



Secure Remote Maintenance with GeNUBox and Rendezvous Server

This document presents a remote maintenance solution for the maintenance of any systems in customer IT networks. It begins with a discussion of the shortcomings presented by standard maintenance access, and gives a step-by-step description of the clear improvements that result from using the GeNUBox from GeNUA on the one hand, and a rendezvous server in the firewall system on the other.

1 Introduction

Remote maintenance of computer systems is a topic that is growing in importance. One reason for this is the growing number of operators that transfer responsibility for the maintenance of their systems (or part of them) to external service providers as part of an outsourcing strategy, with the aim of cutting costs.

A further reason is the fact that virtually every manufacturer of complex software, hardware, and computer-assisted industrial systems insists on network-based access to the systems supplied to its customers, for maintenance and diagnosis purposes. These products may include, for example, customized professional software solutions, computerized tomography scanners, and giant equipment such as turbines.

For the purposes of remote maintenance, the customer's IT network needs to be partially opened for the maintenance company. Such an opening is basically unavoidable, but – for security reasons – it should be minimized as much as possible. At this point, customers frequently have misgivings about standard methods of implementing remote maintenance access, because these expose unnecessarily large portions of their IT network. In addition, there is generally inadequate security for the identification and authentication of the accessing service provider.

An improvement in this situation is clearly in the interest of customers who wish to (or have to) avail themselves of a remote maintenance service, without compromising their network security to any serious degree. But from the point of view of the remote maintenance provider, too, an access system that is efficient in terms of security will increase the level of acceptance on the part of its customers.

This document presents such a system step by step. Section 2 presents the typical starting situation for customers that have secured their IT network against third-party access. Section 3 describes the risks accompanying standard solutions for remote maintenance access. Section 4 looks at safeguarding the system with IPsec, which is sometimes proposed, and the associated risk of unintended coupling with other customer networks.

Next, Section 5 illustrates the first stage in the improved remote maintenance system, whereby the maintenance object is isolated from the rest of the customer's IT network using a GeNUBox appliance. Finally, Section 6 describes the second stage of the solution, where the hazardous opening of the firewall for external access is replaced by a coupling via a rendezvous server. In order that the different functions are clearly explained, the terms *remote maintenance provider* and *customer* will be used consistently in the following.



The term *maintenance object* refers to the system (or collection of systems) that is serviced by the remote maintenance provider.

2 Starting Situation

Figure 1 shows the typical network topology for a customer that has secured its Internet connection with a firewall. The firewall permits access to the Internet from the customer network, but blocks access from the Internet to the customer network.

The maintenance object is located within the customer network, and, since it may provide services for other systems within the network, it needs to be addressed by these. In such a configuration, the remote maintenance provider is unable to reach the maintenance object, because its access to the latter is blocked at the firewall.

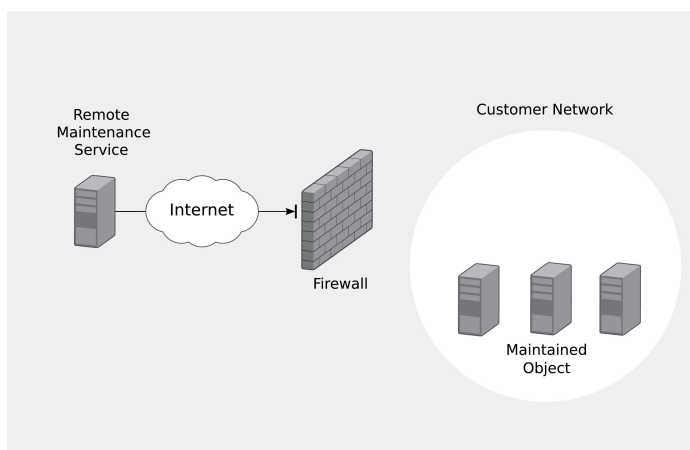


Figure 1: Starting situation in the customer network

3 The Unsatisfactory Standard Solution

In order to enable access for remote maintenance, the customer generally opens the firewall for the remote maintenance provider's sender IP address and for the target IP address of the maintenance object.

This situation is shown in Figure 2. An almost identical arrangement is the establishment of another access path using a modem or ISDN past the firewall.

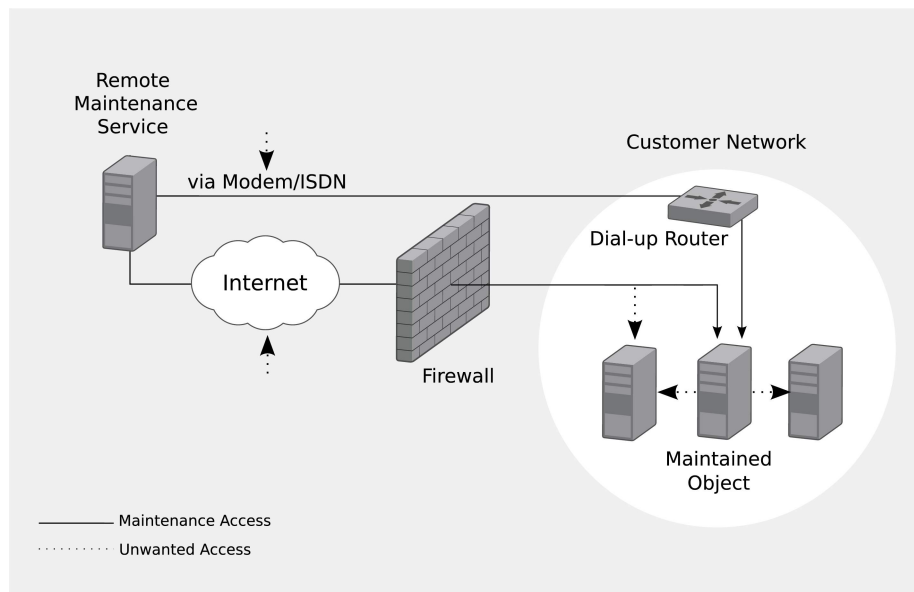


Figure 2: Unsatisfactory standard solution for remote maintenance access

In both cases, the remote maintenance provider gains access to the maintenance object whenever required, via the route shown with a broken line. However, this standard solution harbors the following risks:

1. The remote maintenance provider is not identified (or is inadequately identified) or authenticated for access. This means there is a risk of access by third parties.
2. Attackers can listen in on and hijack the remote maintenance access (dotted lines).
3. Disloyal employees at the manufacturer's company or attackers that have penetrated its network can gain access via the maintenance object to other PCs in the customer network (dotted lines).
4. Any implementation errors in the firewall could allow direct access to other computers on the customer network without using the maintenance object (dotted lines).

Because of these risks, the entire customer network (the area with light-colored background) is at risk when using the standard solution.

4 The Risky Imagined Solution: IPsec

The suggestion is sometimes made that the remote maintenance access could be safeguarded using the VPN protocol IPsec, as shown in Figure 3. While it is true that this eliminates risk factors 1 and 2 described above, factors 3 and 4 still need to be addressed.

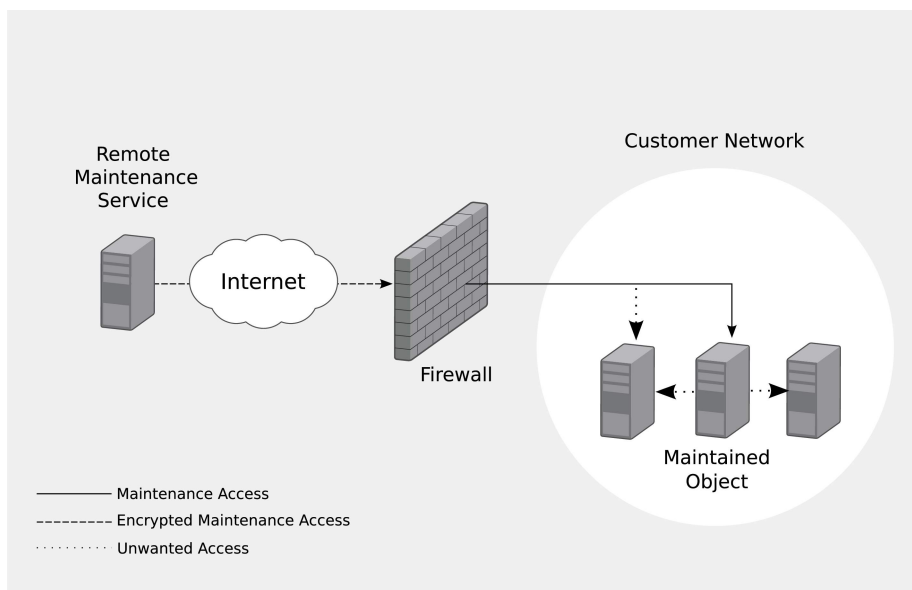


Figure 3: Remote maintenance access using IPsec tunnel

Furthermore, this attempted solution harbors an additional risk. Since IPsec implements a completely transparent and routed network access, the IT networks of different customers that are undergoing maintenance via IPsec at the same time may now unintentionally communicate with one another. In view of the specialization of third-party maintenance firms on maintenance objects that are frequently typical for an industry, there is a real danger that networks operated by competing companies may come into contact with one another.

5 A First Step Towards a Solution: Deployment of the GeNUBox

Two measures are needed to eliminate the principal risks described in Section 3:

- The use of VPN techniques eliminates risk factors 1 and 2. The SSH protocol is ideally suited to this purpose. In comparison with the IPsec method described in the previous section, it offers the advantage of more flexible and individual identification of the remote maintenance provider (elimination of risk factor 1), while heavy encryption prevents eavesdropping on or manipulation of the communication, or the hijacking of the session by an attacker (elimination of risk factor 2).
- The customer network is divided into two areas using a further filter function. The area containing the maintenance object can be accessed by the remote maintenance provider, whereas the other, larger area is not accessible. It is particularly advantageous if the filtering can be carried out on OSI Level 2 (in the *bridging mode*). With normal filtering on OSI Level 3 (in the *routing mode*), the customer network would additionally need to be restructured into two independent sub-networks. This is not required in the bridging mode.



The twin functions of a VPN gateway based on SSH and a packet filter as an additional firewall in the bridging mode are combined in the GeNUBox from GeNUA (see *GeNUBox Technical Information*). The GeNUBox, as shown in Figure 5, is placed at the interface between the two abovementioned areas in the customer network.

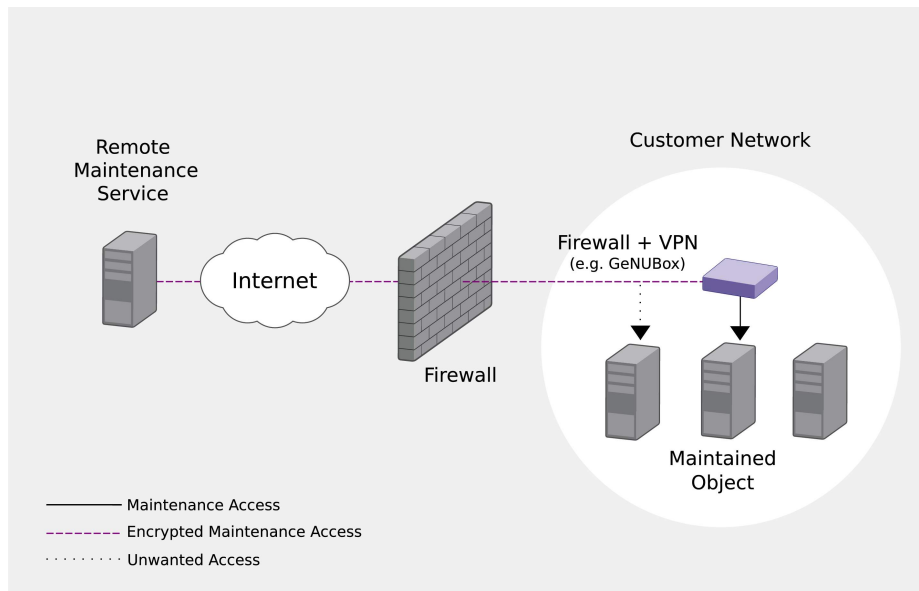


Figure 4: Isolating the maintenance object with GeNUBox

The remote maintenance provider first establishes a VPN tunnel to the GeNUBox (broad broken line), and is authenticated there. Using the tunnel, it can then (using the *local forward* mechanism of SSH) gain access to the maintenance object with any TCP-based applications (unbroken line).

The GeNUBox packet filter function is configured in such a way that existing access options from other customer systems to the maintenance object are unaffected. In contrast, the filter prevents unauthorized connections that the remote maintenance provider intentionally or unintentionally tries to establish between the maintenance object and other customer systems. This basically limits the risks from the remote maintenance access to the area of the maintenance object.

The only risk that remains is risk factor 4 mentioned above, which allows the customer network to be compromised only if there is a malfunction in the main firewall. This risk encompasses the network area shown in Figure 4.

6 A Second Step Towards a Solution: Use of a Rendezvous Server

The remaining risk mentioned in the previous section can ultimately be eliminated by preventing any direct dial-up to the customer network by the remote maintenance provider. Instead, the latter is permitted to connect only to a rendezvous server that is located in a



so-called *demilitarized zone* (DMZ) in the main firewall. This server can also be conveniently implemented using a GeNUBox compact system. This configuration is shown in Figure 5.

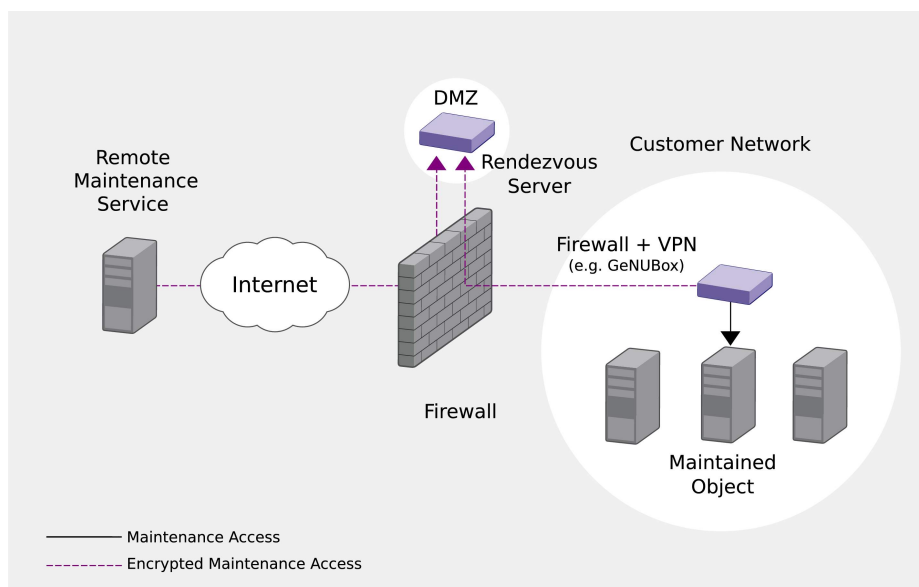


Figure 5: Rendezvous method at the server in the firewall DMZ

For the purpose of the remote maintenance access, the remote maintenance provider first establishes an SSH tunnel to the rendezvous server. From there, however, it cannot establish a connection to the customer network, since any connection requests of this kind are blocked by the firewall. The remote maintenance provider obtains a viable route to the maintenance object only after a further tunnel has been established from the GeNUBox to the rendezvous server by the administrator of the customer network. The overall process comprises the following steps:

1. The remote maintenance provider starts an SSH client application locally, and establishes a connection to the rendezvous server. Appropriate *local forwarding* entries are configured in relation to the rendezvous server for all of the TCP ports required by the maintenance software.
2. The remote maintenance provider identifies itself at the rendezvous server, and, if authentication is successful, a VPN tunnel is established between the PC of the remote maintenance provider and the rendezvous server.
3. The customer network administrator starts an SSH client application on the GeNUBox and establishes a connection from within to the rendezvous server. *Remote forwarding* entries are configured in relation to the maintenance object for all TCP ports required by the maintenance software. Additionally, on the GeNUBox upstream of the maintenance object, the filter kit for productive use is replaced with a maintenance filter kit before the



tunnel is established; in emergencies, this can completely isolate the maintenance system from the rest of the network.

4. The administrator must identify itself if an authentication is configured for the establishment of connections from within. If identification is successful, a VPN tunnel is established between the GeNUBox and the rendezvous server.

5. The remote maintenance provider starts its maintenance software, which connects to the maintenance object via the external VPN tunnel, the rendezvous server, and the internal VPN tunnel. Work may begin once the remote maintenance provider has been successfully authenticated on the maintenance object.

6. When the maintenance work has been completed, the remote maintenance provider closes firstly the tunnel connection to the maintenance object, and then the external VPN tunnel between its local PC and the rendezvous server. The administrator then deletes the internal VPN tunnel between the GeNUBox and the rendezvous server.

This solution eliminates all the risks mentioned in Section 3, and at the same time offers the following advantages:

- The influence of the remote maintenance provider and all associated risks are limited to a smallest possible area around the maintenance object.
- Remote maintenance access is impossible without the co-operation or approval of the customer network administrator.
- All actions taken by the remote maintenance provider, in addition to the maintenance object, can also be logged on the GeNUBox and the rendezvous server in plain text.
- The external VPN tunnel protects the remote maintenance access against eavesdropping, manipulation, or hijacking of the session.
- The internal VPN tunnel prevents direct access by the remote maintenance provider to customer systems that are not in the area of the maintenance object.
- The filter function of the GeNUBox prevents access by the remote maintenance provider from the maintenance object to customer systems that are not in the area of the maintenance object.
- This remote maintenance solution can be implemented irrespective of the type of firewall used by the customer.

GB-WP-0110-1-E

Contact:

GeNUA mbH • Domagkstrasse 7 • 85551 Kirchheim • Germany
phone +49 (89) 99 19 50 0 • fax +49 (89) 99 19 50 999 • info@genua.eu • www.genua.eu