Remote Service Appliance
genubox
Facts & Features

**Definition:**
The genubox combines crypto and filter functionality with a compact application platform. It is developed for the remote management of single servers as well as complex industrial plants via unsecured networks. For the exchange of data, the appliance initializes VPN tunnels to the managed servers with strong encryption and authorization. Highly secure encryption algorithms such as AES are used. An integrated stateful packet filter separates the maintained systems from the rest of the network, so that external access only is possible to the maintenance area.
The genubox application platform supports the implementation of custom applications for any location: monitoring and maintenance of machinery, electronic building control, or information processing e.g. to optimize data exchange over satellite connections.

**Typical Use:**
- Monitoring, remote control and maintenance of machinery like automation systems, printing machines, wind turbines, diesel engines of ships
- Remote administration of “Windows” server systems

**Customer Service:**
- Customer service directly from the manufacturer genua
- Security system management
- Hotline service / update service
- Free hardware support for three years from date of purchase
- Comprehensive training courses

**Reasons to Choose genubox:**
- A versatile platform for intelligent remote maintenance applications
- Strongly encrypted VPN data transfer
- SSH-based VPN to connect overlapping networks
- Connections via all terrestrial networks, and satellite
- Two factor authentication (Yubikey)
- User-friendly Windows app for convenient operation
- Remote access session can be monitored and recorded (RDP, SSH)
- Connection logging
- Redundant network access optionally, e.g. with UMTS interface
- High availability through clusters
- High security standards guaranteed by the OpenBSD operating system
- Maintenance-free industrial hardware installed on DIN rails
- Easy integration of applications for machine monitoring, remote diagnosis, remote management access, tunnels for ASP applications, and preventive service systems
- Easy configuration via USB stick
- Administration of numerous appliances via Central Management Station genucenter

**Reasons to Choose genua:**
- Leading German specialist for IT security
- Founded in 1992 – implementation of numerous major projects for industrial, government, and military organizations
### Firewall

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

### Virtual Private Network (VPN)

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHld VPN</td>
<td>VPN on the protocol layer (layer 4, TCP)</td>
</tr>
<tr>
<td>IPsec</td>
<td>VPN on the network layer (layer 3)</td>
</tr>
<tr>
<td>Bridging IPsec</td>
<td>VPN on the link layer (layer 2)</td>
</tr>
<tr>
<td>L2TP</td>
<td>Support for Android, Windows, iOS, Mac OS X (layer 2)</td>
</tr>
</tbody>
</table>

### IPsec VPN

#### General

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAT-Traversal (NAT-T)</td>
<td>Supports connections between NATed devices</td>
</tr>
<tr>
<td>NAT for VPN</td>
<td>Connect locations with overlapping network ranges</td>
</tr>
<tr>
<td>High availability (async)</td>
<td>Synchronise security associations between multiple appliances to minimize failover outage</td>
</tr>
<tr>
<td>High performance replay protection</td>
<td>Increased replay windows</td>
</tr>
</tbody>
</table>

#### Operation Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tunnel mode</td>
<td>Entire IP packet is encrypted and encapsulated</td>
</tr>
<tr>
<td>Transport mode</td>
<td>Only the payload is encrypted</td>
</tr>
<tr>
<td>Network mode</td>
<td>Supports routing protocols such as OSPF over VPN connections</td>
</tr>
<tr>
<td>Layer 2 bridging</td>
<td>Use IPsec to connect two locations on layer 2</td>
</tr>
<tr>
<td>Transparent IPsec router</td>
<td>Encrypt your WAN traffic without changing your topology</td>
</tr>
<tr>
<td>IKEv2</td>
<td>Connect mobile or third party devices</td>
</tr>
<tr>
<td>L2TP</td>
<td>Support for Android, Windows, iOS, Mac OS X (layer 2)</td>
</tr>
</tbody>
</table>

#### Authentication

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RSA</td>
<td>De facto public-key standard</td>
</tr>
<tr>
<td>Elliptic curves</td>
<td>Fast key exchange</td>
</tr>
<tr>
<td>Pre-shared keys</td>
<td>Manually exchange secret pair of keys</td>
</tr>
<tr>
<td>PKI (X.509)</td>
<td>Use a certificate authority (CA) to verify keys</td>
</tr>
</tbody>
</table>

#### Algorithms

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>AES-128, AES-192, AES-256, 3DES, Blowfish, CAST</td>
</tr>
</tbody>
</table>

### SSHld VPN

#### General

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Single TCP connection</td>
<td>Outgoing only, no problems with firewalls or NAT</td>
</tr>
<tr>
<td>Comes with NAT</td>
<td>Connect locations with overlapping network ranges</td>
</tr>
<tr>
<td>No interlinking</td>
<td>Easily prevent unwanted traffic</td>
</tr>
<tr>
<td>Compression</td>
<td>Increase net throughput</td>
</tr>
</tbody>
</table>

#### Operation Modes

<table>
<thead>
<tr>
<th>Mode</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bidirectional</td>
<td>Like any other VPN</td>
</tr>
<tr>
<td>One-direction</td>
<td>Offer centralised services to hundreds of branch offices (e.g. SAP)</td>
</tr>
<tr>
<td>Semi-bidirectional</td>
<td>E.g. allow printing at the branch office from central SAP server</td>
</tr>
</tbody>
</table>
## Networking

### General
- **Redundant network access**: Multiple uplinks
- **DNS**: Enabling local DNS caching
- **UMTS/WLAN option**: External UMTS or WLAN interface
- **NTP client**: Obtain time from NTP servers
- **DHCP server**: Automatically assign IP address to clients
- **DHCP relay**: Forward DHCP queries to central DHCP server
- **Trunking**: Aggregate multiple network interfaces on one virtual interface
- **PPPoE**: DSL uplinks
- **Native IPv6**: Fully IPv6 ready
- **Tunnelling**: Use tunnelling to cross legacy IPv4 networks
- **NAT64**: NAT between IPv4 and IPv6

### IPv6
- **Tunnelling**: Use tunnelling to cross legacy IPv4 networks
- **IPv6**: Native IPv6

### 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
- **RIP**: Routing Information Protocol
- **MPLS/LDP**: Multiprotocol Label Switching/Label Distributing Protocol

## High Availability

### Active-active with load balancing
- Distribute load on several appliances depending on the source/destination IP address

### Link aggregation
- LACP: easy integration in a redundant/high-performance switch setup

### Hot standby
- Reserve appliance for automatic failover

## Monitoring

### System
- System status (memory, load)

### VPN
- Supervise VPN connection status

### NetFlow export
- Monitor network traffic with the NetFlow protocol
- Retrieve information via SNMP GET requests, or send SNMP TRAPs

## Rendezvous

### Secure
- SSH Tunnels for remote maintenance

### Full control
- Communication must be launched from both sides

### Operator GUI
- Easy to use web interface to manage remote maintenance

### Access authorisation
- Assign or withdraw access for maintenance engineer on the fly

### Observes
- Intercept cleartext on the rendezvous system

### Isolate
- Separate the target system from the rest of the network

### Audit
- Complete logging of all transactions

## Extensibility

### Optional modules
- Cache (DNS, HTTP), URL filter

### Application platform
- Add your own custom software

## Administration

### General
- **Web GUI**: Powerful web-based user interface secured with TLS/SSL (HTTPS)
- **Online help**: Instant help via user interface
- **Shell access**: Local using console or serial interface, remotely using SSH
- **Cronjobs**: Schedule jobs at specific times
- **Flexible configuration**: Easily modify/add files to the system
- **USB update**: Fix inaccessible systems with an 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

### Debugging
- **Network**: Powerful command-line-tools: tcpdump, traceroute, ping, etc.
- **Firewall**: Monitor firewall states, rules and logs
- **VPN**: VPN connection status overview and problem analysis
- **Root shell**: The shell offers full root access

### Central Management
- **Central Management**: Easy administration of several (hundred) systems with Management Station genucenter
Secure Remote Maintenance via Rendezvous in the DMZ

Companies with a large number of machines on the one hand, and providers of remote maintenance on the other, are faced with the need to set up an increasing number of remote maintenance connections. This means remote maintenance service providers need to have access to external company networks. This touches directly on the sensitive area of IT security: If unauthorized persons or malicious codes manage to hack into the LAN via this maintenance access, this can have serious consequences.

genua has developed a solution that allows you to keep a close eye on every maintenance access. The concept: One-way access to external networks is not permitted. Instead, at an agreed time, the remote maintenance provider and the customer create VPN connections to a server in a demilitarized zone (DMZ), i.e. outside their own networks. A continuous connection is created only once the rendezvous has been established on the server. This connection now allows the remote maintenance provider to access the machine that is being monitored. In this process, the maintenance connection allows access only to the machine being monitored, since the genubox uses its firewall function to isolate this area from the rest of the LAN.

This prevents any access to other areas of the external network. In addition, all activity is logged, so that access can be traced at all times. This rendezvous solution makes it possible for both service providers and companies to operate in a secure way as many remote maintenance connections as they like.

Application Example

Setup with Rendezvous in the DMZ of the Service Provider