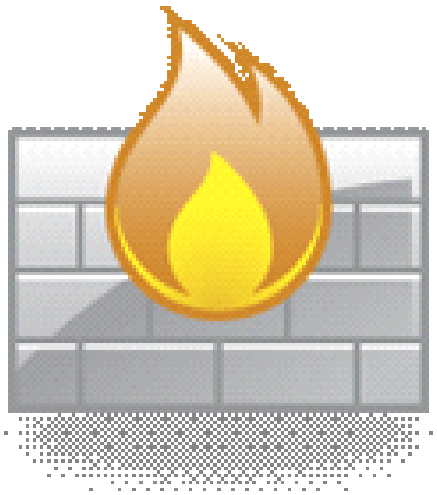
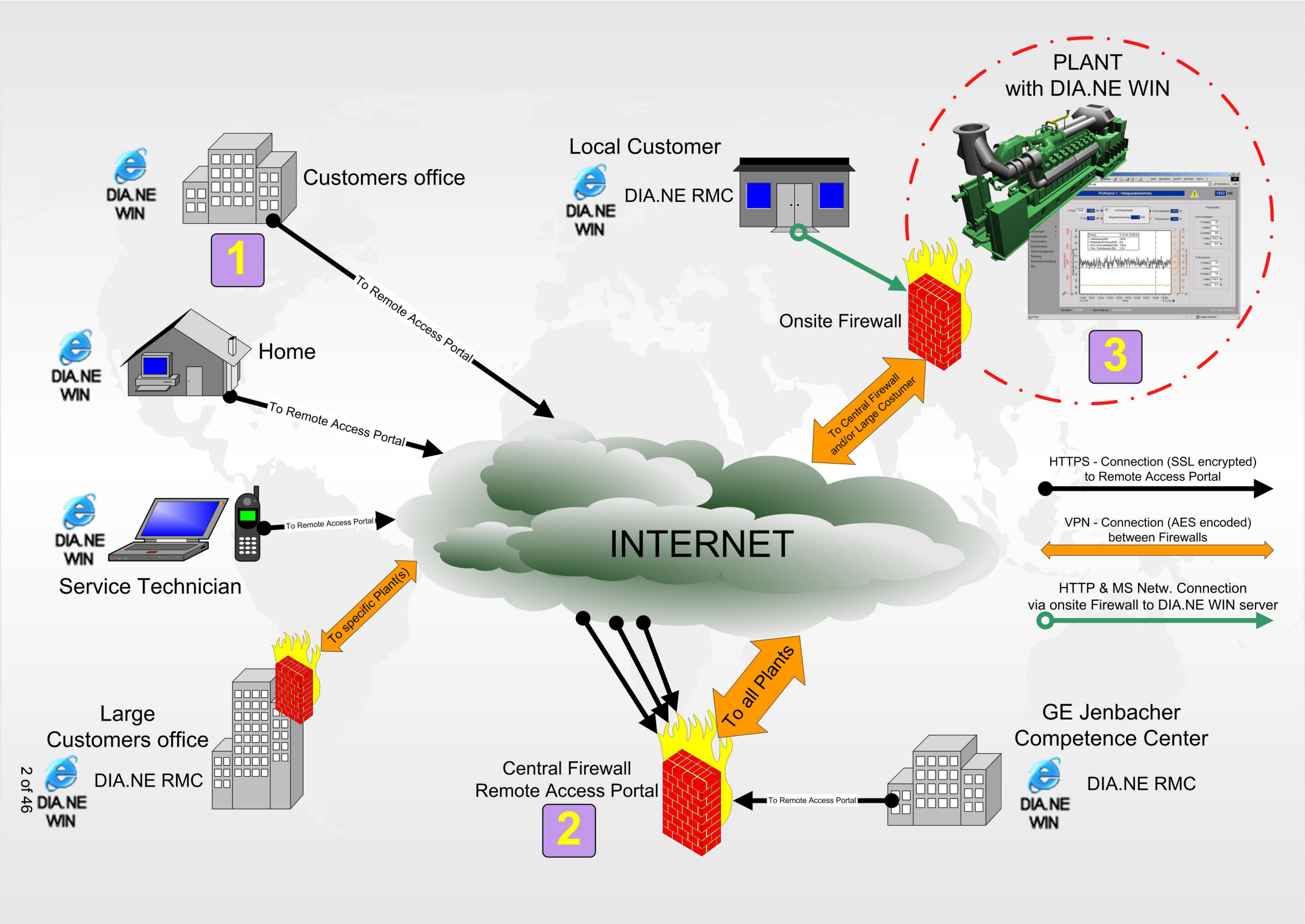
Internet Firewall Information

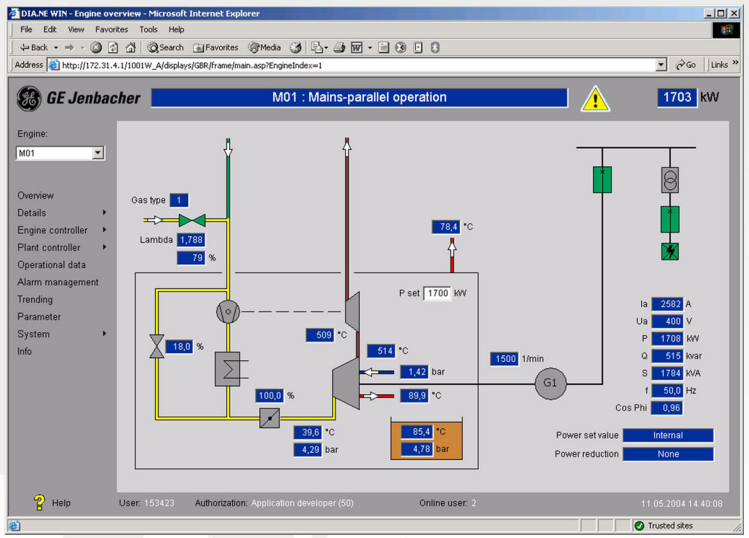
NOTE:

Configuration Request Form to be filled out by customer and returned to NES / WES
Configuration Request Form in Word Document on CD Disk
Or, can be obtained by request to skomraus@neesys.com



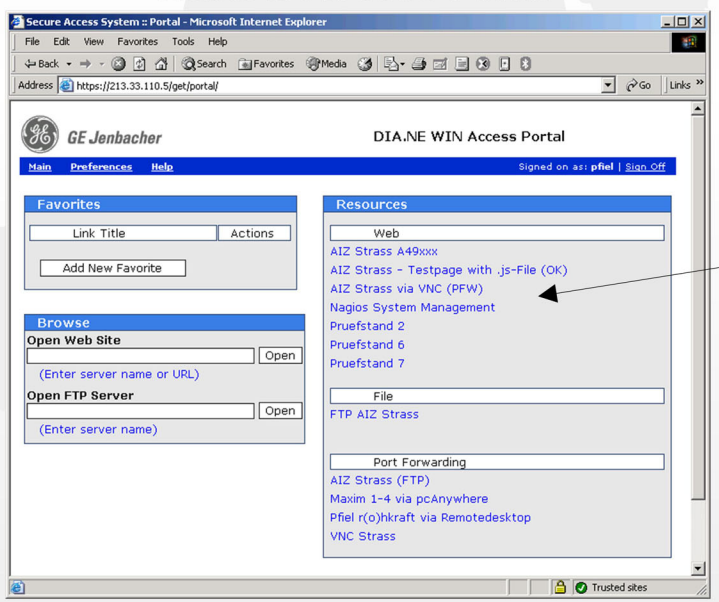

PLANT
with DIA.NE WIN
Customers office
DIA.NE WIN
1
To Remote Access Portal
Local Customer
DIA.NE RMC
DIA.NE WIN
Onsite Firewall
To Central Firewall and/or Large Costumer
3
Home
DIA.NE WIN
To Remote Access Portal
To Remote Access Portal
DIA.NE WIN
Service Technician
INTERNET
HTTPS - Connection (SSL encrypted) to Remote Access Portal
VPN - Connection (AES encoded) between Firewalls
HTTP & MS Netw. Connection via onsite Firewall to DIA.NE WIN server
To specific Plant(s)
Large Customers office
DIA.NE RMC
DIA.NE WIN
Central Firewall Remote Access Portal
2
To all Plants
To Remote Access Portal
GE Jenbacher Competence Center
DIA.NE RMC
DIA.NE WIN

DIA.NE WIN Server onsite

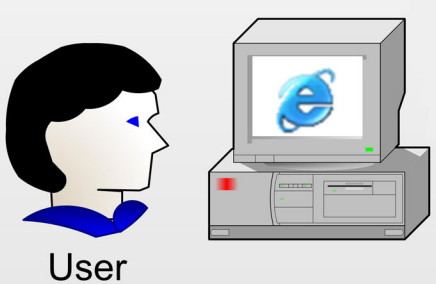


Encrypted VPN Connection between Central Firewall and Site Firewall

Remote Access Portal



Encrypted HTTPS - Connection to Remote Access Portal



User

The Remote Access Portal provides easy access of the desired DIA.NE WIN Application via Hyperlink.
In addition also File Transfer (FTP) and Remote Control (pcANYWHERE*) is possible.

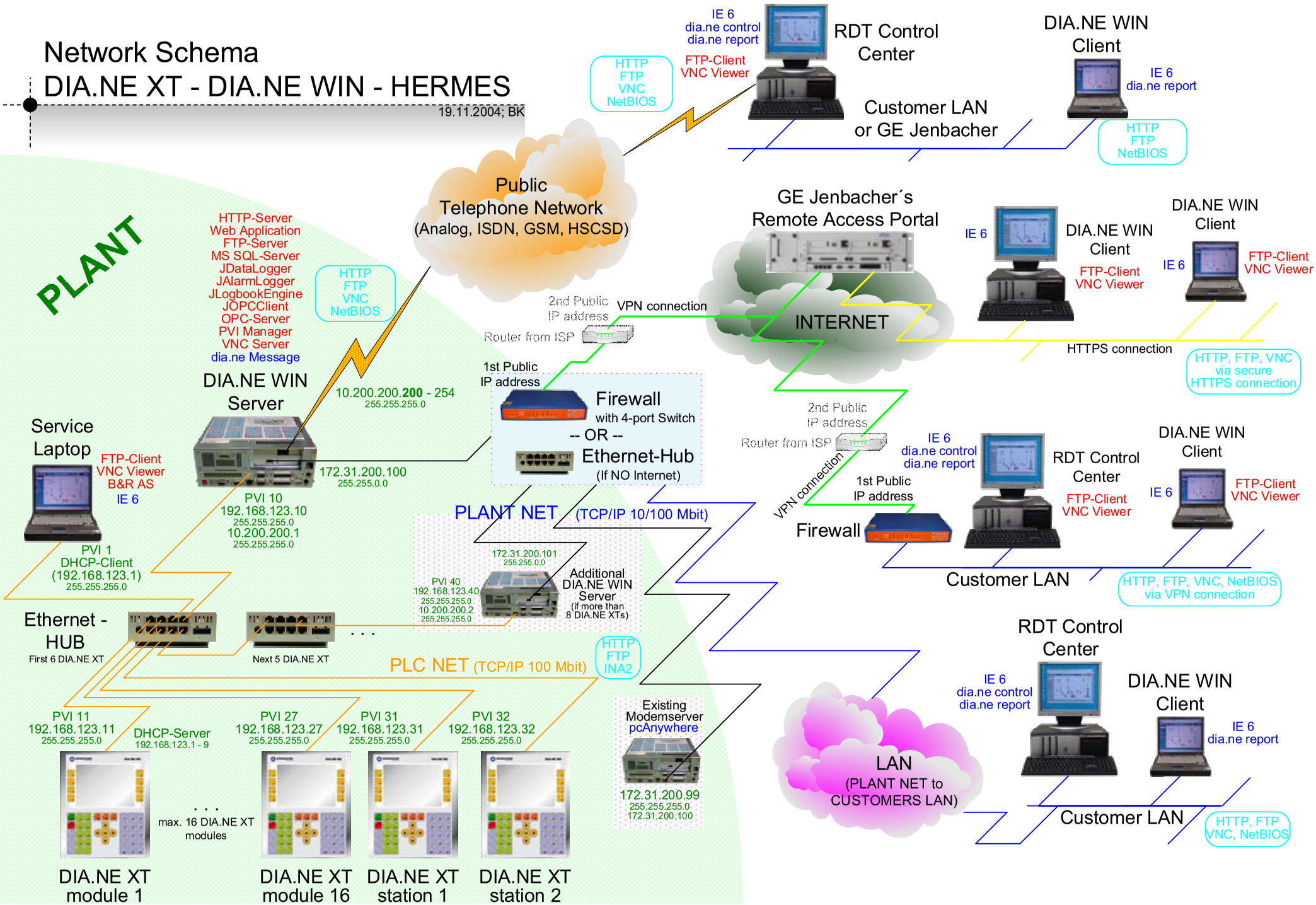
These links are customer specific and may be differ for each user.

The Remote Access Portal needs therefore user authentication and is password protected.

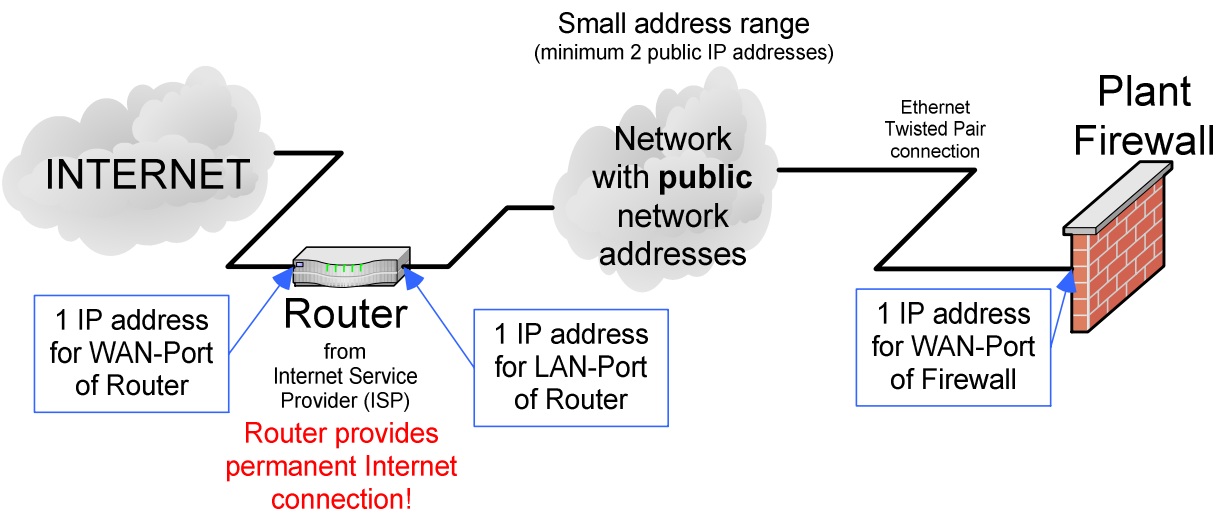
* for plants with older DIA.NE modemservers

Network Schema
DIA.NE XT - DIA.NE WIN - HERMES

19.11.2004; BK



1 Internet connection using ISP's router and public network address range
(Standard Solution for Internet connectivity of Jenbacher Plants)



Elements of solution

- Router: Provided by Internet Service Provider (ISP). Router has 1 public, static IP address against the Internet and provides a permanent connection to the Internet. The ISP is completely responsible for the reliability of the Internet connection.
- Network with public network addresses: The router provides a network of public IP addresses on the LAN side. 1 IP address is used by the router's LAN interface and 1 IP address will be used by the Plant Firewall. From this follows that the network must contain at least 2 IP addresses. If the customer would like to add also other devices to this network (e.g. for customer's network Internet access), additional IP addresses must be provided. (Typical amount of addresses: 2, 4, 8, 16, ...)
- Plant Firewall: The firewall uses 1 IP address of the public network between router and firewall.

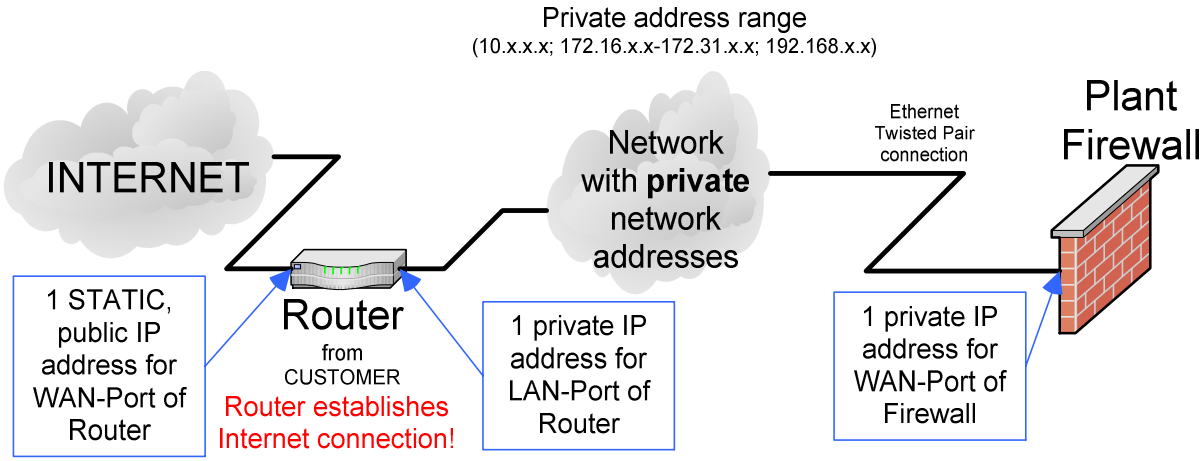
Pros

- Monitoring of Internet connection all the way to the router is possible
- Connection to Plant Firewall can be monitored
- The responsibility in case of an error can be strictly defined.
- The Firewall is always available for maintenance
- Higher reliability of Internet connection by using business solution

Cons

- Higher acquisition and periodical cost because of business solution

2 Internet connection using customer-side router without public network range, but 1 public, static IP address



Elements of solution

- Router: Provided and managed by customer. The router establishes the Internet connection and receives 1 public, static IP address on the Internet side. ISP and customer are responsible for the reliability of the Internet connection. (In case of a misconfiguration of the router no Internet connection will be possible.)

- Network with private network addresses: Between the router and the Plant Firewall resists a network with private IP addresses. Each device, router and Plant Firewall, uses 1 IP address of this private range. From this follows that the network must contain at least 2 IP addresses. If the customer would like to add also other devices to this network (e.g. for customer's network Internet access), additional IP addresses must be provided. (Typical amount of addresses: 2, 4, 8, 16, ...)
  This network cannot be access from the Internet by default. A partial forwarding of incoming data to the Plant Firewall can by provided by a specially configured router using "Network Address Translation" (NAT).

- Plant Firewall: The firewall uses 1 IP address of the private network between router and firewall. In this case, the Plant Firewall must establish the VPN connection (secured connection) by itself, because a connection establishment from the Internet is not possible. (Plant Firewall cannot be reached)

Pros

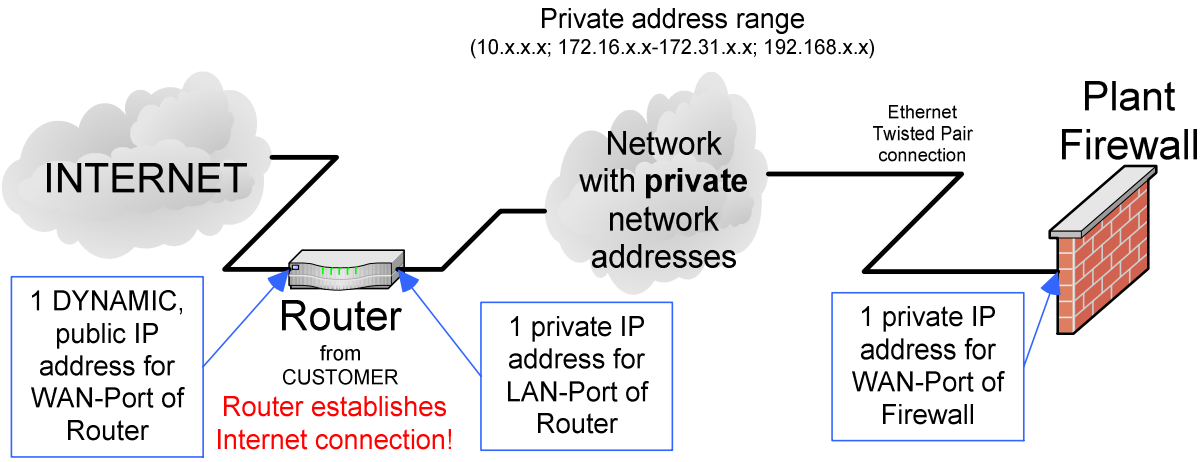
- Medium acquisition and periodical cost because of non-business internet connection

- Monitoring of Internet connection all the way to the router is possible.
  The responsibility in case of an error can not be accurately defined! (ISP or customer)

Cons

- Connection to Plant Firewall can only be monitored in case of an active VPN connection
- A statement regarding the responsibility in case of an error cannot be issued, because a separation between ISP, customer and Jenbacher cannot be performed.
- Maintenance of the Plant Firewall can only be made if a VPN connection is available
  -> Errors can be solved by an onsite technician only!
  Exception: Using a specially configured router (data forwarding to Plant Firewall using NAT)
- Typically lower connection availability because of non-business internet connection

3 Internet connection using customer-side router without public network range and public IP address



Elements of solution

- Router: Provided and managed by customer. The router establishes the Internet connection and receives 1 public but dynamic IP address on the Internet side. ISP and customer are responsible for the reliability of the Internet connection. (In case of a misconfiguration of the router no Internet connection will be possible.)
  The router cannot be reached from the Internet because of the frequently changing IP address.
- Network with private network addresses: Between the router and the Plant Firewall resists a network with private IP addresses. Each device, router and Plant Firewall, uses 1 IP address of this private range. From this follows that the network must contain at least 2 IP addresses. If the customer would

like to add also other devices to this network (e.g. for customer's network Internet access), additional IP addresses must be provided. (Typical amount of addresses: 2, 4, 8, 16, ...)
This network cannot be access from the Internet by default. A partial forwarding of incoming data to the Plant Firewall is not possible, because of the dynamic IP address.

- Plant Firewall: The firewall uses 1 IP address of the private network between router and firewall. In this case, the Plant Firewall must establish the VPN connection (secured connection) by itself, because a connection establishment from the Internet is not possible. (Plant Firewall cannot be reached)

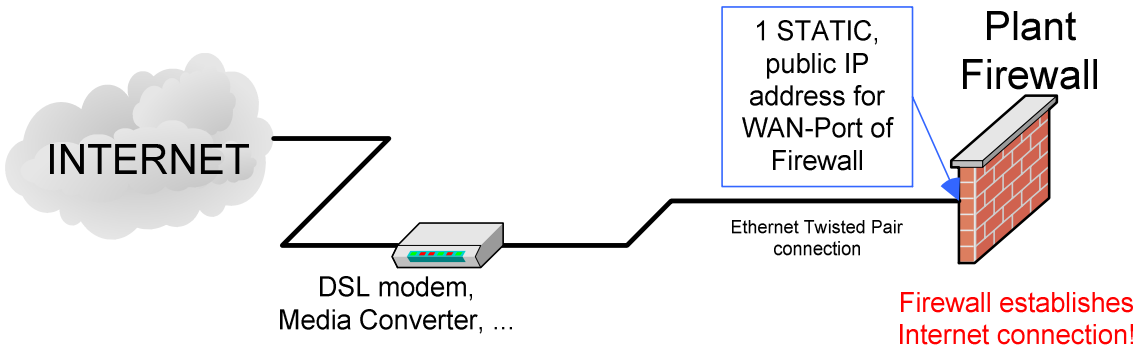
Pros

- Low acquisition and periodical cost because of non-business internet connection

Cons

- Monitoring of Internet connection all the way to the router is impossible.
- Connection to Plant Firewall can only be monitored in case of an active VPN connection
- A statement regarding the responsibility in case of an error cannot be issued, because a separation between ISP, customer and Jenbacher cannot be performed.
- Maintenance of the Plant Firewall can only be made, if a VPN connection is available
  -> Errors can be solved by an onsite technician only!
- Typically lower connection availability because of non-business internet connection

4 Internet connection using Plant Firewall without public network range, but 1 public, static IP address



Elements of solution

- DSL modem, Media converter, ...: Used for physical connection to the Internet Service Provider (ISP). Provided by ISP. Cannot be monitored.

- Plant Firewall: The Plant Firewall is responsible for building up the Internet connection. After successful connection establishment the Plant Firewall receives 1 public, static IP address. In this case, the Plant Firewall needs to build up the Internet connection by itself first to enable a VPN connection (secured connection).

Pros

- Low acquisition and periodical cost because of non-business internet connection

- Monitoring of Internet connection and connection to the Plant Firewall is possible.
  The responsibility in case of an error can not be accurately defined! (ISP, customer or Jenbacher)

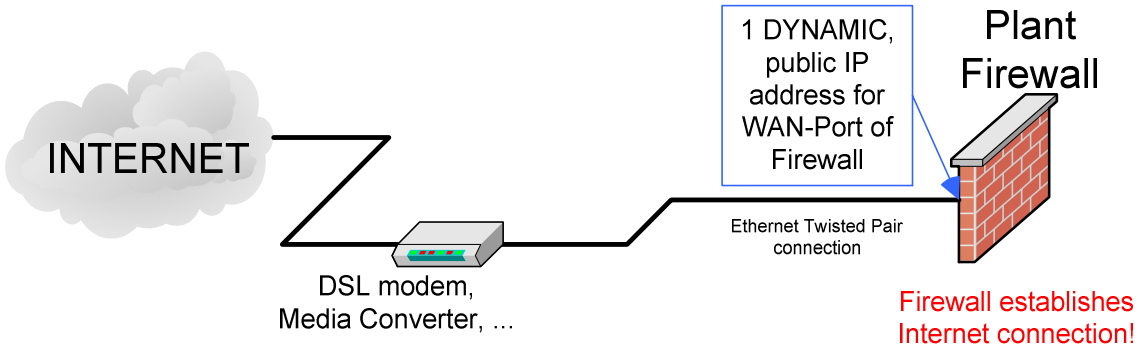
Cons

- A statement regarding the responsibility in case of an error cannot be issued, because a separation between ISP, customer and Jenbacher cannot be performed.

- Maintenance of the Plant Firewall can only be made if the Internet connection could be successful established by the Plant Firewall.
  -> Errors can be solved by an onsite technician only!

- Typically lower connection availability because of non-business internet connection

5 Internet connection using Plant Firewall without public network range and static IP address



Elements of solution

- DSL modem, Media converter, ...: Used for physical connection to the Internet Service Provider (ISP). Provided by ISP. Cannot be monitored.

- Plant Firewall: The Plant Firewall is responsible for building up the Internet connection. After successful connection establishment the Plant Firewall receives 1 public but dynamic IP address. In this case, the Plant Firewall needs to build up the Internet connection by itself first to enable a VPN connection (secured connection).

Pros

- Low acquisition and periodical cost because of non-business internet connection

Cons

- Monitoring of Internet connection is impossible.
- Connection to Plant Firewall can only be monitored in case of an active VPN connection
- Maintenance of the Plant Firewall can only be made, if a VPN connection is available
  -> Errors can be solved by an onsite technician only!
- A statement regarding the responsibility in case of an error cannot be issued, because a separation between ISP, customer and Jenbacher cannot be performed.
- Typically lower connection availability because of non-business internet connection

1. General:

GE Jenbacher's HMI (Human Machine Interface) provides customer connectivity via network connections. Using this connection the customer is able to access GE Jenbacher's DIA.NE WIN® –application and thus control the plant remotely.

This network connection was exclusively planned for connections to local customer networks.

By the use of today's technologies and because of wide spread Internet connectivity the mentioned network connections offers a possibility for connecting the plant to the Internet. Customers often use a network router with port-forwarding for this application.

This technical instruction explains the danger implied with this solution and shows the appropriate solution from a security standpoint provided by GE Jenbacher.

2. Safety risks / danger:

Using such routers with port-forwarding contain a wide range of **serious security issues!**
Some examples:

- Unencrypted transmission of data over the Internet
  - Inquiry of transmitted unencrypted passwords by HACKERS!
  - Possibility for HACKERS to start a Man-In-The-Middle attack (Online-modification of transmitted data, e.g. set values, parameters, …).

- Using correctly configured routers (correct port limitations):
  Possibility of direct access to the Web server installed at the DIA.NE® WIN-Server:
  - No protection against web server directed virus-, worm-, Denial of Service (DoS)– and Exploit-attacks (e.g. Code Red)!
  - Little protection against password-cracking-attacks by HACKERS (Inquiry of passwords)!

- Using mismanaged routers or using outdated router firmware (Security updates not installed):
  Direct access to the server's operating system!
  - No protection against all sorts of virus–, worm–, trojan– and Denial of Service (DoS) attacks (e.g. Blaster, Sasser, Spybot, Beagle, …)!
  - Password protection can be bypassed by HACKERS on all levels!

- No access control and access logging by GE Jenbacher's Remote Access Portal (2-Layer authentication)

These serious security problems cause **direct danger for customer and plant**:

- Access to the plant using inquired passwords or Man-In-The-Middle attacks by unauthorized persons: This means full access to all set values, plant parameters, historical data including modification and deletion.

- Take over of full control of the server by strangers:
  - Bypassing all security restrictions provided by the operation system and thereby full access to all application's set values, plant parameters and historical data.
  - Unauthorized use of the server's hardware and the Internet connection for criminal activities (Spam-Mailing, DoS-Attacks, …).

- Destruction of the DIA.NE WIN-server:
  Total loss of the server (data, accessibility, hardware) by destroying the server's harddisk by HACKER intervention or by a VIRUS.

These manipulations can cause catastrophic damage of the plant and can risk life!

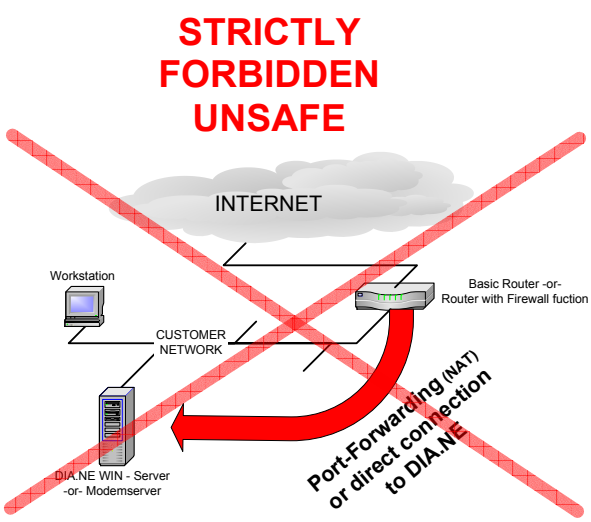
3. Solution by GE Jenbacher Firewall:

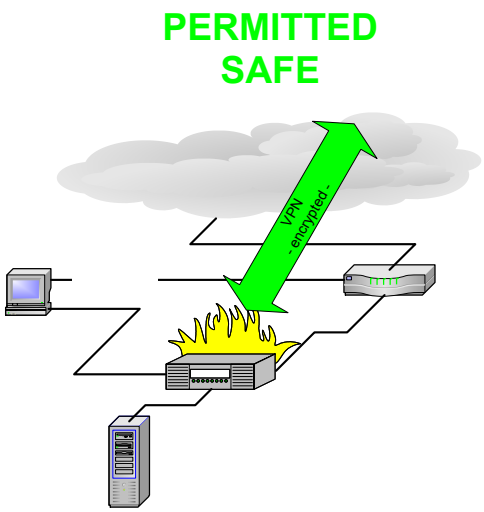
To solve the shown problems, GE Jenbacher has developed a specific solution for accessing plants over Internet.

GE Jenbacher uses an onsite Firewall to protect the plant, which can handle a highly secured, encrypted connection to a central Firewall at GE Jenbacher (Virtual Private Network, VPN). These connections and all involved devices are directly controlled and maintained by GE Jenbacher specialists, who ensure fastest reactions on system based security problems (updates) or HACKER activities (proactive and reactive).

By using the firewall and VPN connections a direct access from the Internet to the plant is impossible and only authenticated users gain access to the plants over GE Jenbacher's Remote Access Portal. This portal is also controlled and maintained by GE Jenbacher, who guarantees highest security standards.

4. Security advise:





Router with Port-Forwarding:
Direct access to DIA.NE® WIN and unencrypted login with DIA.NE® password

GEJ-Firewall-Solution:
Access to DIA.NE® WIN via GEJ Remote Access Portal only (1st Step: Login to portal with encrypted authentication, 2nd Step: encrypted Login with DIA.NE password)

GE Jenbacher is not liable for any damages or defects resulting from port forwarding or direct connection to the DIA.NE® WIN Server GE Jenbacher. Such damages or defects are not covered by GE Jenbacher warranty.

1. Commissioning and hardware testing (original, non-configuered firewall):

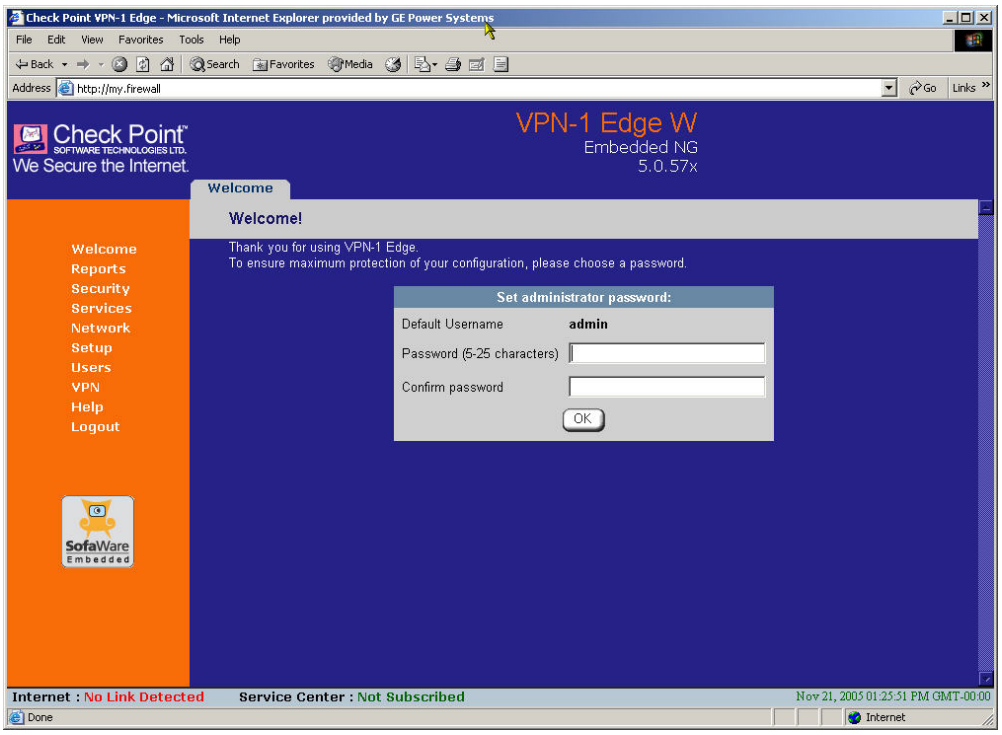
Implemented by: central test stand

1.1 Establishing a network connection to the firewall:

- Connect the control network cable (yellow) to the firewall's **LAN – port 1**.

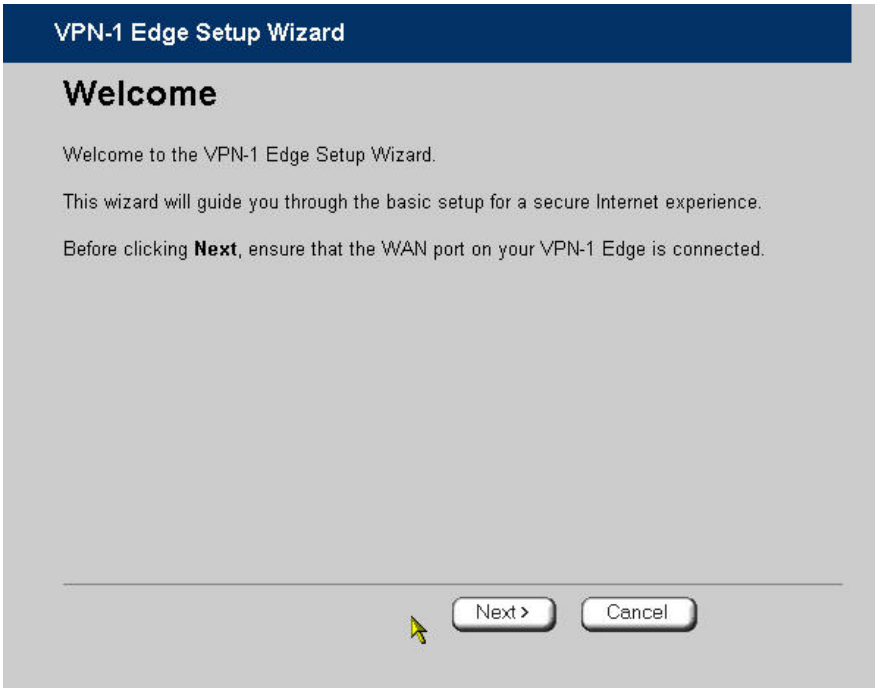
1.2 Activating the Management website for the first time:

- Open Internet Explorer
- Enter the **my.firewall** address in the address bar: the firewall's login page now appears.

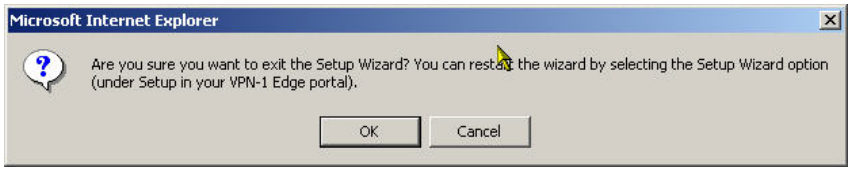


- Enter the default password:
  Enter the default password: **gejenbacher** twice; i.e. once in every entry field.

- Confirm by clicking on the OK button: the „VPN-1 Edge Setup Wizard" now appears:



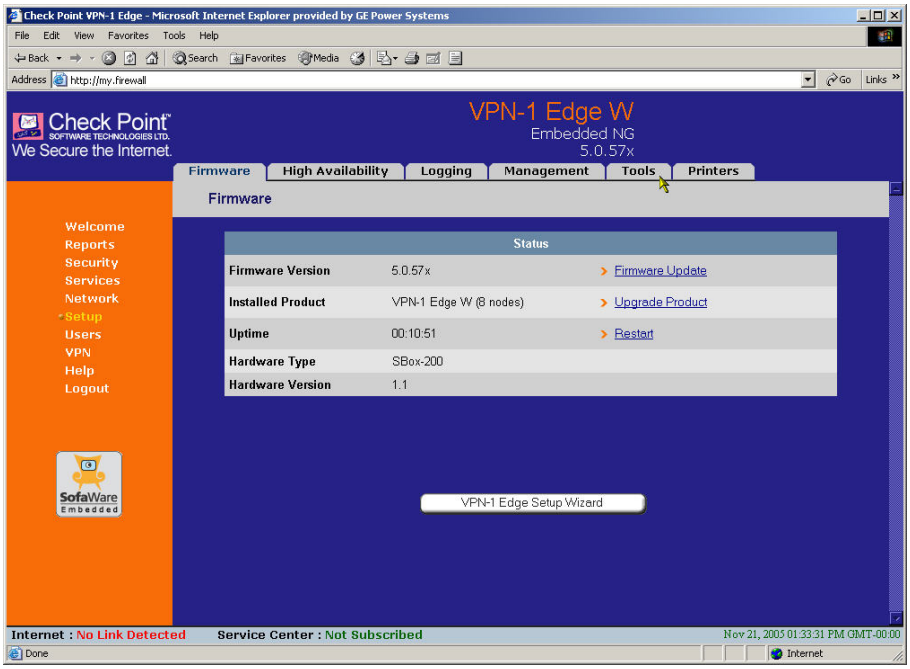
- Exit the „VPN-1 Edge Setup Wizard“ by clicking on the OK button:



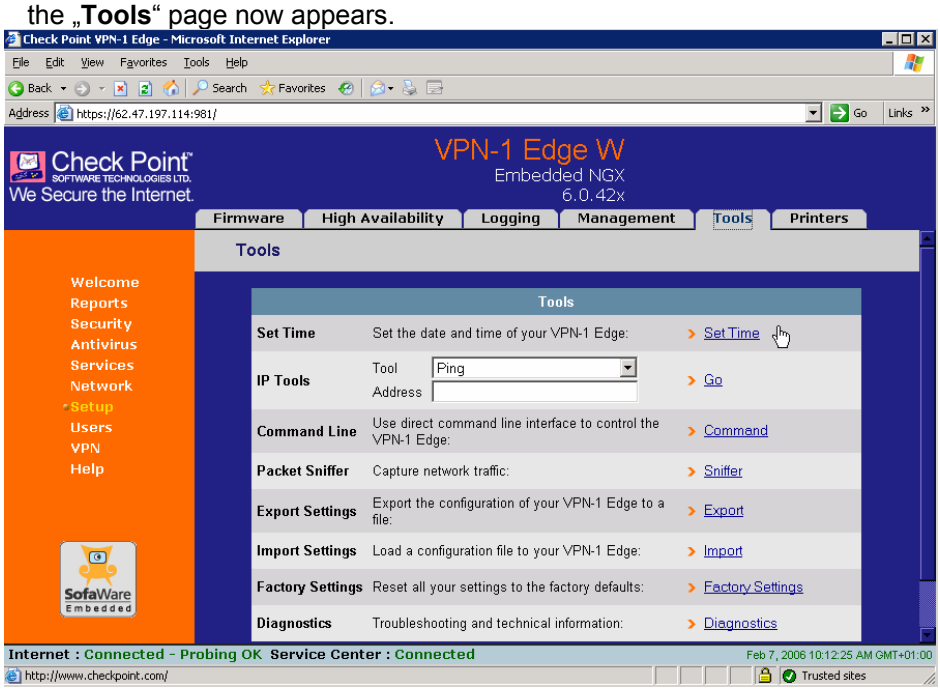
the main firewall management now appears.

1.2.1 Setting the firewall system time:

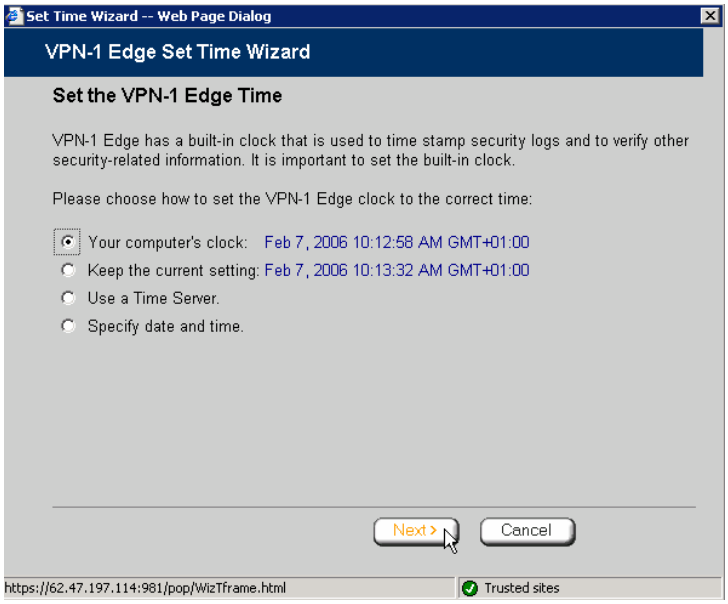
- select the „**Setup**“ menu item in the left menu: the „**Firmware**“ page now appears .



- Select the „**Tools**“ tab from the series of tabs at the top of the page:
  the „**Tools**“ page now appears.



- Select the „**Set Time**“ menu item in the middle of the page:
  the „**VPN-1 Edge Set Time Wizard**“ dialogue now appears.



- Select the item: „**Your computer's clock**"; continue by clicking on the „**Next**" button and exit the dialogue that follows by clicking on the „**Finish**" button.

The firewall is now successfully configured!

1.3 Checking the proper functioning of the firewall's network connections (ports):

1.3.1 Testing the LAN and DMZ ports:

- Start the MS-DOS command prompt.
- Execute the „ **ping my.firewall -t** " command in the MS-DOS command prompt.
- Check the test results for the LAN – port 1 connection against the DOS result example messages in Annex B.
- Check the relevant LEDs on the front of the firewall: the 100Mbps and LINK/ACT LEDs must light up or be flashing!
- Unplug the network cable of port 1 and subsequently plug it into **ports 2 to 4** and the **DMZ port** respectively. When doing so, check the result of the ping command which is still actively pinging.

  Tip! When changing the plugs and shortly after, status messages such as „Hardware error" or „Destination host not reachable" may appear. Normally, these messages will be replaced by the regular „Reply from ……" status message after a short while. -> OK
- When finished, deactivate the ping command by entering „ctrl + c".

1.3.2 Testing WAN port:

- Connect the network cable to the firewall's **WAN port**.
- Check the relevant LEDs on the front of the firewall:
  the 100Mbps and LINK/ACT LEDs must light up or be flashing!

2. On-site commissioning:

Implemented by: commissioning mechanic, customer.
To configure the firewall on the installation, a configuration file must be imported via the firewall's Web interface. This configuration file is enclosed with the commissioning documentation or can be requested at the Jenbacher Competence Center.

2.1 Step 2: Establishing a network connection to the firewall:

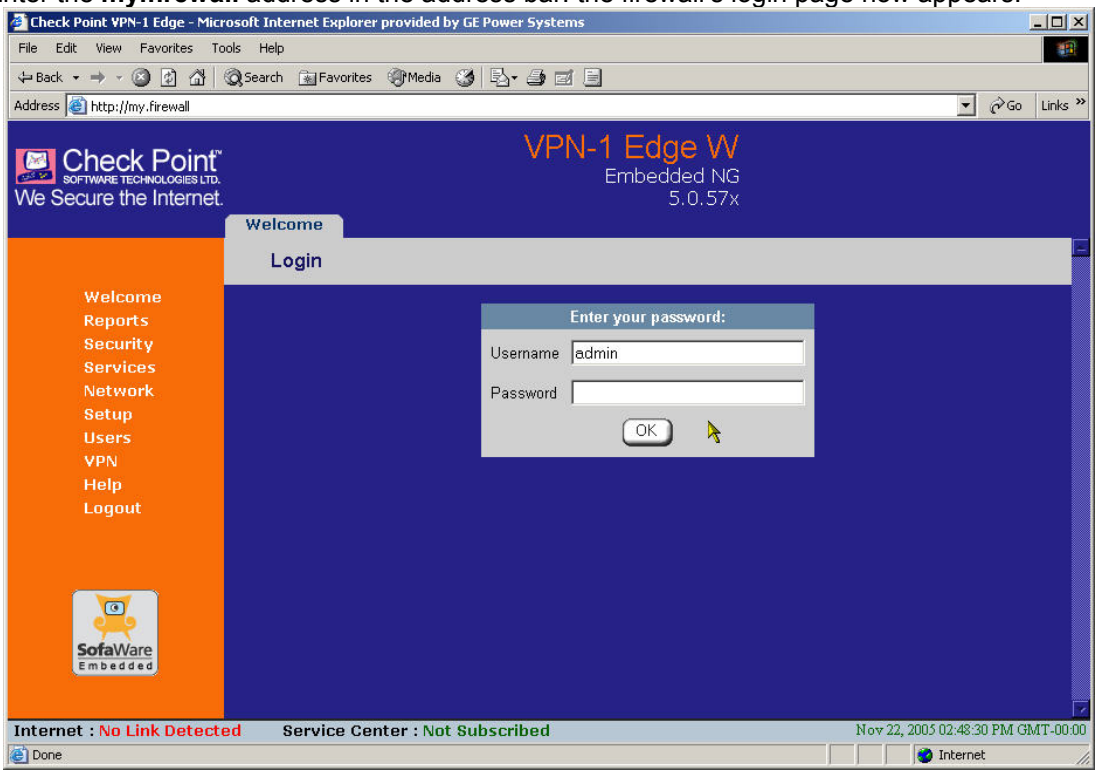
- See Annex C

2.2 Step 2: Establishing a network connection to the firewall:

- See Annex A

2.3 Step 3: Activating the Management website:

- Open Internet Explorer.
- Enter the **my.firewall** address in the address bar: the firewall's login page now appears.

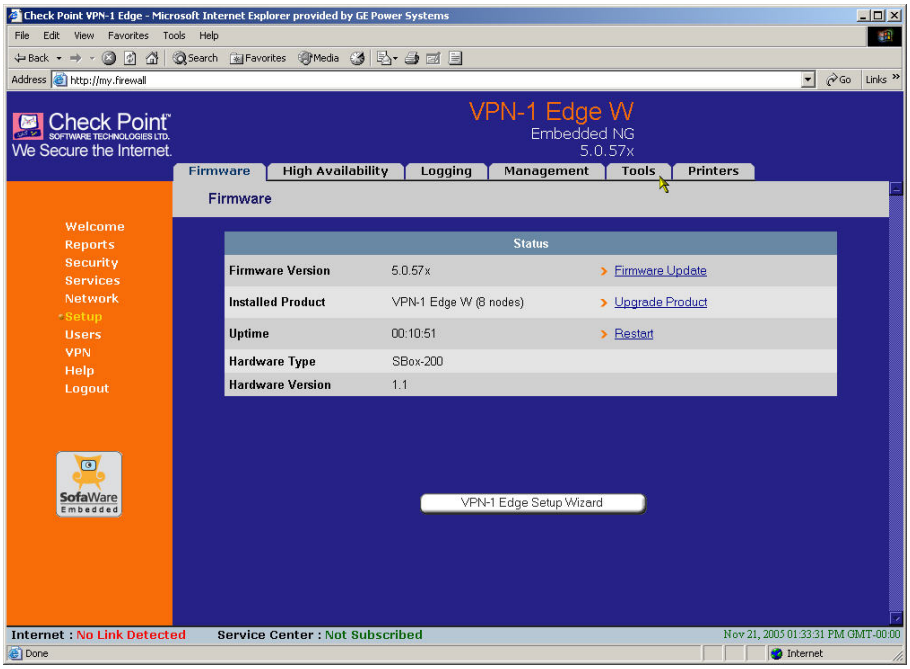


- Enter the admin password: **gejenbacher.**
- Confirm by clicking on the **OK** button: the main firewall management now appears.

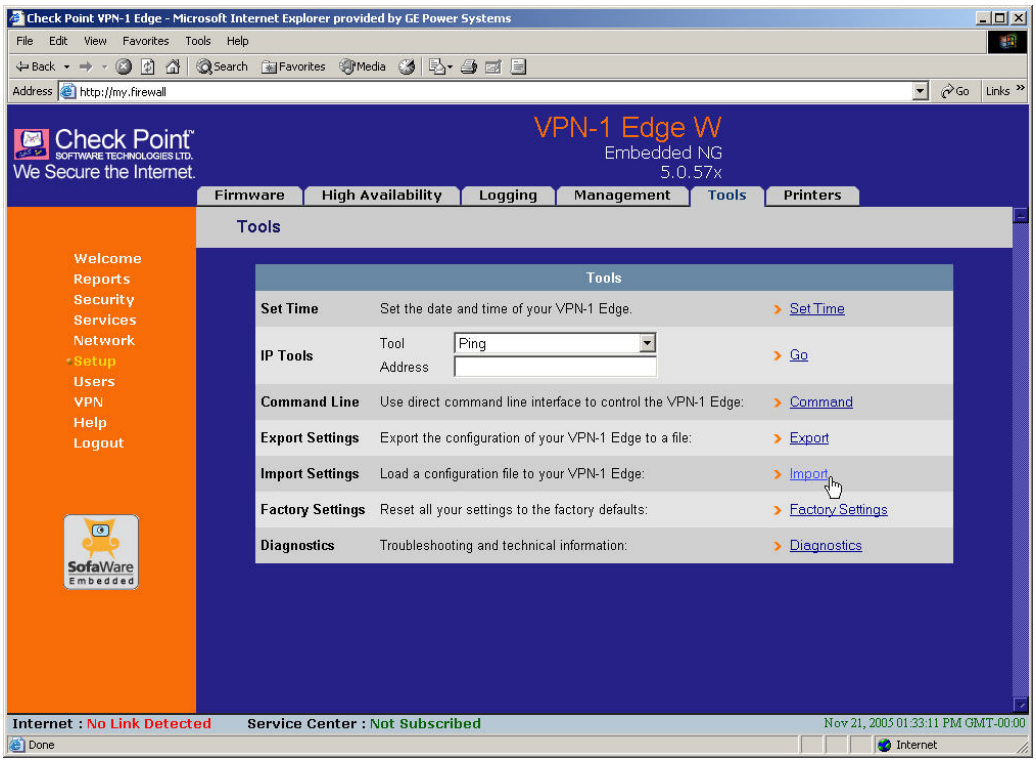

Check Point
SOFTWARE TECHNOLOGIES LTD.
We Secure the Internet.
VPN-1 Edge W
Embedded NG
5.0.57x
Welcome
Welcome
Welcome
Reports
Security
Services
Network
Setup
Users
VPN
Help
Logout
SofaWare
Embedded
Welcome to the VPN-1 Edge Portal!
Your VPN-1 Edge is running Check Point VPN-1 Embedded NG developed by SofaWare Technologies, a Check Point company. The VPN-1 Edge protects your network from hacker attacks and allows sharing your broadband Internet connection among several PCs.
This Internet security appliance supports additional subscription services, available from select service providers, including firewall security updates service, web filtering, email antivirus, dynamic DNS and more.
Additional Product Documentation and Resources Online
Register this appliance in the user center
© Copyright 2005 SofaWare Technologies Ltd.
SofaWare is a registered trademark of SofaWare Technologies Ltd.
Check Point is a registered trademark of Check Point Software Technologies Ltd.
Legal Notice
Internet : No Link Detected
Service Center : Not Subscribed
Nov 21, 2005 01:29:08 PM GMT-00:00

2.4 Step 4: Importing the firewall configuration file:

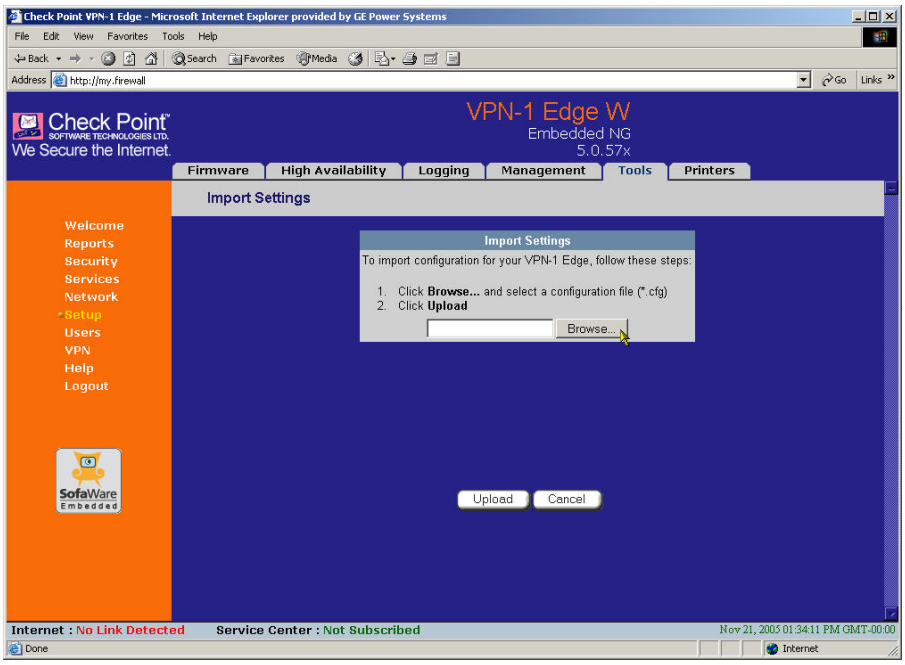
- select the „**Setup**“ menu item in the left menu: the „**Firmware**“ page now appears.



- Select the „**Tools**“ tab from the series of tabs at the top of the page: the „**Tools**“ page now appears.



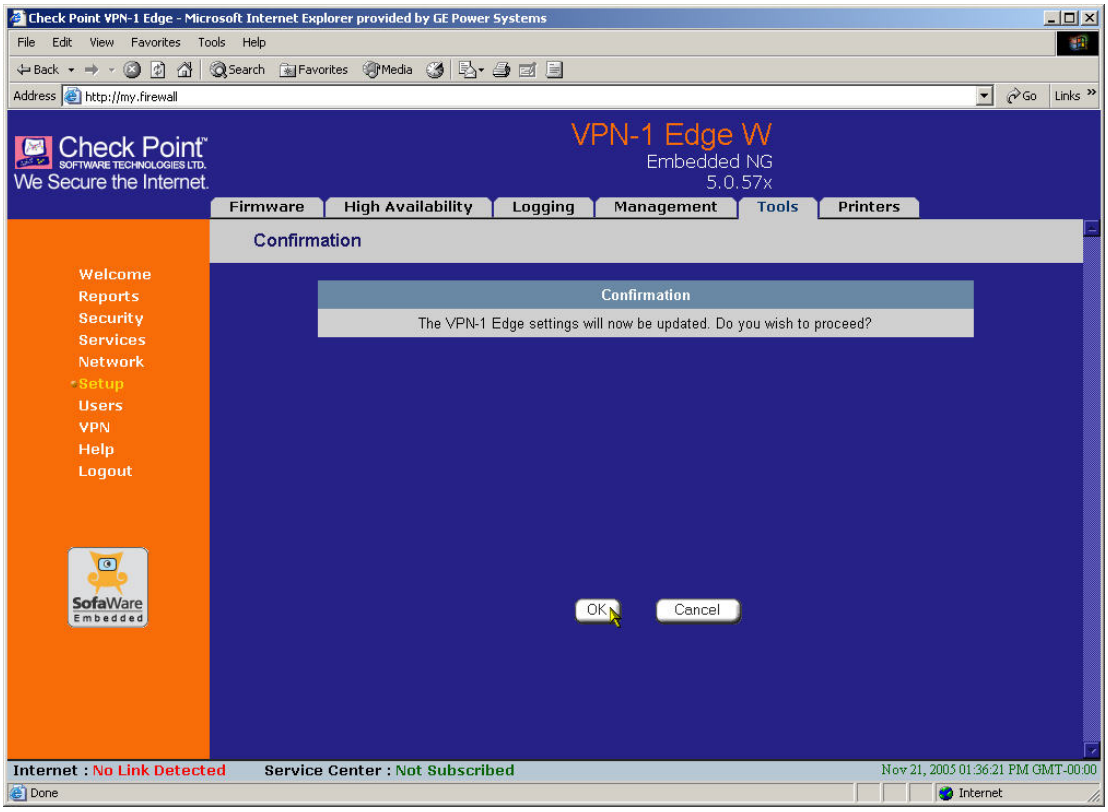
- Select the „**Import**“ menu item in the middle of the page:
  the „**Import settings**“ page now appears.



- Use the **„Browse…“** key to open a selection dialogue screen; now select the „**GEJ_xxxx.cfg**“ configuration file. (xxxx = plant (J) number).

The file name now appears in the text field next to the „Browse…“ key.

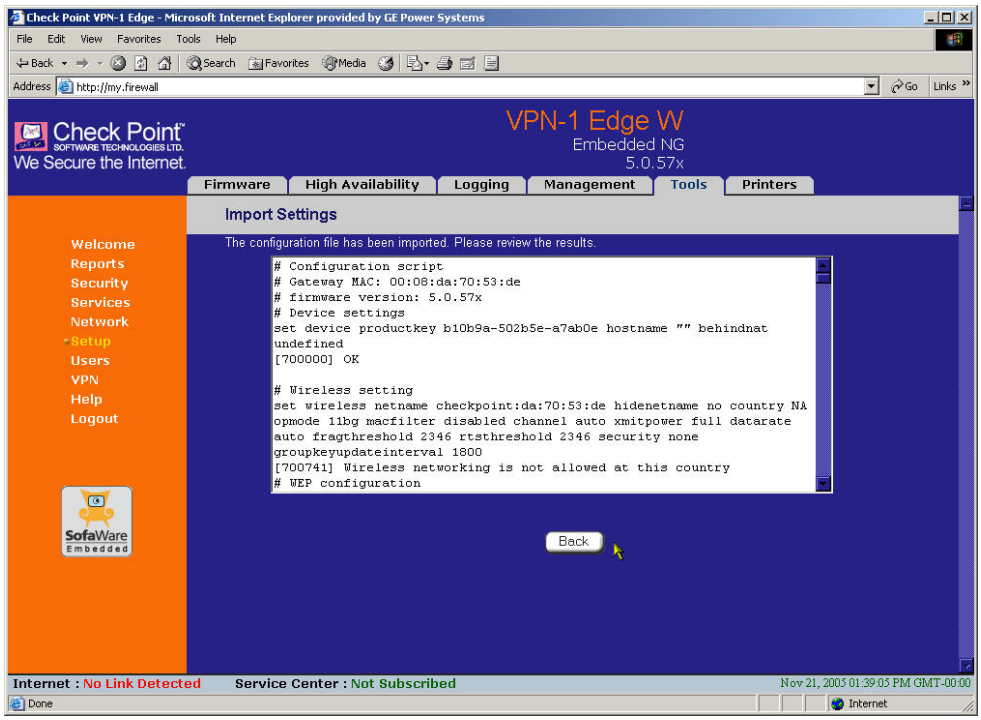
- Select the „**Upload**“ key: a „Confirmation“ page now appears.



- Activate the import procedure by clicking on the „**OK**“ button.

Following the import procedure, the next page containing the „The configuration file has been imported. Please review the results.“ message appears in the top of the page.

If any other messages appear, please contact the Competence Center (+43 5244 600 2000)!



- Select the „**Logout**“ menu item in the left menu.

- v Contact the Jenbacher Competence Center for a functionality check.

Tel. +43 5244 600 2000
Fax: +43 5244 600 42000
eMail: ccenter@ge.com

2.5 ANNEX:

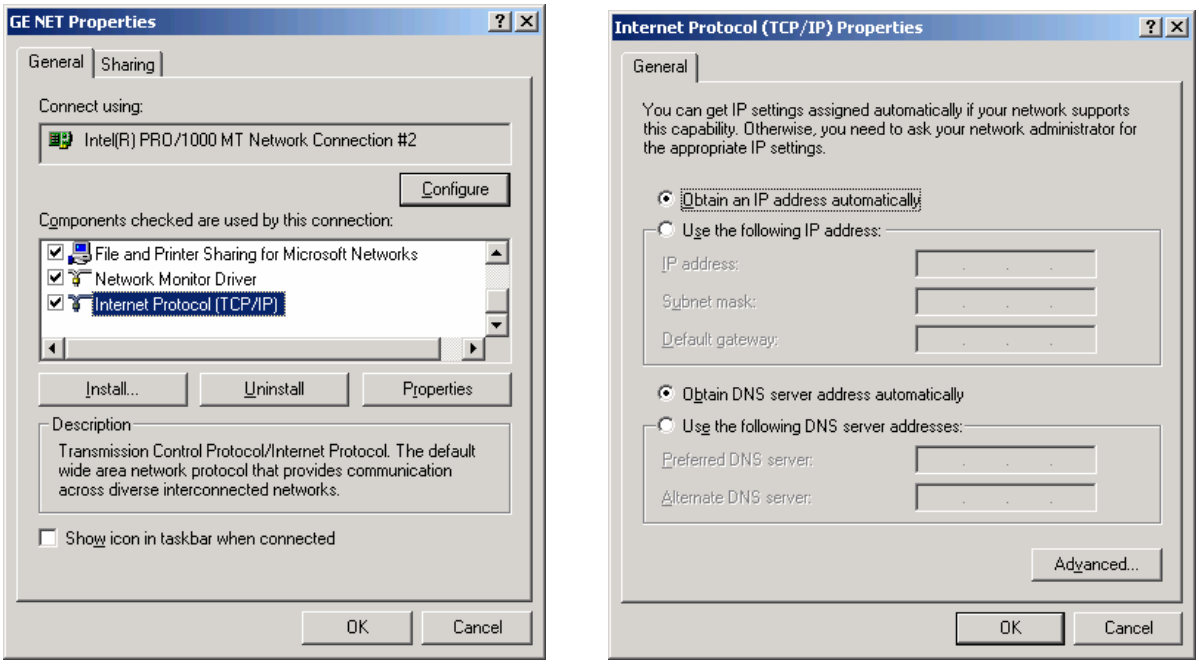
2.5.1 ANNEX A: Connecting to the firewall:

Use a patch cable (1:1) to establish the connection.

Connect the cable with the computer's network card (RJ 45 socket).

Now plug the cable into the **connection socket (port) 4** in the firewall's **LAN section**.

Your computers network parameters must be as follows(computer as DHCP client):



ill. 1: The network connection's „Internet Protocol TCP/IP" screen.

The computer is provided with an IP address in the 192.168.10.x range.

2.6 ANNEX B: possible DOS result messages for the ping test:

CORRECT result:
Pinging my.firewall [192.168.10.1] with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64
Reply from 192.168.10.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milliseconds:
Minimum = 2ms, Maximum = 2ms, Average = 2ms.

INCORRECT results:

Hardware error.
Hardware error.
Hardware error.
Hardware error.

Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Cause: cable incorrectly plugged in

C:\Documents and Settings\BrunnerK>ping my.firewall
Unknown host my.firewall.

Cause: Computer cannot find firewall's IP address.
Possible corrective measure:
Using the command: **ping 192.168.10.1 (LAN range) or ping 192.168.253.1 (DMZ range)**

:\Documents and Settings\BrunnerK>ping my.firewall

Pinging my.firewall [192.168.10.1] with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.

Request timed out.

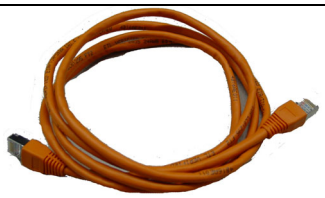
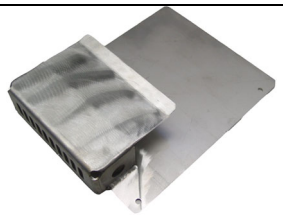
Ping statistics for 192.168.10.1:
Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
Approximate round trip times in milliseconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

Cause: connection check unsuccessful.
Possible corrective measure:
Using the command: **ping 192.168.10.1 (LAN range) or ping 192.168.253.1 (DMZ range)**

If any other error messages keep appearing, please contact the Competence Center (+43 5244 600 2000)!

2.7 ANNEX C: Hardware – installation instructions:

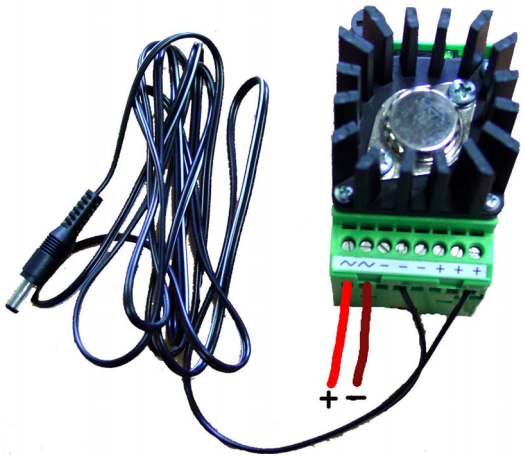
Das Hardware – Paket umfasst folgende Bestandteile:

Firewall (Check Point VPN-1 EDGE Internet Security Appliance) incl. instruction manual	
network cable (1:1 patch cable)	
AC adapter (option power supply using VAC 220; other voltages optional)	
Support for firewall	
DC / DC converter (type may vary)	
DC connecting cable	

In the case of new installations, the firewall supports, the DC/DC converter with DC connecting cable and the firewall are pre-installed in the control cabinet.

Preliminary installation work (retrofitting only):

1. Connect the DC / DC converter as shown in the illustration:
   Green version (Phönix, EMG 45-NZG/G15/S) for **X Series** firewalls
   AC input (~): 24 VDC power supply connection (polarity not important)
   DC output (+, -): DC connecting cable connection (polarity not important)



Black version (MTM Power, HMG 15 24S05) for **W series** firewalls
DC input (-IN, +IN): 24 VDC power supply connection (polarity important!)
DC output (GND, +5V): DC connecting cable connection (polarity: marked core = +5V)

2. Assembling and connecting the firewall:

- Place the firewall in the relevant support in the control cabinet.
  - or -
  Position the firewall at the location specified by the customer.

- Plug the DC connecting cable in the control cabinet or the connecting cable of the power supply into the firewall's „PWR" socket
  -> The „PWR/SEC" LED at the left of the orange-coloured front lights up or starts to flash.

- Connect the network cable (part of the supply) to the network card of the DIA.NE WIN server.

- Now plug this network cable into port 1 in the "LAN" part of the firewall.
  -> LED 1 at the „LAN" front part now lights up/starts to blink.

- Connect the network cable of the Internet connection (e.g. coming from the router) to the „WAN" port of the firewall.
  -> The LED at the „WAN" front part now lights up/starts to blink.

Carry out the next step also in the case of an additional customer network connection (Customer LAN):

- Connect the network cable of the customer network connection to the „DMZ/WAN2“ port of the firewall.
  -> The „DMZ/WAN2“ LED at the front part now lights up/starts to blink.
  -> The connection between the DIA.NE WIN application and a customer PC can be tested.

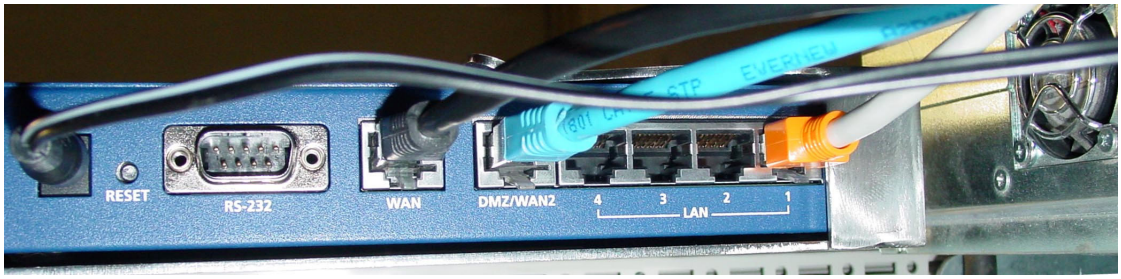


Illustration 2: Connected firewall with DC supply, Internet connection, customer network and DIA.NE WIN server

To complete the firewall commissioning you must contact the Jenbacher Competence Center for a functionality check.

Tel. +43 5244 600 2000
Fax: +43 5244 600 547
eMail: ccenter@ge.com

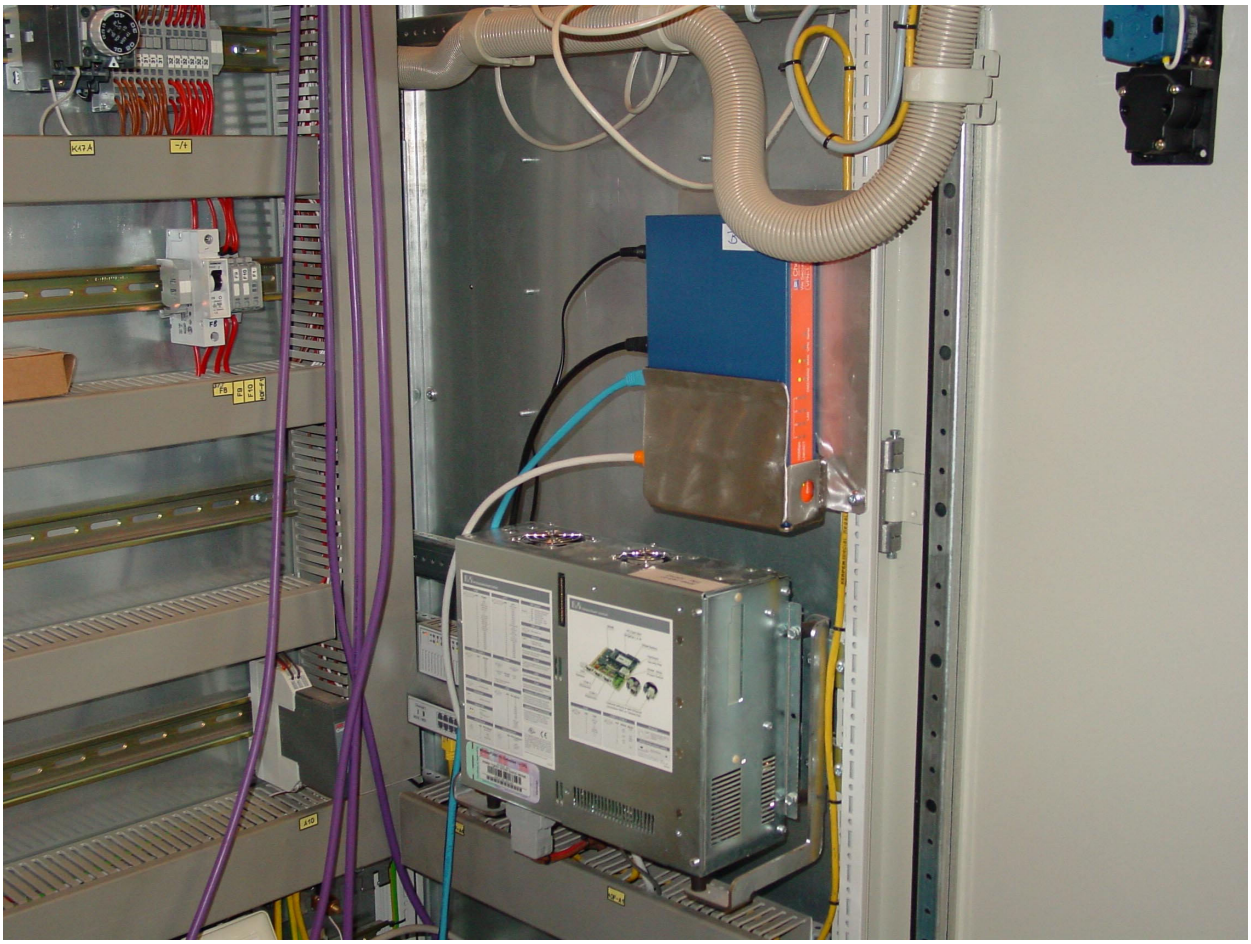


Illustration 3: Installation firewall, fully assembled and installed

2.8 ANNEX B: Troubleshooting:

- The DIA.NE WIN application cannot or can no longer be accessed from the PCs in the customer network:
  Check IP address The access address is the IP address of the DIA.NE WIN server installed by the service mechanic (not the address as indicated by the customer).
  Check the default gateway and/or route:
  In the network settings on the client computer, the address of the firewall in the customer network must be entered as default gateway. This address can be obtained from the Jenbacher Competence Center and/or is shown on a sticker on the firewall.
  If you cannot enter this default gateway as it is already assigned (which is frequently the case in larger networks), you must add a static route on the customer PC:
  Command prompt entry:
  route –p add <DIA.NE WIN server IP address> **MASK 255.255.255.224** <firewall IP address in customer network>

  Example: route –p add 172.29.0.1 MASK 255.255.255.224 10.0.0.33

1 General

In order to configure the Internet connectivity of your Jenbacher gas engine site please fill in the fields concerning your Internet / Network configuration mentioned in the table below.

GE Jenbacher, the gas engine division of GE Energy, needs this information to configure the firewall for the internet connection of your site. Jenbacher will keep this information confidential.

At the last page of this document you will find a summary of the requirements for the Internet connection needed at site. This information can be used during the purchase of the Internet connection from an Internet Service Provider (ISP).

The requested information has to be provided to GE Jenbacher 4 weeks before commissioning of the plant at the latest enabling us to proceed with the required configuration in time and provide the service technician with the needed files for the commissioning.

If the information is sent too late, the configuration file will be provided by GE Jenbacher subsequently but the upload onto the firewall has to be done by the customer. If technical assistance at site is required, GE Jenbacher reserves the right to charge it to the customer.

Please send the following request form back to NES / WES Competence Center:

Fax: 215-335-3641 (ATTN: Steve Komraus)

eMail: skomraus@neesys.com

*Northeast Energy will log an iSupport Case to work with GE Jenbacher on your site connection

In case of any missing information about the Internet configuration please ask your Internet Service Provider (ISP) or your network administrator.

In case of any general questions about the network schematic or the requested information please contact NES / WES Competence Center (215-384-5922 or skomraus@neesys.com).

2 Allowed Internet connection variants

Please see Technical Instruction 2300-0006 **"Security note regarding Internet connectivity of GE Jenbacher plants"** for further information about risks using other, unsupported connectivity variants.

2.1 Jenbacher delivers firewall to establish secured VPN connection

Jenbacher delivers a VPN capable firewall to set up the secured connection between the plant and Jenbacher / the customer. Hardware, Software and labor (initial set up) are included.
See network schema on page 10.

To enable Jenbacher setting up the firewall / the VPN connection, fill out the configuration forms from page 3 (Appendix A) to page 9 (Appendix B).

2.2 Use of customer's firewall to establish secured VPN connection

The customer provides a capable firewall/VPN device for setting up a site-to-site VPN to Jenbacher's central datacenter. (e.g. Checkpoint VPN-1, Cisco VPN router)

Jenbacher provides connectivity to devices listed as IPsec V1 compatible by ICSAlabs. (www.icsalabs.com) or by the Virtual Private Network Consortium (www.vpnc.org, http://www.vpnc.org/testing.html#AESInterop).

See network schema on page 13 for general understanding.

To enable Jenbacher setting up the VPN connection to the customer, fill out the configuration form at page 3 (Appendix A) and page 11 to page 12 (Appendix B).

Jenbacher reserves its right to refuse the request based on technical or commercial causes.

Appendix A General plant and Internet account information

GENERAL	
Plant Name **(mandatory)**	
Plant Number (J-Number Jxxxx) **(mandatory)**	
Customer's company name	
Customer's contact information (Name, Phone, eMail)	
Location of the Plant (Country, State) **(mandatory)**	
Internet account information	
Name of Internet Provider	
Product Name of Internet connection	
Connection type (DSL, Satellite, …)	
Connection speed (Downlink / Uplink)	

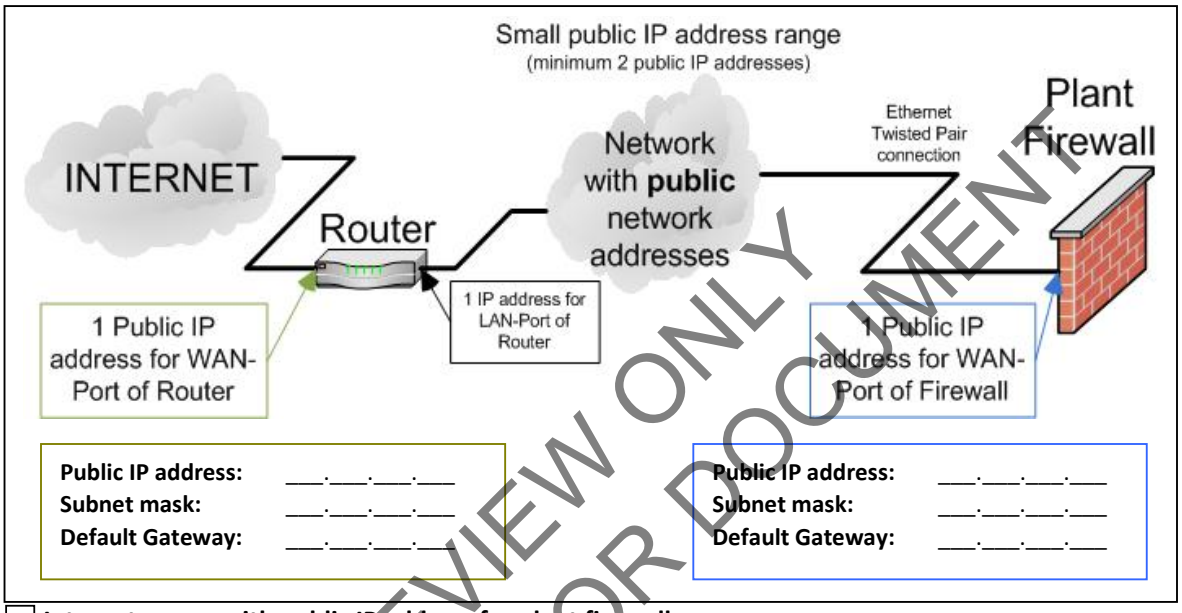
Additional comments

Date and Customer's Signature: _____

Appendix B Variants of Internet connection infrastructure at the plant
(needed only if Jenbacher delivers firewall)

How to:

1. **Choose one connection variant and fill in the necessary data (page 4 to page 9)**
2. **Choose if direct customer's network connection is desired (page 9)**



☐ **Internet access with public IP address for plant firewall**

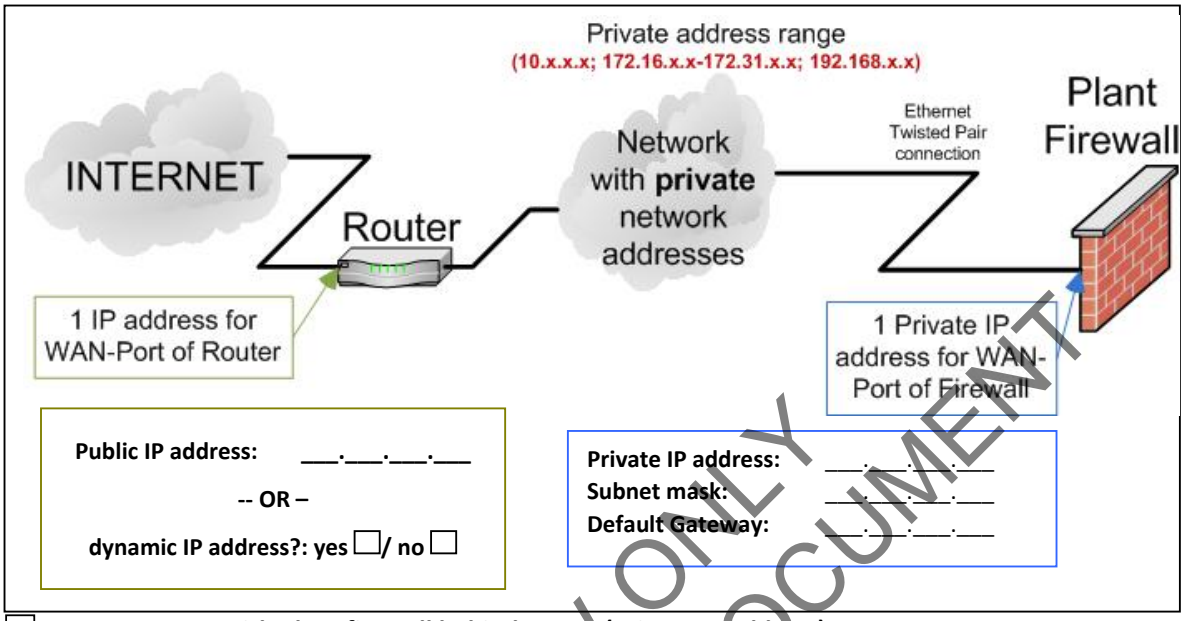
Required services (ask Provider if not sure)

- Ingoing (Internet → Firewall)

Protocol	Allowed	Denied
TCP 981 (Firewall management website) *	☐	☐
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐

- Outgoing (Firewall → Internet)

Protocol	Allowed	Denied
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐
UDP 123 (Network Time Protocol, NTP)	☐	☐
UDP 53 (Domain Name Service, DNS)	☐	☐



☐ **Internet access with plant firewall behind router (private IP address)**

Required services (ask Provider if not sure)

- Ingoing (Internet → Firewall via Network address translation (NAT / Port Forwarding))

Protocol	**Allowed**	**Denied**
TCP 981 (Firewall management website) *	☐	☐
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐

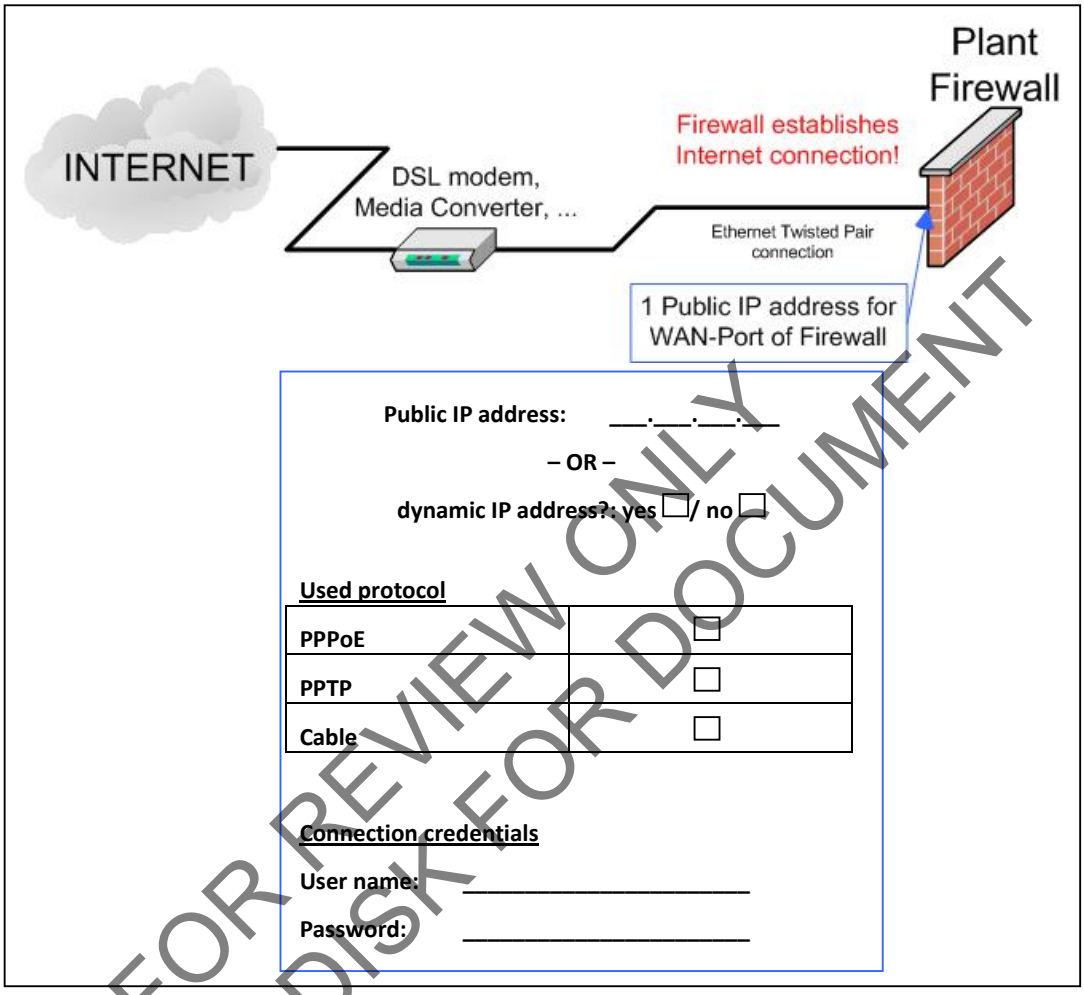
- Outgoing (Firewall → Internet)

Protocol	**Allowed**	**Denied**
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
UDP 4500 (IPsec NAT-Traversal; NAT-T) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐
UDP 123 (Network Time Protocol, NTP)	☐	☐
UDP 53 (Domain Name Service, DNS)	☐	☐

- Additional router settings

	Allowed	**Denied**
Enable IPsec pass-through *	☐	☐

☐ **Internet access where plant firewall connects directly via modem/media converter using PPPoE (PPP over Ethernet), PPTP (Point-to-Point Tunneling) or Cable modem**



Required services (ask Provider if not sure)

- Ingoing (Internet → Firewall)

Protocol	Allowed	Denied
TCP 981 (Firewall management website) *	☐	☐
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐

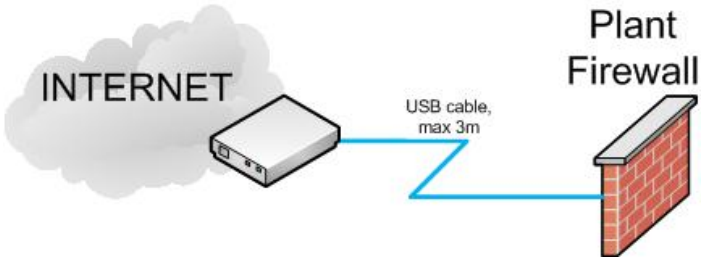
- Outgoing (Firewall → Internet)

Protocol	Allowed	Denied
UDP 500 (Internet Key Exchange, IKE) *	☐	☐

IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐
UDP 123 (Network Time Protocol, NTP)	☐	☐
UDP 53 (Domain Name Service, DNS)	☐	☐

*** Mandatory**

☐ **Internet access via cellular modem (UMTS/GPRS/EVDO)**



Public IP address (if available and static):

___.___.___.___

– OR –

dynamic IP address?: yes ☐ / no ☐

Connection credentials

APN (Access Point Name): _____

Phone number: _____

User name (if needed): _____

Password (if needed): _____

Required services (ask Provider if not sure)

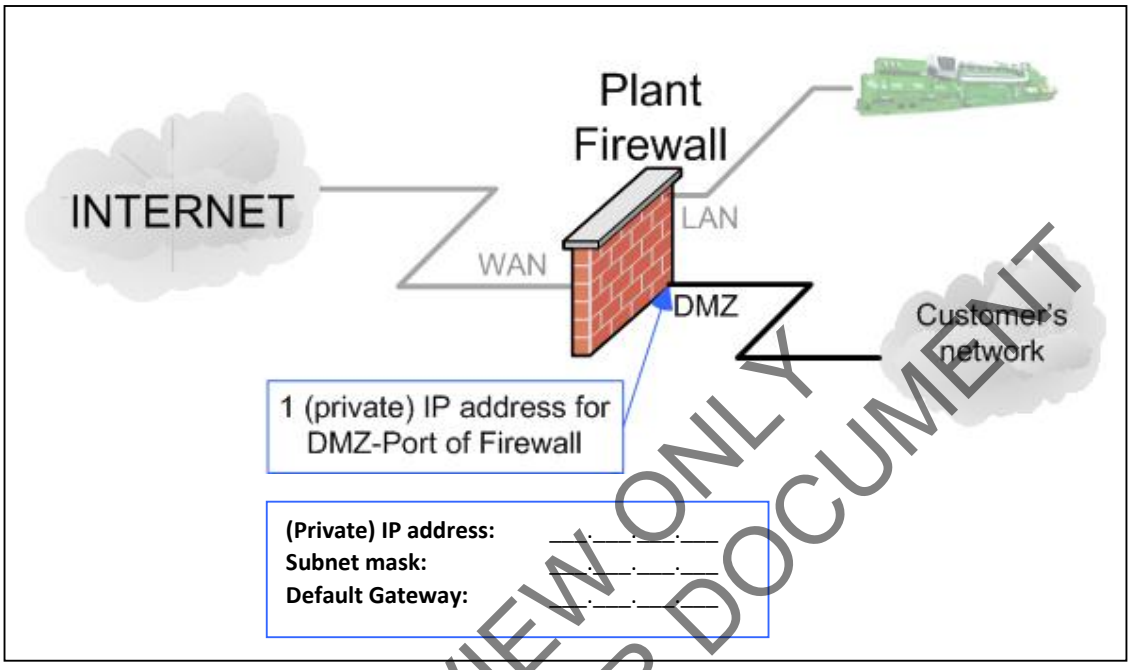
- Ingoing (Internet → Firewall)

Protocol	Allowed	Denied
TCP 981 (Firewall management website) *	☐	☐
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐

- Outgoing (Firewall → Internet)

Protocol	Allowed	Denied
UDP 500 (Internet Key Exchange, IKE) *	☐	☐
IP 50 (Encapsulating Security Payload, ESP) *	☐	☐
UDP 9281 (Checkpoint management port)	☐	☐
UDP 9282 (Checkpoint management port)	☐	☐
UDP 123 (Network Time Protocol, NTP)	☐	☐
UDP 53 (Domain Name Service, DNS)	☐	☐

☐ **OPTIONAL: Direct connection between Jenbacher engine visualization (DIA.NE WIN) and customer's company network**

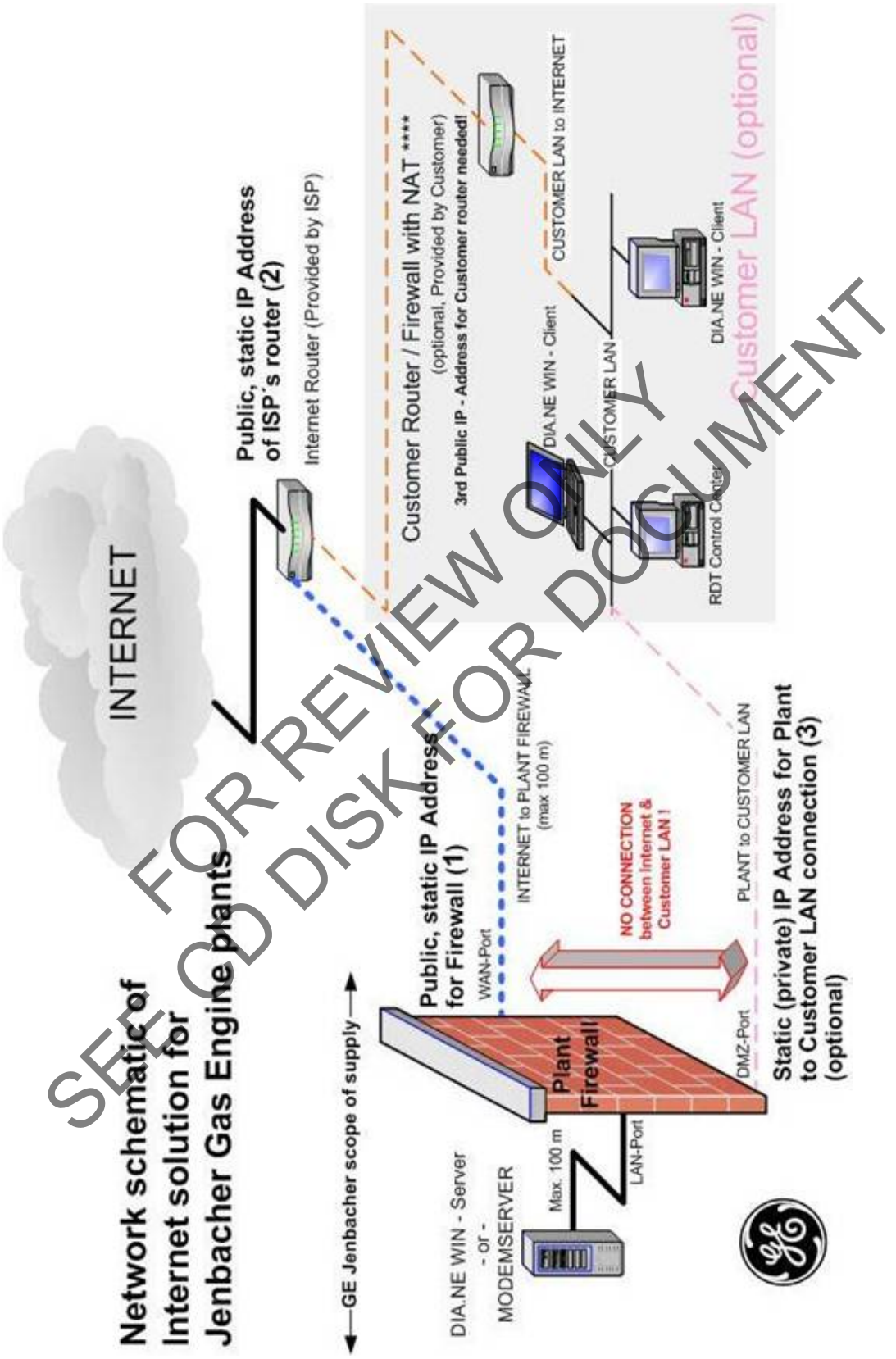


Allowed services from customer's network to Jenbacher engine visualization (DIA.NE WIN):
HTTP, FTP, VNC (TCP 5900)

Allowed services from Jenbacher engine visualization (DIA.NE WIN) to customer's network:
Netbios (UDP 137, UDP 138, TCP 139), Microsoft CIFS over TCP (TCP 445), ICMP requests

Access from the customer's network to the Internet is generally BLOCKED.
If customer needs access to the Internet, this can be opened up on special request.
Therefore select the check box below. Jenbacher will open up any outgoing port, special restrictions cannot be implemented.

Open up Internet access from the customer's network via the Jenbacher Plant Firewall	☐



Appendix B VPN parameter request form
(needed only if customer provides firewall)

Fill out right column to confirm the possibility of the specified parameters. If suggested parameters cannot be met by your VPN device, please enter possible values for crosscheck with Jenbacher.

	GE JENBACHER	3rd Party VPN
Contact:	**NES – WES Energy Competence Center**	
Phone:	**+1 215-335-3641**	
Email	**skomraus@neesys.com**	

	GE JENBACHER	3rd Party VPN
IP Address	**80.120.67.33**	
Firewall Type/Version	**Checkpoint VPN-1 / NGX 65**	

Table 2: IKE Phase-1 Properties Supported

	GE JENBACHER	3rd Party VPN
Encryption Scheme	IKE	IKE
Key Exchange methods	AES-256	AES-256
Hashing Algorithm	**SHA1**	**SHA1**
Authentication Method	Pre shared secret (will be send by fax or phone)	
Aggressive Mode Support	No	No
Key Exchange For Subnet	Yes	Yes
Diffie Helmen Group for Phase1	Group 2 (1024bit)	Group 2 (1024bit)
IKE SA (phase 1) lifetime	1440 min.	1440 min.

Table 3: VPN Domain Properties

	GE JENBACHER	3rd Party VPN
Name	**HERMES_Central**	
IP (range, network or hosts)	**192.168.15.0/255.255.255.0** **192.168.16.0/255.255.255.0** **192.168.17.0/255.255.255.0** **192.168.18.0/255.255.255.0** or at minimum 192.168.16.12, 192.168.17.13, 192.168.17.14, 192.168.18.2	**Enter real IP range of network which contains Jenbacher DIA.NE WIN server above – if undefined, Jenbacher will define a range at 172.28.0.0/15**

Table 4: IKE Phase-2 properties

	GE JENBACHER	3rd Party VPN
Encryption Scheme	IKE	IKE
Transform (IPsec Protocol)	ESP	ESP
Encryption Algorithm	AES-256	AES-256
Data Integrity	SHA1	SHA1
Use Perfect Forward Secrecy (PFS)	No	No
Diffie Helmen group for PFS	not relevant	not relevant
IPSEC SA (phase 2) lifetime	3600 sec	3600 sec

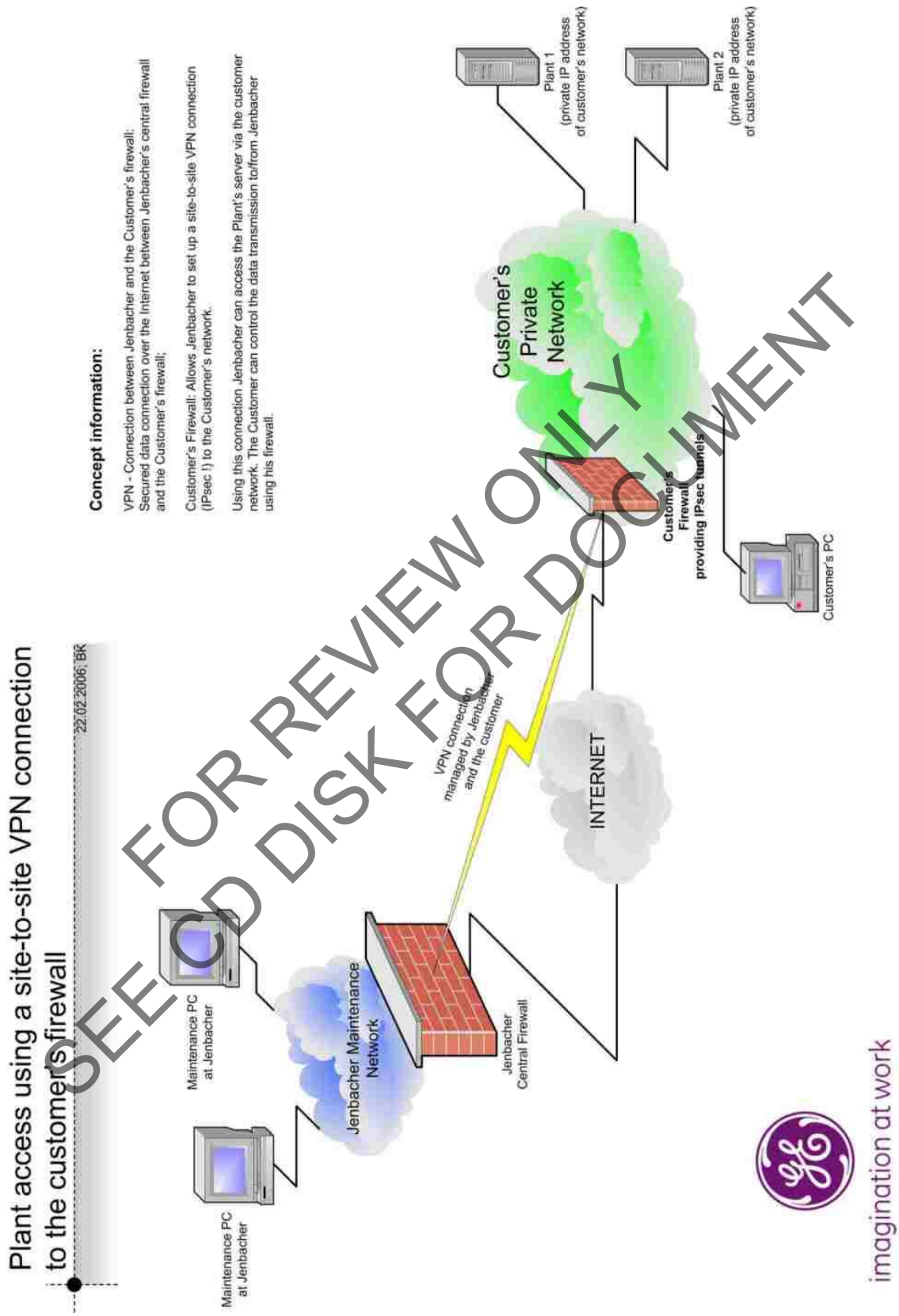
Required services

- Ingoing (Jenbacher → Plant server (DIA.NE WIN or modem server))

Protocol	**Enabled**	**Disabled**
TCP 80 (HTTP)	☐	☐
TCP 21 (FTP)	☐	☐
TCP 5900 (VNC)	☐	☐
ICMP (Ping)	☐	☐

- Outgoing (Plant server (DIA.NE WIN or modem server) →Jenbacher)

Protocol	**Enabled**	**Disabled**
TCP 445 (SMB)	☐	☐
ICMP (Ping)	☐	☐



Internet connection requirements

for Jenbacher Gas engine sites

- Permanent Internet connection (e.g. DSL)
- Connection speed: min. 128 kB/s Upload
- Data volume: min. 3 GB
- Router with customer side Ethernet interface
  (No internal firewall functionality allowed! All data must be put through!)
  -- or --
  Cellular modem with USB connector
  (must meet our list of approved modem types shown in Appendix E of TI 2300-0007)
- IP address for plant firewall:
  - Recommended: 1 public, static IP address for plant firewall
  - Minimum: 1 dynamic IP address for plant firewall

- Optional: Upgrade of data volume to „Flat Rate“ (no volume restriction)