Title (en)

SYSTEM, METHOD AND APPARATUS THAT EMPLOY VIRTUAL PRIVATE NETWORKS TO RESIST IP QoS DENIAL OF SERVICE ATTACKS

Title (de)

SYSTEM, VERFAHREN UND VORRICHTUNG, DIE VIRTUELLE PRIVATE NETZWERKE VERWENDEN, UM IP-QoS-DENIAL-OF-SERVICE-ATTACKEN ZU WIDERSTEHEN

Title (fr)

SYSTEME, PROCEDE ET APPAREIL UTILISANT DES RESEAUX PRIVES VIRTUELS POUR RESISTER AUX ATTAQUES ENTRAINANT UN REFUS DE SERVICE TEL QUE LA QUALITE DE SERVICE DANS UN PROTOCOLE INTERNET

Publication

EP 1374057 A1 20040102 (EN)

Application

EP 02728525 A 20020320

Priority

- US 0208577 W 20020320
- US 27692301 P 20010320
- US 27695301 P 20010320
- US 27695501 P 20010320
- US 2304301 A 20011217

Abstract (en)

[origin: WO02075548A1] A network architecture (30) in accordance with the present invention includes a communication network that supports one or more network-based Virtual Private Networks (VPNs) (44, 46). The communication network includes a plurality of boundary routers (40, 42) that are connected by access links (35) to CPE edge routers (34) belonging to the one or more VPNs (44, 46). To prevent traffic from outside a customer's VPN (e.g., traffic from other VPNs or the Internet at large) from degrading the QoS (Quality of service) provided to traffic from within the customer's VPN, the present invention gives precedence to intra-VPN traffic over extra-VPN traffic on each customer's access link through access link prioritization or access link capacity allocation, such that extra-VPN traffic cannot interfere with inter-VPN traffic. Granting precedence to intra-VPN traffic over extra-VPN traffic in this manner entails special configuration of network elements and protocols, including partitioning between intra-VPN and extra-VPN traffic on the physical access link using layer 2 multiplexing and the configuration of routing protocols to achieve logical traffic separation. By configuring the access networks, the VPN boundary routers (40, 42) and CPE edge routers (34) and the routing protocols of the edge and boundary routers in this manner, the high-level service of DoS (Denial of Service) attack prevention is achieved.

IPC 1-7

H04L 29/06; H04L 12/46

IPC 8 full level

H04L 12/56 (2006.01); H04L 12/14 (2006.01); H04L 12/46 (2006.01); H04L 29/06 (2006.01); H04L 29/08 (2006.01); H04L 29/12 (2006.01); H04M 3/22 (2006.01); H04M 3/436 (2006.01); H04M 7/00 (2006.01); H04M 15/00 (2006.01); H04Q 3/00 (2006.01); H04W 12/12 (2009.01)

CPC (source: EP)

H04L 12/14 (2013.01); H04L 12/1403 (2013.01); H04L 12/1446 (2013.01); H04L 61/4523 (2022.05); H04L 61/4535 (2022.05); H04L 61/4557 (2022.05); H04L 63/0272 (2013.01); H04L 63/1458 (2013.01); H04L 65/103 (2013.01); H04L 65/104 (2013.01); H04L 65/1043 (2013.01); H04L 65/1069 (2013.01); H04L 65/1096 (2013.01); H04L 65/1104 (2022.05); H04L 65/612 (2022.05); H04L 65/762 (2022.05); H04L 67/303 (2013.01); H04L 67/306 (2013.01); H04L 67/51 (2022.05); H04M 3/2218 (2013.01); H04M 3/436 (2013.01); H04M 7/006 (2013.01); H04M 15/00 (2013.01); H04M 15/43 (2013.01); H04M 15/44 (2013.01); H04M 15/49 (2013.01); H04M 15/51 (2013.01); H04M 15/52 (2013.01); H04M 15/53 (2013.01); H04M 15/55 (2013.01); H04M 15/58 (2013.01); H04M 15/745 (2013.01); H04Q 3/0029 (2013.01); H04L 69/329 (2013.01); H04M 2215/0104 (2013.01); H04M 2215/0108 (2013.01); H04M 2215/0168 (2013.01); H04M 2215/0172 (2013.01); H04M 2215/0176 (2013.01); H04M 2215/0188 (2013.01); H04M 2215/2046 (2013.01); H04M 2215/46 (2013.01); H04M 2215/54 (2013.01)

Designated contracting state (EPC)

AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR

DOCDB simple family (publication)

WO 02075548 A1 20020926; BR 0208223 A 20040302; CA 2441712 A1 20020926; CN 1498368 A 20040519; EP 1374057 A1 20040102; EP 1374057 A4 20041110; JP 2004533149 A 20041028; MX PA03008421 A 20040129

DOCDB simple family (application)

US 0208577 W 20020320; BR 0208223 A 20020320; CA 2441712 A 20020320; CN 02806820 A 20020320; EP 02728525 A 20020320; JP 2002574087 A 20020320; MX PA03008421 A 20020320