mouse clicks and to start and stop maintenance with just one click. It can be downloaded from our website at no cost. It only requires normal user permissions on a Windows computer and can therefore be easily employed by all users.

The only remote maintenance configuration required is generated and encrypted on the Central Management Station genucenter and transferred, for example, via e-mail. Later changes to the central management, for example the addition of a maintenance object, are automatically adopted by the App. The remote maintenance provider only has to open this configuration in their Remote Maintenance Application and they are ready to start working.



Remote Maintenance App for a simple workflow

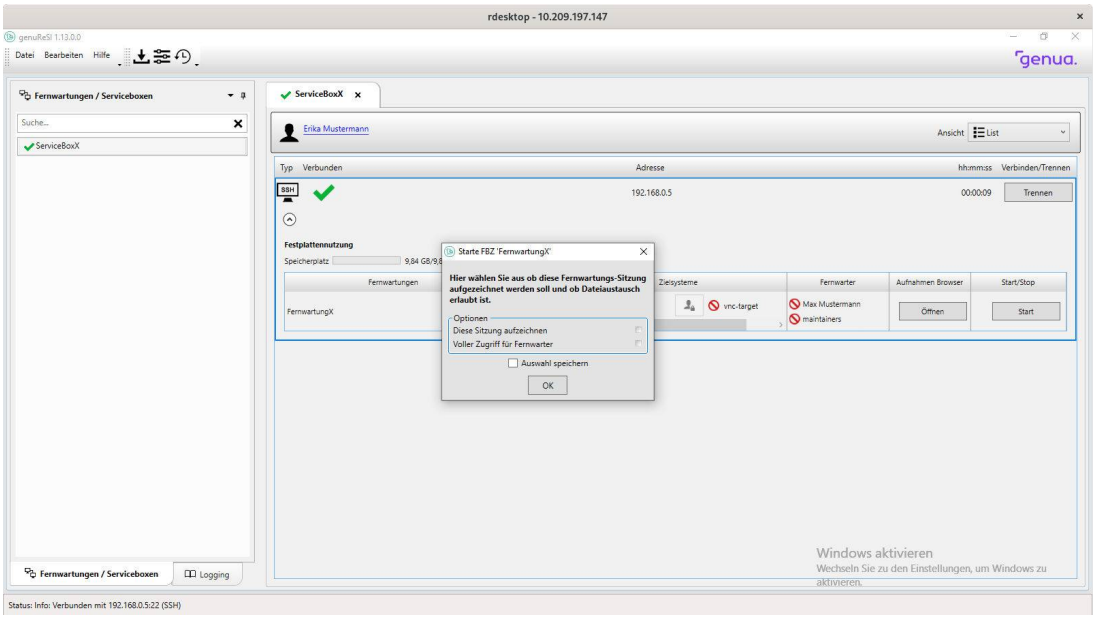
2.4. Web Browser-Based Remote Maintenance

In addition to the Windows app, the rendezvous solution now offers the option of remote maintenance via a standard web browser. In this way, service employees can flexibly set up a maintenance connection with all common end devices, e.g. a Windows/Linux PC, an Apple MacBook or a tablet.

The platform-independent solution via a standard web browser ensures compatibility and the underlying application is always up-to-date thanks to system updates. Operation is user-friendly and requires no technical expertise. Two-factor authentication and the protected data transmission via Hypertext Transfer Protocol Secure (HTTPS) ensure the secure connection between the service employee and the rendezvous server.

2.5. Traceability through Recording and Monitoring

genubox provides additional security and traceability for remote maintenance by making the recording and live monitoring of all remote maintenance access possible. It enables the operator to restrict the remote maintenance provider to specific actions. This only requires the customer and the remote access provider to both use the comfortable Remote Maintenance App. Maintenance sessions such as those carried out by remote desktop, VNC or SSH, can then be made available on genubox in video form, where they can be accessed by the customer.



Remote Maintenance App – easy video recording via one mouse click

2.6. Option: genuview

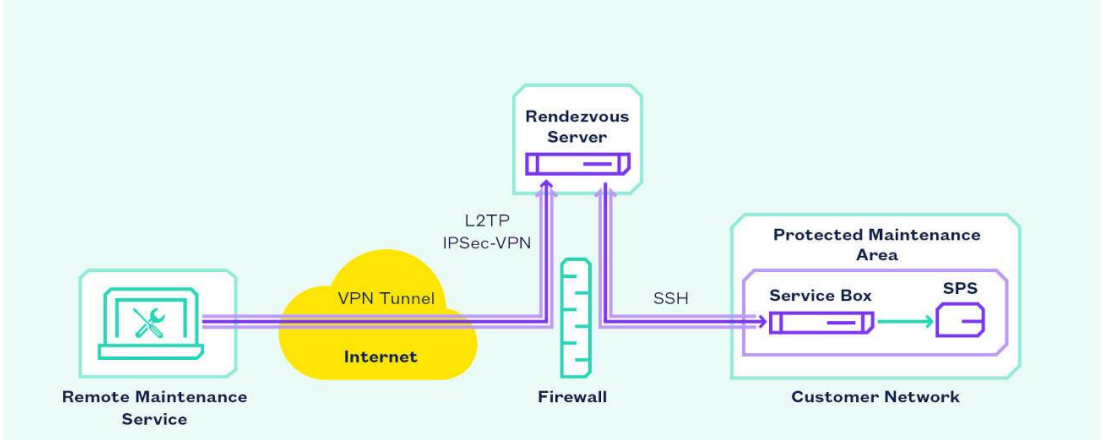
With genuview, genua offers an access and storage management solution for remote desktop recordings.

After remote maintenance access has taken place, the recording is forwarded uncompressed in raw format to a genuview server and archived there in a memory-saving manner. Access to the recordings can be conveniently managed via a central rights management system.

2.7. Optional Remote Access Using L2TP-IPsec-VPN

It is also possible to use an L2TP-IPsec-VPN to make the connection between the service provider and rendezvous server instead of using SSH. This can either be done alternatively to or in parallel with SSH, with the target system in the customer's LAN continuing to be only accessible via the service box SSH tunnel. This means that only packets that are allowed will be forwarded to the SSH tunnel by the firewall integrated in the rendezvous server. As with the solution described above, network coupling is not possible, and the customer retains full access control.

The simplified VPN configuration gives the service provider an additional advantage: He no longer has to use auxiliary programs such as PuTTY as L2TP-IPsec-VPN is natively supported by the majority of current operating systems, including MS Windows, Mac OS X and iOS (iPhone, iPad) as well as Android. Suitable clients are also available for Linux. Additionally, genua's Remote Access App supports L2TP.

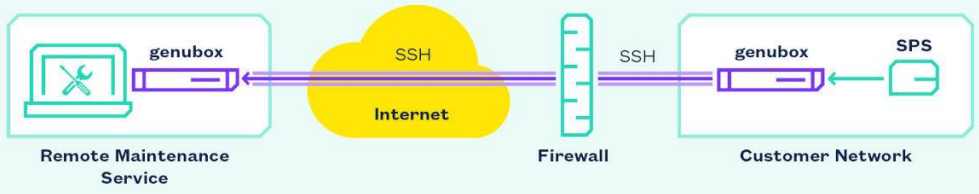


Rendezvous with L2TP-IPsec-VPN

2.8. Remote Access utilizing SSH-VPN

Granting remote access using SSH-VPN is another typical operational scenario of genubox. This solution, for instance, is employed if industrial equipment is supposed to permanently send sensor data to a control station for analysis. During

this process, a genubox at the equipment operator and a genubox at the service provider or the equipment manufacturer respectively, provide data security. On grounds of the permanent transmission, this monitoring solution does not utilize a rendezvous-server.



Secure Monitoring Solution via SSH

3. genubox Overview

The possibilities provided by genubox far exceed those of a traditional VPN appliance. In addition to basic cryptographic functions (basic module), genubox offers an application platform on which you can integrate any application for any purpose. Because of its different interfaces, as well as flexible communication options, genubox is suitable for virtually all fields of application.

3.1. Basic Module

3.1.1. Crypto Tunnels for TCP Sessions

Whether between genuboxes or between a genubox and the application server, encryption technologies can be employed at various network layers. These technologies may include remote bridges for encrypted linking of two network subareas (layer 2), IPsec gateways for IP packet encryption (layer 3), or service-specific tunnels using SSH or SSL (layer 4).

Only strong algorithms are used for encryption. In particular, by using application tunnels for TCP connections, genuboxes can be used in undefined IP environments, e.g. for dial-up or DSL access, or behind firewalls and NAT routers. This also enables access to private address areas that are segregated by proxies or NAT routers, even if several of these areas use identical IP addresses.

3.1.2. Industrial Firewall in Bridging Mode

genubox features a high-performance stateful industrial firewall that can monitor all connections that are established or handled via genubox, up to OSI layer 4. Since genubox is able to perform both routing (layer 3) and bridging (layer 2), these security functions can be used at both levels. In other words, in the case of bridging, genubox can be used as an invisible firewall to segregate a system, or an entire network.

3.1.3. IPsec Gateway

With this application, genuboxes can be used as regular, layer 3-based IPsec routers. Even if a genubox is positioned behind a NAT router, this does not present any problems, due to NAT support.

Another advantage is the scalability of IPsec VPNs, achieved by combining tunnels. This makes it possible to operate highly complex IPsec VPNs with numerous networks, without significantly increasing the load on several gateways. Furthermore, on-demand functions are supported which establish the VPN only when necessary.

In addition, the DPD protocol (Dead Peer Detection) can be used to quickly identify partners who have lost their connection.

3.1.4. The Application Module

A customer may wish to use individual applications within a project. These can be integrated in genubox. If required, genua is there to support you as your expert development partner – we can either implement the application in accordance with your specifications, or assist with this task.

Possible individual applications include equipment monitoring, remote diagnosis, remote management access, complex application tunnels for ASP applications, and preventive maintenance systems. A specific example would be recording and packaging the sensor data from industrial machinery, and sending this data to the maintenance provider at specified intervals.

4. Use Cases

Numerous businesses and public authorities already use genubox in matters of secure remote applications. In the following we will demonstrate possible use cases.

For all use cases mentioned, genua provides the benefit of having a central management solution, which offers the monitoring of all hardware components and software versions. Due to the centralized distribution of patches, the whole system is always up-to-date and state of the art secure. The ability to record all operations within this solution provides transparency, traceability, and auditability.

4.1. Maintenance with Rendezvous

When employing the rendezvous solution, all maintenance connections are routed through a rendezvous server, which is installed in the cloud or a demilitarized zone (DMZ) next to the firewall, located at the service provider or customer. To this point, both the maintenance provider and the customer connect at an arranged time. Only by means of the rendezvous on this server, a continuous maintenance connection is established.

Through this connection, the service provider is able to access the machine or IT system in the customer network, using unlocked applications. This way, the customer maintains full control over all maintenance procedures in his network. The rendezvous solution provides dependable IT security, records all actions of the service provider in a revision-optimized manner, is flexibly deployable in different environments and can easily be operated by our Remote Maintenance App.

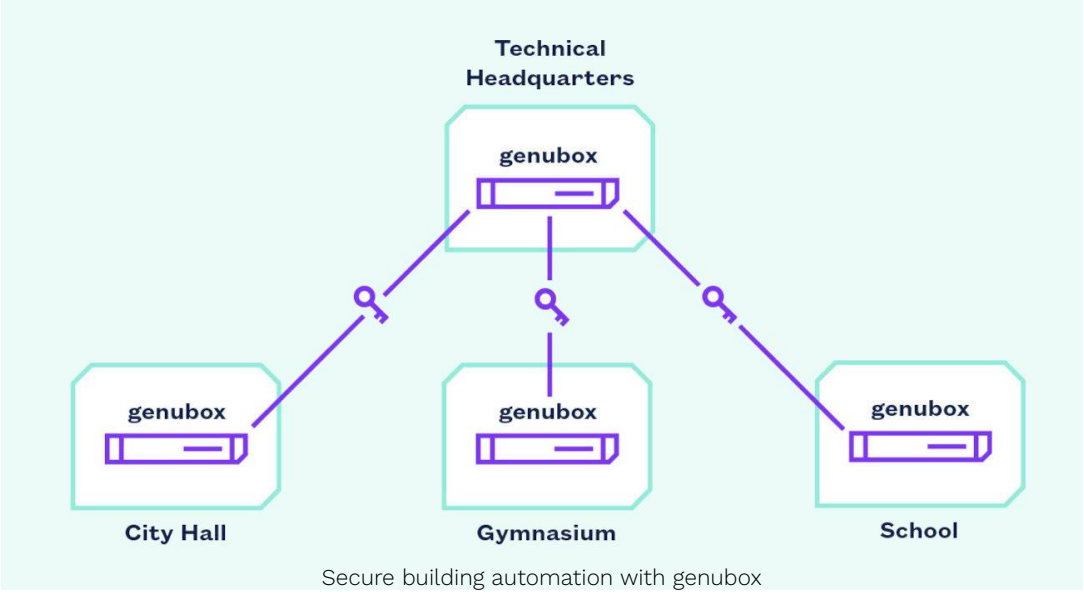
The ability to connect a virus scanner to the rendezvous server or the service box allows the data sent by the service provider to be checked for malicious code. This option offers additional protection against attacks and ensures plant availability. Typical maintenance objects are industrial machinery, IT infrastructures, automation systems, document management systems, etc. In this way a technician can for example use the Siemens Simatic Manager in a secure remote maintenance connection to access the automation system of a production line. Due to the genua Remote Maintenance App he doesn't need to make adjustments to his project software at a later on-site appointment with the customer.

4.2. Secure VPN Connections via SSH or IPsec

A common application of genubox is the provision of encrypted, authenticated connections. genubox however has a special feature in this highly competitive market: It is a product variant of the CC EAL 4+ certified genuscreen. The architecture meets the requirements of the German federal office of secure information technology (BSI), which periodically and rigorously tests the genuscreen in security audits. Since genubox possesses an application module, and therefore has an interface for individual applications, it is not certifiable. However, because of it's high level of security, it is especially well suited for critical areas of application, in which VPN solutions with lower transparency are not supposed to be employed.

4.3. Customer-Specific Solutions

genua works together with customers to develop individual solutions: Software applications of the customer – or developed by genua for the customer – are combined with genua's VPN solution by use of the application module. Reliable and fast manufacturer support and the security of the VPN connection are priorities for our clients. Common use cases are applications for building automation in the private and public sector, amongst others.



Secure building automation with genubox

4.4. Secure Connection of Mobile Applications to a Network of an Organization

The connection of mobile devices such as smartphones and tablets is an increasingly important issue in businesses. In this field genubox, too, is a possible solution with an enhanced level of security. As a gateway based on the CC EAL 4+ certified genuscreen, it allows for encrypted and authenticated connections between mobile employees and the network of the corporate headquarters. Data transmissions are reliably secured at all times.

5. Interface to SIEM Systems

genubox has an interface to SIEM systems (Security Information and Event Management) for the central recording of all security-related information from the remote maintenance solution. You can use this to intelligently link these to messages from other systems and trace attempted attacks that remain undetected when only looking at individual systems.

6. Support of Zero Trust Concepts

With Zero-Trust networking, trust in the security of the entire network is replaced by trust in the security of specific communication endpoints, i. e. devices, services, and applications. A compromise of individual endpoints is thus limited to the permitted communication relationships and no longer endangers the entire network.

This approach gives the operator back control of his systems and proactively reduces the attack surface.

The remote maintenance solution from genua supports Zero Trust concepts. In this context, the rendezvous server takes on the role of the software-defined perimeter and allows authenticated external users to access only specific services. This is where the target system connects from the inside. The remote maintainer, in turn, also establishes encrypted communication with this perimeter. After successful authentication, access is only granted to specifically required services, e.g. on the desktop of the machine to be maintained, the terminal or on selected ports.

This is done according to the principle of least privilege: only the desired protocol of the software determines the connection, all other applications or even both networks are not linked.

7. Connection to Central User and Rights Management Systems

An interface to identity and access management systems enables the remote maintenance solution to be flexibly connected to a central user and rights management system. genubox supports OKTA, Keycloak, Azure Active Directory, Microsoft Active Directory and RADIUS (Remote Authentication Dial-In User Service).

8. Central Management via genucenter

A substantial advantage of genua's remote maintenance solution is the possibility of central administration. The Central Management Station genucenter serves as an effective and resource-conserving tool for configuring, monitoring, and administrating of genuboxes. It offers an overview of the installation in question, and ensures that all systems are up to date and functioning faultlessly.

Changes and updates can be applied simultaneously to any number of systems via user-friendly grouping functions. This enables you to implement policies consistently across the entire network. In installations that are under development, newly added systems can be easily integrated into the central management station, from which they can be immediately supplied with proven configurations.

9. Product Variants

genubox is available in different models:

genubox XS: This version features a smart card reader, three network interfaces, and is suitable for operation in 19" rack cabinets.

genubox XSo: This is our basic version for office use.

genubox XSi: This rugged hardware version offers three network interfaces, and can be installed simply in a machine using a DIN rail mounting.

genubox S, M, and L: The versions are suitable for operation in 19" rack cabinets and are primarily used as high-performance Rendezvous Servers.

genubox is also available as a software version for operation on customer systems or in public clouds (Microsoft Hyper-V, Linux KVM, VMWare ESXi, and VMWare vSphere virtualizers) in different performance classes.

10. Customer Service

Customer service for genubox is provided directly by the manufacturer, genua, a leading specialist in network administration and IT security. If requested, we will handle all aspects of managing your remote maintenance solution. Our specialists will then keep a constant watch on your system via strongly encrypted Internet connections and take care of the entire administration, so that you can rely on the systems running smoothly at all times.

We also offer a support hot-line to answer your questions by telephone or by e-mail, as well as a regular update service. We will be happy to put together a customized service package for you. Please contact us for further information.

GB-WP-0523-18-E

Contact us:

genua GmbH, Domagkstrasse 7, 85551 Kirchheim, Germany

T +49 89 991950-0, F +49 89 991950-999, E info@genua.de, www.genua.eu