(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 April 2009 (16.04.2009)

PCT

(10) International Publication Number
WO 2009/047065 A4

(51) International Patent Classification:
H04L 29/06 (2006.01) *H04L 29/12* (2006.01)

(21) International Application Number:
PCT/EP2008/061915

(22) International Filing Date:
9 September 2008 (09.09.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
07118044.2 8 October 2007 (08.10.2007) EP

(71) Applicant *(for all designated States except US)*: **NOKIA SIEMENS NETWORKS OY** [FI/FI]; Karaportti 3, FI-02610 Espoo (FI).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **RÄSÄNEN, Juha** [FI/FI]; Sinirinnantie 21, FI-02660 Espoo (FI).

(74) Agents: **LESON, Thomas, J., A.** et al.; Bavariaring 4 - 6, 80336 Munich (DE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

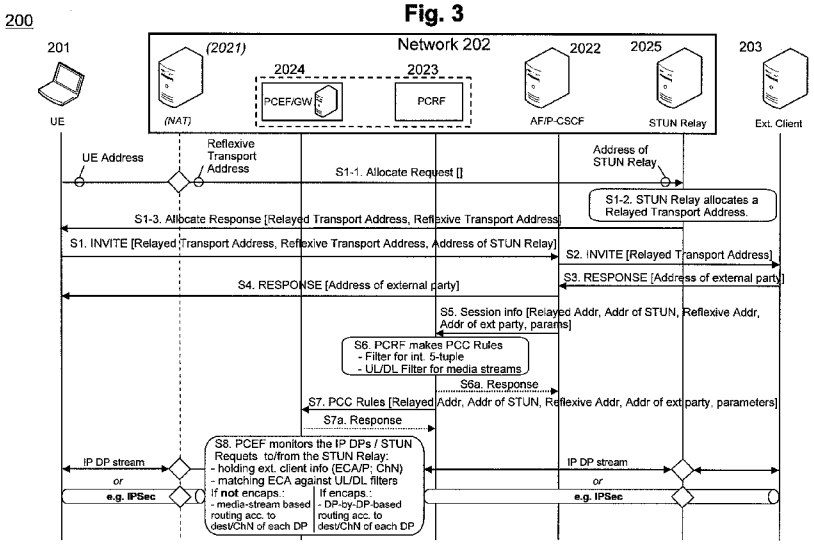
— *with amended claims (Art. 19(1))*

(88) Date of publication of the international search report:
16 July 2009

Date of publication of the amended claims: 8 October 2009

(54) Title: METHODS, APPARATUSES, SYSTEM, AND RELATED COMPUTER PROGRAM PRODUCT FOR POLICY CONTROL

Fig. 3



(57) Abstract: It is disclosed a method comprising receiving first address information relating to a terminal and a network traffic relay entity, obtaining second address information relating to the network traffic relay entity and a network traffic destination entity, and sending the first address information and the second address information to a controlling entity; and a method comprising receiving the first and second address information, generating policy information based on the received first and second address information, and monitoring network traffic based on the generated policy information.

WO 2009/047065 A4

AMENDED CLAIMS
received by the International Bureau on 03 August 2009 (03.08.09)

1. A method, comprising:

supporting data transmission between a terminal and one of an external client and server;

relaying, by means for relaying, at least one of data flows, media streams and data packets between the terminal and the one of the external client and server;

enforcing policy control to the relayed at least one of service data flows, media streams, and data packets;

receiving, at a policy enforcement function, a first kind of address information related to the at least one of service data flows, media streams, and data packets;

receiving, at the policy enforcement function, a second kind of address information used by the terminal and the means for relaying for data transmission between the terminal and the means for relaying;

monitoring, at the policy enforcement function, data traffic between the terminal and the means for relaying based on policy information related to the first and second kind of address information;

detecting, at the policy enforcement function, a used transmission scheme between the terminal and the means for relaying;

holding, at the policy enforcement function, address information of the at least one of service data flows, media streams, and data packets in the data transmission; and

enforcing, at the policy enforcement function, by using the first kind of address information, policy control to the at least one of service data flows, media streams, and data packets by matching the first kind of address information against the address information of the at least one of service data flows, media streams, and data packets.

2. The method according to claim 1, further comprising

supporting address translation between the terminal and the means for relaying;

the detecting further comprises monitoring the data transmission between the terminal and the means for relaying, and detecting the address information of the at least one of service data flows, media streams, and data packets in the data transmission based on the detected data transmission scheme.

3. The method according to claim 1, further comprising

examining, if the result of matching is negative, whether a data packet is constituted by a simple traversal of user datagram protocol over network address translations request message comprising a source address of the terminal and indicating a network traffic destination entity, and

examining, if the result of the examining of the data packet is affirmative, whether the indicated network traffic destination entity accords with at least one of the policy information and at least one for the first kind of address and filter functions, and

updating, if the result of the means for examining is affirmative, at least one of the first kind of address and filter functions with at least one of the source address and a port of the terminal.

4. The method according to claim 1, further comprising

examining, if the data packet causes the network traffic relay entity to permit a new destination address, and

dropping the data packet, if the result by the examining indicates that the data packet causes the network traffic relay entity to permit a new destination address not matching at least one of the first kind of address and filter functions.

5. The method according to claim 1, further comprising

examining, if the data packet causes the network traffic relay entity to permit a new destination address, wherein

the enforcing comprises passing the data packet through, if the result by the examining indicates that the data packet causes the network traffic relay entity to permit a new destination address matching at least one of the first kind of address and filter functions.

6. The method according to any one of claims 1 to 5, further comprising:

generating the policy information based on the received first and second kinds of information; and

determining whether the network traffic is encapsulated network traffic, and, if so, the enforcing further comprises enforcing policy on individual at least one of service data flows, media streams and data packets inside the encapsulation based on the policy information generated by the means for generating and the destination address information held by the means for holding.

7. The method according to any one of claims 1 to 6, wherein the first kind of address information comprises at least one of a source address of the terminal, a source port of the terminal, a destination address of the network

traffic relay entity, a destination port of the network traffic relay entity, a protocol to be used between the terminal and the network traffic relay entity and a channel number relating to a media stream.

8. The method according to claim 7, wherein at least one of the source address of the terminal and the source port of the terminal further comprises network address translation information.

9. The method according to any one of claims 1 to 8, wherein the second kind of address information comprises at least one of a source address of the network traffic relay entity, a source port of the network traffic relay entity, a reflexive destination address of the terminal entity, a reflexive destination port of the terminal entity, a protocol to be used between the network traffic relay entity and the terminal entity and a channel number relating to a media stream.

10. An apparatus, comprising:

means for supporting data transmission between a terminal and one of an external client and server;

means for relaying at least one of data flows, media streams and data packets between the terminal and the one of the external client and server;

means for enforcing policy control to the relayed at least one of service data flows, media streams, and data packets;

means for receiving, at a policy enforcement function, a first kind of address information related to the at least one of service data flows, media streams, and data packets;

means for receiving, at the policy enforcement function, a second kind of address information used by the

terminal and the means for relaying for data transmission between the terminal and the means for relaying;

means for monitoring, at the policy enforcement function, data traffic between the terminal and the means for relaying based on policy information related to the first and second kind of address information;

means for detecting, at the policy enforcement function, a used transmission scheme between the terminal and the means for relaying;

means for holding, at the policy enforcement function, address information of the at least one of service data flows, media streams, and data packets in the data transmission; and

means for enforcing, at the policy enforcement function by using the first kind of address information, policy control to the at least one of service data flows, media streams, and data packets by matching the first kind of address information against the address information of the at least one of service data flows, media streams, and data packets.

11. The apparatus according to claim 10, further comprising

means for supporting address translation between the terminal and the means for relaying;

the means for detecting is further configured to detect by monitoring the data transmission between the terminal and the means for relaying, and to detect the address information of the at least one of service data flows, media streams, and data packets in the data transmission based on the detected data transmission scheme.

12. The apparatus according to claim 10, further comprising

means for examining, if the result of matching is negative, whether a data packet is constituted by a simple

traversal of user datagram protocol over network address translations request message comprising a source address of the terminal and indicating a network traffic destination entity, and for examining, if the result of the examining of the data packet is affirmative, whether the indicated network traffic destination entity accords with at least one of the policy information and at least one for the first kind of address and filter functions, and

means for updating, if the result of the means for examining is affirmative, at least one of the first kind of address and filter functions with at least one of the source address and a port of the terminal.

13. The apparatus according to claim 10, further comprising

means for examining, if the data packet causes the network traffic relay entity to permit a new destination address, and

means for dropping the data packet, if the result by the means for examining indicates that the data packet causes the network traffic relay entity to permit a new destination address not matching at least one of the first kind of address and filter functions.

14. The apparatus according to claim 10, further comprising

means for examining, if the data packet causes the network traffic relay entity to permit a new destination address, wherein

the means for enforcing policy control measures is configured to pass the data packet through, if the result by the means for examining indicates that the data packet causes the network traffic relay entity to permit a new destination address matching at least one of the first kind of address and filter functions.

15. The apparatus according to any one of claims 10 to 14, further comprising:

means for generating the policy information based on the received first and second kinds of information; and

means for determining whether the network traffic is encapsulated network traffic, and, if so, the means for policy enforcement is further configured to enforce policy on individual at least one of service data flows, media streams and data packets inside the encapsulation based on the policy information generated by the means for generating and the destination address information held by the means for holding.

16. The apparatus according to any one of claims 10 to 15, wherein the first kind of address information comprises at least one of a source address of the terminal, a source port of the terminal, a destination address of the network traffic relay entity, a destination port of the network traffic relay entity, a protocol to be used between the terminal and the network traffic relay entity and a channel number relating to a media stream.

17. The apparatus according to claim 16, wherein at least one of the source address of the terminal and the source port of the terminal further comprises network address translation information.

18. The apparatus according to any one of claims 10 to 17, wherein the second kind of address information comprises at least one of a source address of the network traffic relay entity, a source port of the network traffic relay entity, a reflexive destination address of the terminal entity, a reflexive destination port of the terminal entity, a protocol to be used between the network traffic relay

entity and the terminal entity and a channel number relating to a media stream.

19. The apparatus according to any one of claims 10 to 18, wherein the terminal is constituted by a user equipment.

20. The apparatus according to any one of claims 10 to 19, wherein the network traffic relay entity is constituted by a simple traversal of user datagram protocol through network address translations relay server.

21. The apparatus according to any one of claims 10 to 20, wherein the apparatus is constituted by at least one of a gateway function, a policy and charging rules function and a policy and charging enforcement function.

22. The apparatus according to any one of claims 10 to 21, wherein the apparatus is implemented as a chipset or module.

23. A system, comprising:

a user equipment;

an apparatus according to claim 10; and

an application function or proxy call state control function comprising:

means for receiving the first kind of address information;

means for obtaining the second kind of address information; and

means for sending the first and second kinds of address information to the apparatus.

24. A computer program product comprising code means for performing methods steps of a method according to any one of the claims 1 to 9, when run on a computer.