



# GeNUBox

A Security Platform with a Wide Range of  
Applications

Technical Information



# Table of Contents

<b>1</b>	<b>GeNUBox: A Security Platform with a Wide Range of Applications.....</b>	<b>1</b>
1.1	Description of the Problem.....	1
1.2	Possibilities and Limitations of Traditional Remote Maintenance Methods.....	1
1.2.1	Opening the Firewall, or Access via Modem/ISDN.....	1
1.2.2	Access via IPsec.....	2
<b>2</b>	<b>The Solution: Secure Access for Remote Maintenance with the GeNUBox.....</b>	<b>2</b>
2.1	Using the GeNUBox as a VPN Gateway.....	2
2.2	Setting up a Rendezvous Server.....	3
<b>3</b>	<b>Overview of the GeNUBox.....</b>	<b>4</b>
3.1	The Basic Module.....	4
3.1.1	Crypto Tunnels for TCP Sessions.....	4
3.1.2	Bridging Packet Filter.....	4
3.1.3	Console Servers.....	4
3.1.4	IPsec Gateway.....	5
3.1.5	Access Router.....	5
3.2	The Application Module.....	5
<b>4</b>	<b>Traffic Optimization for Satellite Communication.....</b>	<b>5</b>
<b>5</b>	<b>Application Cases.....</b>	<b>6</b>
5.1	Continuous Equipment Maintenance.....	6
5.2	Client-Server Connection.....	6
5.3	Remote Maintenance of CNC Machines.....	7
5.4	Remote Maintenance of Printing Machines.....	7
<b>6</b>	<b>Performance.....</b>	<b>8</b>
6.1	Hardware Models.....	8
6.2	High-Availability Solutions.....	8
<b>7</b>	<b>Central Management via GeNUCenter.....</b>	<b>9</b>
<b>8</b>	<b>Customer Service.....</b>	<b>9</b>



# **1 GeNUBox: A Security Platform 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, whether they are manufacturers or users.

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

## **1.1 Description of the Problem**

Whether you are dealing with a work stoppage at the plant, or travel expenses incurred by a maintenance team – time is money. If you are able to monitor equipment permanently, it is a lot easier to solve problems quickly and to avoid or reduce downtimes.

Manufacturers who sell their high-maintenance industrial machinery, manufacturing equipment, or drive systems all around the world usually use 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.

## **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 entails risks – identification and authentication of the remote maintenance provider is either inadequate, or non-existent (risk factor no. 1). This means



there is a danger of third parties gaining access. In addition, a hacker could intercept and possibly take control of the access established for remote maintenance purposes (risk factor no. 2). Furthermore, if there are any implementation errors in the firewall, this may enable direct access to other areas in the customer's network.

Because of these risks, the standard solution represents a threat to the customer's entire network.

### 1.2.2 Access via IPsec

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.

## 2 The Solution: Secure Access for Remote Maintenance with the GeNUBox

The security platform GeNUBox offers the flexible operating system OpenBSD with a TCP/IP stack, routing functions, a packet filter, authentication methods, and important cryptographic functions. In the following, you will discover how these can be used effectively to protect remote maintenance access.



Fig. 1: The security platform GeNUBox 100i

### 2.1 Using the GeNUBox as a VPN Gateway

The first and second risk factors can be eliminated by using the VPN protocol SSH with 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.

A filter function serves to divide the customer's network into two areas. One area is containing 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 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.

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

The GeNUBox packet filter function 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.

## 2.2 Setting up a Rendezvous Server

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.

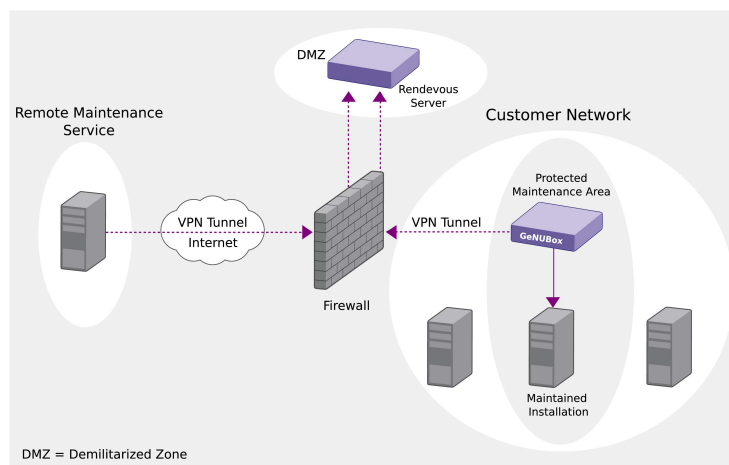


Fig. 2: Rendezvous in the DMZ as a secure solution

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



In summary: the GeNUBox, used in combination with a rendezvous server, offers maximum control and security for remote maintenance solutions, without the need for any adjustments to be made to the firewall or other systems in the customer's network.

You can find more detailed information on this topic in our white paper: "Secure Remote Maintenance with GeNUBox and Rendezvous Server."

## **3 Overview of the GeNUBox**

The possibilities provided by the GeNUBox far exceed those of a traditional VPN appliance. In addition to basic cryptographic functions (basic module), the GeNUBox offers an application platform (application module) on which you can integrate the application that suits your purposes in each case. Because of its different interfaces (four network interfaces, a serial port, and USB), as well as flexible communication options via modem, ISDN, DSL, GMS, UTMS, GPRS, and satellite, the GeNUBox is suitable for virtually all fields of application.

### **3.1 The 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 with sufficiently long keys (e.g. 3DES, AES, Blowfish) 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 isolated by proxies or NAT routers, even if several of these areas use identical IP addresses.

#### **3.1.2 Bridging Packet Filter**

The GeNUBox features a high-performance stateful packet filter that can be used to monitor all connections that are established or handled via the GeNUBox, up to OSI layer 4. Since the 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, the GeNUBox can be used as an invisible firewall to isolate a system, or an entire network.

#### **3.1.3 Console Servers**

Servers can be administrated very easily via a serial console. Even changing the configuration in single user mode (no network) is not a problem. In addition, this access is



encrypted by the GeNUBox, and additional authentication (GeNUBox + server) is carried out, ensuring secure out-of-band administration.

#### **3.1.4 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, thanks 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.

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

#### **3.1.5 Access Router**

The GeNUBox can also be used as an access router, which gives you the advantage of redundant network access (RNA). In the event that a main line is down, this allows you to use an alternative access path until the main line has been restored. It is also possible, of course, to protect the access using the integrated packet filter.

### **3.2 The Application Module**

A customer may wish to use individual applications within a project. These can be integrated in the 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 Traffic Optimization for Satellite Communication**

Wind turbines in remote regions, oil-drilling installations, or ships at sea often cannot be reached via terrestrial networks. In this case, setting up stable satellite links is not a problem: the actual challenge lies in using the bandwidth efficiently, as waiting for a TCP response to enable a controlled data transfer may take only a split second with terrestrial networks, but with satellite communications can be a severe test of your patience.

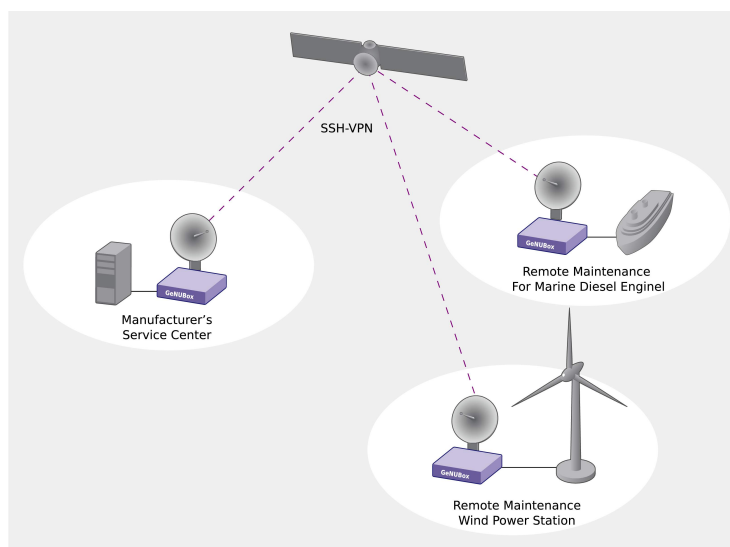


Fig. 3: Satellite communication with three GeNUBoxes

In order to avoid long transfer times and high costs, GeNUA has developed a traffic optimization feature for high-speed, reliably encrypted communication via satellite. In favorable conditions, this can make the transfer speed 20 times faster.

## 5 Application Cases

When it comes to secure remote applications, many companies and authorities already rely on the GeNUBox. Below are some possible scenarios for its use.

### 5.1 Continuous Equipment Maintenance

Large industrial installations are often equipped with Ethernet-capable measuring and control systems that the manufacturer can access for maintenance purposes, and for which a regular data transfer can be set up. These installations cannot be accessed by routing. Instead, they are hidden behind a firewall and can be accessed only via layer 4 tunnels. This means you need a solution that activates and controls the data transfer. In such cases, everything points to the GeNUBox as a solution.

### 5.2 Client-Server Connection

An application service provider (e.g. of SAP services) would like its customers or branch offices to have a secure connection for the application protocol, which does not allow for encryption, and at the same time would like to access printers in the user's network. Neither the client nor the printers are accessible via IP because they are located behind a DSL/NAT router. The GeNUBox creates the tunnel for the application, as well as the return tunnels for the print jobs.



### 5.3 Remote Maintenance of CNC Machines

A provider of CNC machines would like to access the end customer's CNC machine for maintenance purposes via pcAnywhere™ software. With access via pcAnywhere™ software, the maintenance technician has the same level of access to the end customer's network as a local user, which is often unacceptable to the end customer. With a GeNUBox, the service technician's access is handled securely via SSH. At the same time, the bridging packet filter function of the GeNUBox isolates the CNC machine from the network so that the maintenance provider can access the CNC console, but not the local LAN.

### 5.4 Remote Maintenance of Printing Machines

A printing machine manufacturer has customers who use its products all over the world. The machines themselves contain several logically separated computer networks linked by routers. These are needed for job management, as well as for control and maintenance functions. The machines are connected to the Internet via the customer's networks, which are protected by a firewall. In order for the service technician to access the machines remotely for maintenance purposes, there are two possibilities:

Dial-up: the service technician dials up the machine via the telephone line. However, this is an expensive solution that results in a very high telephone bill.

Network coupling: the service technician uses IPsec to connect to the customer's network via the Internet to access the machine's networks. The disadvantage here is that the manufacturer needs to know about all of the customer's networks, and many customer networks have a high proportion of identical logical addresses. This leads to unavoidable problems on both sides. Furthermore, the customer needs to have a permanent Internet connection, so that the parameters do not have to be reconfigured for each access.

GeNUBox has the solution: if the customer does not have a permanent Internet connection, the GeNUBox is simply connected to an access router. The manufacturer dials up this router as required, sends a specially formatted and signed UDP packet to the GeNUBox, and immediately disconnects again after just a few seconds. In response to this, the GeNUBox connects to the Internet (e.g. via the local provider), and creates either an SSH tunnel to the manufacturer, or a common meeting point. The manufacturer can now carry out maintenance activities in an application-based manner via this tunnel.

If the customer does have a permanent Internet connection, there is the option of either establishing a permanent tunnel, or allowing the customer to create a tunnel using the method described above, only when remote maintenance work is needed.

Both solutions are extremely cost-effective and offer a high level of security and flexibility – for both the customer and the manufacturer.





## 7 Central Management via GeNUCenter

The GeNUCenter central management station serves as a tool for configuring, monitoring, and administrating the 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.

## 8 Customer Service

Customer service for the 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 hotline 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-0110-1-E

**Contact us:**

GeNUA mbH • Domagkstrasse 7 • 85551 Kirchheim • Germany  
phone +49 (89) 99 19 50-0 • fax +49 (89) 99 19 50-999 • [info@genua.eu](mailto:info@genua.eu) • [www.genua.eu](http://www.genua.eu)