Internal distribution code:

(A) [-] Publication in OJ
(B) [-] To Chairmen and Members
(C) [-] To Chairmen
(D) [X] No distribution

Datasheet for the decision of 12 October 2017

Case Number: T 1054/13 - 3.5.05

Application Number: 00300371.2

Publication Number: 1024627

IPC: H04L12/24, H04L29/06, H04L12/22

Language of the proceedings: EN

Title of invention:
A method and apparatus for managing a firewall

Applicant:
Alcatel-Lucent USA Inc.

Headword:
Network firewall/ALCATEL

Relevant legal provisions:
EPC 1973 Art. 56
RPBA Art. 13(1)

Keyword:
Inventive step - (no)

Decisions cited:

Catchword:

Europäisches Patentamt
European Patent Office
Office européen des brevets

Beschwerdekammern

Boards of Appeal

Chambres de recours

Boards of Appeal of the
European Patent Office
Richard-Reitzner-Allee 8
85540 Haar
GERMANY
Tel. +49 (0)89 2399-0
Fax +49 (0)89 2399-4465

Case Number: T 1054/13 - 3.5.05

D E C I S I O N
of Technical Board of Appeal 3.5.05
of 12 October 2017

Appellant: (Applicant)	Alcatel-Lucent USA Inc. 600-700 Mountain Avenue Murray Hill, NJ 07974 (US)
Representative:	Hirsch & Associés 137, rue de l'Université 75007 Paris (FR)
Decision under appeal:	**Decision of the Examining Division of the European Patent Office posted on 11 December 2012 refusing European patent application No. 00300371.2 pursuant to Article 97(2) EPC.**

Composition of the Board:

Chair	A. Ritzka
Members:	P. Cretaine
	G. Weiss

Summary of Facts and Submissions

I. This appeal is against the decision of the examining division, posted on 11 December 2012, refusing European patent application No. 00300371.2 on the grounds of lack of novelty (Article 54 EPC 1973) having regard to the disclosure of

D1: EP 0 658 837.

II. Notice of appeal was received on 8 February 2013 and the appeal fee was paid on the same day. The statement setting out the grounds of appeal was received on 29 March 2013. The appellant requested that the decision be set aside and that a patent be granted based on claims 1 to 26 filed with the statement setting out the grounds of appeal.

III. A summons to oral proceedings was issued on 24 July 2017. In an annex to this summons, the board gave its preliminary opinion that the claims did not comply with Article 54 EPC 1973, having regard to the disclosure of D1. Further, the board raised clarity objections against independent claims 23 to 26 (Article 84 EPC 1973).

IV. With a letter of reply dated 6 October 2017, the appellant submitted a set of amended claims 1 to 24 to replace the previous set of claims.

V. Oral proceedings were held on 12 October 2017 during which the appellant withdrew the set of claims filed with letter dated 6 October 2017 and filed a main request comprising a new claim 1, filed during the oral

proceedings, and claims 2 to 24 filed with letter dated 6 October 2017, and an auxiliary request comprising a new claim 1, filed during the oral proceedings, and claims 2 to 24 filed with letter dated 6 October 2017. The appellant requested that the decision under appeal be set aside and that a patent be granted on the basis of the main or auxiliary request.

VI. Independent claim 1 according to the main request reads as follows:

"A method for generating a security policy for a network, said network including a plurality of hosts (380), said method comprising the steps of:
receiving a definition for a plurality of roles that specify a role name, a type of service, one or more peers type to or from which the service applies, wherein each of said roles are capable of being assigned to said hosts (380) independently of a topology of said network, and said one or more of said plurality of hosts (380) inherit definitions associated with an assigned role;
receiving an assignment of said roles to one or more of said plurality of hosts (380) in said network; and
generating said security policy from said received definitions and assignments, said generating comprising generating rules for one or more of said plurality of hosts (380) based on said assigned roles, said rules determining whether a packet is passed to a destination host."

Independent claim 1 according to the auxiliary request reads as follows:

"A method for generating a security policy for a network, said network including a plurality of hosts (380), said method comprising the steps of:
receiving a definition for a plurality of roles that specify a role name, a type of service, one or more peers type to or from which the service applies in the form of:
- name of the role
- direction
- list of peers
- service name
wherein each of said roles are capable of being assigned to said hosts (380) independently of a topology of said network, and said one or more of said plurality of hosts (380) inherit definitions associated with an assigned role;
receiving an assignment of said roles to one or more of said plurality of hosts (380) in said network; and
generating said security policy from said received definitions and assignments, said generating comprising generating rules for one or more of said plurality of hosts (380) based on said assigned roles, said rules determining whether a packet is passed to a destination host."

The main and auxiliary requests both comprise a further independent claim 21 which reads as follows:

"A system for generating a security policy for a network, said network including a plurality of hosts (380), said system comprising:
a memory for storing computer-readable code; and
a processor operatively coupled to said memory, said processor configured to execute said computer-readable code, said computer-readable code configuring said processor to:

receive a definition for a plurality of roles that specify the ability of a host (380) to send and receive packets, wherein each of said roles are capable of being assigned to said hosts (380) independently of a topology of said network, and said hosts (380) inherit definitions associated with an assigned role;
receive an assignment of roles to said hosts (380) in said network; and
generate said security policy from said received definitions and assignments, said generating comprising generating rules for one or more of said plurality of hosts (380) based on said assigned roles, said rules determining whether a packet is passed to a destination host."

Reasons for the Decision

1. The appeal is admissible.

2. Main request

2.1 Admissibility

The main request was filed during the oral proceedings before the board. The amendments made to the claims as submitted with the statement setting out the grounds of appeal have reduced the number of independent system claims to one and introduced new features into independent method claim 1 and system claim 21. As these amendments were directly occasioned by the clarity and novelty objections raised by the board in its communication pursuant to Article 15(1) RPBA and do not add any substantial legal or technical complexity to the issues at stake, the board decided to exercise

its discretion under Article 13(1) RPBA and admit this request into the appeal proceedings.

2.2 Inventive step

D1 discloses, according to the essential features of claim 1 and using the wording of the application, a method of generating a security policy for a network (*see page 2, lines 32 and 33: "security method which controls information flow on a computer network"*), said network including a plurality of hosts (*see Figure 1: "workstations 104"*), said method comprising the steps of :

receiving a definition for a plurality of roles (*the plurality of security rules implemented at a host can be considered as a role specifying the ability of a host to send and receive packets; see page 3, lines 51 and 52: "workstations each have a packet filter so that the information flow to/from these workstations is separately controlled" and lines 55 to 57: "Each of the packet filters is installed at the time that the network is set up or the security system is installed"; page 4, lines 4 to 6: "each packet filter can handle... multiple security rules"*),

wherein each of said roles is capable of being assigned to said hosts independently of the topology of the network (*see page 3, lines 32 to 35*), and said hosts inherit definitions associated with an assigned role (*see page 4, line 7: "The system administrator enters the security rules"; page 4, lines 9 and 10: "the resulting code is transmitted to the appropriate packet filter or filters in the network to perform the function that is desired"*);

receiving an assignment of said roles to hosts in said network (*see page 4, lines 1 and 2: "Each of the packet filters operates on a set of instructions which has been generated by the packet filter generator"; page 4, lines 4 to 6: "each packet filter can handle ... multiple security rules"*), and

generating said security policy from said received definitions and assignment (*see page 4, lines 7-10: "the resulting code is transmitted to the appropriate packet filter or filters in the network to perform the function that is desired"*),

said generating comprising generating rules for hosts based on their assigned roles, said rules determining whether a packet is passed to a destination host (*see page 2, line 43: "to either accept or reject the passage of said packet in said network"*).

The difference between the subject-matter of claim 1 and the disclosure of D1 is thus that the roles assigned to hosts are defined more specifically in claim 1 by a role name, a type of service, and one or more peer host types to or from which the service applies, whereas in D1 each of the multiple security rules forming a role and implemented at a host is only based on a service, a single source, and a single destination in the network (see page 4, lines 44 to 49).

The technical effect of this distinguishing feature is that a host can be assigned to a group of hosts, defined by their type and sharing the same type of service, and that the security rules are then generated based on this assignment. In that respect, it is further to be noted that the indication of a name in

the role's definition is a mere representation of a cognitive content, a name, which does not imply any technical effect in relation to the network security policy.

The objective technical problem can thus be defined as how to group hosts in the network depending on their type and the service they may exchange.

D1 however discloses (see page 4, lines 20 to 33, in combination with Figure 3A) that workstations of an enterprise network can be grouped by enterprise departments in order to control the data flow within the network by the appropriate placement of packet filters. D1 suggests (see page 4, line 27 and in "SMTP" in Figure 3A) that electronic mail is a type of service which can be selectively allowed between workstations depending on which departments the workstations belong to. This passage would thus lead the skilled person to define, before building the network of D1, which workstations are intended to be used in which departments. In doing so, the skilled person would define roles for these workstations, a role specifying a type of service (e.g. email) and peer type (affiliation to department) to and from which the service applies. In defining these roles within the network of D1, the skilled person would arrive at the subject-matter of claim 1.

The appellant stressed that a security rule in D1 was not equivalent to a role as defined in claim 1. The board has acknowledged this difference in the above inventive-step assessment and rather has considered that a workstation's belonging to a department and its ability to communicate with workstations of other

departments both define a role of the workstation in the sense of claim 1.

The appellant further argued that the allocation of roles to hosts, as defined in claim 1, allows the building of a security policy independently of the topology of the network, unlike the system of D1. The board is however not convinced by this argument since the allocation of a workstation to a department in D1 corresponds to defining a peer type for this workstation prior to defining the different connections within the workstations of the different departments of the network, i.e. before setting the topology of the network.

For these reasons, the board judges that the subject-matter of claim 1 fails to meet the requirements of Article 56 EPC 1973, having regard to the disclosure of D1.

3. Auxiliary request

3.1 Admissibility

The auxiliary request was filed during the oral proceedings before the board. For the same reasons as those given in point 2.1 with respect to the main request, the board admitted it into the appeal proceedings in accordance with Article 13(1) RPBA.

3.2 Inventive step

Claim 1 adds to claim 1 of the main request the feature that a role is further defined
"in the form of:
- name of role,

- direction,
- list of peers,
- service name".

This feature defines how technical specifications included in a role's definition, namely the "type of service" and the "one or more peers type to or from which the service applies" are presented in list form. Thus, this feature relates to a mere, non-technical, presentation of information with no inventive merit.

For these reasons, the board judges that the subject-matter of claim 1 likewise fails to meet the requirements of Article 56 EPC 1973, having regard to the disclosure of D1.

4. Conclusion

Neither of the appellant's two requests is allowable under Article 56 EPC 1973.

Order

For these reasons it is decided that:

The appeal is dismissed.

The Registrar: The Chair:

K. Götz-Wein A. Ritzka

Decision electronically authenticated