Contract No. 004420

eu-DOMAIN - enabling **u**sers for
Distance-working & **O**rganizational **M**obility
using **A**mbient **I**ntelligence **N**etworks

D5.2 Prototype of communication infrastructure

Specific Targeted Research or Innovation Project

Project start date 1st June 2004 **Duration 36 months**

Published by the eu-DOMAIN Consortium **4th May 2007 Version 2.0**
Lead Contractor C International Ltd.

Project co-funded by the European Commission
within the Sixth Framework Programme (2002 -2006)

Dissemination Level: Confidential (CO)

Document file: D5.2 Prototype of communication infrastructure_v2.0.doc

Work package: WP5 – Communications infrastructure

Task: T5.1 + T5.2

Document owner: Pablo Antolín Rafael (TID)

Document history:

Version	Author(s)	Date	Changes made
1.0	Pablo Antolín Rafael	13/04/2007	
2.0	Pablo Antolín Rafael	03/05/2007	Minor formatting changes
			Final version submitted to the EC

Review history:

Reviewed by	Date	Validated
Klaus Marius Hansen	23/04/2007	
Jesper Thestrup	02/05/2007	

Index:

1. Executive Summary

1.1 The purpose of this document

This document describes the communication infrastructure adopted by eu-DOMAIN prototypes. This communication infrastructure is based on the analysis presented in the deliverable *D5.1 Communication architecture description* which presents different communication technologies and decides the ones to be used in the final platform. This document is describing the communication infrastructure prototype set up at Telefónica I+D facilities in Valladolid (Spain) and used to deploy the eu-DOMAIN software infrastructure, which is the real deliverable D5.2.

1.2 Contents of this deliverable

The document presents the main features of the communication infrastructure of the eu-DOMAIN prototype. This infrastructure is fully operational at Telefónica I+D facilities.

First of all, it reviews each single element presented in the prototype communication infrastructure. Then, the fixed access and wireless access is exposed. It compiles the technical and physical issues of each access.

The communication infrastructure of eu-DOMAIN has to enable the communication links between the client side and the Server Park, among the services in the Server Park and between terminals and the Server Park. The prototype makes use of different communication technologies (based on TCP/IP communication mainly) to allow this interconnection. Ethernet is used to communicate the servers of the Server Park, client gateways are using Ethernet and WiFi, the same as terminals (laptop, PDA, etc.) do and GSM communication is used to send SMS notifications to users.

Finally, a brief overview about the basic server network security is given. This network security implementation is complementary to the software security architecture described in the project. The Server Park is protected behind a set of network firewalls, including Packet Filter Firewall and Circuit-level Gateways. Moreover, a Network Address Translation (NAT) is used to completely hide the network protected by the firewall by using many-to-one address translation. Besides, a demilitarized zone (DMZ) isolates the Server Park (the Interaction Server) from internal servers.

1.3 Reader prerequisites

The reader is assumed to be familiar with the deliverables *D5.1 Communication Architecture Description* and D3.1+D4.1 *Software Architecture Specification* of eu-DOMAIN.

2. Communication Infrastructure Prototype

Figure 2 shows the communication infrastructure prototype deployed within the eu-DOMAIN project scope. Different areas can be distinguished:

- The Server Park, which is located at TID facilities, is composed by a number of servers running software components that interchange information by programming code calls in the same machine (in the case of accessing the Domain Model) or using SOAP messages (web service calls). In order to make the entire system work, these machines have to be interconnected. The different machines that make up the Server Park are allocated in the same facility and thus they are interconnected using the TID intranet with one of the machine offering access to Internet making use of NAT (Network Address Translation) functionality.
- A WAP and SMS Gateway is installed at TID facilities and is controlled by the Notification Manager to be able to send SMS to users using commercial GSM networks.
- Client Gateways could be fixed or mobile. For the current prototype, a fixed client gateway is installed in TID facilities. Any other gateway could be running outside TID as long as they are connected to the Server Park. This is demonstrated during validation of both scenarios (ESN and PaC) with real users, where client installations are deployed in Denmark, Germany and Italy and will access the functionality provided by the Server Park at TID.
- User Terminal makes use of Telco operators' networks available in the market. For the prototypes in TID facilities, terminals within TID facilities will make use of the wired and wireless Intranet to be able to access the Server Park. GPRS/UMTS connectivity is also supported but it will not be used in the prototype.

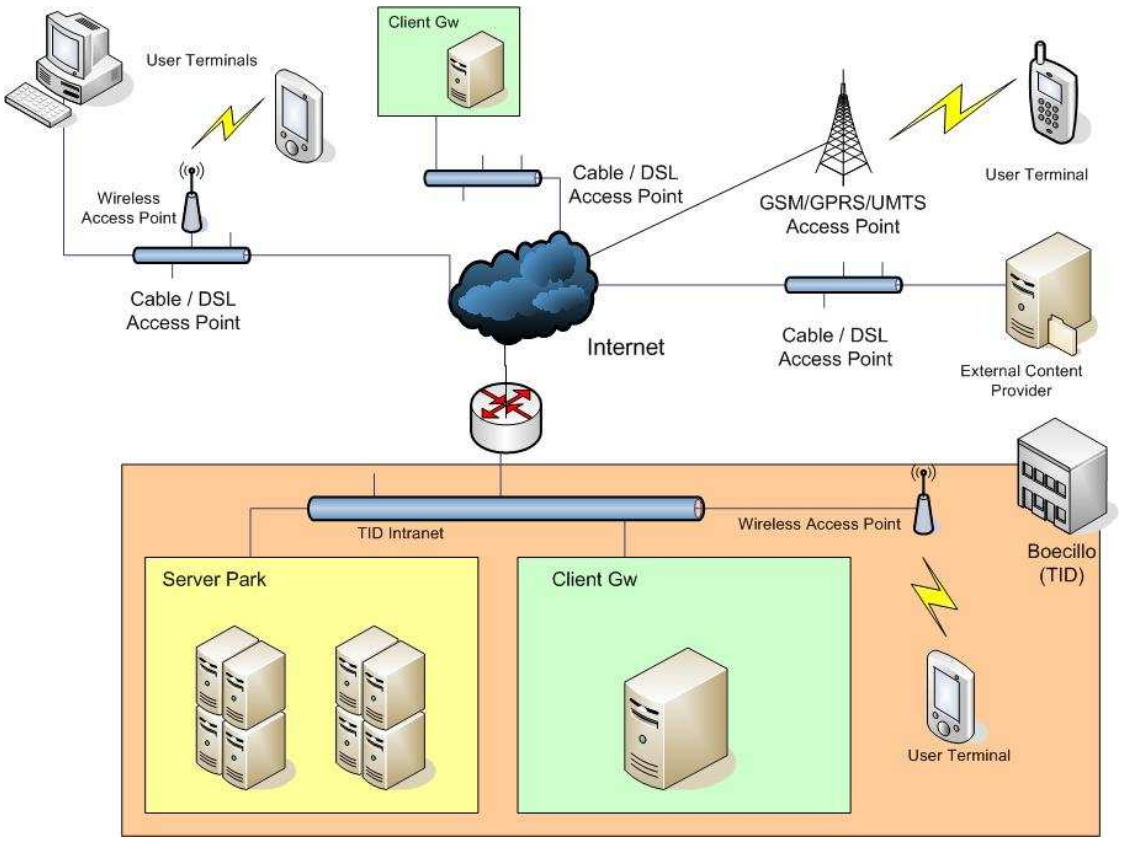

Figure 1 Communication infrastructure prototype

Moreover, a possible final exploitation eu-DOMAIN solution can be seen from Figure 2. The eu-DOMAIN functionality will be available via the commercial communication infrastructure. The components described before are included in the diagram, with the Server Park in the bottom of it and a number of gateways using different communication technologies accessing the functionality of the platform worldwide.

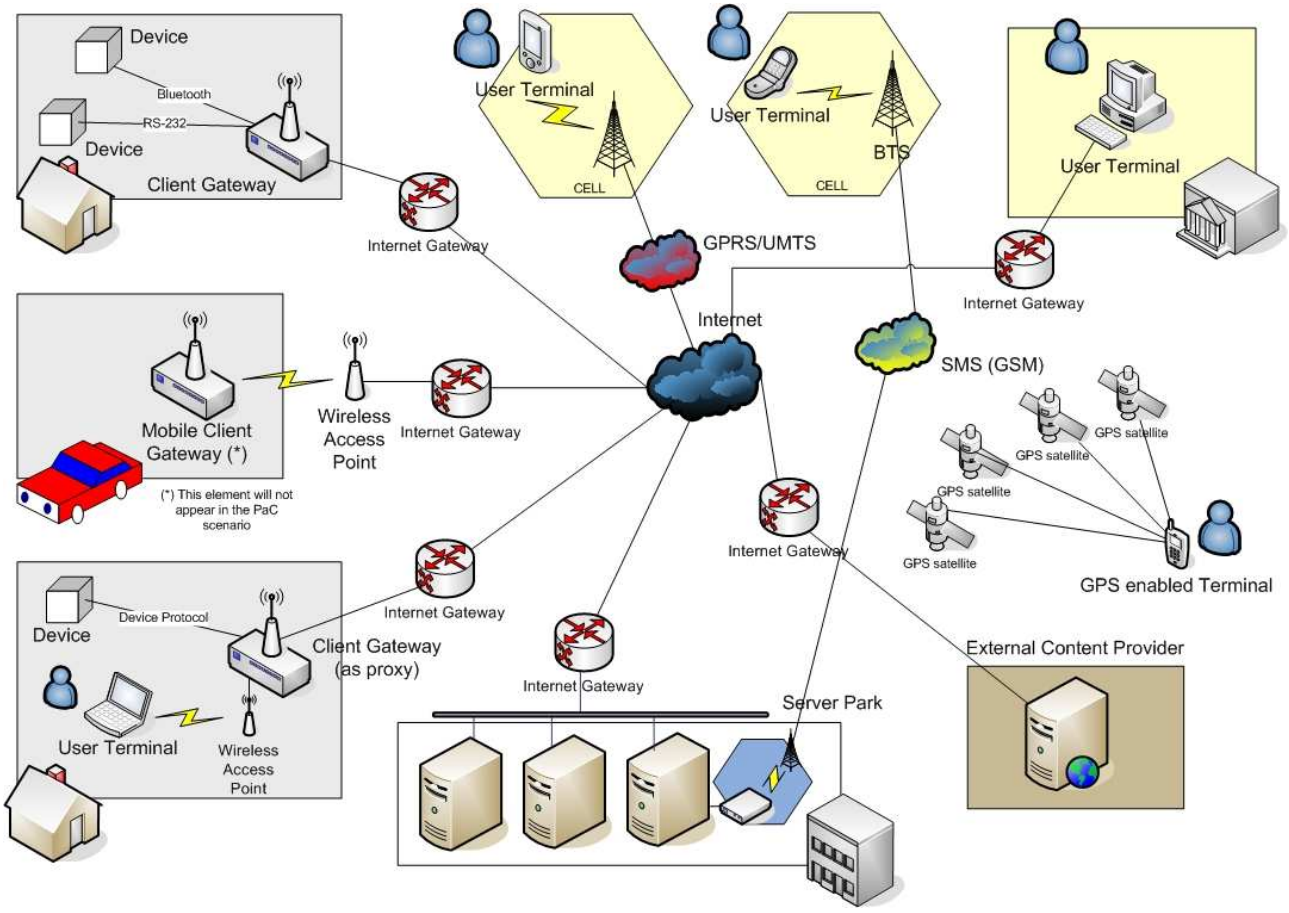

Figure 2 eu-DOMAIN prototype in exploitation

The following sections will present the technical and physical elements of the three different network accesses presented in the eu-DOMAIN infrastructure.

2.1 Fixed Access Points

Figure 3 shows the interconnection among the different servers at the Server Park. They are connected via the TID intranet.

TID network communications relies on a DSL backbone. The backbone is a line or set of lines where local area networks connect to in order to obtain a wide area network connection or where local area networks are connected to span distances efficiently, for example between TID buildings which are geographically distributed. The DSL backbone line at TID has a capacity of 30 Mbps upload and of 30Mbps download. The network topology of the backbone is Optical Fibre.

Local area networks are deployed in each location. The network topology of these LANs is Ethernet. Ethernet has been standardized as IEEE 802.3. Its star-topology, twisted pair wiring became the most widespread LAN technology in use from the 1990s to the present, largely replacing competing LAN standards such as coaxial cable Ethernet, token ring, FDDI, and ARCNET. This is the typical situation of the client installations that access the functionality provided by the Server Park, although

wireless access points are also envisioned (see next section). Nevertheless, the communication prototype deployed at TID is implemented using fixed access points for the client installation. Terminals using the Interaction Server will use also this fixed access points in the communication prototype at TID. Moreover, PDAs will make use of wireless access points available at TID (see next section).

The Server Park is accessible from outside TID facilities. The access to the Server Park is controlled by the NAT (Network Address Translation) standard. It involves re-writing the source and/or destination address of IP packets as they pass through a router or a firewall. In section 3, the use of the NAT in the eu-DOMAIN prototype is explained in depth.

Fixed access points enable server-side communication and client-side/server-side communication.

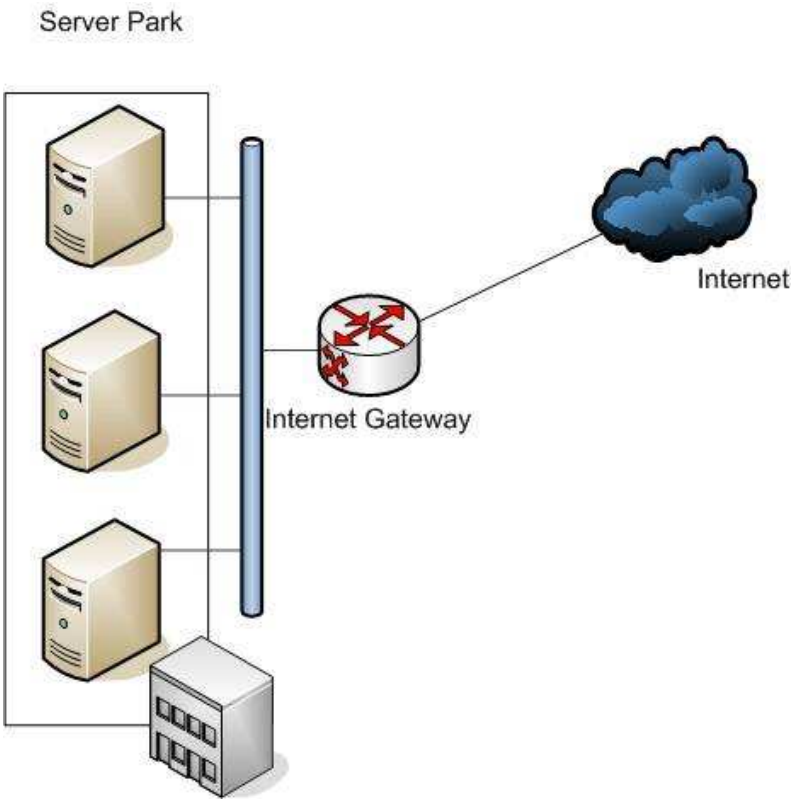

Figure 3 Fixed Access Point

2.2 Wireless Access Points

As it was previously stated, user terminals and client gateways will make use of Telco operators' networks available in the market. For the prototypes in TID facilities, terminals within TID facilities will make use of the wired and wireless Intranet to be able to access the Server Park. The wired access has just been described. Therefore, this chapter compiles the features of the wireless access points at TID facilities.

The wireless technology used is Wi-Fi, more precisely the IEEE 802.11b/g. There are several access points around the TID buildings which help devices to gain a wireless connection. This wireless network is protected, and it implements two well-known security and control access protocols:

- WEP is a scheme that is part of the IEEE 802.11 wireless networking standard to secure IEEE 802.11 wireless. WEP was intended to provide comparable confidentiality to a traditional wired network. Several serious weaknesses were identified by cryptanalysts and WEP was superseded by Wi-Fi Protected Access (WPA). Despite the weaknesses, WEP provides a level of security that can deter casual snooping.

- WPA provides improved data encryption, which was weak in WEP, and user authentication, which was for the most part missing in WEP. WPA utilizes its Temporal Key Integrity Protocol (TKIP) for improved data encryption. TKIP addresses all of the known vulnerabilities in WEP. WPA implements 802.1x and the Extensible Authentication Protocol (EAP) to strengthen user authentication.

This wireless local area network works with up to 54 Mbps.

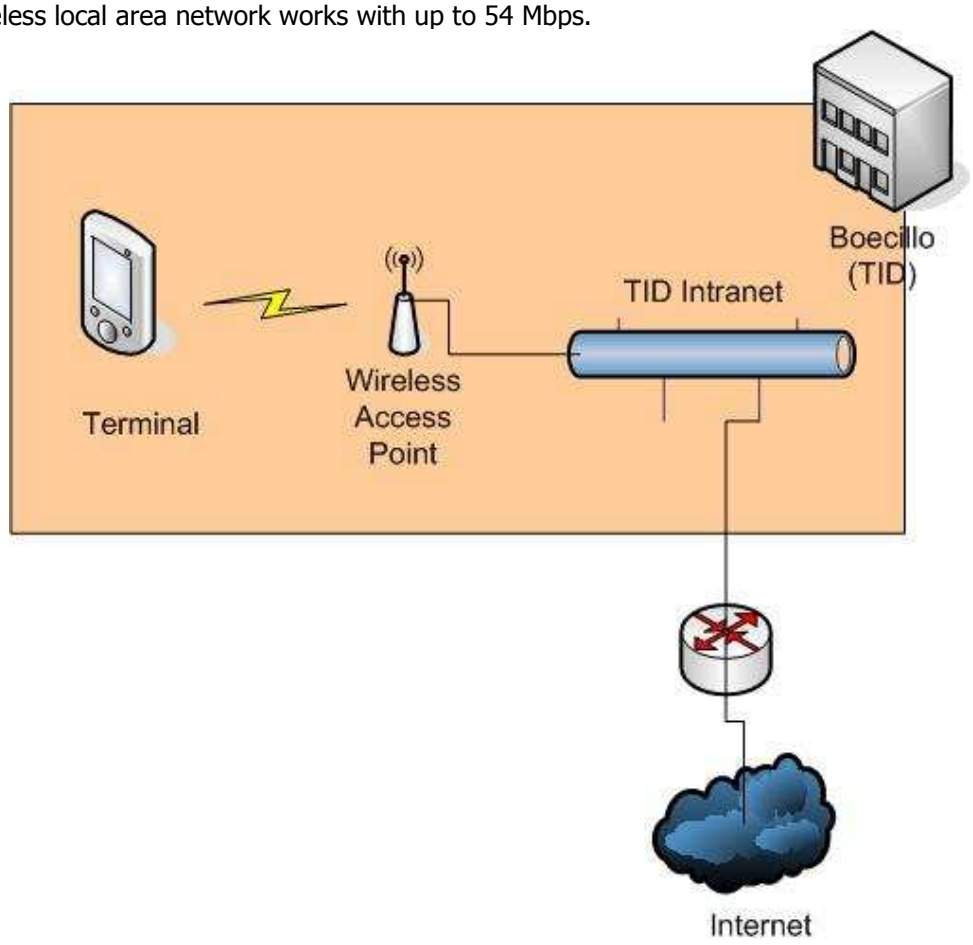

Figure 4 Wireless Access Point

2.3 External Clients & Terminals

Outside TID's facilities, External Clients and Terminals use commercial communication infrastructures, both wired and wireless. In this group, GSM, GPRS, UMTS, Cable or ADSL communication technologies can be used as Figure 5 depicts.

External clients or terminals can also access the Server Park installed at TID facilities because the Server Park is offered as a public interface. Nevertheless, only the client installations that are previously logged in the system can use the functionality due to security reasons. Moreover, terminal users need to have a valid certificate to use the Interaction Server for the same reasons.

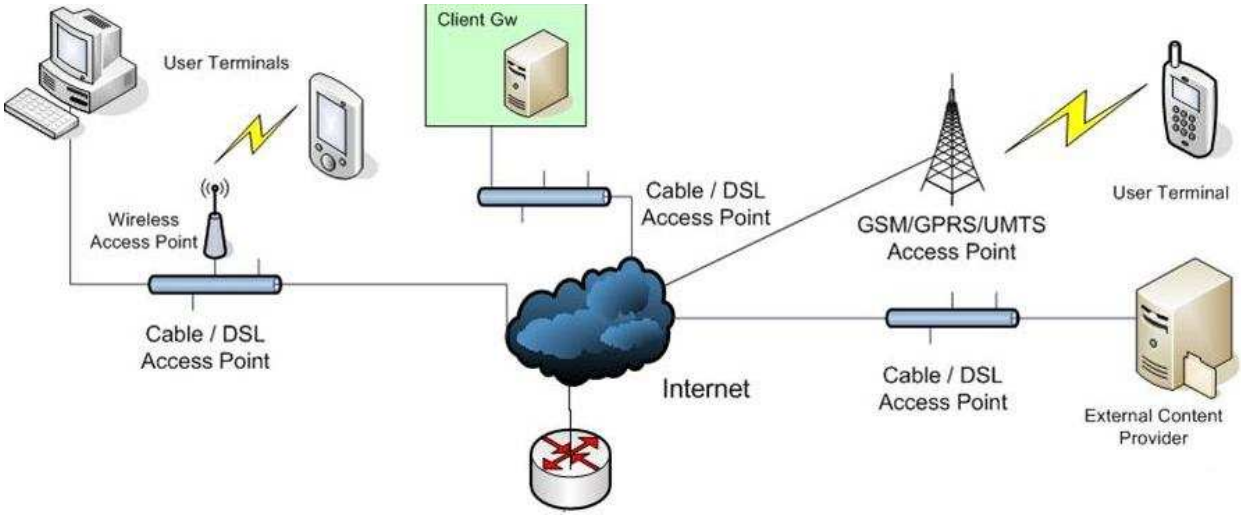

Figure 5 Commercial Infrastructure Access

In general, a large number of communication technologies can be used, which means that the eu-DOMAIN platform can operate on heterogeneous commercial networks and that this is done transparently to users. They just need an Internet connection, no matter the communication technology they use. All communication, apart from the one between devices and the Client Gateways, are based on HTTP(S) transfers (TCP/IP). This is possible because eu-DOMAIN infrastructure implements a Service Oriented Architecture (SOA) based on web services.

3. Server Network Security issues

As it is well-known, the Server Park is a secure environment completely under TID control whereas the client side is not a controlled set of components (it is for the prototype client installation at TID but not for external clients accessing the functionality provided by the platform). This chapter summarizes the main security concerns regarding network communications on the server-side.

The communication among software agents is secure since the environment is secure. The main concern here is access control from the outside. For this reason, the server side is protected behind a set of network firewalls. TID LAN uses different firewalls to protect the elements in the internal network. The first line of defence in firewall protection is the Packet Filter Firewall which operates at the Network Layer to examine incoming and outgoing packets and apply a fixed set of rules to the packets to determine whether they will be allowed to pass. It is typically very fast because it does not examine any of the data in the packet. It simply examines the IP packet header, the source and destination IP addresses, and the port combinations, and then it applies filtering rules. Further, Circuit-level Gateways are used to monitor all connections and only those connections that are found to be valid are allowed to pass through the firewall. This generally means that a client behind the firewall can initiate any type of session, but clients outside the firewall cannot see or connect to a machine protected by the firewall. Moreover, a Network Address Translation (NAT) is used to completely hide the network protected by the firewall by using many-to-one address translation. The Server Park will offer a single public IP address. All packets going outside the network have their internal IP addresses hidden for security, so any incoming packets are delivered to the network's public IP address. To handle ensuing port conflicts, a Port Address Translation (PAT) needs to be added to NAT. Finally, a demilitarized zone (DMZ) isolates the Server Park (the Interaction Server) from internal servers. The external hosts are placed in a separate network zone, on a separate adapter, connected to the firewall. Each subnetwork is also configured with its own security zone by connecting it to a separate firewall adapter. All traffic between zones, and all traffic from the Internet to all zones, is checked by the firewall. This infrastructure is shown in Figure 6

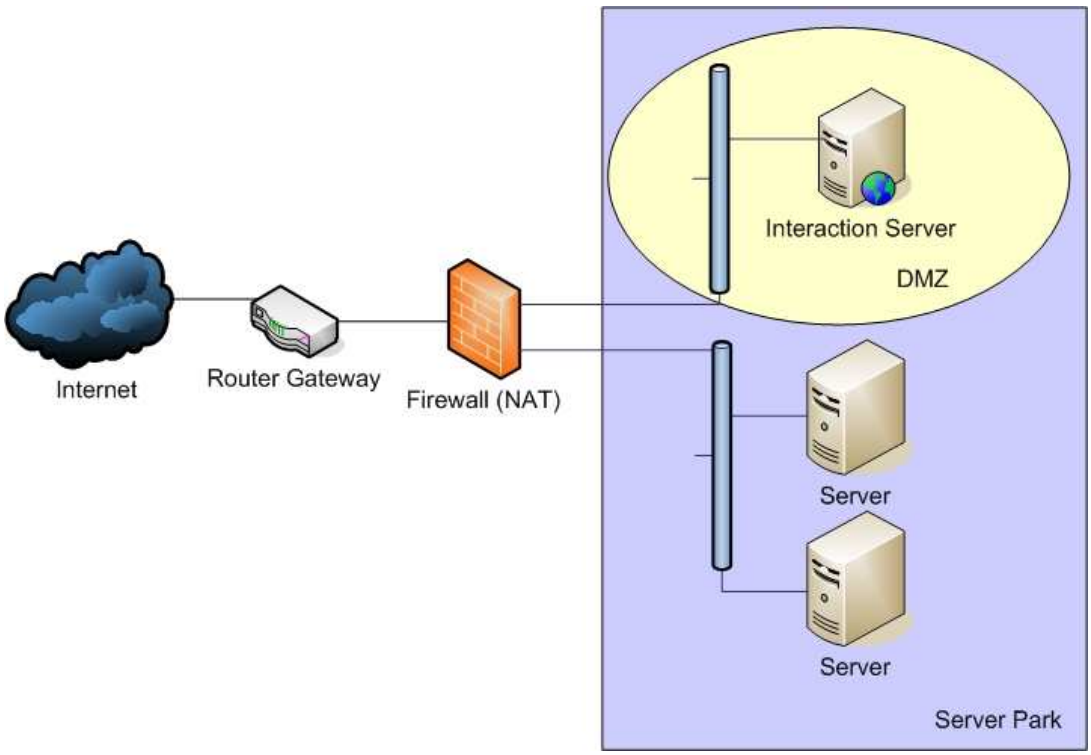

Figure 6 Server Firewall Security

4. Conclusions

The communication infrastructure to be used in eu-DOMAIN prototypes is presented in this document. The deliverable is by nature a prototype, but this document was written to complete and document the specifications of the communication infrastructure prototype.

This communication prototype is fully operational at TID facilities in Boecillo (Valladolid – Spain) where the Server Park is integrated and a client gateway is set up. This prototype will be available for one year after the project ends and it will make use of the available fixed and wireless access points. In particular, the communication prototype at TID will make use of fixed access points (ADSL) for the server park, the client installation and the fixed terminals (laptop, PC) and wireless access points (WiFi) for the mobile terminals (PDA) to be used as user terminal.

Moreover, external client installations and terminals will make use of commercial communication infrastructure to access the public interfaces of the eu-DOMAIN platform deployed at TID facilities.

Finally, the security of the server side has been presented. The communication prototype infrastructure will make use of different firewall, NAT and DMZ to isolate the public interfaces from the private ones and to assure that only allowed communication is performed among the actors playing a role in the infrastructure. This security implementation is complementary to the software security architecture defined in the scope of the project.

5. References

[eu-DOMAIN D3.1+D4.1, 2005] UAAR, CNET (2005), *Software Architecture Specification,* eu-DOMAIN deliverable

[eu-DOMAIN D5.1, 2005] Antolín P, et all (2005), *D5.1 Communication Architecture Description*, eu-DOMAIN deliverable

[WEP, 2006] "Wired Equivalent Privacy" http://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

[WPA, 2006] "Wi-Fi Protected Access" http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[Ethernet, 2007] "Ethernet" http://www.answers.com/topic/ethernet