

genubox

Facts & Features



Remote Maintenance Solution

genua.



genubox is available in various hardware and virtualized versions.

Definition

genubox combines remote maintenance, monitoring, crypto, and filter functionality with a compact application platform. It is developed for the secure remote management of application servers as well as complex industrial plants via insecure networks. For the exchange of data, genubox initializes SSH-based tunnels to the maintained systems with strong authorization and encryption algorithms such as AES. genubox completely separates the network of the service provider and the network of the system operator. The integrated application level gateway even separates remote desktop connections on application level.

Reasons to Choose genubox

- A versatile solution for smart remote maintenance applications
- Different hardware versions for operation in 19" rack cabinets or DIN rail installation as well as genubox Virtual variant for operation e.g. on customer systems or in private and public Azure clouds
- Strongly encrypted data transfer
- OpenID Connect to support identity providers such as Microsoft Entra ID (formerly Azure Active Directory), OKTA, and Keycloak for on-premises operation
- Windows app for maintainers and operators supports host integrity check via Windows security center
- Additional browser-based app for maintainers supports remote desktop sessions (RDP, VNC, SSH)
- Remote access session can be monitored and recorded (RDP, VNC, SSH)
- Monitoring via SNMPv3 and Syslog logging
- Security event logging in Common Event Format for SIEM integration

- Based on genuscreen, a firewall & VPN appliance certified according to Common Criteria and approved by the German Federal Office for Information Security BSI
- Easy integration of applications for machine monitoring, remote diagnosis, remote management access, and preventive service systems
- Central administration of all components
- Storage and access management solution genuvview for remote desktop session recordings (the recommended hard drive storage is at least 32 GB)

Typical Use

- Remote maintenance access to target systems, e.g. IT/OT objects based on TCP such as machine/plant control stations or production lines via OPC UA, S7, MODBUS TCP etc.
- Remote administration of Windows-related systems via RDP or SSH

Customer Service

- Customer service directly from the manufacturer
- Security system management
- Hotline and update service
- Comprehensive training courses

SecurITy
made
in
Germany

Excellence in Digital Security.

Rendezvous

| | |
|--|---|
| Secure access | SSH tunnels for remote maintenance, multi-factor authentication via RADIUS, Smart Card or Yubikey |
| Full control | Communication must be launched from both sides, operator can stop communication at any time |
| Operator GUI | Easy to use web interface to manage remote maintenance |
| Access authorization | Assign or withdraw write access for maintenance provider on the fly |
| Observe | Intercept clear text on the rendezvous system |
| Isolate | Separate the target system from the rest of the network |
| Audit | Complete logging of all transactions, recording of remote desktop sessions |
| Application Level Gateway (Remote Desktop) | Separation by window manager instance with VNC server and VNC/RDP client for each target system |
| Windows app | Dedicated app for Windows devices allows user-friendly and secure remote access control for operators and service providers |
| Browser-based app | High flexibility through dedicated app for Safari, Chrome, and Edge web browsers on laptops, tablets, and desktop computers |
| File transfer | Secure data transfer through integration of virus scanner option via ICAP and storage of the transferred data |

Firewall

| | |
|-----------------------------------|--|
| Stateful packet filter | State of the art firewall for manageable rule sets |
| Bridging firewall | Invisible firewall on the data link layer (layer 2) |
| Network Address Translation (NAT) | Masquerade networks behind one address |
| Quality of Service (QoS) | Guarantee service priorities |
| Queuing (traffic shaping) | Bandwidth management to control traffic volume |
| Traffic redirection | Forward public services to internal services |
| Filter criteria | Filtering decision can be based on IP address, network protocol, port, interface, flags, and state |
| Filter action | Choice of packet handling: pass, block, drop |
| DDoS protection | Proxy for the TCP handshake protects services against TCP SYN floods used by DDoS attacks |
| Spoofing protection | Block forged packets |
| Packet normalization | Reassemble fragmented packets, generate random IP identification, enforce IP header settings such as TTL and MSS |
| Enhanced protection | Privileged separation, sandboxing |

Virtual Private Network (VPN)

| | |
|----------------|---|
| SSHid | VPN on the protocol layer (layer 4, TCP) |
| IPsec | VPN on the network layer (layer 3) |
| Bridging Ipsec | VPN on the link layer (layer 2) |
| L2TP | Support for Android, iOS, Mac OS X, Windows (layer 2) |

Networking

General

| | |
|--------------------------|--|
| Redundant network access | Multiple uplinks |
| DNS | Enable local DNS caching |
| NTP client | Obtain time from NTP servers |
| DHCP server | Automatically assign IP addresses to clients |
| DHCP relay | Forward DHCP queries to central DHCP server |
| VLAN | Supports virtual LANs to separate networks |
| Trunking | Aggregate multiple network interfaces on one virtual interface |

Networking

| IPv6 | |
|-------------------------|---|
| Native IPv6 | Fully IPv6 ready |
| Tunnelling | Use tunnelling to cross legacy IPv4 networks |
| NAT64 | NAT between IPv4 and v6 |
| Routing | Policy based routing Based on IP addresses/networks |
| Static routes | For small and easy setups |
| OSPFv2, v3 | Popular routing protocol among large corporate networks |
| Virtual routing domains | Separate routing domains on one appliance |

Integration

| | |
|--------------------------|--|
| Application platform | Development and integration of customer-specific software |
| Maintainer Box | Appliance as access point for external applications enables access to target systems |
| genuview | Scalable access and storage management solution for remote desktop session video recordings (not recommended for XS and XSo hardware) |
| Virus scanner | Optional external virus scanner with ICAP interface |
| Access management system | Microsoft Active Directory, Microsoft Entra ID (formerly Azure Active Directory), OKTA, RADIUS, and Keycloak (on premises or in the cloud) |

Administration

General

| | |
|----------------------|--|
| Web GUI | Powerful web-based user interface secured with TLS/SSL (HTTPS) |
| Online documentation | Instant help via user interface |
| Shell access | Local using console or serial interface, remotely using SSH |
| USB update | Fix offline systems with USB stick |

Patch Management

| | |
|-------------------|--|
| GUI | Get and install patches via GUI |
| Automatic updates | Automate the process of fetching updates for the appliance |
| Patch rollback | Return to previous patch level |

Logging

| | |
|---------------------|--|
| Syslog | Use a third party syslog server to store logs |
| Hard drive | Use appliance hard drive for storage, if available |
| Memory | Logs are recorded in memory |
| Central | Use genucenter to concentrate the logs on one system |
| Common Event Format | Enable monitoring of remote maintenance access by SIEM systems |

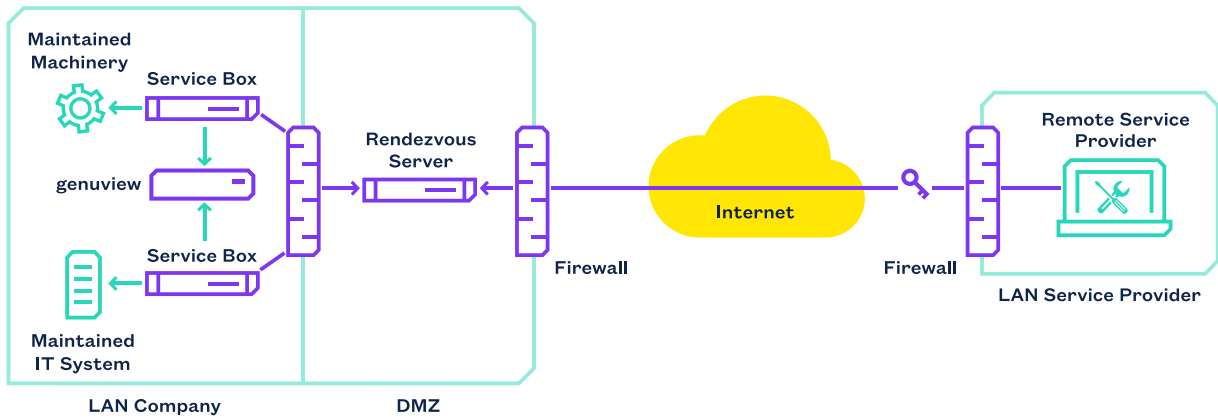
Debugging

| | |
|--------------------|--|
| Network | Powerful command-line tools: tcpdump, traceroute, ping, etc. |
| Firewall | Status, rules, and logs monitoring |
| VPN | Connection status overview and problem analysis |
| Central Management | Easy administration of several (thousand) systems with management station genucenter |
| Integrity check | Rendezvous configuration is checked for integrity at configuration time |

More product information



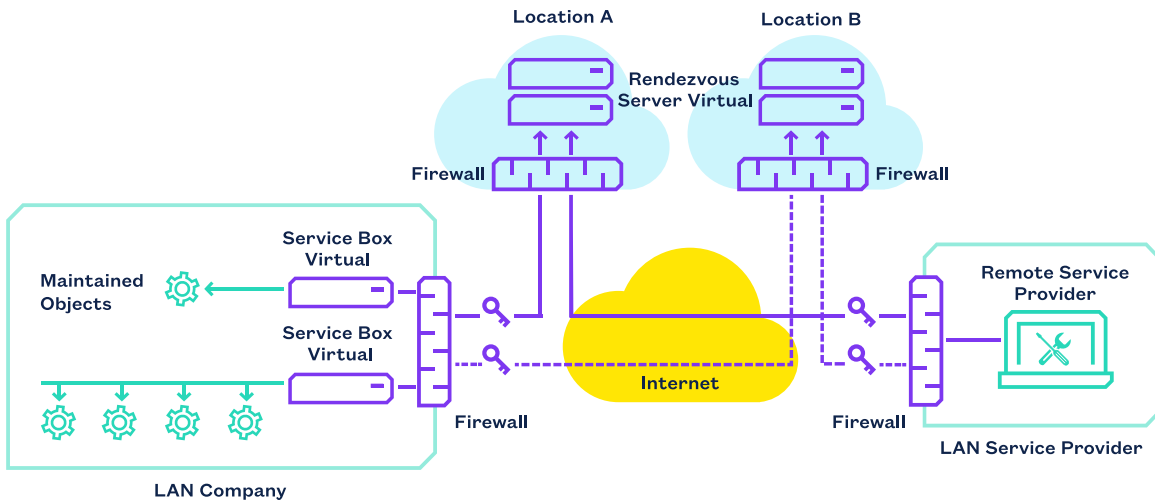
Use Cases



Secure Remote Maintenance via Rendezvous in the DMZ

The genua rendezvous solution allows extensive maintenance access control. The remote maintenance provider and the system operator create connections to a rendezvous server in a DMZ (demilitarized zone).

Access to target systems is provided for users or user groups based on a whitelisting policy. As default, access must be granted at runtime by the operator. All activity is logged and can be monitored in real-time as well as recorded on video.



Secure Remote Maintenance within Virtualized Environments

The rendezvous server can be operated georedundantly as a software application in private and public clouds such as Azure. It is also possible to operate virtualized service boxes locally. For this use case, various hypervisors are supported.

Further Information:

www.genua.eu/genubox

genua GmbH

Domagkstrasse 7 | 85551 Kirchheim | Germany
+49 89 991950-0 | info@genua.eu | www.genua.eu