(19) OFICIUL DE STAT
PENTRU INVENŢII ŞI MĂRCI
Bucureşti

ROMÂNIA

(11) RO 131306 A2
(51) Int.Cl.
H04L 12/26 (2006.01)

(12) # CERERE DE BREVET DE INVENŢIE

(21) Nr. cerere: **a 2014 00994**

(22) Data de depozit: **16/12/2014**

(41) Data publicării cererii:
29/07/2016 BOPI nr. **7/2016**

(71) Solicitant:
• **IXIA**, *A CALIFORNIA CORPORATION, 26601 WEST AGOURA ROAD, CALABASAS, CA, US*

(72) Inventatori:
• **NISTUR PAVEL MARIUS**, *STR.MITROPOLIT VARLAAM NR.88, AP.4, SECTOR 1, BUCUREŞTI, B, RO*

(74) Mandatar:
RATZA ŞI RATZA SRL, *B-DUL A.I. CUZA, NR. 52-54, SECTOR 1, BUCUREŞTI*

(54) # METODE, SISTEME ŞI SUPORT CITIBIL PE CALCULATOR PENTRU INIŢIEREA ŞI EXECUŢIA TESTELOR DE PERFORMANŢĂ A UNEI REŢELE PRIVATE ŞI/SAU A COMPONENTELOR ACESTEIA

(57) **Rezumat:**

Invenţia se referă la o metodă, la un sistem şi la un suport citibil de calculator, pentru iniţierea şi execuţia testelor de performanţă ale unei reţele private şi/sau ale componentelor acesteia. Metoda conform invenţiei constă în iniţierea, într-un punct de capăt receptor, dintr-o reţea privată, a unei conexiuni la nivelul stratului de transport, cu un punct de capăt expeditor dintr-o reţea publică, alocarea în scopuri de testare, la nivelul punctului de capăt expeditor, a unui port, legarea la port şi transmiterea unei adrese IP şi a unui număr al portului prin conexiunea de la nivelul stratului de transport, transmiterea, la nivelul punctului de capăt receptor, a unei datagrame de perforare a unei breşe de comunicaţie, de la reţeaua privată la reţeaua publică, pentru a crea o breşă într-un firewall care separă reţelele publică şi privată, şi, la nivelul punctului de capăt expeditor, recepţionarea datagramei de perforare a breşei de comunicaţie, şi folosirea adresei IP şi a informaţiilor referitoare la port din datagrama de perforare a breşei de comunicaţie, pentru a transmite trafic de testare la punctul de capăt receptor din reţeaua privată, prin breşa creată în firewall. Sistemul (**100**) conform invenţiei cuprinde un punct de capăt receptor (**E2**) într-o reţea privată, şi un punct de capăt expeditor (**E1**) într-o reţea publică, ce sunt configurate să efectueze etapele metodei conform invenţiei. Suportul citibil de calculator are stocate instrucţiuni care, atunci când sunt executate de către un procesor sau de un calculator, efectuează etapele metodei conform invenţiei.

Revendicări: 19
Figuri: 7

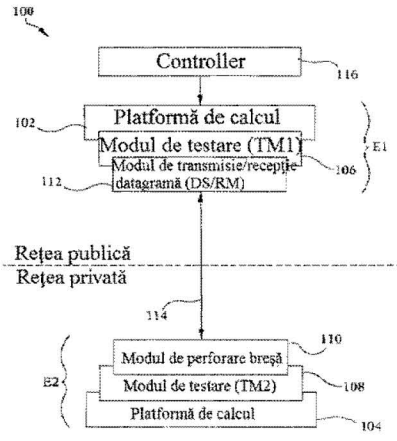

Fig. 1

RO 131306 A2

95

DESCRIERE

METODE, SISTEME ŞI SUPORT CITIBIL DE CALCULATOR PENTRU INIŢIEREA ŞI EXECUŢIA TESTELOR DE PERFORMANŢĂ ALE UNEI REŢELE PRIVATEŞI/SAU ALE COMPONENTELOR ACESTEIA

DOMENIUL TEHNIC DE APLICARE

Obiectele prezentei invenții se referă la efectuarea testelor de performanță ale unei rețele și/sau ale componentelor aesteia. Mai precis, obiectele invenției se referă la metode, sisteme și suport citibil de calculator pentru iniţierea şi execuţia testelor de performanţă ale unei reţele privateşi/sau ale componentelor acesteia.

STADIUL ANTERIOR AL TEHNICII

O rețea privată este o rețea aflată în spatele unui dispozitiv firewall/de traducerea adresei de rețea (NAT - network address translation) și/sau unui dispozitiv de traducere adresă de port (PAT - port address translation). Este de dorit să se testeze dispozitivele unei rețele private situate în spatele unui dispozitiv firewall (denumit în continuare firewall). Cu toate acestea, trebuie să existe un mecanism pentru a permite traficului de testare să traverseze firewall.

În cazul în care firewall-ul este performant doar pentru funcții NAT, atunci poate fi creată și stocată o mapare a unei singure adrese IP publice la o singură adresă IP privată într-un tabel NAT, ceea ce permite ca un număr de porturi să fie deschise în firewall. Porturile deschise permit trafic de testare de la adresa IP de rețea publică la adresa IP privată, pentru a traversa firewall și pentru a ajunge la punctul de capăt de destinație. Pot fi simulați și testați un numar mare de utilizatori, folosind porturile deschise în firewall și adresând traficul la adresa IP privată. Cu toate acestea, deschiderea porturilor în firewall creează probleme de securitate. În plus, în cazul în care firewall-ul pune în aplicare și traducerea adresei de port (PAT), aceasta trebuie să fie făcută prin funcția PAT, pentru fiecare utilizator simulat, astfel încât o intrare care mapează adresa (IP/port) publică prin UDP (protocolul datagramei utilizatorului (UDP) - user datagram protocol) la adresa privată (IP/port) prin UDP trebuie să fie adăugată în tabelul PAT. Această restricție blochează efectiv rularea de teste de performanță, în cazul în care sute de utilizatori trebuie simulați pentru a atinge debitul dorit.

În consecință, există o nevoie de metode, sisteme și suport citibil de calculator pentru iniţierea şi execuţia testelor de performanţă ale unei reţele privateşi/sau ale componentelor acesteia.

a-2014--00994-
16 -12- 2014

94

EXPUNEREA PE SCURT A INVENȚIEI

Sunt dezvăluite metode, sisteme și suport citibil de calculator pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia. La un punct de capăt receptor într-o rețea privată, conform invenției, metoda constă în inițierea unei conexiuni de strat de transport cu un punct de capăt expeditor, într-o rețea publică. La punctul de capăt expeditor în rețeaua publică, metoda mai constă în alocarea unui port în scopuri de testare, legarea la port, precum și transmiterea unei adrese prin Protocolul Internet (Internet Protocol (IP)) și a unui număr de port peste conexiunea de strat de transport. La punctul de capăt receptor, metoda mai constă în transmiterea unei datagrame de perforarea unei breșe de comunicație, de la rețeaua privată la rețeaua publică, pentru a crea o breșă într-un firewall care separă rețelele publice și private. La punctul de capăt expeditor, metoda mai constă în recepționarea datagramei de perforarea unei breșe de comunicație și în folosirea adresei IP și a informațiilor de port în datagrama de perforarea unei breșe de comunicație, pentru a transmite trafic de testare la punctul de capăt receptor în rețeaua privată, prin breșa din firewall.

Conform invenției, pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, sistemul include un punct de capăt receptor într-o rețea privată și un punct de capăt expeditor într-o rețea publică. Punctul de capăt receptor este configurat pentru a iniția o conexiune de strat de transport cu punctul de capăt expeditor. Ca răspuns la recepționarea conexiunii de strat de transport, punctul de capăt expeditor este configurat pentru a aloca un port în scopuri de testare, se leaga de port, și transmite o adresă IP și un număr de port peste conexiunea de strat de transport. Ca răspuns la recepționarea adresei IP și a numărului portului, punctul de capăt receptor este configurat pentru a transmite o datagrama de perforarea unei breșe de comunicație de la rețeaua privat la rețeaua publică pentru a crea o breșă într-un firewall care separă rețeaua privată de rețeaua publică. Ca răspuns la recepționarea datagramei de perforarea unei breșe de comunicație, punctul de capăt expeditor este configurat să utilizeze adresa IP și informațiile de port în datagrama de perforarea unei breșe de comunicație pentru a transmite trafic de testare la punctul la de capăt receptor prin breșa din firewall.

Obiectele invenției descrise aici pot fi implementate în software-ul în combinație cu hardware și/sau firmware. De exemplu, obiectele invenției descrise aici pot fi implementate în software-ul executat de un procesor. Într-un exemplu de implementare, obiectele invenției descrise aici pot fi implementate folosind un suport non-tranzitoriu care poate fi citit de calculator care are

stocate pe acesta instrucțiuni executabile de calculator, care atunci când sunt executate de către procesorul acestuia, comandă calculatorul să efecteze etapele. Suportul citibil de calculator, adecvat pentru punerea în aplicare a obiectelor prezentei invenții, include dispozitive non-tranzitorii, cum ar fi dispozitive de memorie pe disc, dispozitive de memorie cip, dispozitive logice programabile, circuite integrate digitale configurabile de către utilizator și circuite integrate specifice aplicației. În plus, un suport care poate fi citit de calculator, care implementează obiectele prezentei invenții, poate fi amplasat pe un singur dispozitiv sau platformă de calcul sau pot fi distribuite pe mai multe dispozitive sau platforme de calcul.

Așa cum sunt utilizați în prezenta descriere, termenii "puncte de capăt" și "nod" se referă la platforme de calcul fizice, inclusiv unul sau mai multe procesoare, interfețe de rețea și memorie.

Așa cum sunt utilizați în prezenta descriere, fiecare dintre termenii "funcție" și "modul" se referă la hardware, firmware sau software în combinație cu hardware și/sau firmware pentru implementarea caracteristicilor descrise aici.

DESCRIEREA PE SCURT A DESENELOR

Se descriu în continuare obiectele prezentei invenții, în legătură cu Figurile anexate, care reprezintă:

Figura 1 este o diagramă care ilustrează platforme de calcul pentru inițierea și efectuarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a obiectului prezentei invenții;

Figura 2 este o diagramă care ilustrează un mediu pentru inițierea și efectuarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a prezentei invenții;

Figurile 3A și 3B sunt diagrame care ilustrează comunicațiile perechi pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a prezentei invenții;

Figurile 4A și 4B sunt diagrame care ilustruază metodele pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a prezentei invenții; și

Figura 5 este o diagramă care ilustrează o metodă pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a prezentei invenții.

DESCRIEREA DETALIATĂ

Prezenta invenție se referă metode, sisteme și suport citibil de calculator pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia. În conformitate cu unele aspecte ale obiectelor prezentei invenții, datagramele de testare performante sunt schimbate între două sau mai multe puncte de capăt pentru testarea unei rețele private. Datagramele includ adrese sursă/destinație, care, atunci când sunt utilizate într-o combinație (unică) cunoscută, va "perfora o breșă" în rețeaua privată respectivă și peste un dispozitiv de securitate. Dispozitivele de securitate sunt conștiente de faptul că datagramele cu anumite adrese sursă/destinație vor folosi portul deschis în mod automat de datagrama de perforare breșă transmisă din interiorul nodului interior, și permit datagramelor transmise de la nodul public să traverseze firewall/PAT, fără a fi nevoie să se deschidă manual alte porturi. Aceasta înseamnă că dispozitivul firewall intercepteaza mesajele datagramei, și automat, (de exemplu, spre deosebire de modul manual) deschide un port care poate fi reutilizat de către o pereche publică (de exemplu, expeditor) pentru a transmite datagrame înapoi, în interiorul perechilor (de exemplu, private), de unde s-a primit prima datagramă și de unde datagrama inițială a provenit.

În unele expeditor de realizare, punctele de capăt, expeditor și receptor, comunică datagrame de testare pentru măsurarea și analiza diferitelor caracteristici de rețea, a parametrilor de comunicație și/sau a statisticilor, în scopuri de testare. În unele variante de realizare, cel puțin unul dintre punctele de capăt de testare este situat într-o rețea publică, și cel puțin un alt dintre punctele de capăt de testare este situat într-o rețea privată. Datagramele de testare sunt configurate pentru a traversa unul sau mai multe dispozitive legate de securitate (de exemplu, un dispozitiv firewall cu traducerea adresei de port (PAT)), între punctele de capăt (de exemplu, generatoare de trafic de testare). În special, datagramele de testare pot fi schimbate între punctele de capăt, fără a fi nevoie de deschiderea manuală a oricărui port din dispozitivul firewall securizat și/sau fără utilizarea PAT, pentru a crea manual o intrare și/sau pentru fiecare adresă publică mapată prin protocolul datagramei utilizatorului (UDP) (de exemplu, adresa IP și adresa de port) la fiecare adresă UDP privată, pentru fiecare utilizator simulat. În unele exemple, dispozitivul firewall/PAT va deschide automat un port și va închide automat portul, după o perioadă de timp.

În special, în conformitate cu unele aspecte ale prezentei invenții, prin comunicarea datagramelor (de exemplu, cu combinații specifice ale adreselor sursă/destinație și/sau combinații ale acestora) între punctele de capăt publice și private, traficul de testare poate fi transmis fără a deschide porturile din dispozitivul firewall și/sau fără maparea informațiilor de

a-2014--00994-
16 -12- 2014

adresă, pentru fiecare utilizator simulat. În unele variante, punctele de capăt pot face schimb de datagrame pentru testarea performanței unei rețele private și/sau ale componentelor acesteia (de exemplu, noduri, servere, conexiunea la Internet, etc.), în timp ce sunt minimizate sau eliminate modificările la dispozitivele legate de securitate, la marginea rețelei private.

La pregătirea pentru testarea nodurilor de rețea, de obicei, operatorii de testare trebuie să furnizeze informații de configurarea testării la unul sau mai multe noduri. Informațiile de configurarea testării pot fi comunicate la unul sau mai multe puncte de capăt, așa cum este descris în cererea de brevet din SUA, seria nr 14/557418, înregistrată la 01 decembrie 2014, care revendică prioritatea cererii de brevet din România, nr. a/00918/2014, care a fost depusă în 27 noiembrie 2014, ale căror descrieri sunt incorporate, în întregime, în prezenta descriere, prin referință. Configurarea testării poate include informații despre o sesiune de testare, informații de identificare nod, informații de adresă asociate cu un sistem de configurare, informații de port asociate cu sistemul de configurare, informații despre una sau mai multe perechi de intrare pentru unul sau mai multe noduri asociate cu sesiunea de testare și/sau informații despre una sau mai multe perechi de ieșire pentru unul sau mai multe noduri asociate cu sesiunea de testare.

Așa cum sunt utilizați în prezenta, termenii "trafic UDP" se referă la datagramele UDP care includ o adresă sursă prin Protocolul Internet (IP), un identificator de port sursă, o adresă IP destinație și un identificator de destinație. Traficul UDP poate include trafic de testare de configurare, trafic de executare testare, trafic de perforare breșă, etc. Traficul UDP este folosit pentru a transmite adrese UDP între punctele de capăt în format "IP: Port", mesaje IP, mesaje IP versiunea 4 (V4), mesaje IP versiunea 6 (V6), mesaje prin protocolul datagramelor de utilizator (UDP), mesaje prin protocolul de control al transmisiei (TCP), mesaje prin protocolul de control al transmisiei fluxului de date (SCTP), mesaje prin protocolul de transport în timp real (RTP), mesaje prin protocolul de date fiabile (RDP), mesaje prin protocolul de urmărire (GTP) serviciu de pachete comutate pentru comunicații mobile (GPRS), mesaje folosind un alt protocol de tunelare, și/sau orice variante ale acestora. Datagramele UDP permit pachetelor de testare (traficului de testare) să traverseze un firewall/PAT, fără a deschide manual porturile din firewall/PAT și fără a fi nevoie să mapeze manual adrese publice prin UDP la adrese private prin UDP, pentru fiecare utilizator simulat.

Așa cum se utilizează în prezenta, sintagma "perforarea unei breșe", sau o versiune similară acesteia, se referă la transmiterea unui datagrame care are adrese sursă și destinație unice sau specifice, astfel încât un dispozitiv de securitate poate fi evitat pentru efectuarea testelor de performanță și pentru circulația traficului în dispozitivul de securitate (de exemplu, un

firewall/PAT), fără modificări de configurație a dispozitivului de securitate, fără deschiderea manuală a oricărui port asociat cu dispozitivul de securitate și/sau fără nici o referire la o mapare specifică la destinație (de exemplu, porturile publice la private), în configurarea testării. Dispozitivul de securitate poate să recunoască faptul că anumite combinații sursă/destinație sunt indicative de configurarea sau de executarea unei testări, iar dispozitivul de securitate va ruta datagramele la destinatar, fără a fi nevoie să deschidă manual un port. Acest lucru face ca întregul proces de testare să fie complet transparent pentru un utilizator de aplicație.

Așa cum sunt utilizați în prezenta descriere, termenii "expeditor", "punct de capăt public" și "E1" sunt sinonimi și se referă la un nod reședința într-o rețea publică. Așa cum sunt utilizați în prezenta descriere, termenii "receptor", "punct de capăt privat" și "E2" sunt sinonimi și se referă la un nod reședința într-o rețea privată care urmează să fie testată. E1 și E2 pot fi menționați ca "pereche" într-un mediu de testare.

Se dau în continuare exemple de realizare a invenției în legătură cu Figurile anexate. Ori de câte ori este posibil, vor fi utilizate aceleași numere de referință în Figuri, pentru referirea la aceleași elemente sau părți similare.

Figura 1 este o diagramă care ilustrează un sistem **100** pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia. În unele aspecte, sistemul **100** include cel puțin un prim nod sau punct de capăt **E1** și un al doilea nod sau punct de capăt **E2,** furnizate în rețelele publice și, respectiv, private pentru generarea, transmiterea și/sau recepționarea de trafic de testare, în conformitate cu un exemplu de realizare a obiectelor descriese în prezenta descriere.

Conform Figura 1, primul punct de capăt **E1** poate exista într-o rețea publică și poate includ o primă platformă **102** de calcul și al doilea punct de capăt **E2** poate exista într-o rețea privată și poate include o a doua (diferită) platformă **104** de calcul. Prima, și respectiv, a doua platformă **102** și **104** de calcul, sunt fiecare configurate pentru a genera, transmite, și/sau să primească trafic de testare (de exemplu, datagramele de testare), după o fază de configurare inițială, pentru testarea (de exemplu, monitorizarea și/sau de măsurarea) caracteristicilor, parametrilor, statisticilor, etc. asociate cu rețeaua privată și/sau cu componentele acesteia.

În unele exemple și în timpul unei faze inițiale de configurare, între **E1** și **E2**, sunt schimbate datagrame de deschidere "INIT" și de confirmare "ACK", pentru a indica faptul că este executat un test de performanță. Datagramele INIT și ACK includ combinații specifice de adrese sursă și destinație, care indică, la un dispozitiv de securitate, adresa receptorului destinat, situat în spatele dispozitivului de securitate. Mai degrabă decât maparea separată a

fiecarei adrese la expeditor și receptor, dispozitivul de securitate este un dispozitiv de traducerea adresei de port – PAT folosit pentru a înlocui adresa IP/port privată **E2** cu adresa a IP/port publică respectivă, alocată automat. Acest lucru permite traficului de testare să traverseze dispozitivul de securitate, fără a fi nevoie să se deschidă manual porturile. Se simplifică, de asemenea, execuția testării, în cazul în care sunt simulați mai mulți utilizatori. În unele exemple, testele de performanță sunt rulate fără a fi nevoie de a modifica sau configura dispozitivul de securitate (de exemplu, un firewall/PAT) între rețelele publice și private și/sau fără a fi nevoie de a oferi maparea în porturile specifice, în configurarea testării.

În unele exemple de realizare, testele de performanță pot fi inițiate de execuția unuia sau a mai multor fir (e) de program, de către controller, la expeditorul destinat traficului de testare pentru a executa configurarea pentru fiecare utilizator simulat. Firele de program reprezenta unul sau mai multe servicii, aplicații, sau procese (de exemplu, software-ul care este executat pe un procesor) pentru stabilirea conexiunilor și/sau furnizarea de informații de configurarea testării pentru fiecare punct de capăt și/sau pentru fiecare utilizator simulat. În unele exemple, un fir de configurare poate fi asociat cu un anumit punct de capăt (de exemplu, **E1, E2,** etc.) sau o anumită sesiune de testare între punctele de capăt. De exemplu, un prim fir de configurare poate prelucra solicitările de conectare asociate cu primul punct de capăt **E1**, și un al doilea fir de configurare poate prelucra solicitările de conectare asociate cu un punct de capăt **E2**. În unele exemple și la recepționarea unui fir de configurare, al doilea punct de capăt **E2** poate fi configurat pentru a iniția și pentru a comunica pachete sau date de testare la primul un punct de capăt **E1,** la recepționarea datagramei INIT de la **E2**.

În unele exemple de realizare, prima și a doua platformă **102 și 104** de calcul reprezintă dispozitive de rețea, de exemplu, module de rețea, noduri, sau un sistem de dispozitive, noduri, și/sau module. În unele exemple, prima și a doua platformă **102 și 104** de calcul includ un singur nod. În alte aspecte, prima și a doua platformă **102 și 104** de calcul includ funcționalități de testare distribuite pe platforme de calcul și/sau noduri multiple. În unele aspecte, prima platformă **102** de calcul include o platformă de testare într-o rețea publică. În unele aspecte, a doua platformă **104** de calcul include un punct de capăt situat într-o rețea privată (de exemplu, rețeaua de întreprindere) în spatele unuia sau mai multor dispozitive de securitate, cum ar fi un dispozitiv firewall/PAT (de exemplu, Fig. 2), care este configurat pentru a oferi securitate pentru rețeaua privată. În special, primul și al doilea punct **E1 și E2** de capăt și platformele de calcul respective sunt configurate pentru a transmite trafic de testare prin dispozitivul de securitate, fără a fi nevoie să se configureze manual dispozitivul

și/sau să se deschidă manual porturile în dispozitivul de securitate, prin schimbarea de datagrame care au adrese sursă/destinație specifice.

În unele exemple de realizare, platformele **102 și 104** de calcul includ generatoare de trafic de testare configurate pentru a genera, transmite și/sau primi datagrame de testare, conform unei configurări de testare. În special, configurarea testării este lipsită de porturi (de exemplu, publice și private) de destinație specifice, eliminând astfel nevoia de mapare excesivă sau de translația portului prin intermediul unui dispozitiv de securitate (de exemplu, firewall/PAT) care intervine. În timpul configurării, fiecare punct de capăt **E1 și E2** va aloca și se va lega de un anumit port, și va transmite fiecare datagrame INIT, ACK și de testare, folosind aceste porturi. Dispozitivul de securitate va ști să înlocuiască informațiile IP/ port respective cu informațiile punctului de capăt IP/port privat, și invers, la recepționarea datagramelor INIT, ACK și de testare.

În unele aspecte, platformele **102** și/sau **104** de calcul sunt configurate să imite mai mulți utilizatori pentru testarea caracteristicilor de performanță ale rețelei private. A doua platformă **104** de calcul poate "perfora o breșă" în dispozitivul de securitate (de exemplu, firewall/PAT, Fig. 2) care deservește rețeaua privată și fiecare punct de capăt poate folosi apoi "breșa" pentru a transmite trafic de testare. În unele exemple, prima platformă **102** de calcul este configurată pentru a genera, transmite și/sau să primească trafic de testare pentru imitarea unui server web, unui dispozitiv de utilizator, mai multor servere web, și/sau dispozitivelor multiple. A doua platformă **104** de calcul este configurată pentru a măsura statistici de rețea, caracteristici de performanță și/sau pentru a genera și raporta date de performanță asociate cu pachetele de testare primite în rețeaua privată.

În unele exemple, prima și respectiv ,a doua platformă **102** și **104** de calcul, includ fiecare un modul de testare (TM). De exemplu, prima platformă **102** de calcul include un prim TM **106** și a doua platformă **104** de calcul include un al doilea TM **108**. Primul și al doilea TM **106** și respectiv,**108**, (și/sau porțiuni ale acestora) sunt configurate pentru a genera, transmite, și/sau a primi trafic de testare (de exemplu, pachete de date sau datagrame) în funcție de informațiile de configurare testare. În aceast exemplu, după ce a primit informațiile de configurare testare, al doilea punct de capăt **E2** poate "perfora o breșă" în dispozitivul firewall/PAT (Fig. 2) prin intermediul unui modul de perforare (HPM) **110**. În mod similar, după ce a primit informațiile de configurare testare, prima platformă **102** de calcul poate genera, transmite, și/sau primi trafic de testare (de exemplu, să execute un test de performanță) prin comunicarea datelor de testare folosind o datagramă care transmite și recepționează modulul (DS/RM) **112**.

De notat că, informațiile de configurare testare primite de la fiecare punct de capăt sunt lipsite de adrese specifice de destinație/de port, ceea ce elimină necesitatea de mapare manuală. Mai degrabă, HPM **110** generează datagrame cu combinații specifice ale unei surse și unei destinații care sunt asociate cu trafic de testare, astfel încât traficul va curge de-a lungul unei căi de comunicații de date sau prin breșa **114,** care sunt create în conformitate cu o datagrama INIT (de exemplu, o datagrama UDP) generată la și comunicată de la punctul de capăt privat (de exemplu, **E2**). În unele exemple, conform prezentei invenții, breșa **114** include o cale de comunicație date între perechi (de exemplu, **E1, E2**), în care este folosită o singură adresă pentru fiecare utilizator simulat. Prin utilizarea adresei unice ca și a adresei sursă sau de destinație, precum și a unei combinații de adrese sursă specifice (UDP-uri), diferite porturi pot fi alocate în spațiul privat, pentru simularea diferiților utilizatori și pentru efectuarea mai multor teste concurente ale rețelei private.

În unele exemple, HPM **110** generează trafic UDP de ieșire pentru a iniția fluxul de date RTP al traficului de testare, de la primul punct de capăt (public) **E1** la al doilea punct de capăt (privat) **E2**, fără a deschide un port în firewall, în intervenția firewall și/sau în efectuarea semnificativă (în mod special, configurată) a traducerii adresei de port. HPM **110** este configurat pentru a genera o datagramă pentru perforatea unei breșe în firewall/PAT prin care pot fi simulați sute de utilizatori, prin fluxul de date RTP, fără a avea pusă la dispoziție nici o configurare explicită prin care să intervină dispozitivul firewall/PAT (Fig. 2).

În unele exemple de realizare, HPM **110** și DS/RM **112** includ orice entitate sau entități adecvate (de exemplu, o platformă de calcul, software-ul executat de un procesor, un dispozitiv logic, un dispozitiv logic programabil complex (CPLD), un circuit integrat digital configurabil de către utilizator (FPGA) și/sau un circuit integrat cu aplicație specifică (ASIC) pentru efectuarea unuia sau mai multor aspecte legate de generarea, expedierea, recepționarea, comunicarea și/sau schimbul de trafic de testare sau de datagrame de testare. HPM **110** și DS/RM **112** pot fi fiecare combinații de adresă IP și de port, ca surse/destinații pentru datele sau informațiile de testare. De exemplu, comunicațiile către/de la (de exemplu, între) primul și al doilea punct de capăt **E1** și **E2** din sistemul **100,** pot avea loc prin diferite adrese IP/port, în funcție de testare sau de nodul de rețea asociat. În unele aspecte, pot fi imitați mai mulți utilizatori folosind diverse combinații de adresă IP/port între punctele de capăt, în rețelele publice și private. De exemplu, **E2** poate transmite trafic de testare pentru simularea mai multor utilizatori și poate transmite trafic prin rețea pentru mai mulți utilizatori.

Tot cu referire la Figura 1 și în conformitate cu unele exemple de realizare, HPM **110** al celui al celui de-al doilea punct de capăt **E2** este configurat să inițieze unul sau mai multe teste de

performanță, prin generarea și transmiterea unei datagrame "INIT" la primul punct de capăt **E1**. Datagrama poate include informații despre adresa IP privată și informații despre adresa de port privată asociată cu portul de legătură. Dispozitivul de securitate va primi datagrama INIT și va înlocui informațiile despre adresa IP/port privată din datagrama INIT cu adresa/IP port a părții publice a dispozitivului de securitate, astfel că este creată o breșă prin dispozitivul de securitate. Acest lucru permite **E1** să direcționeze traficul la o adresă/port publică (de exemplu, asociată cu partea publică a firewall), pe care dispozitivul de securitate o inlocuieste apoi cu adresa IP/port privată a portului de legatură, prin simpla comutare a adresei de destinație la adresa sursă, în scop de testare. Comunicațiile dintre **E1** și **E2** includ combinații specifice sursă/destinație care elimină necesitatea de a deschide un port într-un dispozitiv firewall/PAT, în același timp cu evitarea pentru PAT a necesității mapării informațiilor pentru fiecare utilizator simulat. În unele exemple, DS/RM **112** este configurat pentru a primi datagrama INIT care semnalizează startul unuia sau mai multor teste de la HPM **110** și apoi folosește informațiile de adresă UDP asociate cu semnalizarea datagramei, pentru a recunoaște și pentru a iniția un test de performanță, prin generarea și transmiterea traficului de testare.

HPM **110** și DS/RM **112** poate fiecare cuprinde una sau mai multe interfețe de comunicație pentru transmiterea și recepționarea traficului de testare divers, inclusiv mesaje IP, mesaje v4, mesaje V6, mesaje TCP, mesaje SCTP, mesaje RTP, mesaje RDP, mesaje GTP, sau versiuni ale acestora . HPM **110** și DS/RM **112** pot reprezenta orice entitate corespunzătoare (de exemplu, un suport non-tranzitoriu care poate fi citit de calculator sau un dispozitiv de memorie) pentru generarea, transmiterea și/sau recepționarea de fluxuri de mesaje, de mesaje, de trafic de testare, de rezultate ale testelor, de statistici, și/sau de orice informații referitoare la testare.

În unele exemple de realizare, sistemul **100** este operabil pentru a configura o testare, perfora o breșă în firewall/PAT printr-o datagrama UDP și pentru a iniția flux de date între mai multe puncte de capăt publice/private pentru executarea unui test de performanță și pentru simularea mai multor utilizatori ai unei rețele private. Platformele **102 și 104** de calcul pot comunica trafic de testare (de exemplu, în mod direct și/sau indirect) de-a lungul unei căi de comunicație sau a breșei **114.** Breșa **114** este prezentată ca o cale fizică, numai în scopuri ilustrative și numai în scopul de a indica faptul că între punctele de capăt există o cale de comunicație UDP. În unele aspecte, breșa **114** include o cale de comunicație care este, în mod direct, între primul **E1** și al doilea **E2** punct de capăt (de exemplu, indicativul platformelor **102 și 104** de calcul care se comunică direct), precum și care este lipsită de intervenția

a-2014--00994-
16 -12- 2014

nodurilor de semnalizare. În alte aspecte, pot fi dispuse o multitudine de noduri de semnalizare, de-a lungul căii de comunicație între puncte **E1 și E2** de capăt, pentru facilitarea indirectă a fluxului de date între punctele **E1 și E2** de capăt și/sau componentele (de exemplu, modulele) acestora.

Așa cum se mai arată în Figura 1 și în conformitate cu unele exemple de realizare, un utilizator (sau un sistem automat controlat de un utilizator) poate selecta și transmite o configurare de testare la primul **E1** punct de capăt folosind un controler **116**. Controlerul **116** poate, de asemenea, controla (de exemplu, începe, lua o pauză, și/sau opri) aspecte legate de testul de performanță, folosind una sau mai multe comenzi de controlul testării (de exemplu, fire de program), comunicate de acesta.

Se va aprecia că Figura 1 este în scopuri ilustrative și că mai multe noduri, locații ale acestora, și/sau funcționalități ale acestora descrise mai sus în legătură cu Figura 1 pot fi schimbate, modificate, adăugate sau eliminate. De exemplu, unele noduri și/sau funcționalități pot fi combinate într-o singură entitate, fără a se îndepărta de la scopul prezentei invenții.

Figura 2 este o diagramă care ilustrează un mediu **200** de rețea pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în conformitate cu un exemplu de realizare a prezentei invenții. Conform Figurii 2, mediul **200** poate include o rețea 'nor' (cloud) **202** având un punct de capăt public conectat la un punct de capăt privat, în cadrul unei rețele **204** (private) de întreprindere, prin rețeaua internet sau prin altă rețea publică. Un dispozitiv **206** firewall/PAT este dispus între componentele punctului de capăt din respectiva rețea cloud **202** și rețeaua **204** de întreprindere.

Cel puțin un punct sau nod de capăt **208** public (de exemplu, platforma **102** de calcul) poate fi dispus în rețeaua cloud **202** pentru testarea mai multor puncte de capăt sau noduri **210A, 210B, 210C, etc.,** private în rețeaua **204** de întreprindere. Punctul de capăt **208** public reprezintă un nod (cum ar fi, platforma de calcul **102**) care are un TM (cum ar fi, **106**, Fig. 1) și un DS/RM (cum ar fi, **112,** Fig. 1) configurate pentru a genera și/sau transmite trafic de testare la unul sau mai multe puncte de capăt în rețeaua privată, conform unei configurații de testare pentru imitarea unei multitudini de utilizatori. Asta înseamnă că, un punct de capăt **208** public poate imita o multitudine de utilizatori pentru testarea unei multitudini de puncte de capăt **210A la 210C** private. Punctul de capăt **208** public poate primi, de asemenea, înapoi de la punctele de capăt **210A la 210C** în rețeaua privată, traficul de testare, în cazul în care configurat să facă acest lucru. Punctele de capăt **208 și 210A la 210C** pot include orice hardware în combinație cu software-ul, de exemplu, platforme de calcul, procesor (oare), memorie, module de testare stocate și executat astfel pe acestea, și/sau servere.

a-2014--00994-
16 -12- 2014

În unele exemple de realizare, punctele de capăt **210A** la **210C** private constituie noduri (de exemplu, platforma de calcul **104**) inclusiv HPM-uri (de exemplu, **110**, Fig. 1) şi/sau funcţionalităţi similare pentru generarea şi transmiterea datagramelor INIT configurate pentru a specifica o "breşă" sau cale de comunicaţie în jurul firewall/PAT **206,** fără a fi nevoie să se deschidă nici un port şi/sau să se configureze în mod specific firewall/PAT **206** cu informaţii de mapare specifice.

Reţeaua cloud **202** poate include o reţea de testare configurată pentru a imita mai mulţi utilizatori publici, prin intermediul a cel puţin un nod **208**. Nodul **208** este configurat pentru a iniţia un test de performanţă, pentru a opri un test, şi/sau în alt mod, pentru a interacţiona cu unul sau mai mulţi operatori de testare (de exemplu, prin intermediul controlerului **116**, Fig. 1), în faţa firewall/PAT **206**. Reţeaua **204** de întreprindere include mai multe noduri sau puncte de capăt **210A** la **210C,** dispuse în spatele firewall/PAT **206**, pentru colectarea, analizarea şi raportarea datelor sau informaţiilor de performanţă referitoare la parametrii şi/sau la caracteristicile de comunicaţie asociate cu reţeaua **204** de întreprindere.

Firewall/PAT **206** poate include orice dispozitiv legat de securitate, cum ar fi un dispozitiv firewall care este activat pentru a efectua PAT. Firewall/PAT **206** poate bloca, modifica şi/sau elimina anumite comunicaţii, în acelaşi timp permiţând acelora care au o anumită adresă UDP sursă/destinaţie să treacă. De exemplu, firewall/PAT **206** poate elimina sau bloca cererile de conexiune primite de la toate nodurile situate într-o reţea exterioară. Aşa cum este descris aici, traficul de testare sigur, care este direcţionat la o adresă publică asociată cu partea publică a firewall/PAT **206** şi de la o adresă sursă specifică (de exemplu, de nod **208**) poate fi dirijat să treacă de firewall/PAT **206**, la primire. Firewall/PAT **206** va înlocui informaţiile IP/port respective cu cele ale punctului de capăt privat (de exemplu, **210A** la **210C**). În unele exemple de realizare, traficul direcţionat către o singură adresă UDP, care corespunde la partea publică a firewall/PAT **206**, poate fi mapat la multiple puncte de capăt **210A** la **210C** private, fără a mapa fiecare punct de capăt public la multiple puncte de capăt private diferite.

În unele exemple de realizare, poate fi iniţiată o breşă sau o cale peste firewall/PAT **206,** prin generarea datagramelor INIT de la nodurile situate în exteriorul reţelei de întreprindere **204** private (de exemplu, **210A la 210C**), deoarece dispozitivele legate de securitate (de exemplu, unul sau mai multe firewall/PAT **206**) pot permite traficului spre exterior să circule liber, în timpul prevenirii unui anumit trafic de intrare. În astfel de exemple, punctele de capăt **210A** la **210C,** în reţea de întreprindere **204** privată, pot primi doar traficul de testare de la punctul de capăt **208** public, prin generarea de conexiuni de ieşire iniţiate de punctele de capăt **210A la 210C** private. Punctele de capăt **210A la 210C** private pot fi configurate pentru a testa,

a-2014--00994-
16 -12- 2014

analiza, măsura, și/sau raporta statisticile de conectivitate sau de comunicație asociate cu dispozitivul de securitate (de exemplu, firewall/PAT **206**), conexiunea la Internet, comunicațiile de la serverele publice sau private, viteza de conectare, fiabilitatea rețelei **204** de intreprindere, etc.

Se va aprecia că Figura 2 este în scopuri ilustrative și că mai multe noduri, locații ale acestora și/sau funcții ale acestora, descrise mai sus în legătură cu Figura 2, pot fi schimbate, modificate, adăugate sau eliminate. De exemplu, unele noduri și/sau funcții pot fi combinate într-o singură entitate sau separat, în multiple entități.

Figurile 3A și 3B sunt diagrame, cu titlu de exemplu, de flux de mesaje care ilustrează comunicațiile între punctele de capăt publice și private (de exemplu, perechi) pentru inițierea și executarea testelor de performanță ale rețelei private și/sau ale componentelor acestria. Conform unor aspecte, Figurile 3A și 3B ilustrează aspecte ale unui punct de capăt privat care perforează o breșă în rețeaua privată și/sau în dispozitivele de securitate asociate cu aceasta (de exemplu, firewall/PAT), pentru a permite flux de intrare pentru traficul de testare.

Conform Figurii 3A, la pasul **1**, este inițiată și trimisă o conexiune de strat de transport (de exemplu, conexiune TCP) de la un punct de capăt **E2** privat (de exemplu, **210A la 210C** localizat într-o rețea privată) la un punct de capăt **E1** public (de exemplu, **208**, localizat într-o rețea publică). Punctul de capăt (**E2**) privat este reprezentat de o adresă IP/port UDP privată: 10.205.12.120:25501 (de exemplu, indicativul de adresa IP privată: 10.205.12.120 și identificatorul de port privat: 25501). Punctul de capăt (**E1**) public este reprezentat de o adresă publică UDP: 91.195.7.1:65535 (de exemplu, indica o adresă IP publică a 91.195.7.1 și un identificator de port public: 65535). Fiecare pachet UDP poate fi compus din combinații numerice, care includ orice adresă IP corespunzătoare (de exemplu, orice etichetă numerică asociată dispozitivului, cum ar fi nodul sau punctul de capăt și platforma de calcul respectivă) și orice identificator de port corespunzător (de exemplu, o etichetă sau un identificator numeric cu cinci digiți), eventual separate prin două puncte (de exemplu, o ":"). Comunicațiile UDP specifice care au anumite adrese sursă/destinație pot traversa un dispozitiv de securitate și pot intra în rețeaua privată. În special, prima comunicație TCP, de la pasul **1**, are permisiunea să traverseze firewall/PAT (de exemplu, **206**, Fig. 2), deoarece este generată în rețeaua privată. Prima comunicație TCP, la pasul **1**, nu este blocată sau împiedicată de un dispozitiv de securitate asociat cu rețeaua privată.

La pași **2A** și **2B**, fiecare punct de capăt alocă un port disponibil și se leaga de el. Tot traficul de testare va fi trimis de la porturile respective la care fiecare punct de capăt (de exemplu, **E1**

și E2) se leagă. În afară de aceasta, datagramele INIT și ACK vor fi transmise de la poarta respectivă, în care fiecare punct de capăt este legat.

La pasul **3**, punctul de capăt **E1** public transmite o datagrama UDP la punctul de capăt **E2** privat. Datagrama UDP conține o adresă IP și un număr de port, pe care punctul de capăt **E1** public le va folosi pentru testare. Adresa IP și numărul de port sunt comunicate printr-o datagrama UDP, în care un câmp de adrese IP sursă comunică adresei IP că punctul de capăt **E1** public obligă unui câmp de adrese IP sursă să comunice numărul de port al punctului de capăt **E1** public.

La pasul **4**, punctul de capăt **E1** public primește un semnal de testare de pornire. Acest lucru poate fi comunicat de la un operator de testare printr-un controler (de exemplu, **116**, Fig. 1). Pașii **1-4** completează o fază de configurare inițială (de exemplu, inițierea testării) asociată cu o sesiune de teste corespunzătoare. În timpul fazei de configurare, punctul de capăt **E1** public alocă un port UDP disponibil și se leagă la el, pentru a bloca alte aplicații de la utilizarea acestuia în timpul testării. Punctul de capăt **E1** public descoperă mai târziu propria datagramă UDP (de ex, de la controlerul **116**, Fig. 1) și așteaptă un semnal (de exemplu, datagramă INIT) pentru a iniția testarea.

La pasul **5**, punctul de capăt **E1** public așteaptă să primească o datagrama INIT de la punctul de capăt **E2** privat, în care **E2** notifică **E1** faptul că o breșă a fost perforată în rețeaua privată.

La pasul **6**, punctul de capăt **E2** privat transmite o datagramă UDP la punctul de capăt **E1** public. Acestă datagramă este datagrama INIT și include o anumită adresă sursă/destinație, care este permisă să traverseze firewall/PAT, deoarece provine din rețeaua privată. La întâlnirea cu firewall/PAT, acesta știe să înlocuiască informațiile despre adresa IP/port privată cu o adresă IP publică și numărul de port. Firewall-ul/PAT stochează, de asemenea, o mapare între adresa IP privată și numărul de port al punctului de capăt **E2** privat și adresa IP publică și numărul de port care se atribuie în tabelul de mapare. Crearea acestei mapări în tabelul de mapare a firewall-ului/PAT deschide o breșă in firewall/PAT pentru pachetele de date adresate la adresa IP publică și la numărul de port, în datagrama INIT.

La pasul **7**, punctul de capăt **E2** privat primește informații IP/port publice de la datagrama INIT recepționată.

La pasul **8**, punctul de capăt **E2** privat așteaptă să primească datagrama ACK de la punctul de capăt **E1** public, ceea ce indică faptul că sesiunea de testare a fost inițiată și recunoscută.

La pasul **9**, punctul de capăt **E** public transmite o datagrama ACK la punctul de capăt **E2** privat. Pași **5-9** sunt indicativul unei faze de perforarea unei breșe, pentru un test de performanță dat. În cazul în care datagramele nu sunt sincronizate în același timp, punctul de

capăt **E1** public este configurat pentru a amortiza datagramele primite de la punctul de capăt **E2** privat și pentru a recupera datagramele INIT, acolo unde este necesar. Astfel, sincronizarea între punctele de capăt **E1 și E2** nu interzice inițierea și/sau executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, în cazul în care mai mulți utilizatori sunt simulați sau imitați.

La pasul **10**, punctul de capăt **E2** privat așteaptă să primească trafic de testare. La pași **11 și 12,** traficul de testare este trimis din punctul de capăt **E1** public la punctul de capăt **E2** privat, și oprit în conformitate cu o configurare de testare. Pașii **10 la 12** sunt indicativul unei faze de execuție a unui test de performanță.

Figura 3B este o diagramă de flux de mesaje care ilustrează faza de perforare a unei breșe și o fază de testare, în detaliu. Conform Figurii 3B, la pasul 1, punctul de capăt **E2** privat generează și transmite o datagrama INIT de la adresa acesteia UDP privată la adresa UDP publică a punctului de capăt **E1** public. Datagrama INIT este configurată să perforeze o breșă în rețeaua privată, de la recepționarea la firewall/PAT **206**. Firewall/PAT **206** intercepteaza datagrama INIT și poate înlocui informațiile UDP sursă, private cu propriile sale informații UDP publice corespunzătoare la IP/port-ul de pe partea publică a firewall/PAT **206**. Firewall/PAT **206** creează, de asemenea, maparea între adresa IP privată și numărul de port și adresa IP publică desemnată și numărul de port și stochează maparea în tabelul de mapare.

La pasul **2**, datagrama INIT este trimisă la punct de capăt **E1** public. Așa cum se vede în mesajul **2**, adresa sursă a punctului de capăt **E2** privat este înlocuită cu aceea de pe partea publică a firewall/PAT **206**.

La pasul **3**, punctul de capăt **E1** public începe transmiterea de datagrame de testare (de exemplu, trafic de testare). Punctul de capăt **E1** public poate iniția pornirea și/sau oprirea traficului pe un semnal de la un controler (de exemplu, **116**, Fig. 1) sau de la utilizator. La pasul **3**, traficul de testare este destinat pentru adresa IP/port asociată cu firewall/PAT **206**. La recepționarea traficului de testare la firewall/PAT **206**, adresa UDP sursă a firewall/PAT **206** se înlocuiește cu adresa IP/port a punctului de capăt **E2** privat.

La pasul **4**, datagramele de testare sunt primite la punctul de capăt **E2** privat ca rezultat al faptului că firewall/PAT **206** este instruit să înlocuiască adresa sa publică UDP cu adresa UDP a punctului de capăt **E2** privat. Firewall/PAT **206** nu mai are nevoie să efectueze funcționalitățile PAT pentru fiecare punct de capăt, dar numai pentru datagramele care au adresa de destinație și portul corespunzător la adresa publică și la port, atribuite de firewall la pasul 1 din Figura 3B și adresa IP sursă și portul de transmiterea punctului de capăt privat communicate la punctul de capăt privat, prin intermediul conexiunii TCP.

Se va aprecia că menționatele comunicații prezentate în Figurile 3A și 3B sunt în scop ilustrativ și că pot fi utilizate acțiuni diferite și/sau suplimentare. Se va aprecia de asemenea că diferite acțiuni descrise aici pot să apară în mod simultan și/sau într-o ordine sau secvență diferită.

Figurile 4A și 4B sunt diagrame care ilustrează metode efectuate la fiecare punct de capăt sau nod (de exemplu, **E1 și E2**) într-un mediu de testare (de exemplu, Fig. 2).

Conform Figurii 4A, o metodă **300** este realizată la un punct de capăt expeditor sau public (de exemplu, **E1**) în timpul configurării și executării unui test de performanță.

În timpul unei faze de configurare și la blocul **302**, expeditorul solicită un port UDP disponibil pentru testare (de exemplu, de la un sistem de operare și/sau controler), și se leagă la el pentru a bloca alte aplicații să folosească portul alocat. Expeditorul va folosi acest port pentru a transmite și a primi o datagramă ACK și tot traficul de testare, pentru imitarea mai multor utilizatori.

În blocul **304**, expeditorul va transmite informațiile sale de adresă IP (de exemplu, care pot fi descoperite de la un controler) și informațiile legate de adresa portului la perechea receptor de pe conexiunea TCP, care au fost trimise de la receptor într-o rețea privată, și pe care expeditorul le-a acceptat. După transmiterea adresei UDP la receptor, expeditorul poate aștepta un semnal de la un controller, pentru a începe un test de performanță. După ce semnalul este primit, expeditorul va aștepta o datagrama INIT de la **E2** pe portul de legătură, ca semnal că "perforarea unei breșe", a fost creată de **E1.**

În blocul **306**, expeditorul primește o indicație că receptorul în rețeaua privată este pregătit să primească trafic de testare printr-o breșă pe care receptorul a perforat-o în rețeaua privată. Indicația poate include o datagramă INIT cu o combinație sursa/destinație specifică. În unele exemple de realizare, expeditorul primește datagrama INIT de la receptor în rețeaua privată. Datagrama INIT poate include o adresă UDP, la care expeditorul poate transmite sau dirija trafic de testare. Datagrama INIT poate instrui expeditorul să înceapă un test de performanță, așa că rețeaua privată este deschisă și o breșă este perforată până la nodul de primire în rețeaua privată.

În blocul **308**, se face un test de performanță, prin transmiterea traficului de testare de la expeditor la receptor. După ce datagrama INIT este primită, expeditorul poate folosi adresa UDP sursă (adresa IP/Port) din datagrama primită, ca o adresă UDP destinație pe datagramele de testare și o transmite la perechea receptor. În unele aspecte, adresa UDP pentru datagramele de testare este adresa UDP corespunzătoare părții publice a unui firewall. Firewall-ul poate efectua PAT pentru a transmite datagramele de testare la nodul receptor

privat. Astfel, o singură adresă UDP poate fi utilizată pentru a executa traficul de flux de date regulat, care constă în transmiterea datagramelor UDP/RTP la receptor, conform unei configurații de testare.

Conform Figurii 4B, o metodă **400,** se efectuează la un receptor sau punct de capăt privat (de exemplu, **E2**) în timpul instalării și executării unui test de performanță.

În blocul **402** (faza de configurare), receptorul va ridica următorul port disponibil și se va lega de el. Acesta va fi portul de pe care receptorul va primi o datagrama ACK, care recunoaște începutul testului de performanță, precum și toate datagramele de testare ulterioare transmise de la expeditor.

În blocul **404**, receptorul va primi informațiile despre adresa IP/Port folosită de către expeditor. În unele aspecte, receptorul transmite aceaste informații în timpul unei faze de configurare, înainte ca o breșă să fie perforată.

În blocul **406** (de exemplu, faza de execuție), receptorul va perfora o breșă în rețeaua privată care generează și transmite o datagramă INIT expeditorului. Datadrama INIT are o adresă UDP destinație care corespunde informațiillor despre adresa IP/Port primită de la adresa expeditorului, în timpul fazei de configurare. Datadrama INIT va avea o adresă sursă care corespunde propriilor receptoare localizate prin IP și, în acest fel, portul său este legat în mod local. Aceste informații pot fi transmise într-o datagramă INIT, de la receptor la expeditor.

Dupa transmiterea datagramei INIT, receptorul poate aștepta apoi pentru o datagrama ACK de la expeditor, astfel încât receptorul știe că perechea expeditor a primit datagrama INIT. Expeditorul și destinatarul nu necesită sincronizare și/sau procese care necesită etape de sincronizare. Pentru a depăși orice probleme potențiale asociate cu datagrama INIT care nu a fost primită la expeditor, acesta se va lega la port imediat după solicitarea portului de la controller, în timpul fazei de setare și înainte de a transmite informațiile de adresă IP/Port la receptor, în rețeaua privată. Odată ce priza este legată, orice datagrame primite vor fi stocate într-o priză cu memorie tampon, până când expeditorul le poate extrage folosind o metodă de recepție pe prize API..

În blocul **408** și după ce "breșa" a fost creată, receptorul merge la faza de execuție unde primește datagrame de testare de la expeditor și măsoară diverse statistici de performanță asociate cu rețeaua, componente ale acesteia (de exemplu, dispozitive de securitate), și/sau Internet-ul care deservește rețeaua privată.

În unele expeditor de realizare, metodele din Figurile 4A și 4B asigură că un port sursă, stabilit prin firewall-ul din datagrama INIT care se transmite expeditorului, este, de asemenea, folosit de către expeditor la viitoarele datagramele ce se vor transmite înapoi. În unele

exemple, expeditorul poate interfera cu o adresă UDP de destinație a datagramelor de testare viitoare, care se vor transmite la receptor, de la o anumită adresă UDP sursă. În unele exemple, expeditorul folosește IP/port local la care este legat ca o adresă sursă pentru tot traficul de testare.

Conform Figurii 5, este prevăzută o metodă **500** pentru a iniția și executa un test de performanță al unei rețele private și/sau al componentelor acesteia, metoda constând în:

În blocul **502** și la un punct de capăt receptor într-o rețea privată, este inițiată o conexiune de strat de transport cu un punct de capăt expeditor, într-o rețea publică.

În blocul **504** și la un punct de capăt expeditor în rețeaua publică, este alocat un port în scop de testare, punct de capătul de capăt expeditor se leagă de port și apoi transmite o adresă IP și un număr de port peste conexiunea de strat de transport.

În blocul **506** și la un punct de capăt receptor, este trimisă o datagramă de perforare breșă, din reteaua privată la rețeaua public, pentru a crea o breșă într-un firewall care separă rețeaua publică și privată.

În blocul **508** și la punctul de capăt expeditor, este primită datagrama de perforare breșă și expeditorul transmite trafic de testare folosind informațiile de adresă IP și de port în datagrama de perforare. Traficul de testare trece prin breșa din firewall.

Trebuie remarcat faptul că platformele de calcul (de exemplu, **102 și 104**, Fig. 1), nodurile (de exemplu, **E1, E2**, etc.), și/sau funcționalitățile descrise, pot constitui dispozitive de calcul cu scop special. Platformele de calcul (de exemplu, **102** și **104**, Fig. 1), nodurile (de exemplu, **E1, E2,** etc.) și/sau funcționalitățile descrise aici pot îmbunătăți domeniul tehnologic de testarea unei rețele private și/sau ale componentelor acesteia, prin furnizarea de mecanisme de rularea testelor de performanță în traficul fluxului de date de intrare, pe un dispozitiv de securitate, prin simularea unui număr mare de utilizatori, fără modificări de configurarea dispozitivului de securitate și fără nici o referire la potiuni destinație publice/private în configurarea testării. Aceasta oferă în mod avantajos un proces de testare, care este complet transparent pentru utilizatorul de aplicație. Aceasta oferă mai multe avantaje (de exemplu, securitate îmbunătățită, testare eficientă, etc.) pentru piața de testare a întreprinderii.

Pentru a primi informațiile de configurarea testării, obiectul prezentei invenții îmbunătățește functionalitățile platformelor de testare și/sau a instrumentelor de testare, prin furnizarea mecanismelor de comunicație a informațiilor de configurarea testării la nodurile dintr-o rețea privată (de exemplu, nodurile din spatele unui dispozitiv firewall și/sau unui dispozitiv NAT), fără necesitatea de a deschise porturi suplimentare sau traducerea adresei de rețea. De asemenea, trebuie remarcat faptul că o platformă de calcul care pune în aplicare obiectele

prezentei invenții, poate cuprinde un dispozitiv de calcul cu scop special (de exemplu, un generator de trafic) folosit pentru a primi informații de configurarea testării.

Se va înțelege că diferite detalii ale obiectelor descris aici pot fi modificate, fără a ne îndepărta de la scopul prezentei invenții. Mai mult decât atât, descrierea de mai sus este numai în scop de ilustrare și nu în scop limitativ, astfel că obiectele prezentei invenții sunt definite de revendicările enunțate mai jos.

a-2014--00994-
16 -12- 2014

REVENDICĂRI:

1. Metodă pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, metoda constând în:

inițierea unei conexiuni de strat de transport cu un punct de capăt expeditor, într-o rețea publică, la un punct de capăt receptor într-o rețea privată;

alocarea unui port în scopuri de testare, legarea la port, precum și transmiterea unei adrese prin Protocolul Internet (Internet Protocol (IP)) și a unui număr de port peste conexiunea de strat de transport, la punctul de capăt expeditor în rețeaua publică;

transmiterea unei datagrame de perforarea unei breșe de comunicație, de la rețeaua privată la rețeaua publică, pentru a crea o breșă într-un firewall care separă rețelele publice și private, la punctul de capăt receptor;

recepționarea datagramelor de perforarea unei breșe de comunicație și în folosirea adresei IP și a informațiilor de port în datagrama de perforarea unei breșe de comunicație, pentru a transmite trafic de testare la punctul de capăt receptor în rețeaua privată prin breșa din firewall, la punctul de capăt expeditor.

2. Metodă, conform revendicării 1, **caracterizată prin aceea că** alocarea unui port pentru scopuri de testare include solicitarea unui port de la un sistem de operare.

3. Metodă, conform revendicării 1, **caracterizată prin aceea că** transmiterea adresei IP și a numărului de port include comunicarea unei datagrame prin Protocolul Datagramelor de Utilizator (UDP), în care câmpul adresei IP stochează adresa IP și un câmp de port sursă stochează numărul portului.

4. Metodă, conform revendicării 1, **caracterizată prin aceea că** datagrama de perforare cuprinde o datagramă INIT prin Protocolul Datagramelor de Utilizator (UDP).

5. Metodă, conform revendicării 4, **caracterizată prin aceea că** datagrama INIT include o adresă IP publică și un număr de port public mapate de firewall pentru o adresă IP privată și un număr de port privat ale punctului de capăt receptor, pentru a primi trafic de testare.

6. Metodă, conform revendicării 5, **caracterizată prin aceea că** transmiterea traficului de testare include adresarea traficului de testare la adresa IP publică și la numărul de port public,

a-2014--00994-
16 -12- 2014

în care firewall-ul primește traficul de testare, mapează adresa IP publică și numărul de port public la adresa IP privată și la numărul de port privat și transmite traficul la punctul de capăt receptor.

7. Metodă, conform revendicării 1, **caracterizată prin aceea că** transmiterea traficului de testare include simularea mai multor utilizatori și transmiterea traficului pentru mai mulți utilizatori, prin rețea.

8. Metodă, conform revendicării 1, **caracterizată prin aceea că** transmiterea traficului de testare include testarea unei conexiuni la Internet, unui dispozitiv de securitate și/sau a conexiunilor, în cadrul rețelei private.

9. Metodă, conform revendicării 1, **caracterizată prin aceea că** un test de performanță este executat fără a deschide manual un port dintr-un firewall asociat cu rețeaua privată.

10. Sistem pentru inițierea și executarea testelor de performanță ale unei rețele private și/sau ale componentelor acesteia, sistemul cuprinzând:
un punct de capăt receptor într-o rețea privată;
un punct de capăt expeditor într-o rețea publică;
în care, punctul de capăt receptor este configurat pentru a iniția o conexiune de strat de transport cu punctul de capăt expeditor;
în care, ca răspuns la recepționarea conexiunii de strat de transport, punctul de capăt expeditor este configurat pentru a aloca un port în scopuri de testare, a se lega de port și a transmite o adresă IP și un număr de port peste conexiunea de strat de transport;
ca răspuns la recepționarea adresei IP și a numărului portului, punctul de capăt receptor este configurat pentru a transmite o datagrama de perforarea unei breșe de comunicație din rețeaua privată la rețeaua public, pentru a crea o breșă într-un firewall-ul care separă rețeaua privată de rețeaua public;
ca răspuns la recepționarea datagramei de perforarea unei breșe de comunicație, punctul de capăt expeditor este configurat să utilizeze adresa IP și informațiile de port în datagrama de perforarea unei breșe de comunicație pentru a transmite trafic de testare la punctul la de capăt receptor, prin breșa din firewall..

11. Sistem, conform revendicării 10, **caracterizat prin aceea că** punctul de capăt expeditor alocă un port pentru scopuri de testare prin solicitarea unui port de la un sistem de operare.

12. Sistem, conform revendicării 10, **caracterizat prin aceea că** adresa IP și numărul de port, transmise la punctul de capăt receptor, sunt o datagramă prin Protocolul Datagramelor de Utilizator (UDP), în care câmpul adresei IP stochează adresa IP și un câmp de port sursă stochează numărul portului.

13. Sistem, conform revendicării 10, **caracterizat prin aceea că** datagrama de perforare cuprinde o datagramă INIT prin Protocolul Datagramelor de Utilizator (UDP).

14. Sistem, conform revendicării 13, **caracterizat prin aceea că** datagrama INIT include o adresă IP publică și un număr de port public mapate de firewall pentru o adresă IP privată și un număr de port privat ale punctului de capăt receptor, pentru a primi trafic de testare.

15. Sistem, conform revendicării 14, **caracterizat prin aceea că** traficul de testare este adresat la adresa IP publică și la numărul de port public, în care firewall-ul primește traficul de testare, mapează adresa IP publică și numărul de port public la adresa IP privată și la numărul de port privat și transmite traficul la punctul de capăt receptor.

16. Sistem, conform revendicării 10, **caracterizat prin aceea că** traficul de testare simulează mai mulți utilizatori și trafic pentru mai mulți utilizatori, prin rețea.

17. Sistem, conform revendicării 10, **caracterizat prin aceea că** traficul de testare este pentru testarea unei conexiuni la Internet, unui dispozitiv de securitate, și/sau a conexiunilor, în cadrul rețelei private.

18. Sistem, conform revendicării 10, **caracterizat prin aceea că** un test de performanță este executat fără a deschide manual un port dintr-un firewall asociat cu rețeaua privată.

19. Suport non-tranzitoriu care poate fi citit de calculator care are stocate pe acesta instrucțiuni executabile de ccalculator, care atunci când sunt executate de către procesorul acestuia, comandă calculatorul să efecteze pașii, care constau în:

inițierea unei conexiuni de strat de transport cu un punct de capăt expeditor, într-o rețea publică, la un punct de capăt receptor într-o rețea privată;

alocarea unui port în scopuri de testare, legarea la port, precum și transmiterea unei adrese prin Protocolul Internet (Internet Protocol (IP)) și a unui număr de port peste conexiunea de strat de transport, la punctul de capăt expeditor în rețeaua publică;

transmiterea unei datagrame de perforarea unei breșe de comunicație, de la rețeaua privată la rețeaua publică, pentru a crea o breșă într-un firewall care separă rețelele publice și private, la punctul de capăt receptor;

recepționarea de perforarea unei breșe de comunicație și în folosirea adresei IP și a informațiilor de port în datagrama de de perforarea unei breșe de comunicație, pentru a transmite trafic de testare la punctul de capăt receptor în rețeaua privată prin breșa din firewall, la punctul de capăt expeditor.

a-2014--00994-
16 -12- 2014

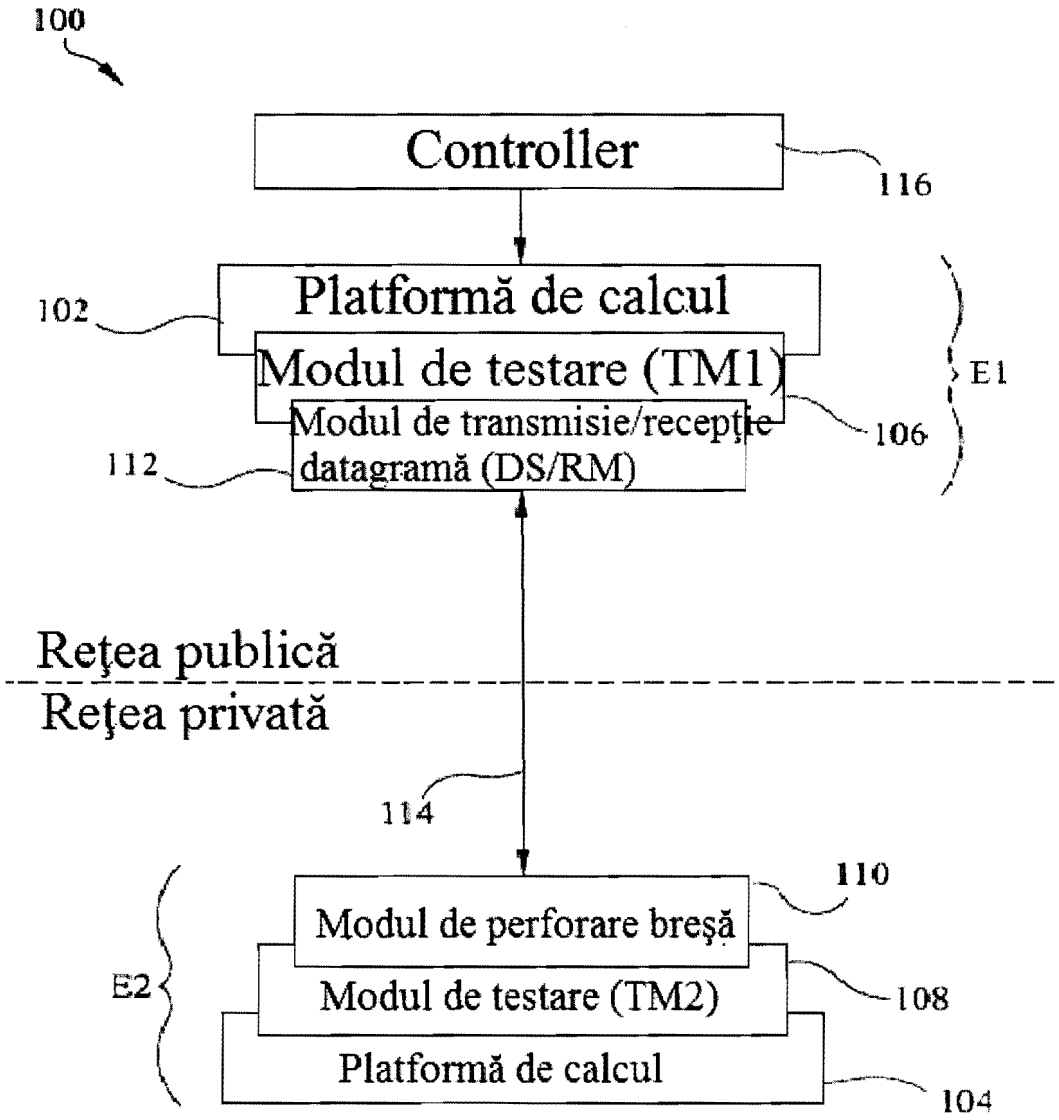

FIG. 1

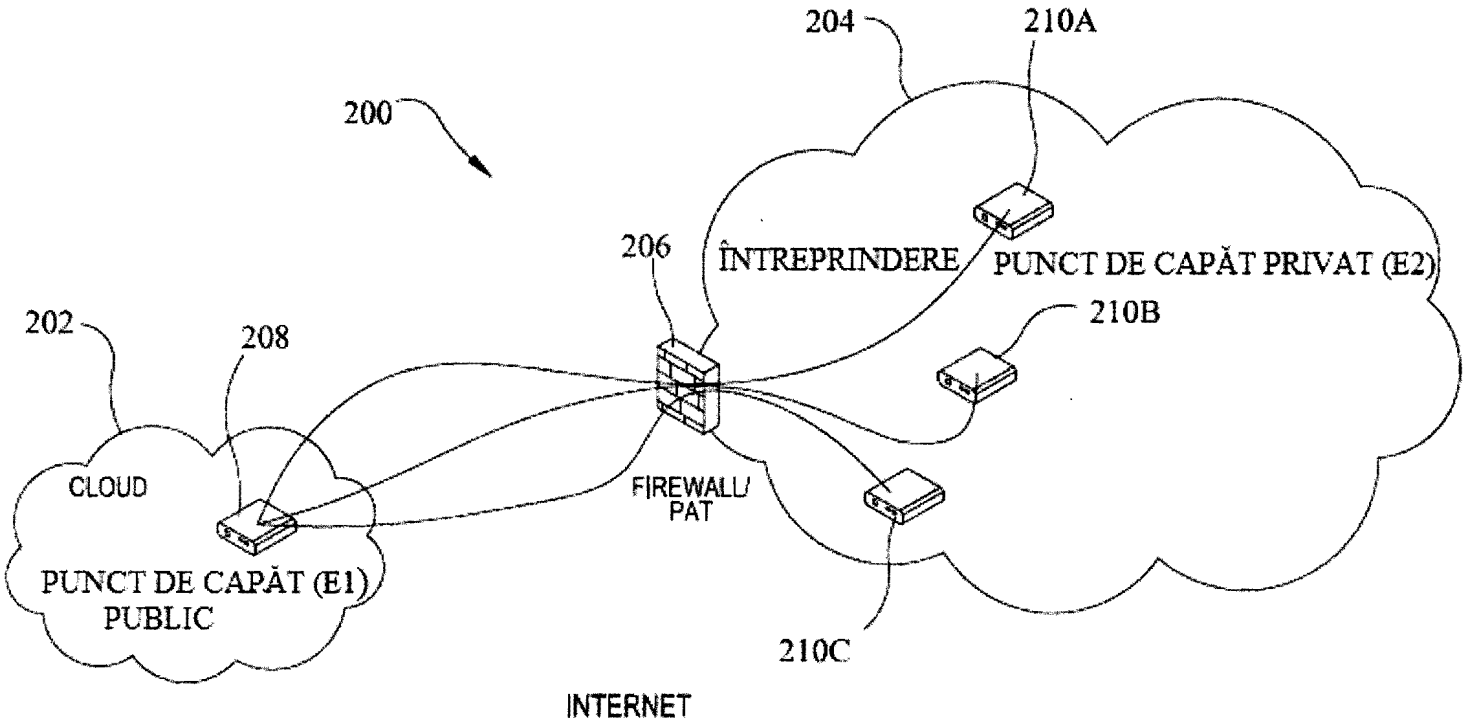

FIG. 2

a-2014--00994-
16 -12- 2014

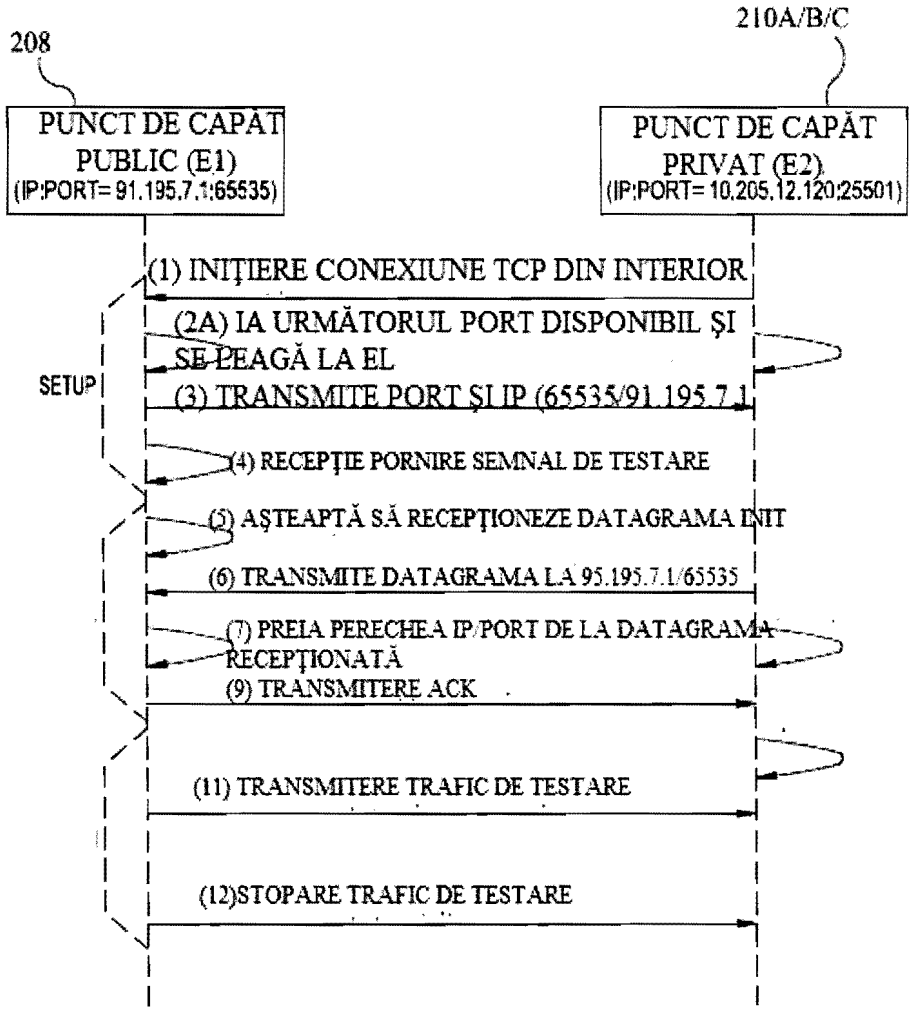

FIG. 3A

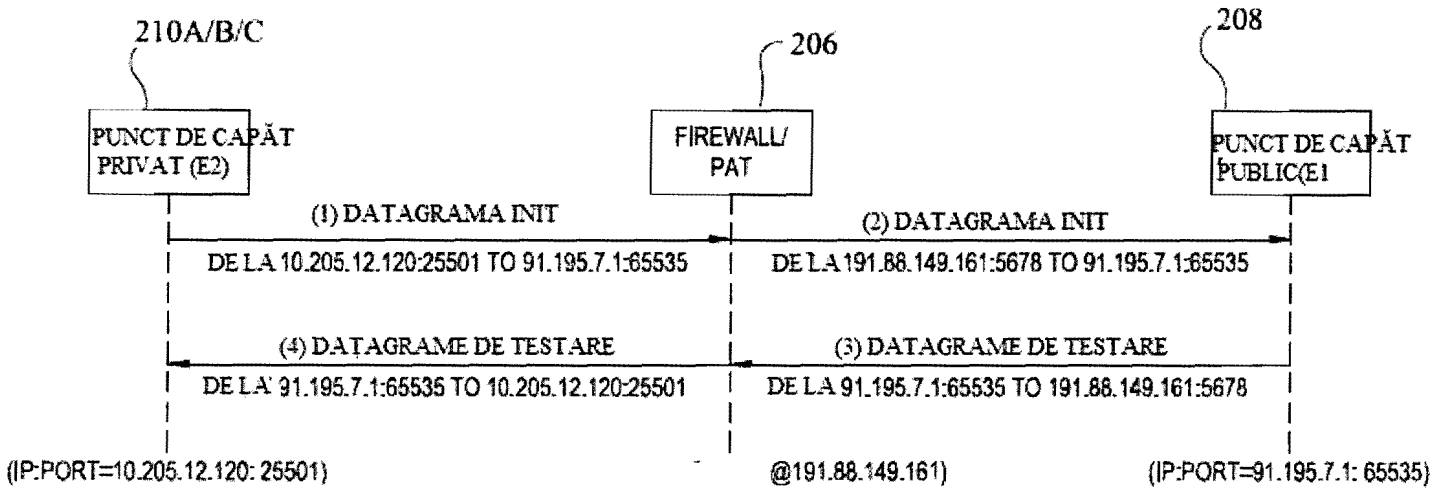

FIG. 3B

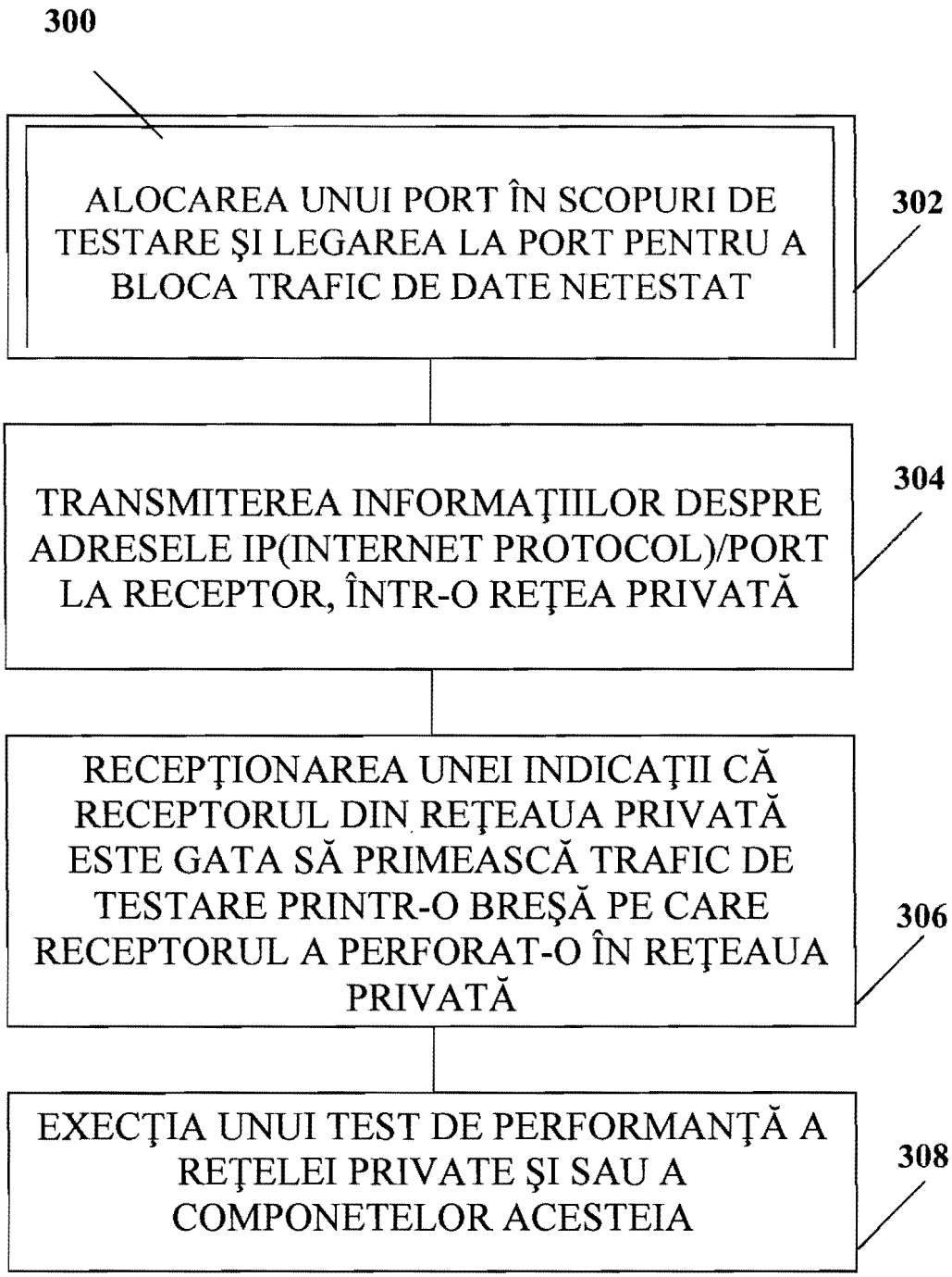
300
ALOCAREA UNUI PORT ÎN SCOPURI DE TESTARE ŞI LEGAREA LA PORT PENTRU A BLOCA TRAFIC DE DATE NETESTAT
302
TRANSMITEREA INFORMAŢIILOR DESPRE ADRESELE IP(INTERNET PROTOCOL)/PORT LA RECEPTOR, ÎNTR-O REŢEA PRIVATĂ
304
RECEPŢIONAREA UNEI INDICAŢII CĂ RECEPTORUL DIN REŢEAUA PRIVATĂ ESTE GATA SĂ PRIMEASCĂ TRAFIC DE TESTARE PRINTR-O BREŞĂ PE CARE RECEPTORUL A PERFORAT-O ÎN REŢEAUA PRIVATĂ
306
EXECŢIA UNUI TEST DE PERFORMANŢĂ A REŢELEI PRIVATE ŞI SAU A COMPONETELOR ACESTEIA
308

Fig.4A

5

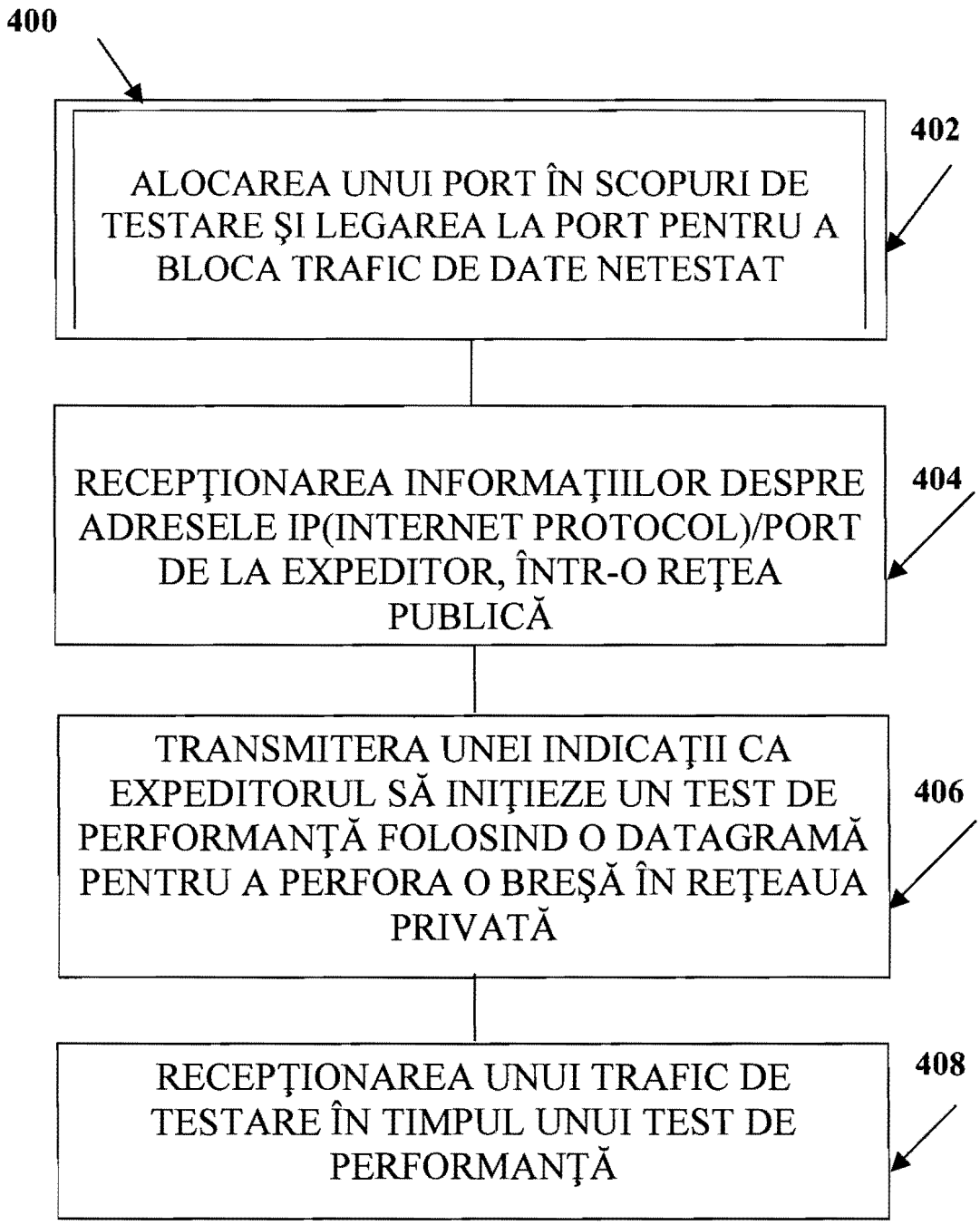
400
ALOCAREA UNUI PORT ÎN SCOPURI DE TESTARE ŞI LEGAREA LA PORT PENTRU A BLOCA TRAFIC DE DATE NETESTAT
402
RECEPŢIONAREA INFORMAŢIILOR DESPRE ADRESELE IP(INTERNET PROTOCOL)/PORT DE LA EXPEDITOR, ÎNTR-O REŢEA PUBLICĂ
404
TRANSMITERA UNEI INDICAŢII CA EXPEDITORUL SĂ INIŢIEZE UN TEST DE PERFORMANŢĂ FOLOSIND O DATAGRAMĂ PENTRU A PERFORA O BREŞĂ ÎN REŢEAUA PRIVATĂ
406
RECEPŢIONAREA UNUI TRAFIC DE TESTARE ÎN TIMPUL UNUI TEST DE PERFORMANŢĂ
408

Fig.4B

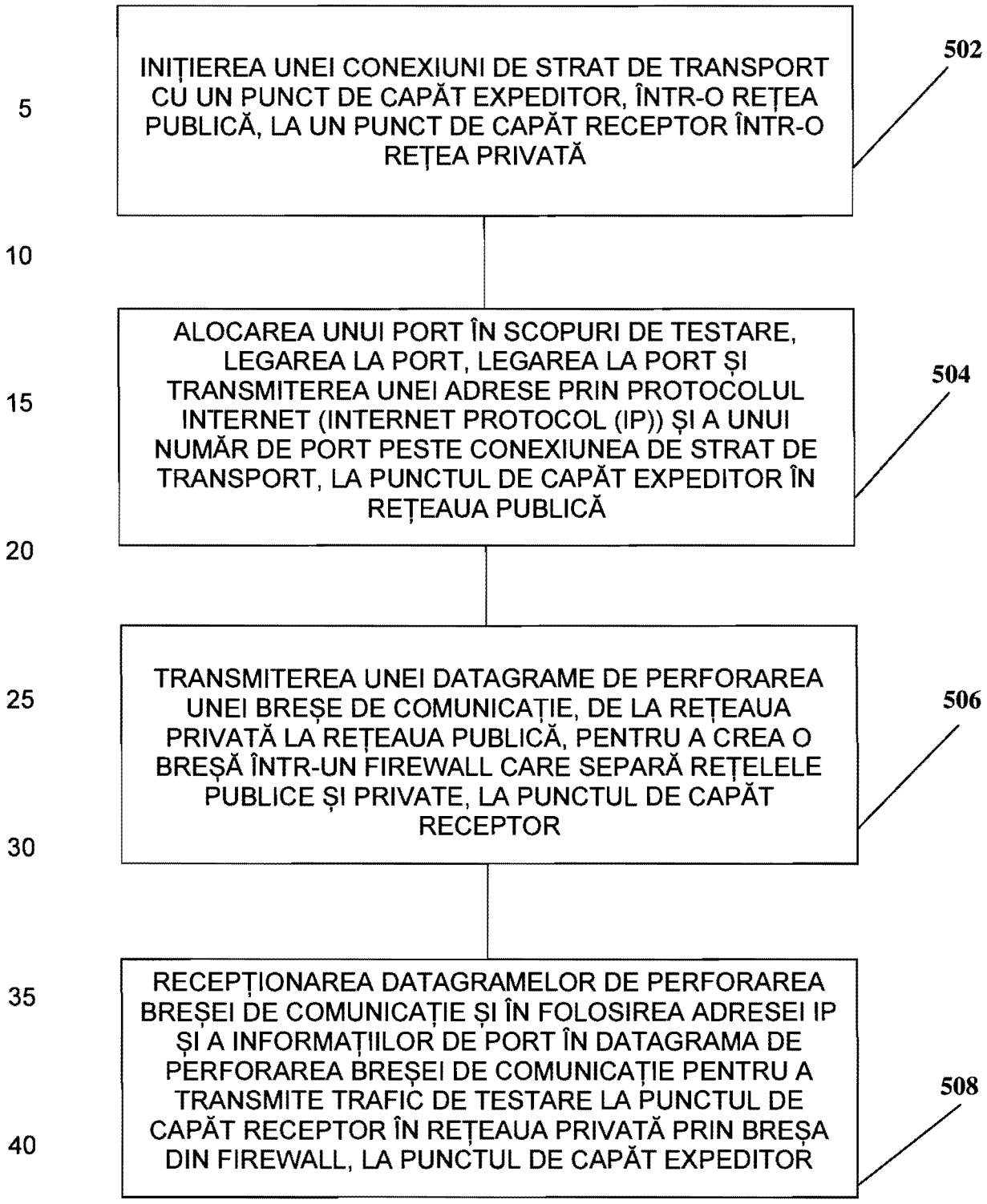
INIȚIEREA UNEI CONEXIUNI DE STRAT DE TRANSPORT CU UN PUNCT DE CAPĂT EXPEDITOR, ÎNTR-O REȚEA PUBLICĂ, LA UN PUNCT DE CAPĂT RECEPTOR ÎNTR-O REȚEA PRIVATĂ
502
ALOCAREA UNUI PORT ÎN SCOPURI DE TESTARE, LEGAREA LA PORT, LEGAREA LA PORT ȘI TRANSMITEREA UNEI ADRESE PRIN PROTOCOLUL INTERNET (INTERNET PROTOCOL (IP)) ȘI A UNUI NUMĂR DE PORT PESTE CONEXIUNEA DE STRAT DE TRANSPORT, LA PUNCTUL DE CAPĂT EXPEDITOR ÎN REȚEAUA PUBLICĂ
504
TRANSMITEREA UNEI DATAGRAME DE PERFORAREA UNEI BREȘE DE COMUNICAȚIE, DE LA REȚEAUA PRIVATĂ LA REȚEAUA PUBLICĂ, PENTRU A CREA O BREȘĂ ÎNTR-UN FIREWALL CARE SEPARĂ REȚELELE PUBLICE ȘI PRIVATE, LA PUNCTUL DE CAPĂT RECEPTOR
506
RECEPȚIONAREA DATAGRAMELOR DE PERFORAREA BREȘEI DE COMUNICAȚIE ȘI ÎN FOLOSIREA ADRESEI IP ȘI A INFORMAȚIILOR DE PORT ÎN DATAGRAMA DE PERFORAREA BREȘEI DE COMUNICAȚIE PENTRU A TRANSMITE TRAFIC DE TESTARE LA PUNCTUL DE CAPĂT RECEPTOR ÎN REȚEAUA PRIVATĂ PRIN BREȘA DIN FIREWALL, LA PUNCTUL DE CAPĂT EXPEDITOR
508

FIG.5