

50 Documents

Publication numbers	Title	Current assignees
US9148408 B1	Systems and methods for protecting network devices	CRYPTZONE NORTH AMERICA
CA2975168 A1	Multi-tunneling virtual network adapter	CRYPTZONE NORTH AMERICA
US9560015 B1	Systems and methods for protecting network devices by a firewall	CRYPTZONE NORTH AMERICA
US9628444 B1	Protecting network devices by a firewall	CRYPTZONE NORTH AMERICA
US20170111310 A1	Name resolving in segmented networks	CRYPTZONE NORTH AMERICA
US20040268121 A1	Reducing network configuration complexity with transparent virtual private networks	MICROSOFT TECHNOLOGY LICENSING
US20170111317 A1	Client network access provision by a network traffic manager	CRYPTZONE NORTH AMERICA
US20040088542 A1	Virtual private network crossovers based on certificates	AT&T
US20050204168 A1	System and method for double-capture/double-redirect to a different location	RPX, ...
WO201319520 A2	System and method for client-server communication facilitating utilization of network-based procedure call	SECUREWORKS, ...
WO200180522 A2	Methods and systems for managing virtual addresses for virtual networks	CORENTE
US9380027 B1	Conditional declarative policies	VARMOUR NETWORKS
US20050273850 A1	Security system with methodology providing verified secured individual end points	CHECK POINT SOFTWARE TECHNOLOGIES
US20140359749 A1	Systems and methods for network analysis and reporting	CATBIRD NETWORKS
US20070118893 A1	Policy based content filtering	FORTINET
US20140245423 A1	Distributed firewall security system for cloud computing environments	ZENTERA SYSTEMS
WO200611464 A1	Connection method, communication system, device, and program	NEC
CA2394455 A1	System for automated connection to virtual private networks related applications	AT&T
US20160072815 A1	Systems and methods for creating and modifying access control lists	CATBIRD NETWORKS
WO200612610 A2	Systems and methods for optimizing communications between network nodes	CITRIX SYSTEMS
US20040167984 A1	System providing methodology for access control with cooperative enforcement	CHECK POINT SOFTWARE TECHNOLOGIES

Publication numbers	Title	Current assignees
CA2497950 A1	Method and apparatus for providing network security based on device security status	OCTEL COMMUNICATIONS, ...
WO200696875 A1	Smart tunneling to resources in a remote network	DELL, ...
WO2010107558 A1	Systems and methods for using end point auditing in connection with traffic management	CITRIX SYSTEMS
US20030041136 A1	Automated configuration of a virtual private network	HUGHES ELECTRONICS
US20100115578 A1	Authentication in a network using client health enforcement framework	MICROSOFT TECHNOLOGY LICENSING
US20060168648 A1	Enabling dynamic authentication with different protocols on the same port for a switch	MCAFEE
WO200612612 A1	Method for routing packets from an endpoint to a gateway	CITRIX SYSTEMS
US20090113540 A1	Controlling network access	MICROSOFT TECHNOLOGY LICENSING
US20060048213 A1	Authenticating a client using linked authentication credentials	CITRIX SYSTEMS
US8353021 B1	Determining firewall rules for an application on a client based on firewall rules and reputations of other clients	SYMANTEC
US20070011733 A1	Unified architecture for remote network access	MICROSOFT TECHNOLOGY LICENSING
CN102104592 A	Session migration between network policy servers	JUNIPER NETWORKS, ...
US20090037763 A1	Systems and methods for providing IIP address stickiness in an SSL VPN session failover environment	CITRIX SYSTEMS
EP1492299 A2	Method of assisting an application to traverse a firewall	MICROSOFT TECHNOLOGY LICENSING
US20080077791 A1	System and method for facilitating secure online transactions	SECUREAUTH
WO200372903 A2	A persistent and reliable session securely traversing network components using an encapsulating protocol	CITRIX SYSTEMS
US20080046993 A1	Systems and methods for enhanced client side policy	CITRIX SYSTEMS
US20080082640 A1	Dynamic virtual private network (VPN) resource provisioning using a dynamic host configuration protocol (DHCP) server, a domain name system (DNS) and/or static IP assignment	ARRAY NETWORKS
US20100313262 A1	Provisioning remote access points	HEWLETT PACKARD ENTERPRISE DEVELOPMENT
US20140259109 A1	Edge server selection for enhanced services network	SURFEASY
US20170070479 A1	Trust status of a communication session	MICROSOFT TECHNOLOGY LICENSING
WO200994657 A1	Systems and methods for fine grain policy driven cookie proxying	CITRIX SYSTEMS
US20050193103 A1	Method and apparatus for automatic configuration and management of a virtual private network	DRABIK JOHN

Publication numbers	Title	Current assignees
US20100218248 A1	Redirection of secure data connection requests	MICROSOFT TECHNOLOGY LICENSING
US20140189808 A1	Multi-factor authentication and comprehensive login system for client-server networks	LOOKOUT
WO2014141283 A1	Access control in a secured cloud environment	FORTYCLOUD
US20170048198 A1	Passport-controlled firewall	IBM
WO200767763 A1	Peer-to-peer remediation	MICROSOFT TECHNOLOGY LICENSING
US20150067815 A1	Configuration of energy savings	CISCO TECHNOLOGY

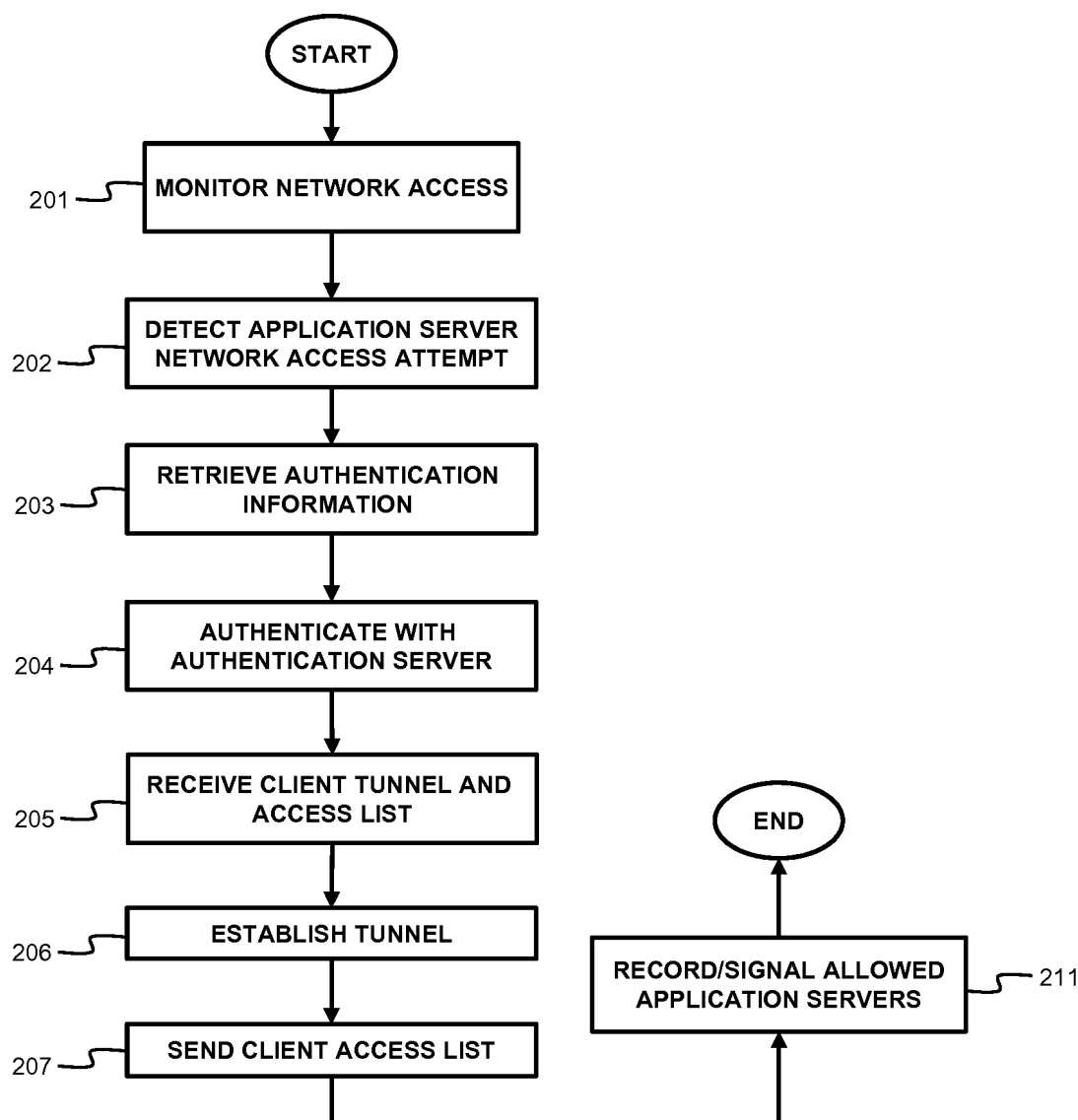
Family 1/50 - FAMPAT - ©Questel

Title

(EP3205073)

Systems and methods for protecting network devices

Images



Publication data including kind & date

US9148408	B1	2015-09-29	US9148408
US20160099916	A1	2016-04-07	US20160099916
US20160099917	A1	2016-04-07	US20160099917
CA2963947	A1	2016-04-14	CA2963947
WO2016057177	A1	2016-04-14	WO201657177
AU2015328628	A1	2017-04-27	AU2015328628
KR20170063795	A	2017-06-08	KR20170063795
CN107005542	A	2017-08-01	CN107005542
EP3205073	A1	2017-08-16	EP3205073
MX2017004292	A	2017-10-02	MX2017004292
EP3205073	A4	2017-10-04	EP3205073
JP2017537501	A	2017-12-14	JP2017537501



US9853947	B2	2017-12-26	US9853947				
US9906497	B2	2018-02-27	US9906497				
US20180139177	A1	2018-05-17	US20180139177				
BR112017007051	A1	2018-05-22	BR112017007051				
BR112017007051	A2	2018-06-19	BR112017007051				

Abstract

(EP3205073)

Embodiments of the present disclosure help protect network devices from unauthorized access. Among other things, embodiments of the disclosure allow full access to application servers and other network devices that a client is allowed to access, while preventing all access (or even knowledge) of network devices the client is not allowed to access.

Inventors

GLAZEMAKERS KURT

HAMILTON MALCOLM

BERBEROGLU GOKHAN

Latest standardized assignees - inventors removed

CRYPTZONE NORTH AMERICA

Publication dates

2015-09-29

2016-04-07

2016-04-07

2016-04-14

2016-04-14

2017-04-27

2017-06-08

2017-08-01

2017-08-16

2017-10-02

2017-10-04

2017-12-14

2017-12-26

2018-02-27

2018-05-17

2018-05-22

2018-06-19

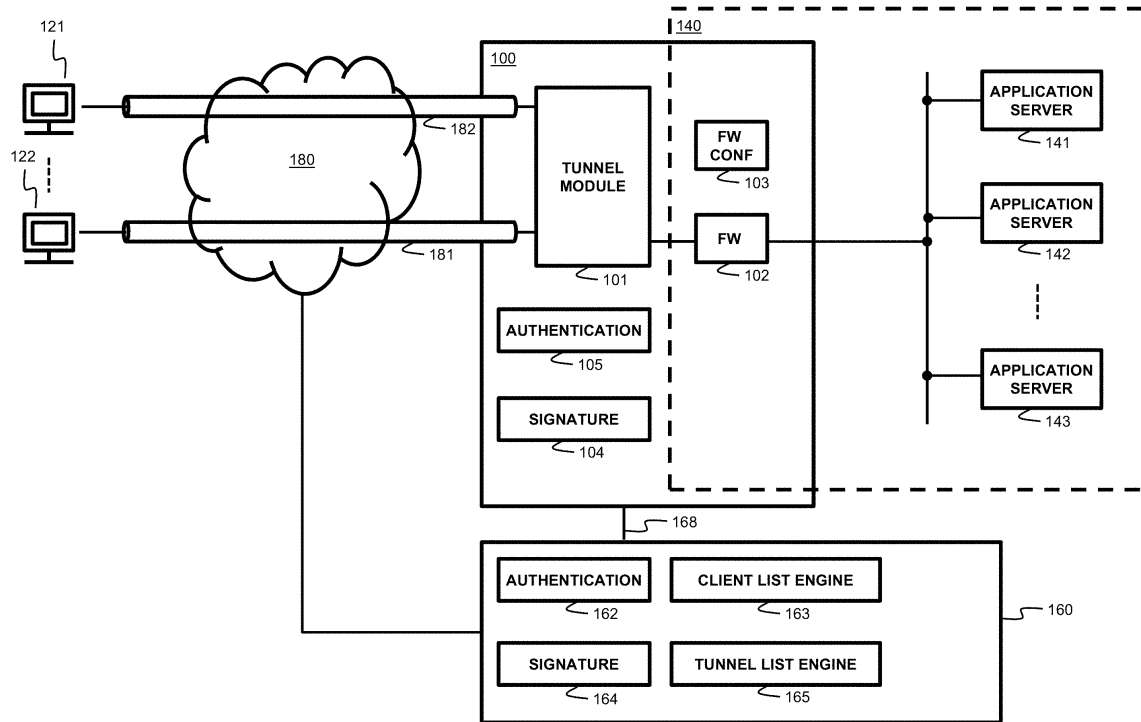
Family 2/50 - FAMPAT - ©Questel

Title

(EP3254415)

Multi-tunneling virtual network adapter

Images



Publication data including kind & date

CA2975168	A1	2016-08-11	CA2975168
WO2016126313	A1	2016-08-11	WO2016126313
IN201747025882	A	2017-07-28	IN201747025882
AU2015381737	A1	2017-08-10	AU2015381737
CN107210956	A	2017-09-26	CN107210956
KR20170128270	A	2017-11-22	KR20170128270
MX2017009906	A	2017-12-07	MX2017009906
EP3254415	A1	2017-12-13	EP3254415
JP2018508140	A	2018-03-22	JP2018508140
AU2015381737	B2	2018-04-19	AU2015381737
BR112017016634	A1	2018-05-29	BR112017016634
JP6343101	B2	2018-06-13	JP6343101
BR112017016634	A2	2018-06-19	BR112017016634
US20180183763	A1	2018-06-28	US20180183763
AU2018206713	A1	2018-08-02	AU2018206713
JP2018139448	A	2018-09-06	JP2018139448



Abstract

(EP3254415)

Among other things, embodiments of the present disclosure allow multiple virtual private network connections to be created without the need for administrative privileges, and allow network traffic to be routed using a single virtual adapter instead of a dedicated virtual adapter for each virtual network connection.

Inventors

GLAZEMAKERS KURT
ALLANSSON PER JOHAN

Latest standardized assignees - inventors removed

CRYPTZONE NORTH AMERICA

Publication dates

2016-08-11

2016-08-11

2017-07-28

2017-08-10

2017-09-26

2017-11-22

2017-12-07

2017-12-13

2018-03-22

2018-04-19

2018-05-29

2018-06-13

2018-06-19

2018-06-28

2018-08-02

2018-09-06

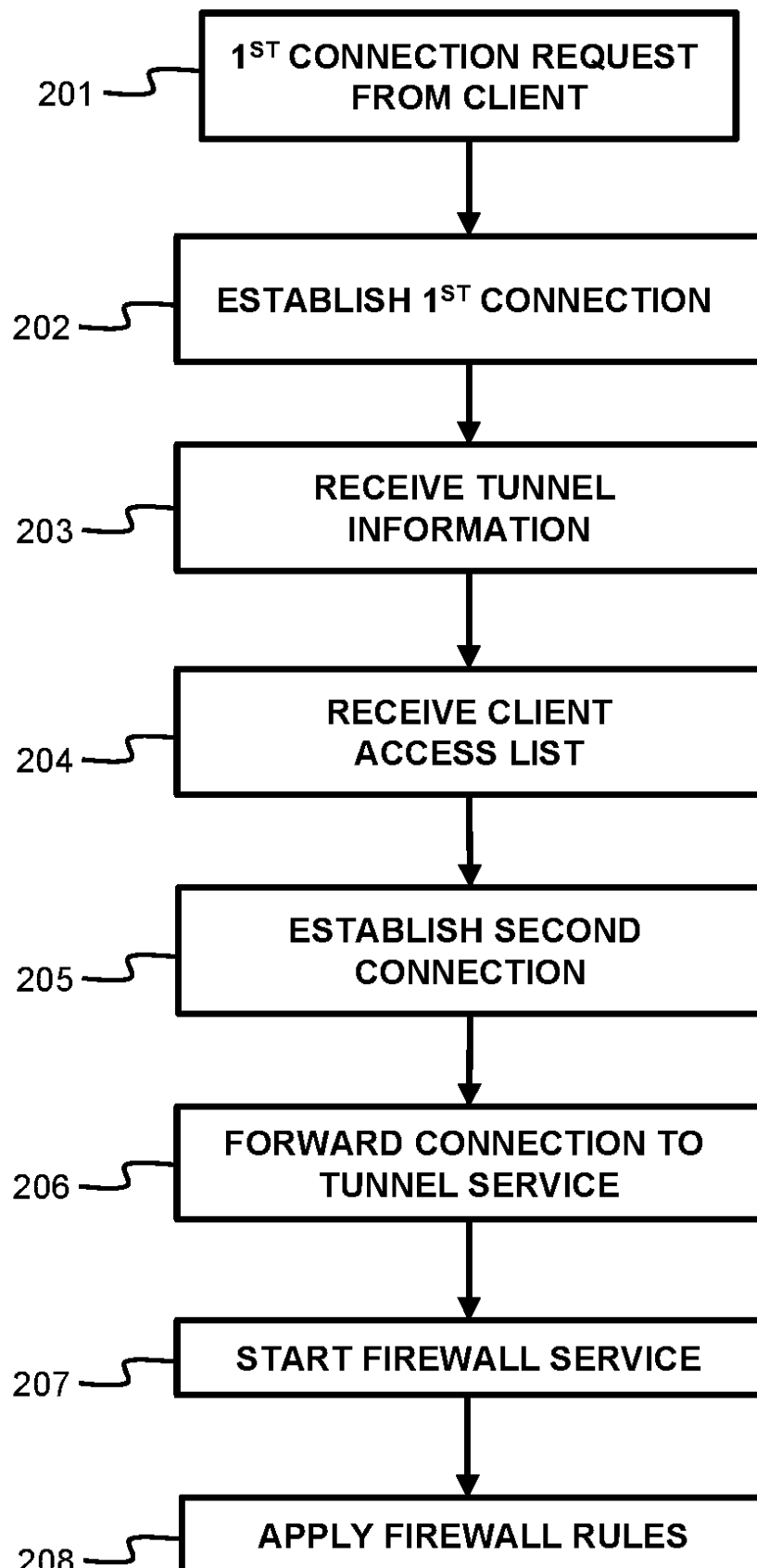
Family 3/50 - FAMPAT - ©Questel

Title

(WO2017180168)

Systems and methods for protecting network devices by a firewall

Images



Publication data including kind & date

US9560015	B1	2017-01-31	US9560015
US20170295140	A1	2017-10-12	US20170295140
WO2017180168	A1	2017-10-19	WO2017180168

**Abstract**

(WO2017180168)

A computer-implemented method, including: upon a request from a client device, establishing, by a computer system implementing a gateway to a private network, a network tunnel between the client device and the gateway; the gateway further implementing a firewall including firewall rules for selectively blocking and allowing network traffic between the client device and one or more network devices in the private network; upon a triggering of a firewall rule by a request for access to the private network by the client device and before applying the firewall rule, checking, by the computer system, if a corresponding condition is met; and if the condition is not met, then, by the computer system, sending to the client device an action to be performed by the client device.

Inventors

GLAZEMAKERS KURT

CELLERIER THOMAS BRUNO EMMANUEL

ABOLAFYA NATAN

BERBEROGLU GOKHAN

ITURRI AITOR PEREZ

LEINO PER

BODLEY-SCOTT JAMIE

Latest standardized assignees - inventors removed

CRYPTZONE NORTH AMERICA

Publication dates

2017-01-31

2017-10-12

2017-10-19

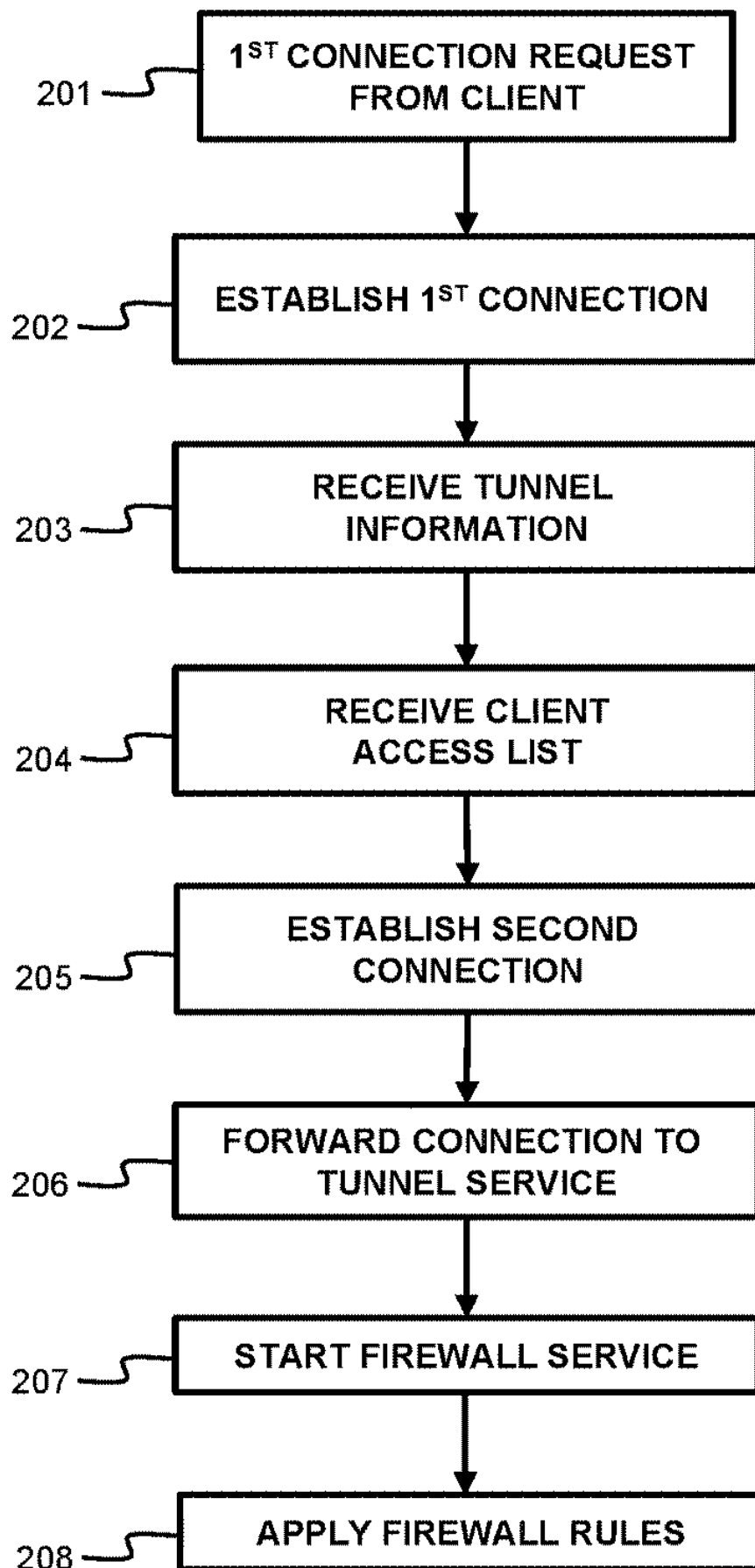
Family 4/50 - FAMPAT - ©Questel

Title

(WO2017138975)

Protecting network devices by a firewall

Images



Publication data including kind & date

US9628444	B1	2017-04-18	US9628444				
US20170230333	A1	2017-08-10	US20170230333				
CA3013059	A1	2017-08-17	CA3013059				
WO2017138975	A1	2017-08-17	WO2017138975				
IN201847028598	A	2018-08-10	IN201847028598				
BR112018015795	A1	2018-08-14	BR112018015795				
AU2016392714	A1	2018-08-16	AU2016392714				
CO2018009316	A2	2018-09-20	CO2018009316				
CN108605041	A	2018-09-28	CN108605041				

Abstract

(WO2017138975)

Systems and methods provide for scaling and management of a gateway. In one embodiment, a method includes: in response to a request from a client device, establishing, by a computer system implementing a gateway to a private network, a network tunnel between the client device and the gateway; and after establishing the network tunnel, starting a separate firewall service with a separate set of firewall rules on the computer system for selectively blocking and allowing network traffic between the client device and one or more network devices in the private network.

Inventors

GLAZEMAKERS KURT

ALLANSSON PER JOHAN

CELLERIER THOMAS BRUNO EMMANUEL

VALIANOS KOSMAS

WEBER TOM VILJO

Latest standardized assignees - inventors removed

CRYPTZONE NORTH AMERICA

Publication dates

2017-04-18

2017-08-10

2017-08-17

2017-08-17

2018-08-10

2018-08-14

2018-08-16

2018-09-20

2018-09-28

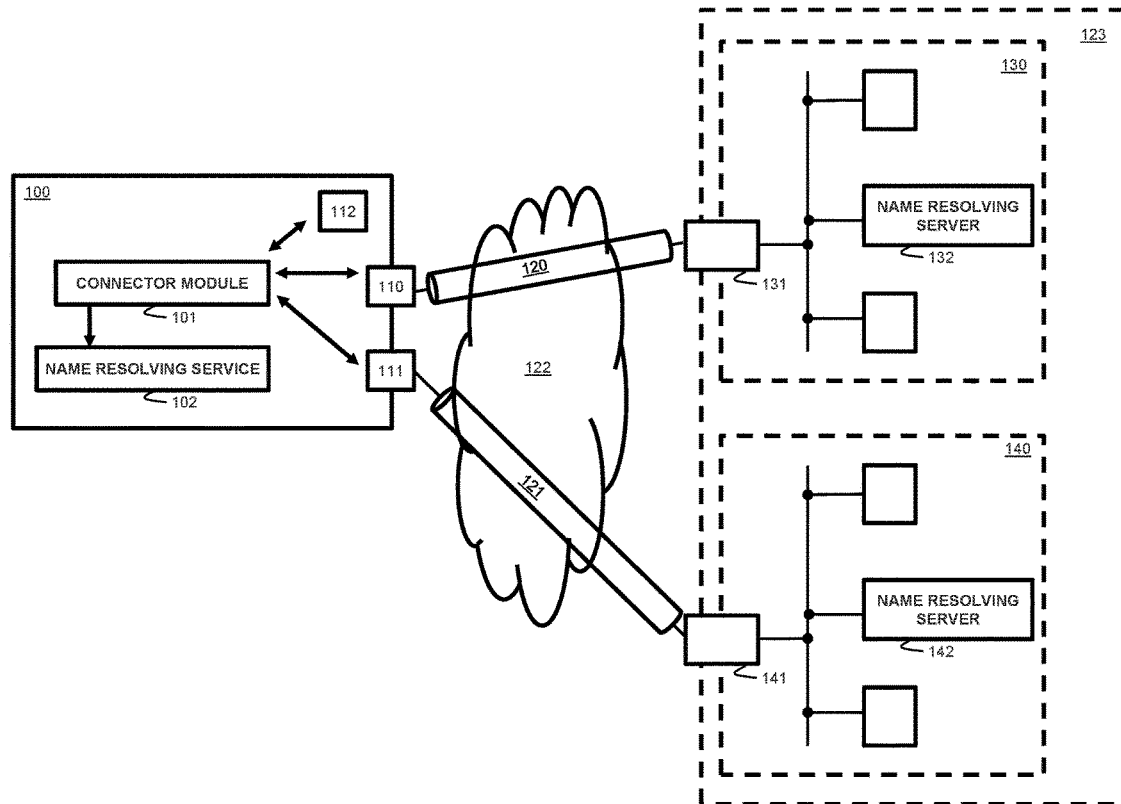
Family 5/50 - FAMPAT - ©Questel

Title

(US9866519)

Name resolving in segmented networks

Images

**Publication data including kind & date**

US20170111310	A1	2017-04-20	US20170111310
US9866519	B2	2018-01-09	US9866519
US20180069826	A1	2018-03-08	US20180069826

**Abstract**

(US9866519)

A method is provided, in one embodiment, which is performed on a client computing device, the method comprising: connecting the client with a plurality of segments of a private network, wherein the private network comprises a plurality of name resolving servers; registering the client as primary name resolving server for serving name requests for names in the private network received from applications on the client; and then forwarding the received name requests simultaneously to the plurality of name resolving servers.

Inventors

GLAZEMAKERS KURT

CELLERIER THOMAS BRUNO EMMANUEL

Latest standardized assignees - inventors removed

CRYPTZONE NORTH AMERICA

Publication dates

2017-04-20

2018-01-09

2018-03-08

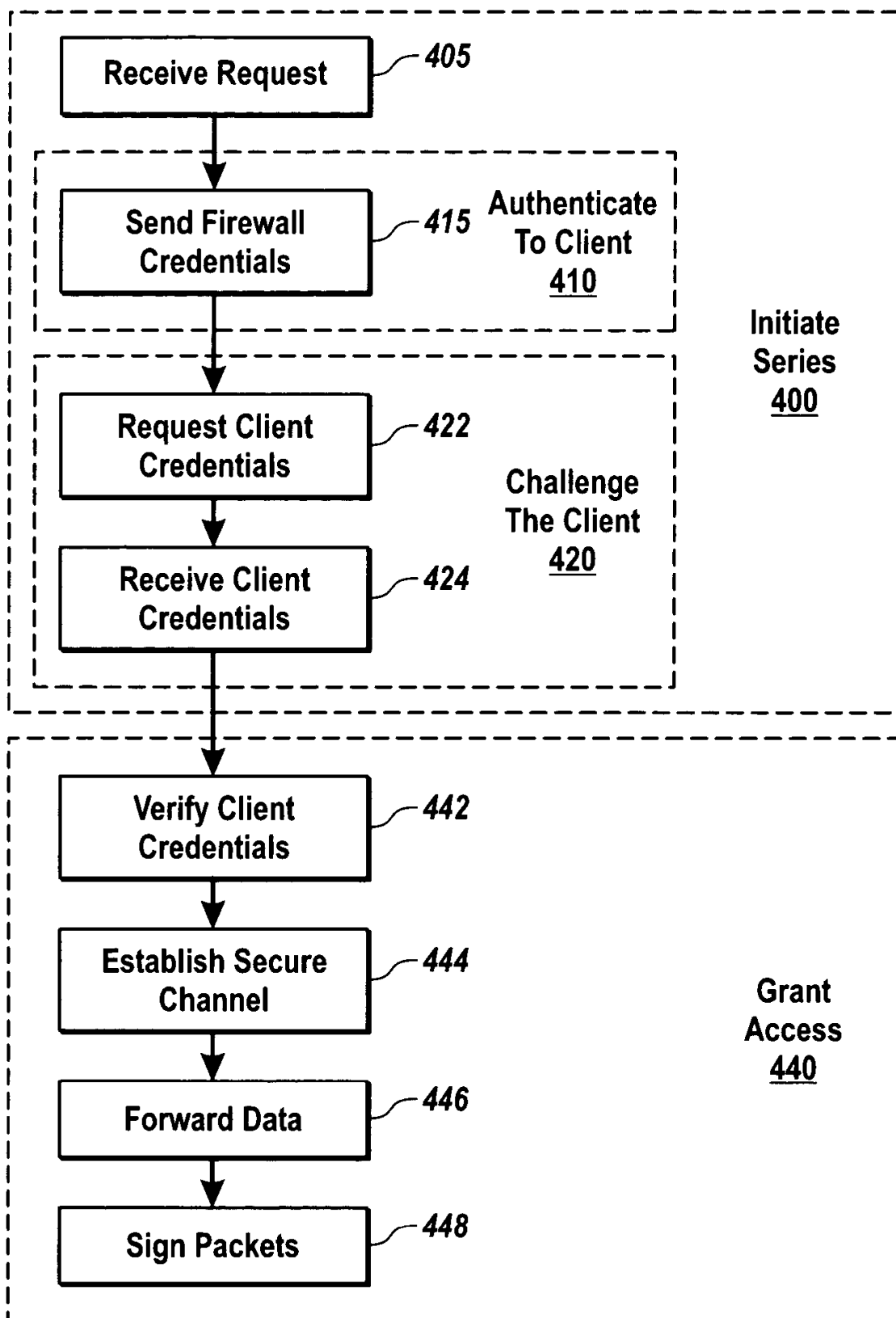
Family 6/50 - FAMPAT - ©Questel

Title

(EP1494420)

Reducing network configuration complexity with transparent virtual private networks

Images



Publication data including kind & date

US20040268121	A1	2004-12-30	US20040268121
EP1494420	A2	2005-01-05	EP1494420
KR20050002632	A	2005-01-07	KR20050002632
JP2005027312	A	2005-01-27	JP2005027312
CN1578218	A	2005-02-09	CN1578218
EP1494420	A3	2006-06-07	EP1494420
US7305705	B2	2007-12-04	US7305705



EP1494420	B1	2010-07-28	EP1494420				
AT476044	T	2010-08-15	ATE476044				
DE602004028316	D1	2010-09-09	DE602004028316				
JP4558389	B2	2010-10-06	JP4558389				
CN1578218	B	2010-12-08	CN1578218B				
KR101076848	B1	2011-10-25	KR101076848				

Abstract

(EP1494420)

A firewall acts as a transparent gateway to a server within a private network by initiating an unsolicited challenge to a client to provide authentication credentials. After receiving the client's credentials, the firewall verifies the authentication credentials and establishes a secure channel for accessing the server. Data destined for the server from the client may be forwarded through the firewall using the secure channel. The firewall may sign, or otherwise indicate that data forwarded to the server is from a client that the firewall has authenticated. The firewall also may provide some level of authentication to the client. While connected to the server, the client may access other servers external to the private network without having the data associated with the other servers pass through the private network. The firewall reduces configuration information that a client otherwise must maintain to access various private network servers.

Inventors

SHELEST ART

HUITEMA CHRISTIAN

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2004-12-30

2005-01-05

2005-01-07

2005-01-27

2005-02-09

2006-06-07

2007-12-04

2010-07-28

2010-08-15

2010-09-09

2010-10-06

2010-12-08

2011-10-25

Family 7/50 - FAMPAT - ©Questel

Title

(US9736120)

Client network access provision by a network traffic manager

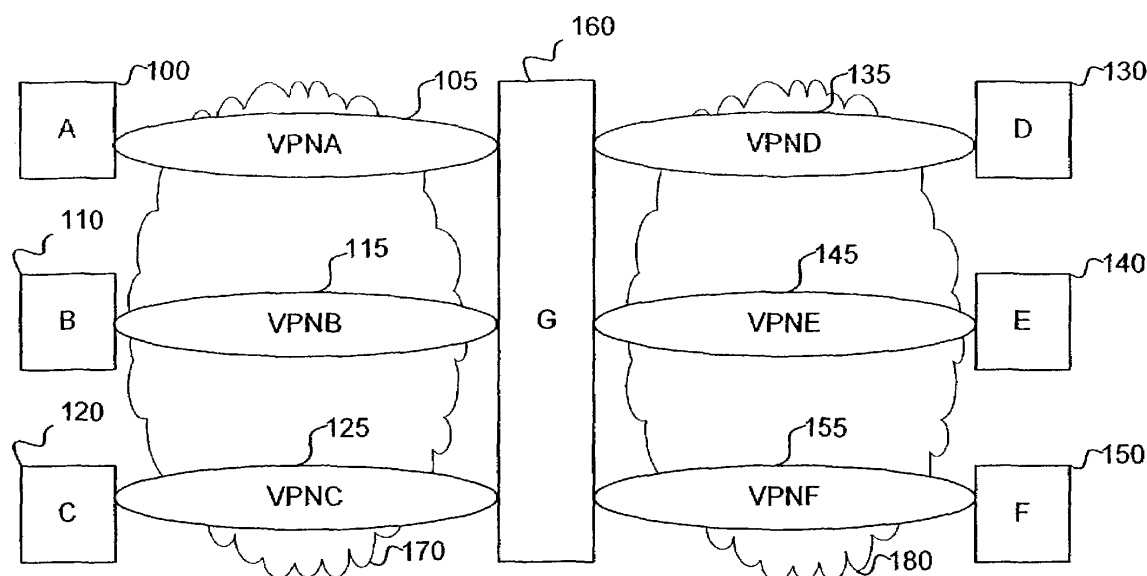
Images

Family 8/50 - FAMPAT - ©Questel

Title

(EP1657885)

Virtual private network crossovers based on certificates

Images**Publication data including kind & date**

US20040088542	A1	2004-05-06	US20040088542
EP1418730	A2	2004-05-12	EP1418730
EP1418730	A3	2004-08-18	EP1418730
EP1657881	A1	2006-05-17	EP1657881
EP1657883	A1	2006-05-17	EP1657883
EP1657884	A2	2006-05-17	EP1657884
EP1657885	A2	2006-05-17	EP1657885
EP1657882	A1	2006-05-17	EP1657882
EP1657880	A1	2006-05-17	EP1657880
EP1657884	A3	2006-06-07	EP1657884
EP1657885	A3	2006-10-11	EP1657885
EP1657880	B1	2007-08-08	EP1657880
DE60315521	D1	2007-09-20	DE60315521
HK1088741	A1	2007-09-28	HK1088741
DE60315521	T2	2008-04-24	DE60315521
EP1418730	B1	2009-04-01	EP1418730
DE60326913	D1	2009-05-14	DE60326913
US7574738	B2	2009-08-11	US7574738
EP1657885	B1	2011-03-09	EP1657885
DE60336352	D1	2011-04-21	DE60336352

**Abstract**

(EP1657885)

A method and system for enabling interconnection of VPNs is disclosed. An interconnection device manages an interconnection process at one or more facilities including, for example, a gateway device. The gateway device has information relating to a plurality of VPNs, and may facilitate interconnection between devices on at least two of the VPNs by determining that one device is in fact a member of a first one of the VPNs, and by forwarding connection parameters of

the first VPN to the second VPN on an as-needed basis. In this way, the gateway allows interconnection without the need for a completely centralized decision-making process, and does so independently of the type of device and/or VPN(s) being used. Moreover, the gateway may implement only those VPN parameters needed by both VPNs to communicate with one another with a desired level of security, thereby simplifying the routing and forwarding processes associated with the actual communication occurring via the interconnection. The information related to the plurality of VPNs and their respective member devices may be stored in a mapping table at the gateway, and identification parameters of a device seeking interconnection and/or associated VPN parameters may be verified by the use of digital certificates.

Inventors

DAUDE OLIVIER

FIESCHI JACQUES

GALAND CLAUDE

HERICOURT OLIVIER

LE PENNEC JEAN-FRANCOIS

Latest standardized assignees - inventors removed

AT&T

Publication dates

2004-05-06

2004-05-12

2004-08-18

2006-05-17

2006-05-17

2006-05-17

2006-05-17

2006-05-17

2006-05-17

2006-06-07

2006-10-11

2007-08-08

2007-09-20

2007-09-28

2008-04-24

2009-04-01

2009-05-14

2009-08-11

2011-03-09

2011-04-21

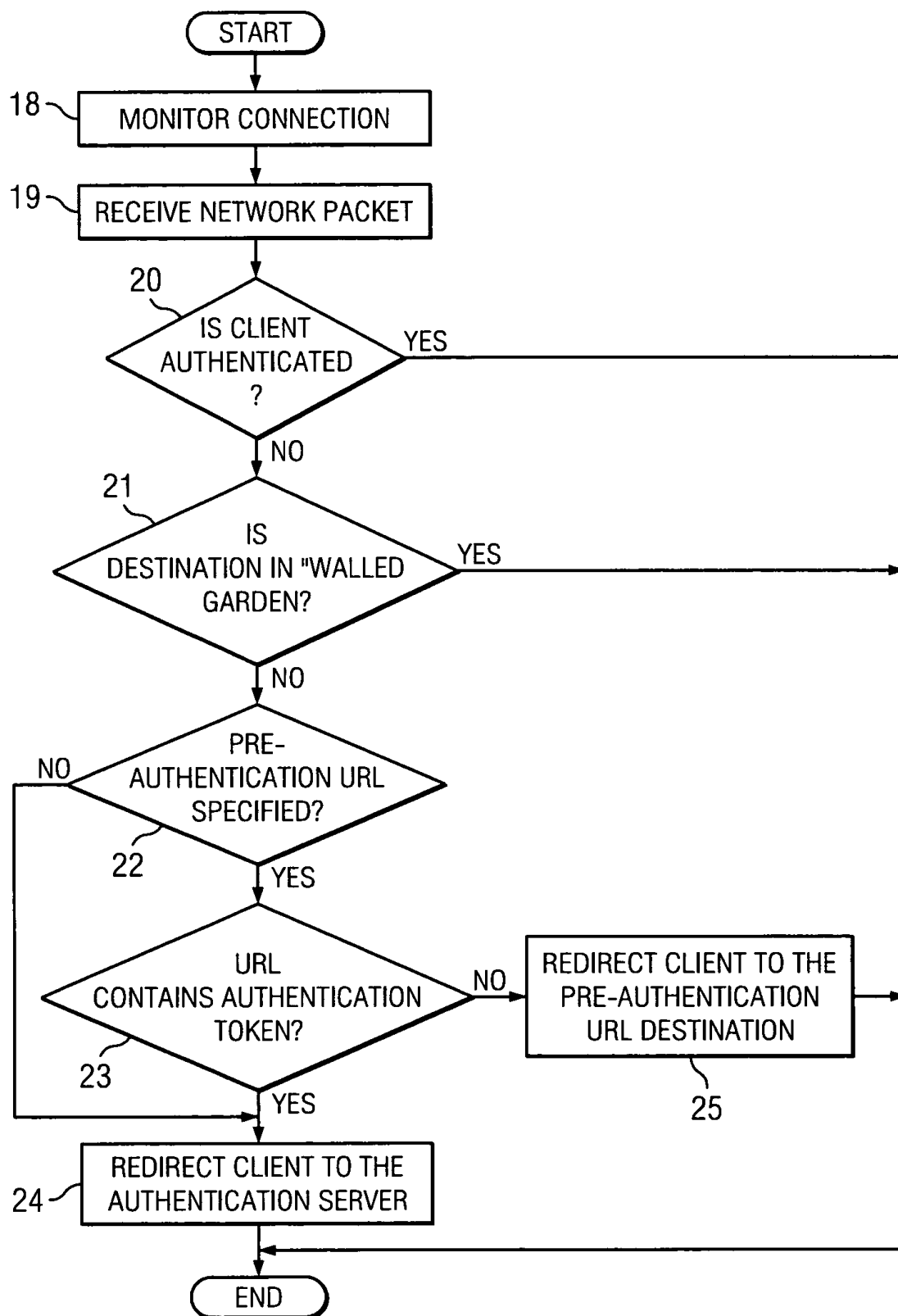
Family 9/50 - FAMPAT - ©Questel

Title

(US8356336)

System and method for double-capture/double-redirect to a different location

Images



Publication data including kind & date

US20050204168	A1	2005-09-15	US20050204168
US7665130	B2	2010-02-16	US7665130
US20100064356	A1	2010-03-11	US20100064356
US8356336	B2	2013-01-15	US8356336



Abstract

(US8356336)

Embodiments disclosed herein provide a system, method, and computer program product for providing network access control for a shared network. One embodiment of a network access controller may intercept a request to access a network resource from a browser application running on a client device associated with an anonymous user and determine whether

the network resource is in a set of network destinations in the shared network. If the network resource is in the set of network destinations, the network access controller may direct the browser application to the network resource. If the network resource is not in the set of network destinations, the network access controller may redirect the browser application to a pre-authentication capture destination in the shared network. From the pre-authentication capture destination the anonymous user is free to visit any of the set of network destinations in the shared network without authentication.

Inventors

JOHNSTON KEITH

WHITE ERIC

MARTIN JOHN

Latest standardized assignees - inventors removed

RPX

WHITE ERIC

Publication dates

2005-09-15

2010-02-16

2010-03-11

2013-01-15

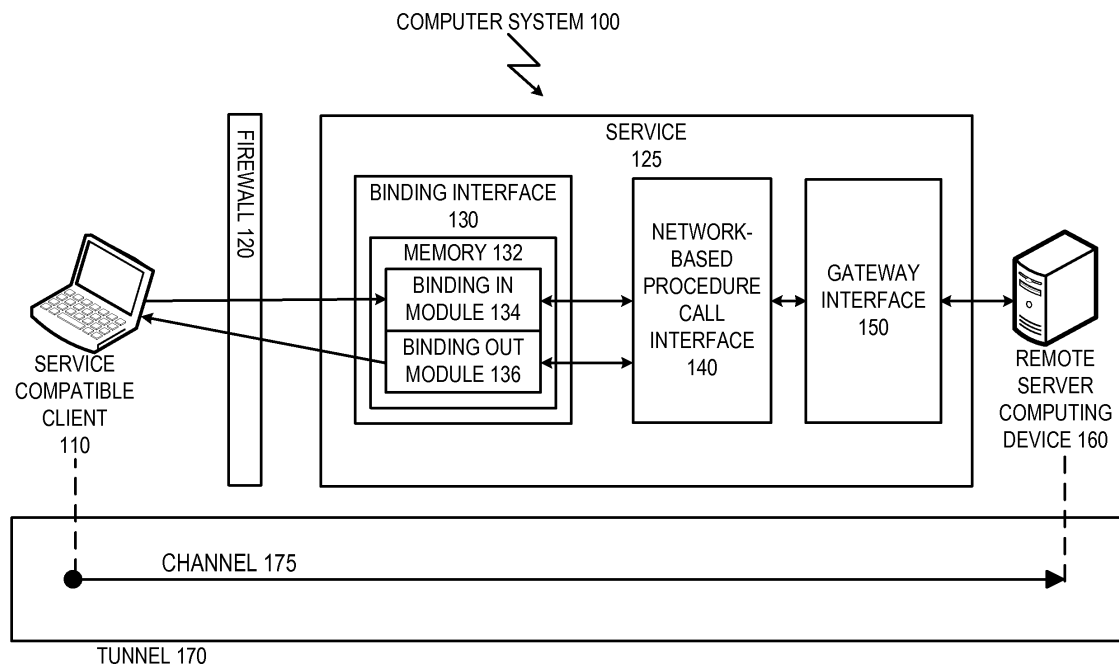
Family 10/50 - FAMPAT - ©Questel

Title

(EP2740046)

System and method for client-server communication facilitating utilization of network-based procedure call

Images



Publication data including kind & date

WO2013019520	A2	2013-02-07	WO201319520
US20130036451	A1	2013-02-07	US20130036451
US20130036192	A1	2013-02-07	US20130036192
US20130325934	A1	2013-12-05	US20130325934
WO2013019520	A3	2014-05-08	WO201319520
EP2740046	A2	2014-06-11	EP2740046



CN104040523	A	2014-09-10	CN104040523				
US8862660	B1	2014-10-14	US8862660				
US8904484	B2	2014-12-02	US8904484				
US8910273	B1	2014-12-09	US8910273				
EP2740046	A4	2015-02-18	EP2740046				
US8984617	B1	2015-03-17	US8984617				
US8990342	B2	2015-03-24	US8990342				
IN715CHN2014	A	2015-04-03	IN2014CN00715				
US9131011	B1	2015-09-08	US9131011				
US9225809	B1	2015-12-29	US9225809				
US9232015	B1	2016-01-05	US9232015				
US9294544	B1	2016-03-22	US9294544				
EP2740046	B1	2017-02-08	EP2740046				
CN104040523	B	2017-03-29	CN104040523B				
US9705729	B2	2017-07-11	US9705729				

Abstract

(EP2740046)

System and method for communicating data are disclosed. Method includes facilitating receiving, from a module of a client computing device, a first message in a universal format. Method includes generating a first encoded message by encoding the first message into a network-based procedure call interface associated with a server, based on a stored encoding for the network-based procedure call interface. Method includes facilitating transmitting the first encoded message to a module of the server. Method includes facilitating receiving, from a module of the server, a second message encoded in the network-based procedure call interface associated with the server. Method includes generating a second decoded message by decoding the second message into the universal format, based on the stored encoding for the network-based procedure call interface. Method includes facilitating transmitting the second decoded message to a module of the client computing device.

Inventors

FAUSAK ANDREW T

Latest standardized assignees - inventors removed

SECUREWORKS

SCALEIO

FORCE10 NETWORKS

MOZY

MAGINATICS

ASAP SOFTWARE EXPRESS

DELL INTERNATIONAL

PEROT SYSTEMS

DELL SYSTEMS

APPASSURE SOFTWARE

CREDANT TECHNOLOGIES

EMC IP HOLDING

SPANNING CLOUD APPS

COMPELLANT TECHNOLOGIES

BOOMI

EMC

AVENTAIL

COMPELLENT TECHNOLOGIES

DELL MARKETING

GALE TECHNOLOGIES

DELL SOFTWARE

DELL

Publication dates

2013-02-07

2013-02-07

2013-02-07

2013-12-05

2014-05-08

2014-06-11

2014-09-10

2014-10-14

2014-12-02

2014-12-09

2015-02-18

2015-03-17

2015-03-24

2015-04-03

2015-09-08

2015-12-29

2016-01-05

2016-03-22

2017-02-08

2017-03-29

2017-07-11

Family 11/50 - FAMPAT - ©Questel

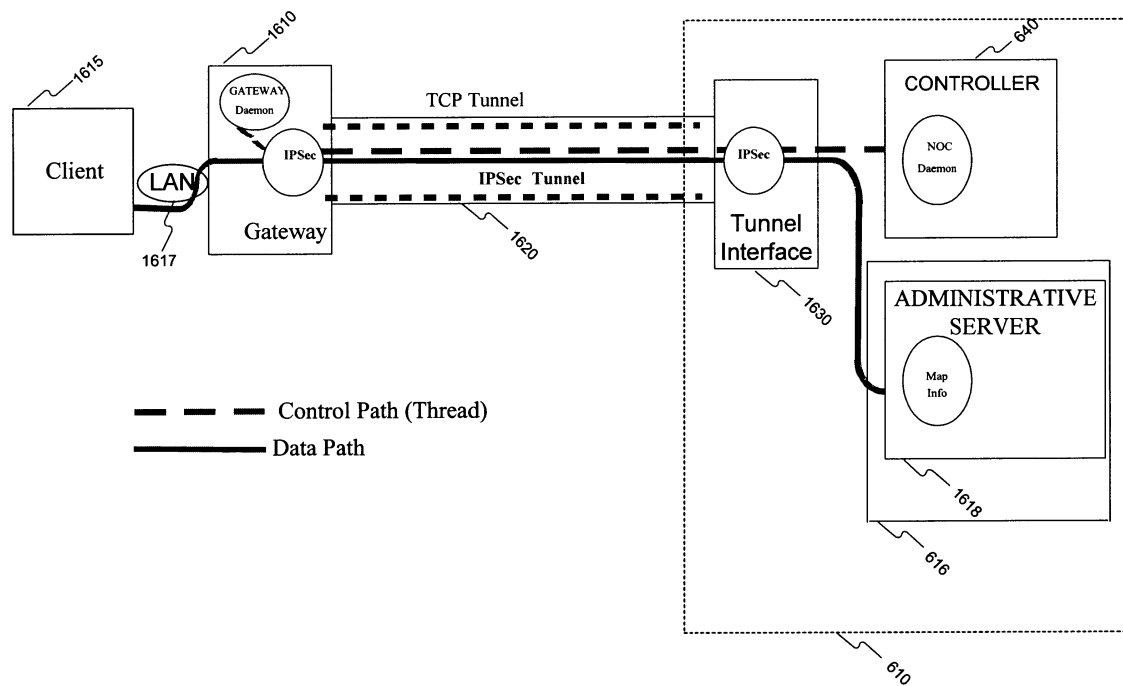
Title

(EP1273156)

Methods and systems for managing virtual addresses for virtual networks

Images

1600B



Publication data including kind & date

WO200180522	A2	2001-10-25	WO200180522
WO200180521	A2	2001-10-25	WO200180521
WO200180490	A2	2001-10-25	WO200180490
WO200180489	A2	2001-10-25	WO200180489
WO200180488	A2	2001-10-25	WO200180488
WO200180487	A2	2001-10-25	WO200180487
WO200180037	A2	2001-10-25	WO200180037
CA2406120	A1	2001-10-25	CA2406120
AU6293501	A	2001-10-30	AU200162935
AU5700001	A	2001-10-30	AU200157000
AU5527501	A	2001-10-30	AU200155275
AU5527401	A	2001-10-30	AU200155274
AU5527301	A	2001-10-30	AU200155273
AU5329301	A	2001-10-30	AU200153293
AU5148201	A	2001-10-30	AU200151482
WO200182533	A2	2001-11-01	WO200182533
AU4762601	A	2001-11-07	AU200147626
WO200182533	A8	2001-12-27	WO200182533
US20020023210	A1	2002-02-21	US20020023210
US20020026503	A1	2002-02-28	US20020026503
US20020026531	A1	2002-02-28	US20020026531
US20020029276	A1	2002-03-07	US20020029276
WO200180490	A3	2002-03-14	WO200180490
WO200180489	A3	2002-04-25	WO200180489
WO200180487	A3	2002-04-25	WO200180487
WO200180488	A3	2002-05-02	WO200180488
WO200180037	A3	2002-05-02	WO200180037
US20020053031	A1	2002-05-02	US20020053031



US20020056008	A1	2002-05-09	US20020056008				
WO200180521	A3	2002-05-16	WO200180521				
WO200182533	A8	2002-05-16	WO200182533				
US20020091859	A1	2002-07-11	US20020091859				
US20020099937	A1	2002-07-25	US20020099937				
WO200180522	A3	2002-08-29	WO200180522				
EP1273156	A2	2003-01-08	EP1273156				
US20030131263	A1	2003-07-10	US20030131263				
US6631416	B2	2003-10-07	US6631416				
JP2004501534	A	2004-01-15	JP2004501534				
US6996628	B2	2006-02-07	US6996628				
US7028334	B2	2006-04-11	US7028334				
US7028333	B2	2006-04-11	US7028333				
US7047424	B2	2006-05-16	US7047424				
US7085854	B2	2006-08-01	US7085854				
US7181766	B2	2007-02-20	US7181766				
US7181542	B2	2007-02-20	US7181542				
EP1273156	B1	2007-08-29	EP1273156				
AT372023	T	2007-09-15	ATE372023				
DE60130203	D1	2007-10-11	DE60130203				
DE60130203	T2	2008-05-15	DE60130203				
US7533409	B2	2009-05-12	US7533409				
CA2406120	C	2010-10-12	CA2406120				
JP4621405	B2	2011-01-26	JP4621405				

Abstract

(EP1273156)

Methods and system are provided for enabling a virtual network between a first processor and a second processor using at least one additional processor separate from the first processor and the second processor. In one embodiment, the at least one additional processor may determine a first virtual address and a first base address for the first processor such that the first virtual address is routable through the virtual network and the first base address is routable through a base network and determine a second virtual address and a second base address for the second processor such that the second virtual address is routable through the virtual network and the second base address is routable through the base network. The at least one additional processor may provide the first virtual address and the first base address to the first processor and the second virtual address and the second base address to the second processor. Moreover, the virtual network may be enabled over the base network based on the first virtual address, the first base address, the second virtual address, and the second base address.

Inventors

KEANE JOHN

MACEY CHRISTOPHER

Latest standardized assignees - inventors removed

CORENTE

Publication dates

2001-10-25

2001-10-25

2001-10-25

2001-10-25

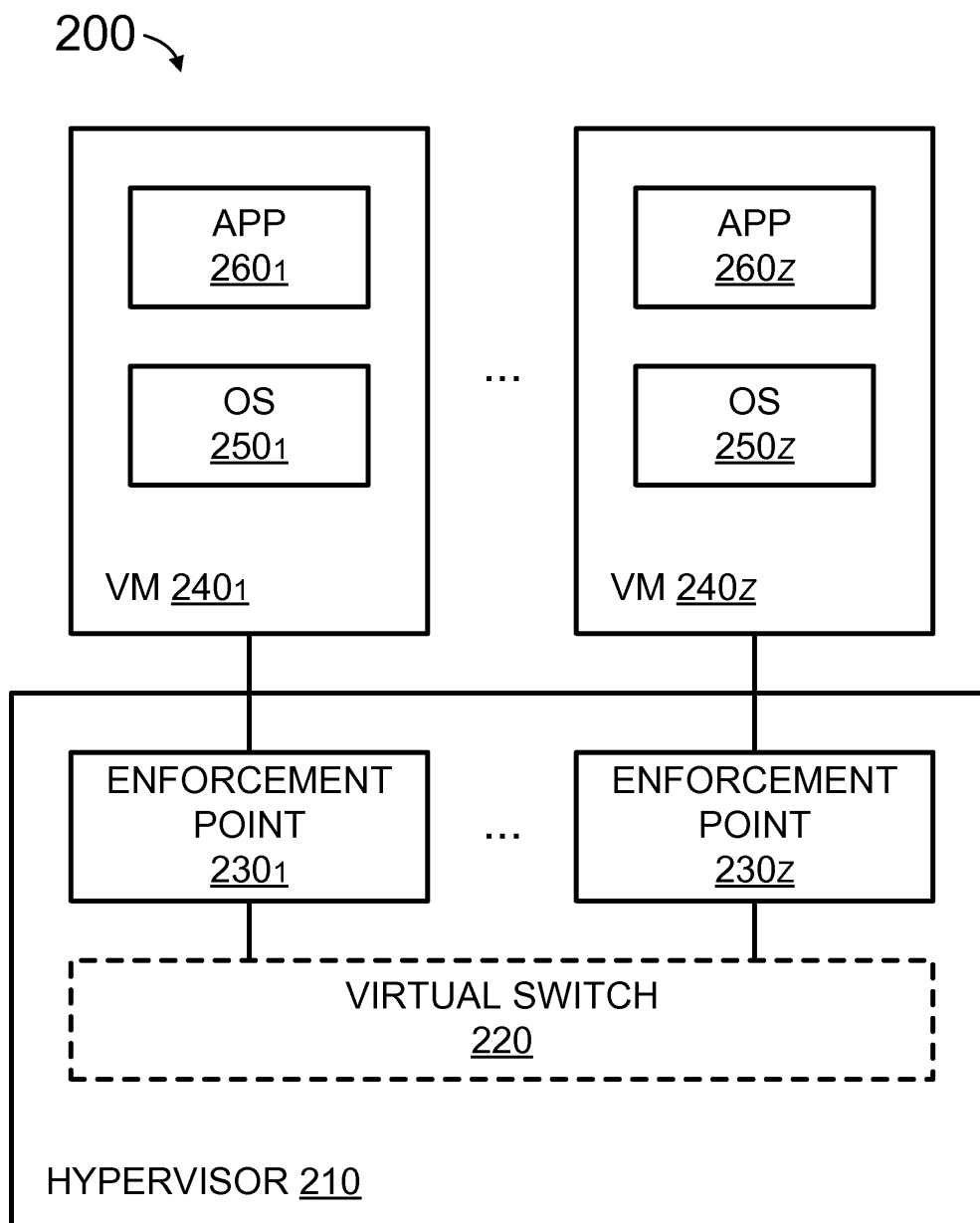
2001-10-25

2001-10-25

2001-10-25
2001-10-25
2001-10-30
2001-10-30
2001-10-30
2001-10-30
2001-10-30
2001-10-30
2001-10-30
2001-11-01
2001-11-07
2001-12-27
2002-02-21
2002-02-28
2002-02-28
2002-03-07
2002-03-14
2002-04-25
2002-04-25
2002-05-02
2002-05-02
2002-05-02
2002-05-09
2002-05-16
2002-05-16
2002-07-11
2002-07-25
2002-08-29
2003-01-08
2003-07-10
2003-10-07
2004-01-15
2006-02-07
2006-04-11
2006-04-11
2006-05-16
2006-08-01
2007-02-20
2007-02-20
2007-08-29
2007-09-15
2007-10-11
2008-05-15
2009-05-12
2010-10-12
2011-01-26

(WO2016160523)

Conditional declarative policies

Images**Publication data including kind & date**

US9380027	B1	2016-06-28	US9380027
WO2016160523	A1	2016-10-06	WO2016160523
TW201642616	A	2016-12-01	TW201642616
US20170063795	A1	2017-03-02	US20170063795
US9621595	B2	2017-04-11	US9621595
US20170208100	A1	2017-07-20	US20170208100

**Abstract**

(WO2016160523)

Methods, systems, and media for producing a firewall rule set are provided herein. Exemplary methods may include receiving a declarative policy associated with a computer network security policy; collecting information from at least one external system of record; generating a firewall rule set using the declarative policy and information, the firewall rule set including addresses to or from which network communications are permitted, denied, redirected or logged, the firewall rule

set being at a lower level of abstraction than the declarative policy; and provisioning the firewall rule set to a plurality of enforcement points of a distributed firewall, the firewall selectively policing network communications among workloads using the firewall rule set.

Inventors

LIAN JIA-JYI

PATERRA ANTHONY

WOOLWARD MARC

Latest standardized assignees - inventors removed

VARMOUR NETWORKS

Publication dates

2016-06-28

2016-10-06

2016-12-01

2017-03-02

2017-04-11

2017-07-20

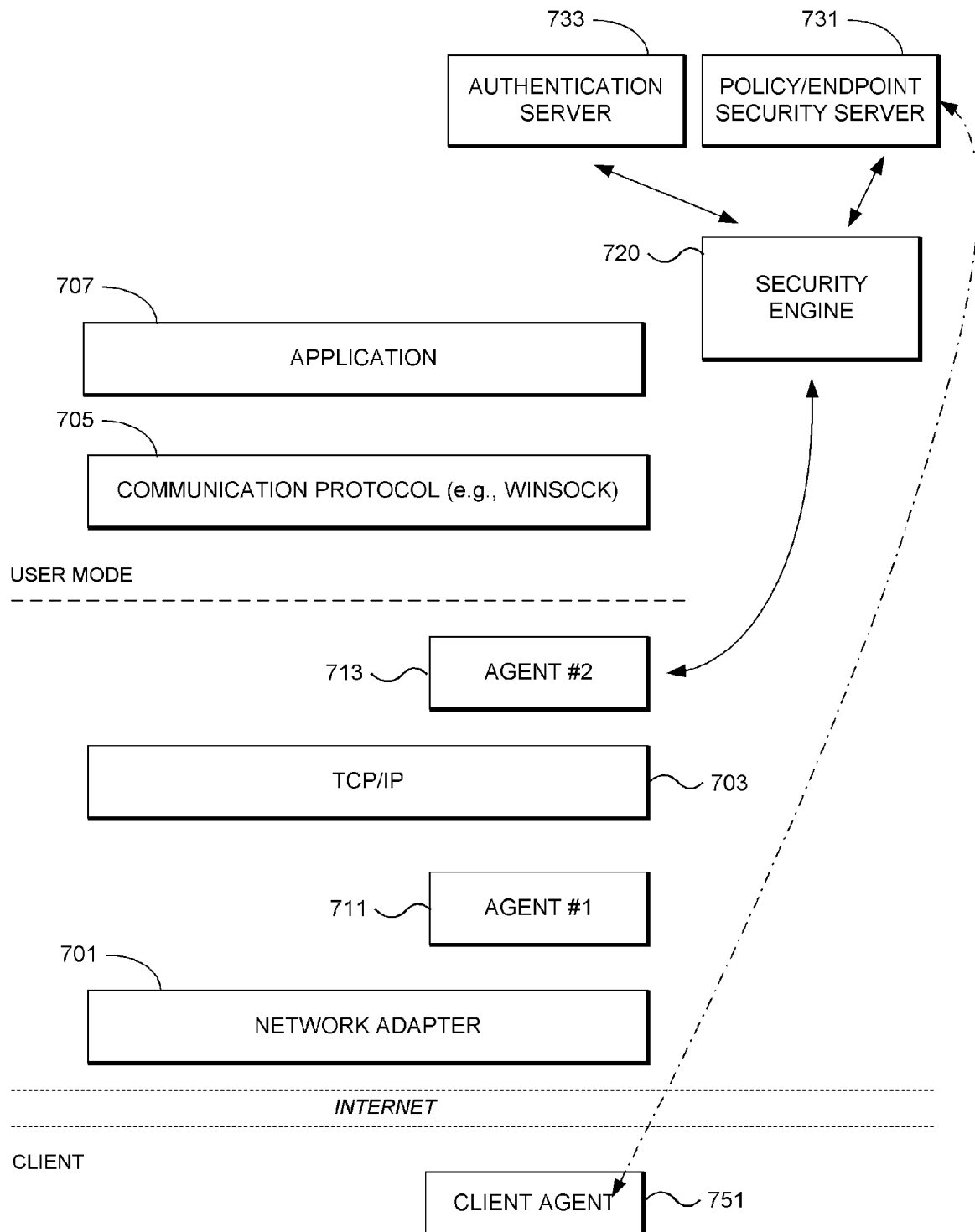
Family 13/50 - FAMPAT - ©Questel

Title

(US8136149)

Security system with methodology providing verified secured individual end points

Images

**Publication data including kind & date**

US20050273850	A1	2005-12-08	US20050273850
US8136149	B2	2012-03-13	US8136149

**Abstract**

(US8136149)

A security system with methodology providing verified secured individual end points is described. In one embodiment, for example, a method of the present invention is described for controlling access to a particular application, the method comprises steps of: defining firewall rules specifying filtering conditions for incoming network traffic, the firewall rules including an application attribute that allows individual rules to be associated with specific applications, the firewall rules also including extended attributes that allow specification of additional conditions that a given end point is required to meet; intercepting incoming network traffic destined for a particular application for which a particular application-specific firewall

rule has been created; examining the extended attributes for the particular application-specific firewall rule, for determining what additional conditions the given end point must comply with in order to communicate with the particular application; if the given end point complies with the additional conditions, allowing the end point to communicate with the particular application; and otherwise blocking the end point to prevent communication with the particular application.

Inventors

FREUND GREGOR PAUL

Latest standardized assignees - inventors removed

CHECK POINT SOFTWARE TECHNOLOGIES

Publication dates

2005-12-08

2012-03-13

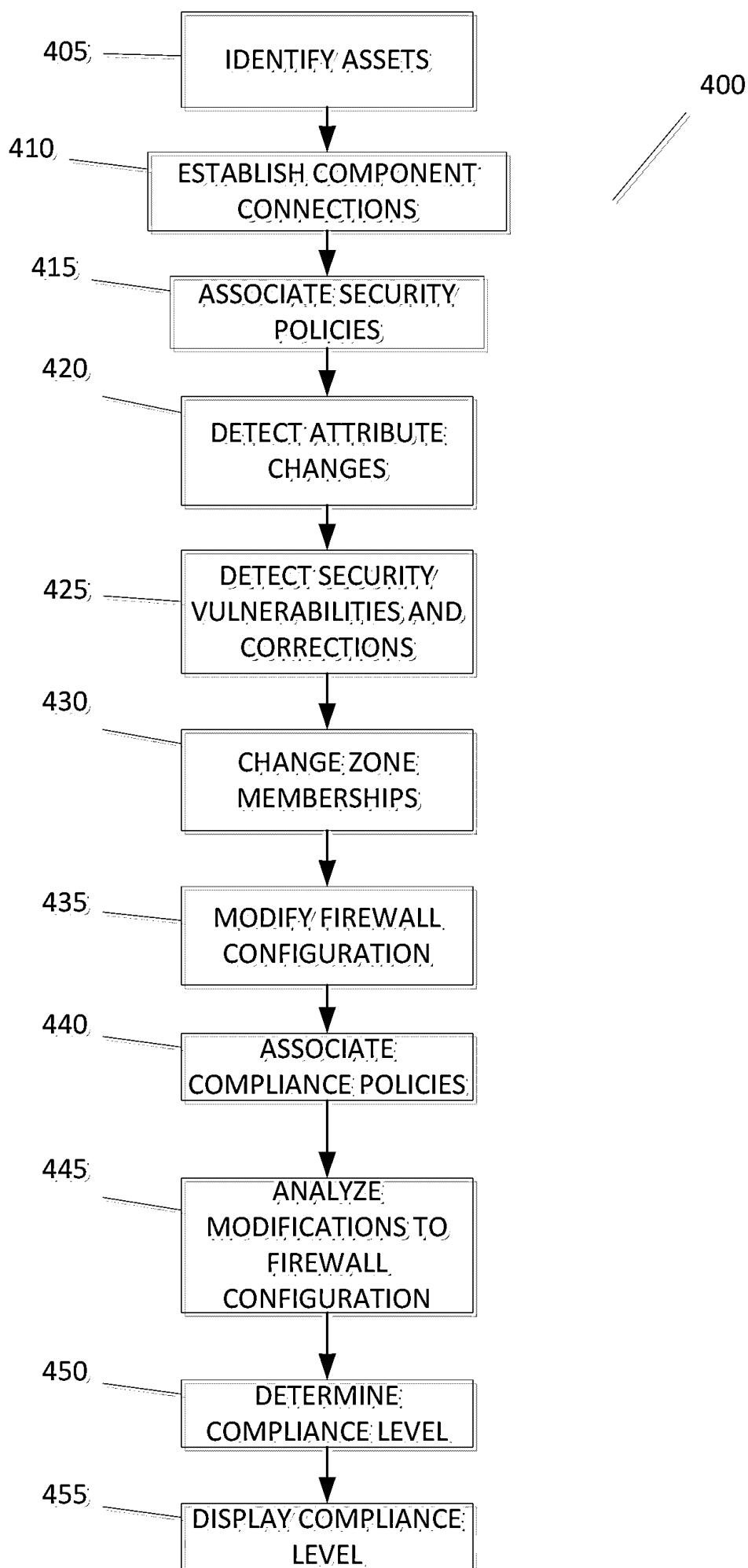
Family 14/50 - FAMPAT - ©Questel

Title

(US9912549)

Systems and methods for network analysis and reporting

Images



Publication data including kind & date

US20140359749	A1	2014-12-04	US20140359749				
US9088541	B2	2015-07-21	US9088541				
US20150264012	A1	2015-09-17	US20150264012				
US20160072831	A1	2016-03-10	US20160072831				
US9509660	B2	2016-11-29	US9509660				
US20170048268	A1	2017-02-16	US20170048268				
US9749351	B2	2017-08-29	US9749351				
US20180020019	A1	2018-01-18	US20180020019				
US9912549	B2	2018-03-06	US9912549				

Abstract

(US9912549)

Among other things, embodiments of the present disclosure can collect and analyze asset and network data from multiple sources, and use such data to present a more complete and accurate representation of the network connections between various systems and software applications and the policies dictating the operation of security controls on a network compared to conventional systems.

Inventors

RIEKE MALCOLM

Latest standardized assignees - inventors removed

CATBIRD NETWORKS

Publication dates

2014-12-04

2015-07-21

2015-09-17

2016-03-10

2016-11-29

2017-02-16

2017-08-29

2018-01-18

2018-03-06

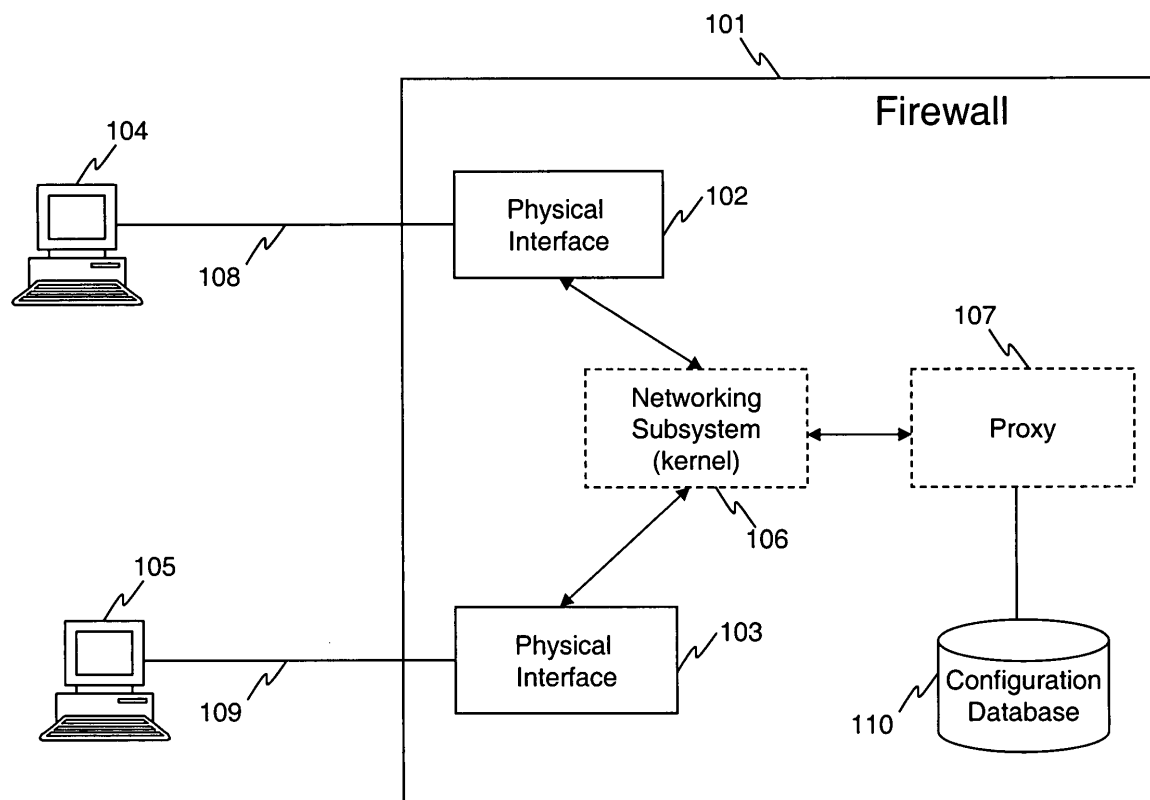
Family 15/50 - FAMPAT - ©Questel

Title

(US9762540)

Policy based content filtering

Images



Publication data including kind & date

US20070118893	A1	2007-05-24	US20070118893
CN1972297	A	2007-05-30	CN1972297
CN1972297	B	2011-02-09	CN1972297B
US7966654	B2	2011-06-21	US7966654
US20110225646	A1	2011-09-15	US20110225646
US8205251	B2	2012-06-19	US8205251
US20120254978	A1	2012-10-04	US20120254978
US8656479	B2	2014-02-18	US8656479
US20140090014	A1	2014-03-27	US20140090014
US20140090013	A1	2014-03-27	US20140090013
US8813215	B2	2014-08-19	US8813215
US20140351918	A1	2014-11-27	US20140351918
US20150312220	A1	2015-10-29	US20150312220
US9729508	B2	2017-08-08	US9729508
US9762540	B2	2017-09-12	US9762540



Abstract

(US9762540)

Methods and systems for processing application-level content of network service protocols are described. According to one embodiment, a network connection is received at a networking subsystem of a firewall. The connection is characterized by a source IP address, a destination IP address and a network service protocol. The network service protocol of the network connection is determined. A matching firewall policy is identified for the connection. When the connection is allowed, it is redirected to a proxy module that is configured to support the network service protocol. A content processing configuration scheme identified by the matching firewall policy is retrieved that includes multiple content processing configuration settings, specifying whether a particular type of content filtering is to be performed, for each of multiple network service protocols. Application-level content of a packet stream associated with the network connection is reconstructed and filtered based on the applicable content processing configuration settings.

Inventors

CRAWFORD WILLIAM J

Latest standardized assignees - inventors removed

FORTINET

Publication dates

2007-05-24

2007-05-30

2011-02-09

2011-06-21

2011-09-15

2012-06-19

2012-10-04

2014-02-18

2014-03-27

2014-03-27

2014-08-19

2014-11-27

2015-10-29

2017-08-08

2017-09-12

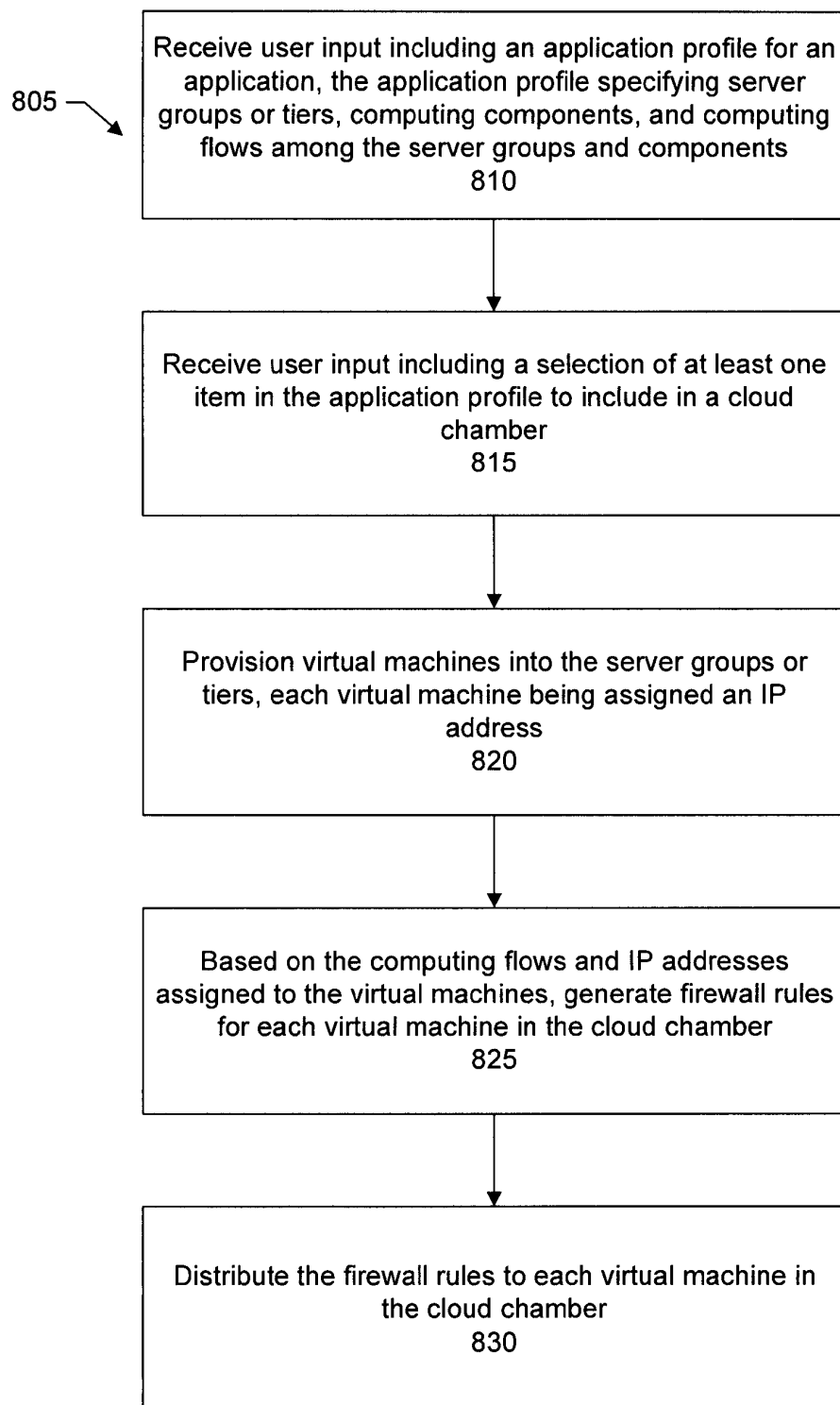
Family 16/50 - FAMPAT - ©Questel

Title

(US9634990)

Distributed firewall security system for cloud computing environments

Images

**Publication data including kind & date**

US20140245423	A1	2014-08-28	US20140245423
US9130901	B2	2015-09-08	US9130901
US20150341318	A1	2015-11-26	US20150341318
US9634990	B2	2017-04-25	US9634990

**Abstract**

(US9634990)

An application profile specifies server groups, components, and computing flows among the server groups and components. Each computing flow may be identified as malicious or not malicious. Firewall rules are generated based on the computing flows. The firewall rules are distributed to a server group. According to the firewall rules distributed to the server group, data that is malicious is directed to another server for quarantine.

Inventors

LEE JAUSHIN

Latest standardized assignees - inventors removed

ZENTERA SYSTEMS

Publication dates

2014-08-28

2015-09-08

2015-11-26

2017-04-25

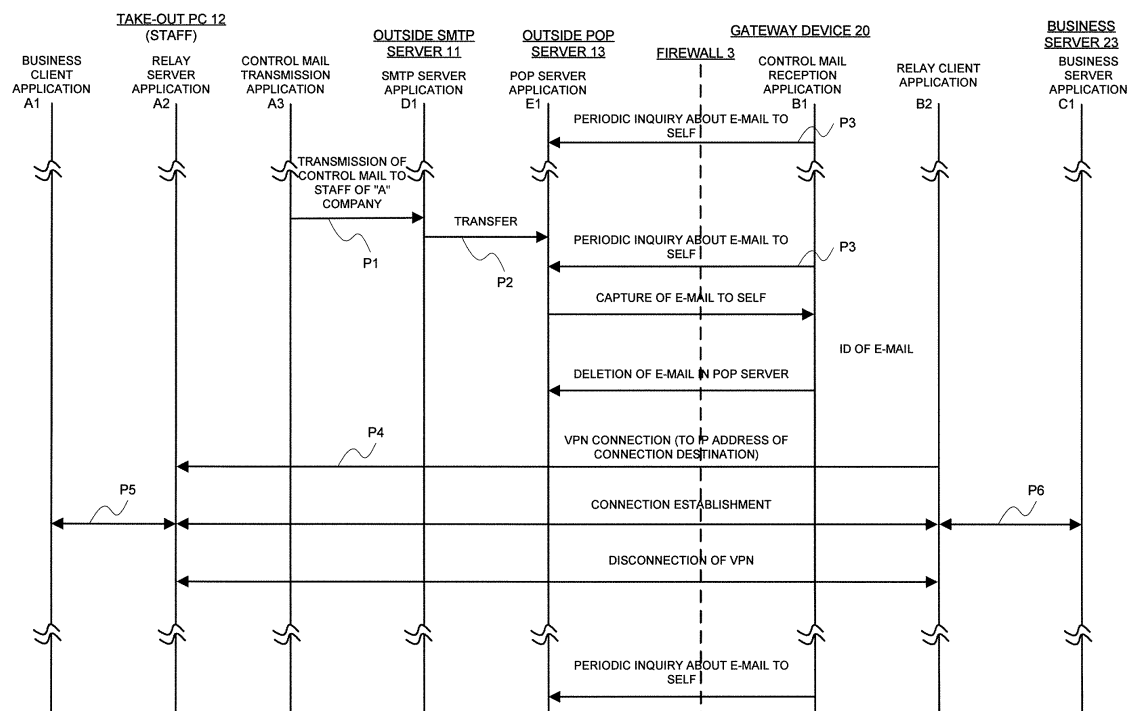
Family 17/50 - FAMPAT - ©Questel

Title

(WO200611464)

Connection method, communication system, device, and program

Images



Publication data including kind & date

WO2006011464	A1	2006-02-02	WO200611464
TW200620913	A	2006-06-16	TW200620913
CN1981496	A	2007-06-13	CN1981496
US20080098472	A1	2008-04-24	US20080098472
JPWO2006011464	A1	2008-05-01	JP2006011464W
JP4352275	B2	2009-10-28	JP4352275
US9088547	B2	2015-07-21	US9088547
CN1981496	B	2016-09-14	CN1981496B



Abstract

(WO200611464)

There are provided a VPN connection method and a communication system capable of communicating from outside to inside of a firewall without requiring setting of a firewall or installation of a relay server. In an internal network (2) connected to an external network (1) via a firewall (3), it is possible to perform communication by an e-mail from the external network (out of the firewall) (1) to a mail server (21) of the internal network (inside the firewall) (2), a telephone, a radio communication, or the like not via the firewall (3). Moreover, although access from out of the firewall to the inside of the firewall by the VPN connection is very difficult, a reverse access can easily be performed. By utilizing this characteristic of the firewall (3), the internal network (2) can receive an e-mail requesting VPN connection from the external network (1) and control information from a telephone line, so that the internal network (2) performs call back performing VPN to the transmission origin of the e-mail or the like. As a result, it is possible to pass through the firewall (3) from the external network (2).

Inventors

ENOMOTO NOBUYUKI

HIDAKA YOUICHI

YOSHIMI HIDEO

IWATA ATSUSHI

ARUTAKI AKIRA

Latest standardized assignees - inventors removed

NEC

Publication dates

2006-02-02

2006-06-16

2007-06-13

2008-04-24

2008-05-01

2009-10-28

2015-07-21

2016-09-14

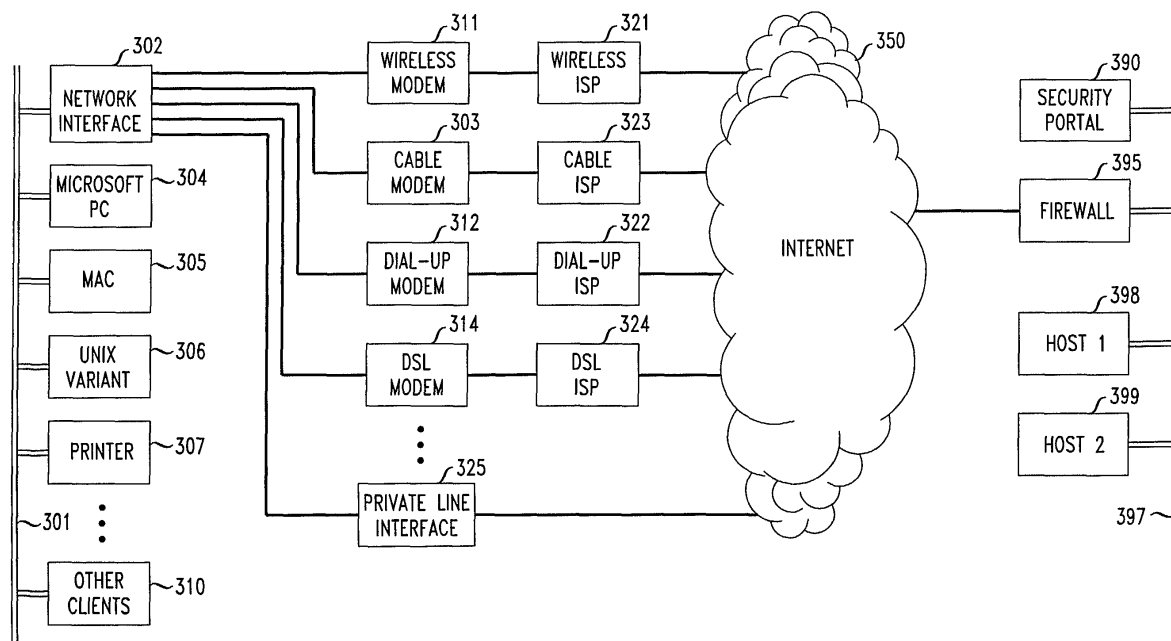
Family 18/50 - FAMPAT - ©Questel

Title

(US7827278)

System for automated connection to virtual private networks related applications

Images



Publication data including kind & date

CA2394455	A1	2003-01-23	CA2394455
US20030200321	A1	2003-10-23	US20030200321
CA2394455	C	2007-06-19	CA2394455
US7827278	B2	2010-11-02	US7827278



Abstract

(US7827278)

A network interface unit is provided for use intermediate a LAN and a public or private network, or a combination of both, for establishing secure links to a VPN gateway. Login by a LAN client with the network interface unit, addressing, authentication, and other configuration operations achieved using a web page-based GUI are applied in establishing tunnels from LAN clients to desired VPN destinations. Illustrative network interface units include a DHCP server and provide encryption-decryption and encapsulation-decapsulation of data packets for communication with VPN nodes. Configuration and connection of a client are further enhanced by a built-in DNS server and other functional servers to provide a high degree of autonomy in establishing connections to a desired VPN gateway via an ISP or other public and/or private network links to. The interface unit then performs required authentication exchanges, and required encryption key exchanges.

Inventors

CHEN YIHSIU
 FOLADARE MARK JEFFREY
 GOLDMAN SHELLEY B
 KILLIAN THOMAS JOSEPH
 SCHRYER NORMAN LOREN
 STONE KEVIN
 WEBER ROY PHILIP

Latest standardized assignees - inventors removed

AT&T

Publication dates

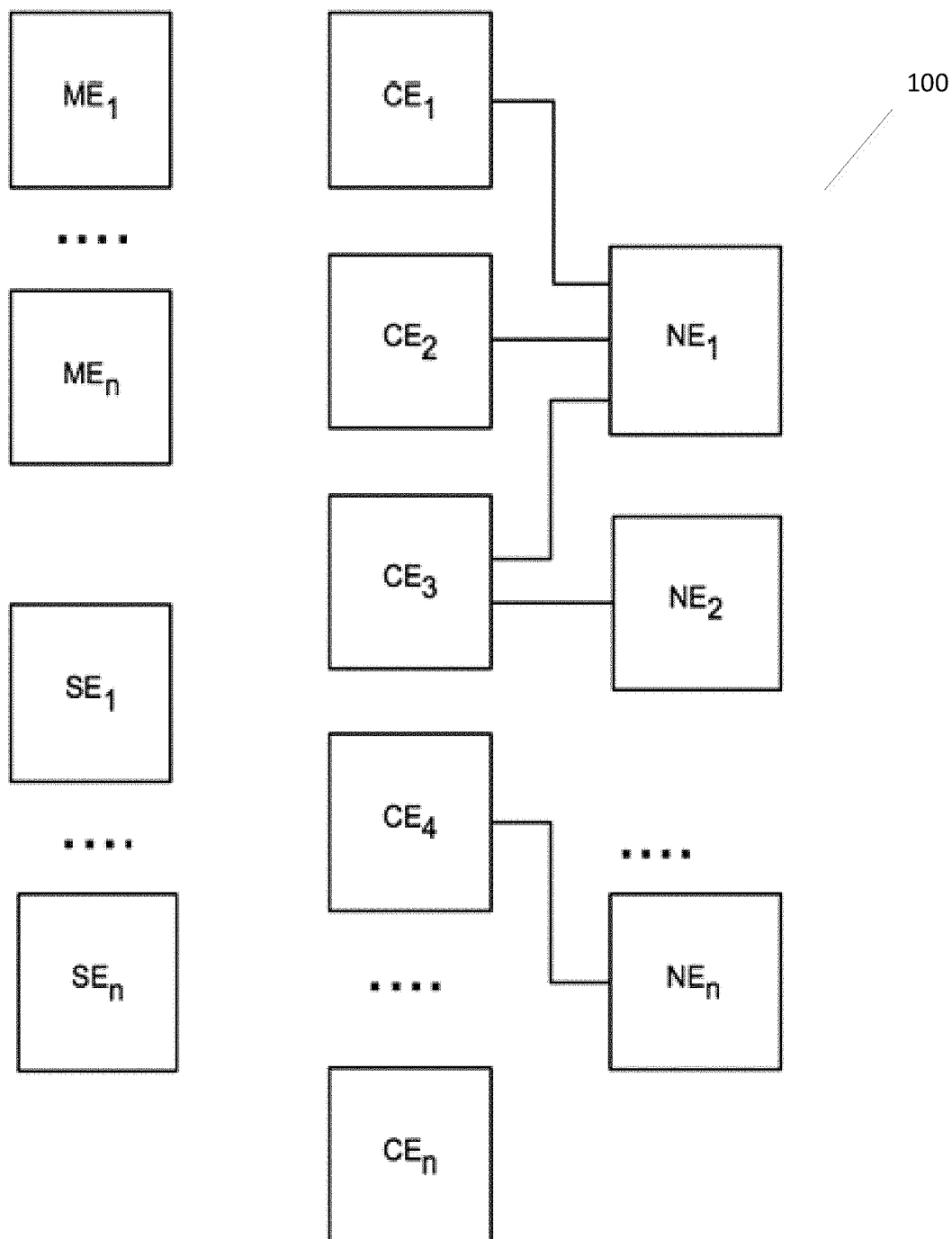
2003-01-23
 2003-10-23
 2007-06-19
 2010-11-02

Family 19/50 - FAMPAT - ©Questel

Title

(US9769174)

Systems and methods for creating and modifying access control lists

Images**Publication data including kind & date**[US20160072815](#) A1 2016-03-10 US20160072815[US9769174](#) B2 2017-09-19 US9769174**Abstract**

(US9769174)

Embodiments of the present disclosure can present information on services hosted and used by various assets on a network, and allow users to control access to such services. In particular, embodiments of the disclosure may be used to

present one or more services hosted by a network asset, and control access to such services by other network assets based on user input.

Inventors

RIEKE MALCOLM

DENNIS JAMES SEBASTIAN

Latest standardized assignees - inventors removed

CATBIRD NETWORKS

Publication dates

2016-03-10

2017-09-19

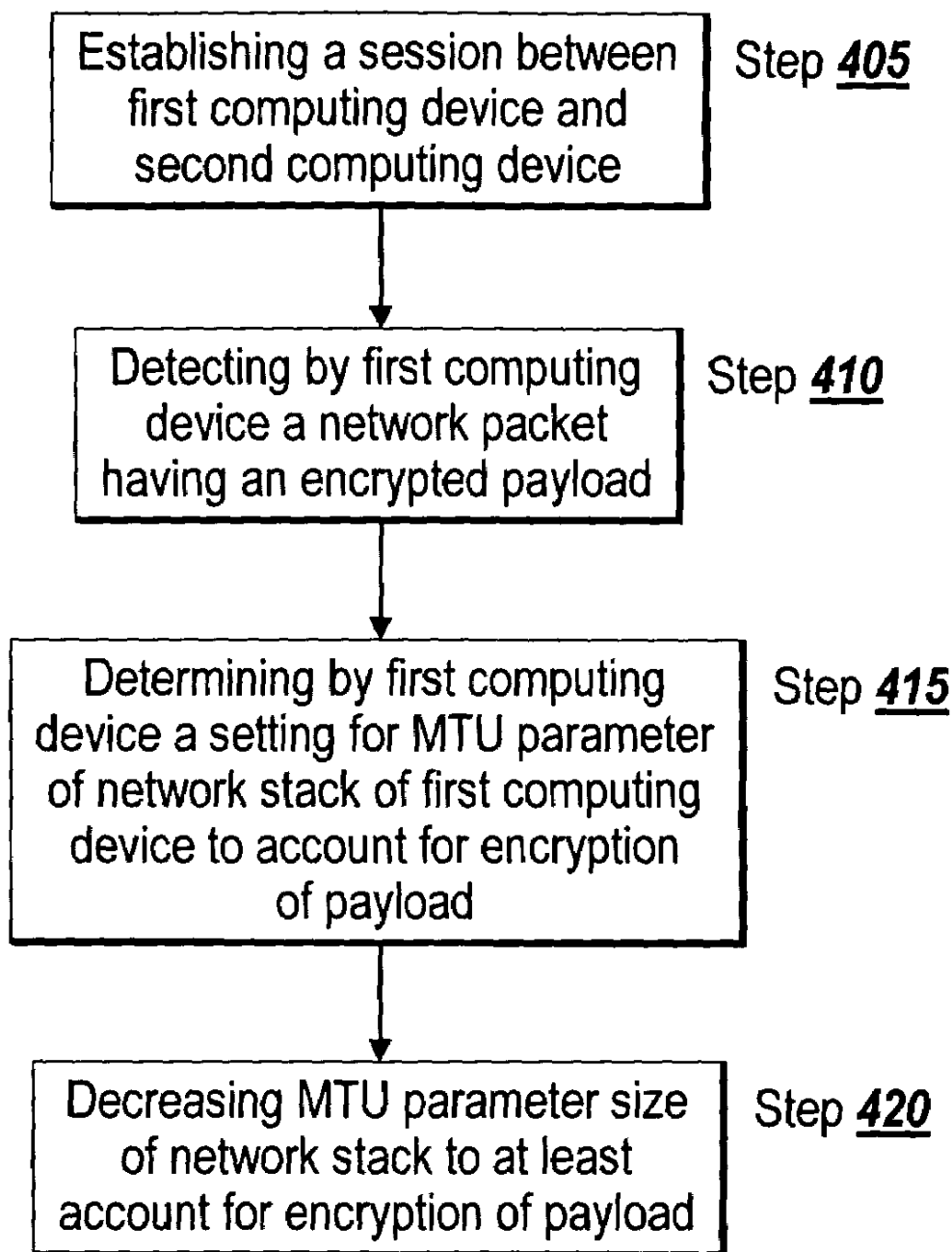
Family 20/50 - FAMPAT - ©Questel

Title

(EP2744175)

Systems and methods for optimizing communications between network nodes

Images

400**Publication data including kind & date**

WO2006012610	A2	2006-02-02	WO200612610
CA2574776	A1	2006-02-02	CA2574776
AU2005266943	A1	2006-02-02	AU2005266943
US20060037072	A1	2006-02-16	US20060037072
US20060039356	A1	2006-02-23	US20060039356
US20060039354	A1	2006-02-23	US20060039354
US20060039355	A1	2006-02-23	US20060039355
US20060039404	A1	2006-02-23	US20060039404
WO2006012610	A3	2006-03-16	WO200612610
US20060190719	A1	2006-08-24	US20060190719
EP1771998			



	A2	2007-04-11	EP1771998				
KR20070045282	A	2007-05-02	KR20070045282				
IL180891	A	2007-07-04	IL-180891				
IN0648/KOLNP/2007	A	2007-07-06	IN2007KN00648				
JP2008507928	A	2008-03-13	JP2008507928				
US7609721	B2	2009-10-27	US7609721				
US20100005288	A1	2010-01-07	US20100005288				
US7724657	B2	2010-05-25	US7724657				
AU2005266943	B2	2010-06-10	AU2005266943				
US20100232429	A1	2010-09-16	US20100232429				
AU2010214746	A1	2010-09-23	AU2010214746				
US7808906	B2	2010-10-05	US7808906				
AU2010214746	B2	2010-11-11	AU2010214746				
US20100325299	A1	2010-12-23	US20100325299				
AU2005266943	C1	2011-01-06	AU2005266943				
US8014421	B2	2011-09-06	US8014421				
US8046830	B2	2011-10-25	US8046830				
US8351333	B2	2013-01-08	US8351333				
US8634420	B2	2014-01-21	US8634420				
EP2744175	A1	2014-06-18	EP2744175				
IN263485	B	2014-10-31	IN-263485				
US8914522	B2	2014-12-16	US8914522				
EP1771998	B1	2015-04-15	EP1771998				
US9219579	B2	2015-12-22	US9219579				
HK1108985	A1	2016-01-29	HK1108985				
EP2744175	B1	2018-09-05	EP2744175				

Abstract

(EP2744175)

The present invention is generally directed towards a remote access architecture for providing peer-to-peer communications and remote access connectivity. In one embodiment, the remote access architecture of the present provides a method for establishing a direct connection between peer computing devices via a third computing device, such as a gateway.; Additionally, the present invention provides the following techniques to optimize peer-to-peer communications: 1) false acknowledgement of receipt of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 2) payload shifting of network packets allowing communications via a lossless protocol of packets constructed for transmission via a lossy protocol, 3) reduction of packet fragmentation by adjusting the maximum transmission unit (MTU) parameter, accounting for overhead due to encryption, 4) application-aware prioritization of client-side network communications, and 5) network disruption shielding for reliable and persistent network connectivity and access.

Inventors

RAO GOUTHAM P

BRUEGGEMANN ERIC

RODRIGUEZ ROBERT

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2006-02-02

2006-02-02

2006-02-02

2006-02-16
2006-02-23
2006-02-23
2006-02-23
2006-02-23
2006-03-16
2006-08-24
2007-04-11
2007-05-02
2007-07-04
2007-07-06
2008-03-13
2009-10-27
2010-01-07
2010-05-25
2010-06-10
2010-09-16
2010-09-23
2010-10-05
2010-11-11
2010-12-23
2011-01-06
2011-09-06
2011-10-25
2013-01-08
2014-01-21
2014-06-18
2014-10-31
2014-12-16
2015-04-15
2015-12-22
2016-01-29
2018-09-05

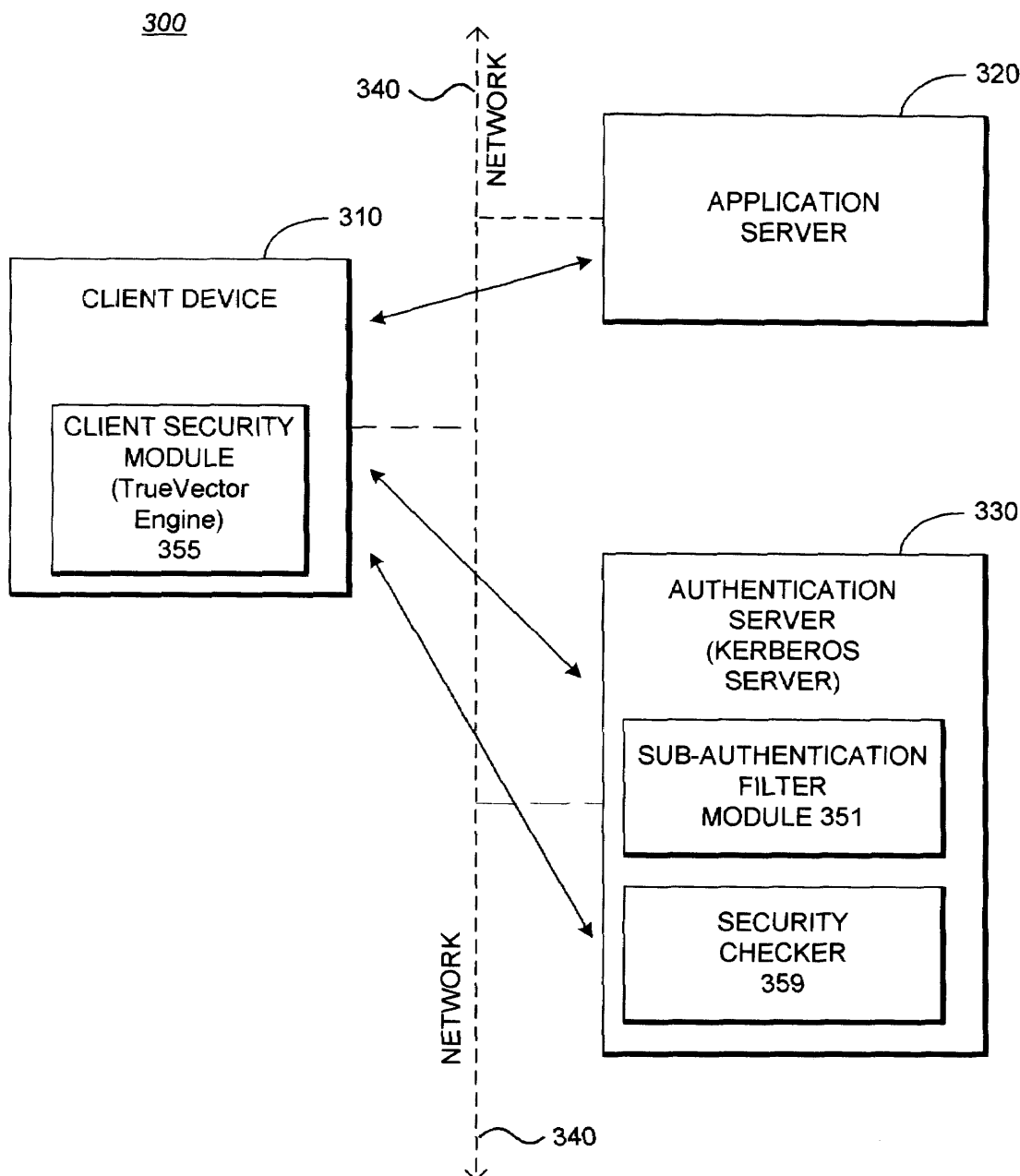
Family 21/50 - FAMPAT - ©Questel

Title

(US7590684)

System providing methodology for access control with cooperative enforcement

Images

**Publication data including kind & date**

US20040167984	A1	2004-08-26	US20040167984
US7590684	B2	2009-09-15	US7590684

**Abstract**

(US7590684)

A system providing methodology for access control with cooperative enforcement is described. In one embodiment, for example, a method is described for authorizing a client to access a service based on compliance with a policy required for access to the service, the method comprises steps of: specifying a policy required for access to the service; detecting a request for access to the service from a client; attempting authentication of the client based on credentials presented by the client; if the client is authenticated based on the credentials, determining whether the client is in compliance with the policy based, at least in part, on attributes of the client; and if the client is determined to be in compliance with the policy, providing access to the service.

Inventors

HERRMANN CONRAD K

Latest standardized assignees - inventors removed

CHECK POINT SOFTWARE TECHNOLOGIES

Publication dates

2004-08-26

2009-09-15

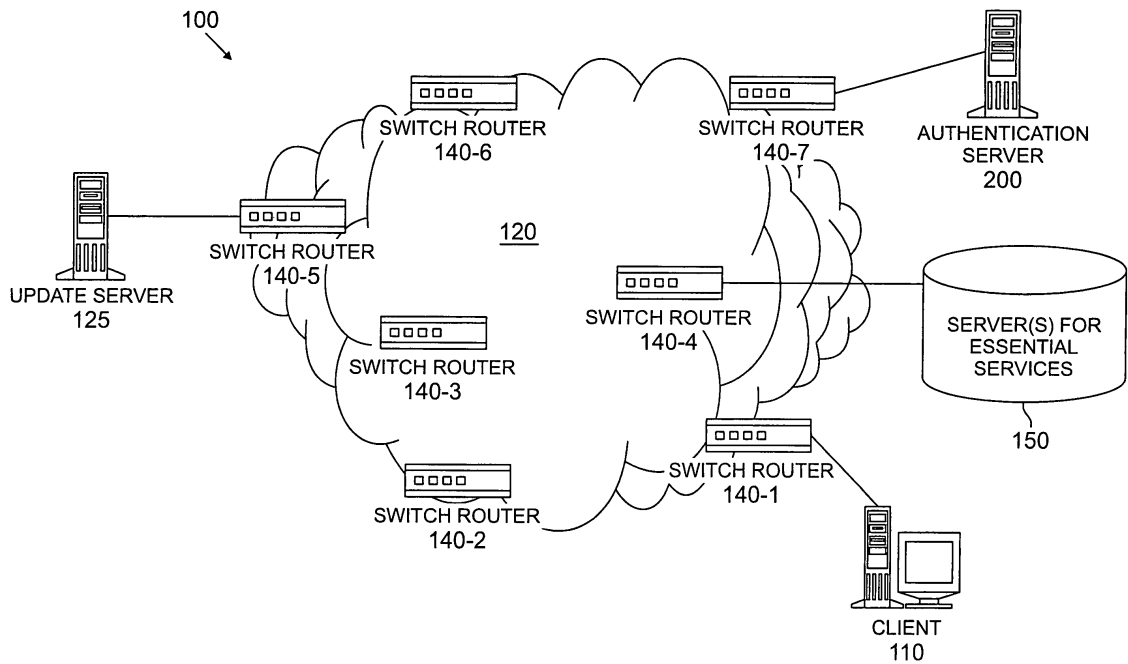
Family 22/50 - FAMPAT - ©Questel

Title

(EP1956463)

Method and apparatus for providing network security based on device security status

Images



Publication data including kind & date

CA2497950	A1	2005-10-26	CA2497950
EP1591868	A1	2005-11-02	EP1591868
US20050246767	A1	2005-11-03	US20050246767
JP2005318584	A	2005-11-10	JP2005318584
KR20060046704	A	2006-05-17	KR20060046704
EP1591868	B1	2008-05-14	EP1591868
DE602005006658	D1	2008-06-26	DE602005006658
EP1956463	A2	2008-08-13	EP1956463
EP1956463	A3	2008-08-20	EP1956463
US8230480	B2	2012-07-24	US8230480



Abstract

(EP1956463)

A method and apparatus are provided for network security based on a security status of a device. A security update status of a device is evaluated; and one or more of a plurality of security policies are selected to apply to the device based on the security update status. The available security philosophies may include, for example, a "protect the good" philosophy, an "encourage the busy" philosophy and a "shut off the non-compliant" philosophy. The security update status can evaluate, for example, a version level of one or more security features installed on the device or can be based on a flag indicating whether the device satisfies predefined criteria for maintaining one or more computer security protection features up-to-date. Further disclosed is a communication method for controlling access to a network service, characterized by: controlling access to one or more network services based on a list of authorized users of said one or more network services; and broadcasting a message based on said list of authorized users.

Inventors

FAZAL LOOKMAN Y

KAPPES MARTIN

KRISHNAKUMAR ANJUR S

KRISHNAN P

Latest standardized assignees - inventors removed

OCTEL COMMUNICATIONS

AVAYA

AVAYA INTEGRATED CABINET SOLUTIONS

ZANG

SIERRA HOLDINGS

Publication dates

2005-10-26

2005-11-02

2005-11-03

2005-11-10

2006-05-17

2008-05-14

2008-06-26

2008-08-13

2008-08-20

2012-07-24

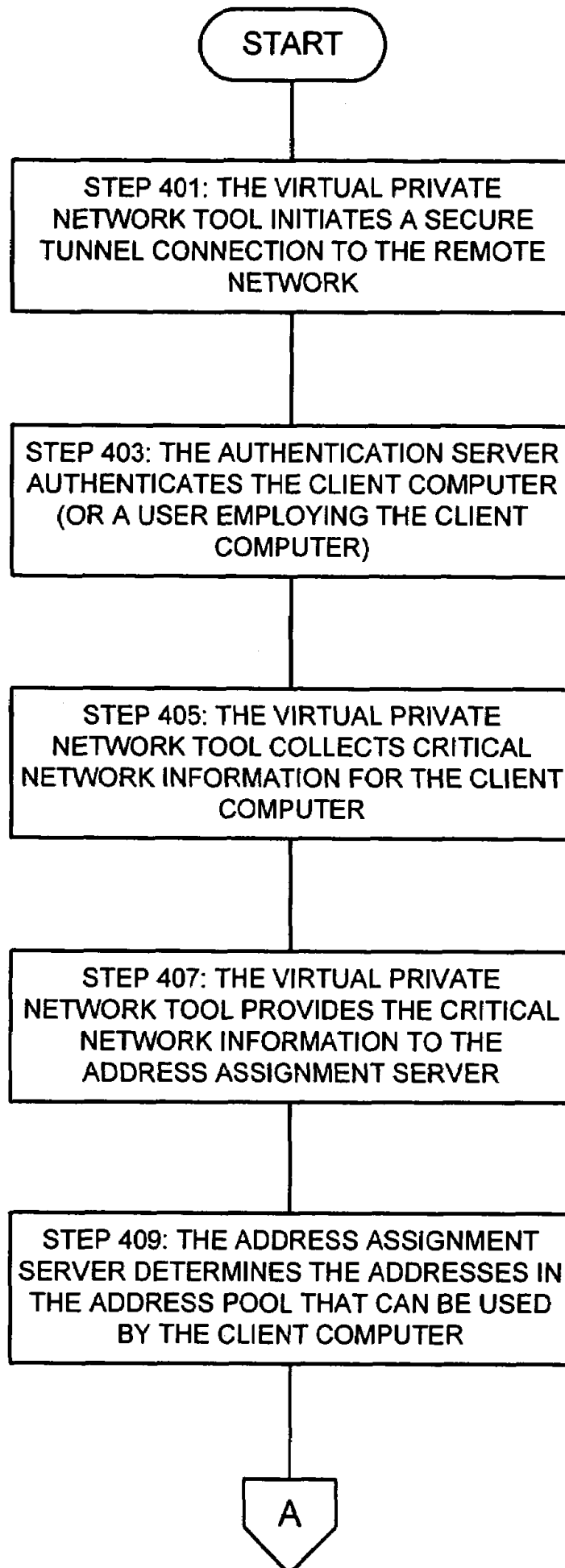
Family 23/50 - FAMPAT - ©Questel

Title

(WO200696875)

Smart tunneling to resources in a remote network

Images



Publication data including kind & date

WO2006096875	A1	2006-09-14	WO200696875				
US20080162726	A1	2008-07-03	US20080162726				
US7698388	B2	2010-04-13	US7698388				
US20100121943	A1	2010-05-13	US20100121943				
US20110167475	A1	2011-07-07	US20110167475				
US8090827	B2	2012-01-03	US8090827				
US9407456	B2	2016-08-02	US9407456				
US20160323286	A1	2016-11-03	US20160323286				

Abstract

(WO200696875)

A client computer (301) hosts a virtual private network tool (311) to establish a virtual private network connection with a remote network. Upon startup, the virtual private network tool collects critical network information for the client computer (405), and sends this critical network information to an address assignment server (319) in the remote network (407). The address assignment server compares the critical network information with a pool of available addresses (325) in the remote network (409), and assigns addresses for use by the client computer that do not conflict with the addresses for local resources. The address assignment server also provides routing information for resources in the remote network to the virtual private network tool (417). The virtual private network tool will postpone loading this routing information into the routing tables (315) of the client computer until the client computer requests access to a specific resource in the remote network. When the client computer requests access to a specific resource in the remote network (601), the virtual private network tool will only provide the routing table with the routing information for that specific remote resource.

Inventors

HOPEN CHRIS A

TOMLINSON GARY B

Latest standardized assignees - inventors removed

DELL

DELL SOFTWARE

SONICWALL US HOLDINGS

AVENTAIL

QUEST SOFTWARE

Publication dates

2006-09-14

2008-07-03

2010-04-13

2010-05-13

2011-07-07

2012-01-03

2016-08-02

2016-11-03

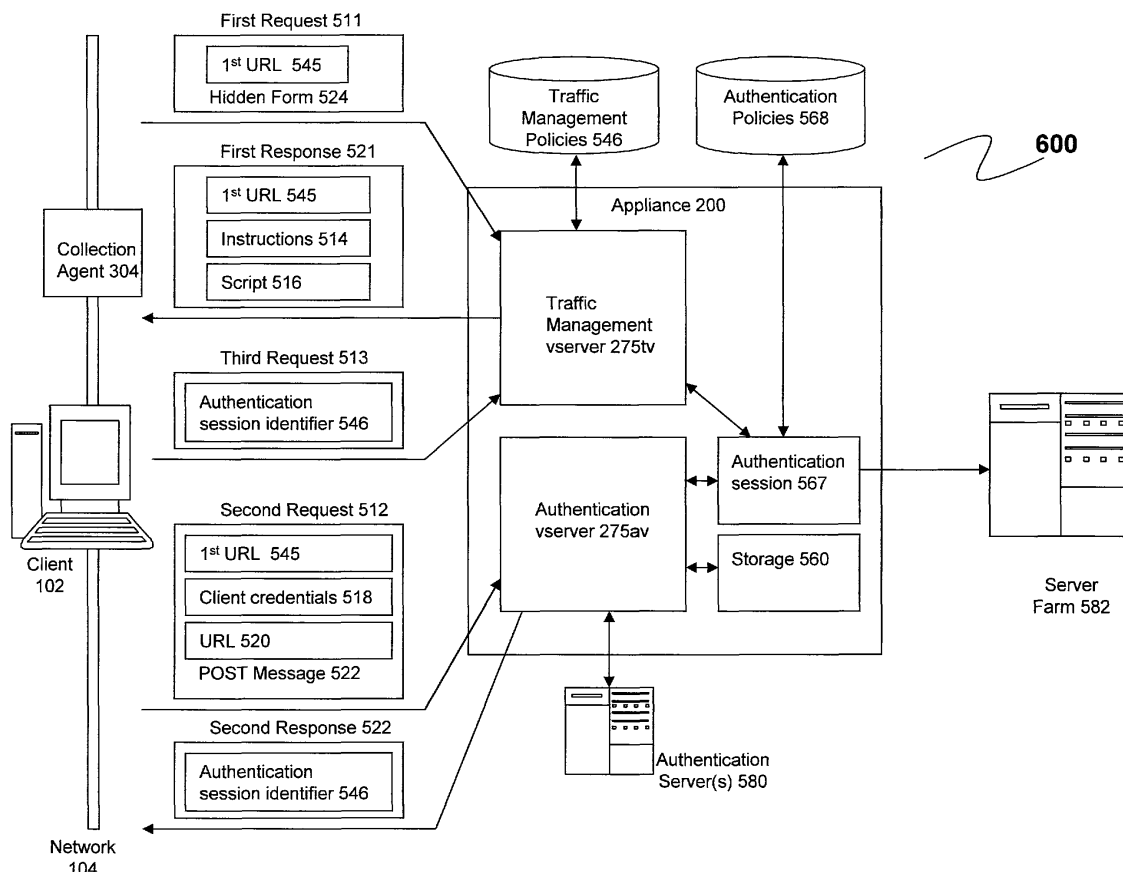
Family 24/50 - FAMPAT - ©Questel

Title

(EP2409472)

Systems and methods for using end point auditing in connection with traffic management

Images



Publication data including kind & date

WO2010107558	A1	2010-09-23	WO2010107558
US20100242106	A1	2010-09-23	US20100242106
US20100242092	A1	2010-09-23	US20100242092
US20100242105	A1	2010-09-23	US20100242105
EP2409472	A1	2012-01-25	EP2409472
CN102577302	A	2012-07-11	CN102577302
US8392982	B2	2013-03-05	US8392982
US8782755	B2	2014-07-15	US8782755
US8844040	B2	2014-09-23	US8844040
US20140359728	A1	2014-12-04	US20140359728
CN102577302	B	2015-11-25	CN102577302B
US9264429	B2	2016-02-16	US9264429



Abstract

(EP2409472)

The present invention provides a system and method of managing traffic traversing an intermediary based on a result of end point auditing. An authentication virtual server of an intermediary may determine a result of an end point analysis scan of a client. Responsive to the determination, the traffic management virtual server can obtain the result from the authentication virtual server. Further, the traffic management virtual server may apply the result in one or more traffic management policies to manage network traffic of a connection of the client traversing the intermediary. In some embodiments, the authentication virtual server may receive one or more expressions evaluated by the client. The one or more expressions identifies one or more attributes of the client. The traffic management virtual server can also determine a type of compression or encryption for the connection based on applying the one or more traffic management policies using the result.

Inventors

HARRIS JAMES

LI RAYMOND

KUMAR ARKESH

THAKUR RAVINDRANATH

AGARWAL PUNEET

CHOUDHARY AKSHAT

GUPTA PUNIT

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2010-09-23

2010-09-23

2010-09-23

2010-09-23

2012-01-25

2012-07-11

2013-03-05

2014-07-15

2014-09-23

2014-12-04

2015-11-25

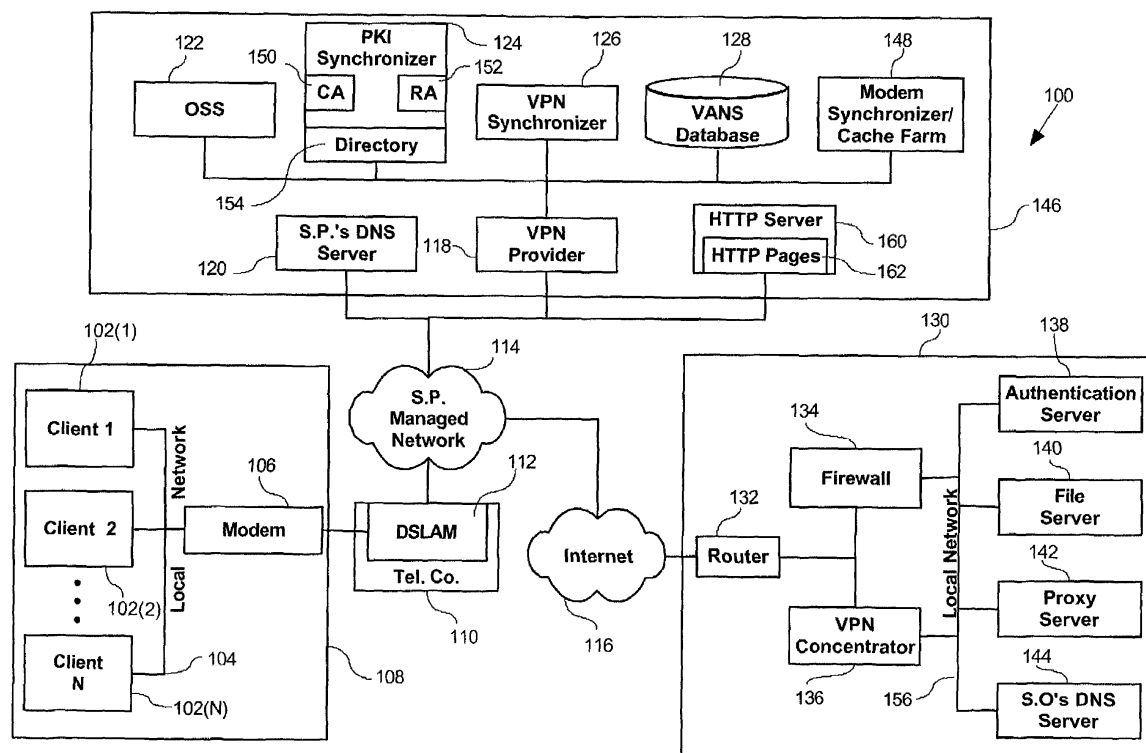
2016-02-16

Family 25/50 - FAMPAT - ©Questel

Title

(US7197550)

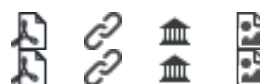
Automated configuration of a virtual private network

Images**Publication data including kind & date**

US20030041136

A1 2003-02-27

US20030041136



[US7197550](#)

B2 2007-03-27 US7197550

Abstract

(US7197550)

Data is received by a service provider that is indicative of a selected server-side system and a selected client-side system between which a VPN is to be established. Security settings are then automatically determined for the client-side system based at least partially on the data. The security settings are preferably public and private keys and/or a Digital Certificate. VPN configuration details, including the security settings, are then automatically transmitted to the client-side system. The client side system then uses the configuration details to automatically configure itself to establish a secure VPN tunnel between the server-side system and itself. VPN configuration details may also be automatically transmitted to a VPN concentrator within the server-side system. A Virtual Private Network tunnel is subsequently established between the client-side system and the server-side system, and the tunnel's operation verified. A computer program product for configuring a VPN system is also provided.

Inventors

CHELINE DOUGLAS A

MA MICHAEL

ZHANG YE

CHONG LESTER J

Latest standardized assignees - inventors removed

HUGHES ELECTRONICS

Publication dates

2003-02-27

2007-03-27

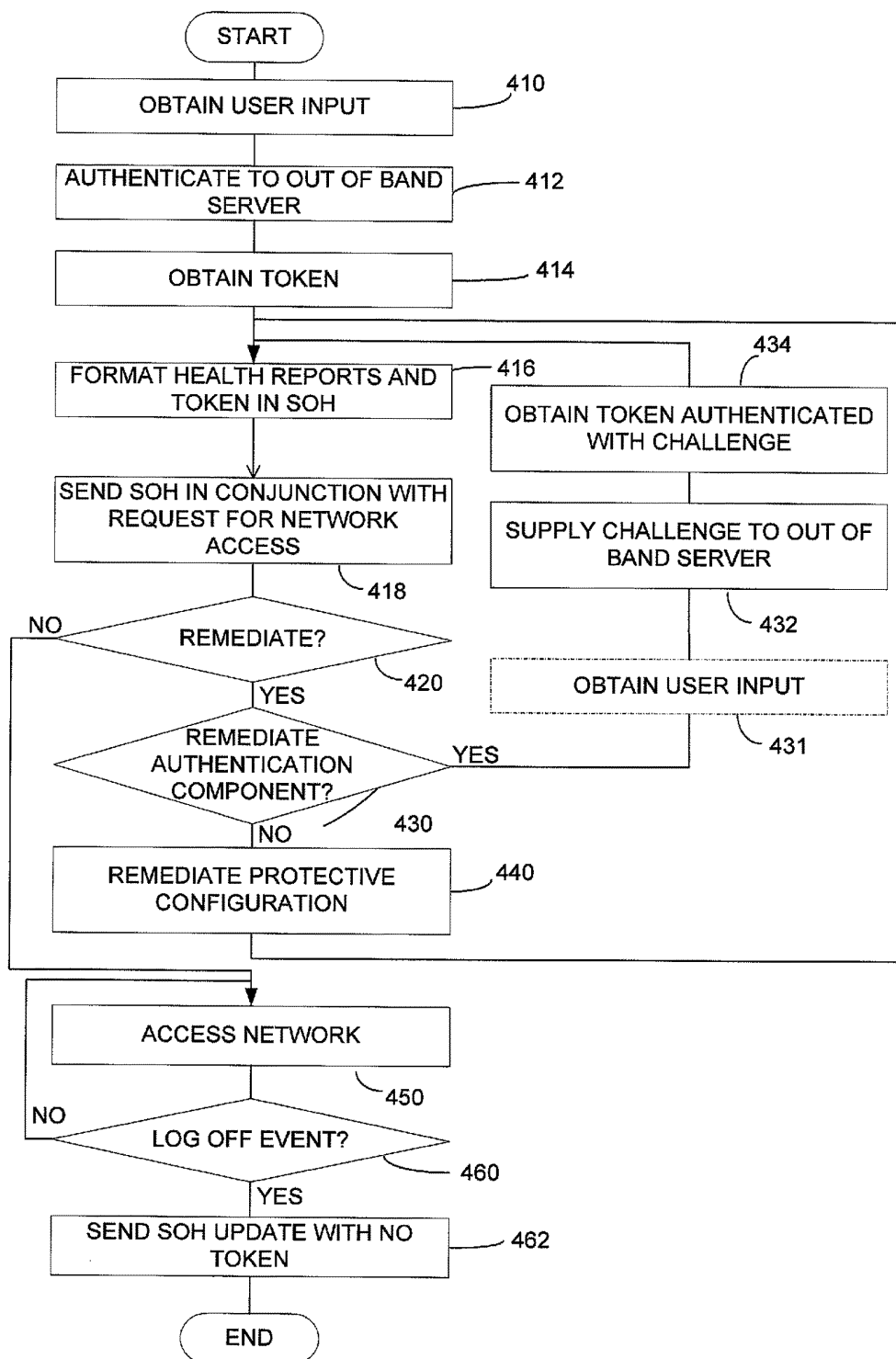
Family 26/50 - FAMPAT - ©Questel

Title

(EP2321928)

Authentication in a network using client health enforcement framework

Images



Publication data including kind & date

US20100115578	A1	2010-05-06	US20100115578
WO2010062491	A2	2010-06-03	WO201062491
WO2010062491	A3	2010-07-29	WO201062491
EP2321928	A2	2011-05-18	EP2321928
CN102204159	A	2011-09-28	CN102204159
EP2321928	A4	2012-02-22	EP2321928
JP2012507972	A	2012-03-29	JP2012507972
JP5519686	B2	2014-06-11	JP5519686
CN102204159	B	2014-12-17	CN102204159B



US9443084

B2 2016-09-13 US9443084

Abstract

(EP2321928)

A network with authentication implemented using a client health enforcement framework. The framework is adapted to receive plug-ins on clients that generate health information. Corresponding plug-ins on a server validate that health information. Based on the results of validation, the server may instruct the client to remediate or may authorize an underlying access enforcement mechanism to allow access. A client plug-in that generates authentication information formatted as a statement of health may be incorporated into such a framework. Similarly, on the server, a validator to determine, based on the authentication information, whether the client should be granted network access can be incorporated into the framework. Authentication can be simply applied or modified by changing the plug-ins, while relying on the framework to interface with an enforcement mechanism. Functions of the health enforcement framework can be leveraged to provide authentication-based functionality.

Inventors

NICE NIR

EYAL ANAT

NUKALA CHANDRASEKHAR

ADDAGATLA SREENIVAS

NEYSTADT EUGENE

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2010-05-06

2010-06-03

2010-07-29

2011-05-18

2011-09-28

2012-02-22

2012-03-29

2014-06-11

2014-12-17

2016-09-13

Family 27/50 - FAMPAT - ©Questel

Title

(WO200681237)

Enabling dynamic authentication with different protocols on the same port for a switch

Images



[US9374353](#)

B2 2016-06-21 US9374353

[US20170019427](#)

A1 2017-01-19 US20170019427

**Abstract**

(WO200681237)

The invention enables a client device that does not support IEEE 802.IX authentication to access at least some resources provided through a switch that supports 802.IX authentication by using dynamic authentication with different protocols. When the client device attempts to join a network, the switch monitors for an 802.IX authentication message from the client device. In one embodiment, if the client fails to send an 802.IX authentication message, respond to an 802.IX request from the switch, or a predefined failure condition is detected the client may be deemed incapable of supporting 802.IX authentication. In one embodiment, the client may be initially placed on a quarantine VLAN after determination that the client fails to perform an 802.IX authentication within a backoff time limit. However, the client may still gain access to resources based on various non-802.IX authentication mechanisms, including name/passwords, digital certificates, or the like.

Inventors

VANK ALEXANDRU ZSOLT

SHEN XIN

COBB MATT BRIAN

ROBEL-FORREST BRAD

WEBB EVAN MCCLENDON

Latest standardized assignees - inventors removed

MCAFEE

Publication dates

2006-07-27

2006-08-03

2007-11-22

2010-10-05

2010-12-30

2013-08-27

2014-05-01

2016-06-21

2017-01-19

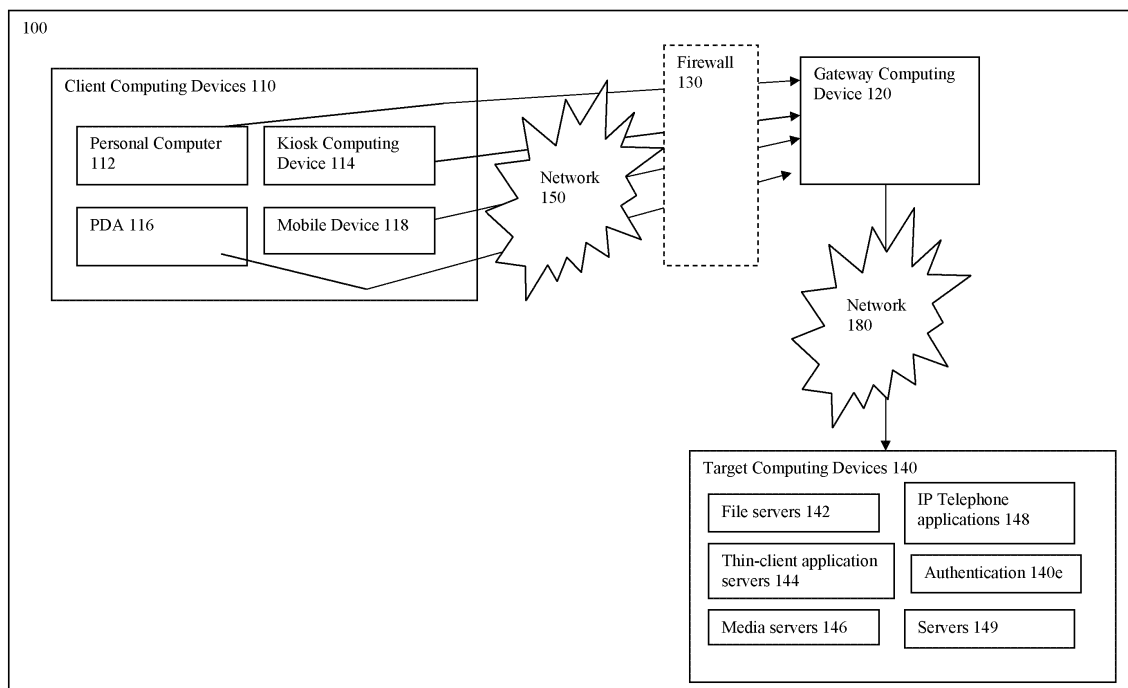
Family 28/50 - FAMPAT - ©Questel

Title

(EP2267951)

Method for routing packets from an endpoint to a gateway

Images



Publication data including kind & date

WO2006012612	A1	2006-02-02	WO200612612
CA2572401	A1	2006-02-02	CA2572401
AU2005266945	A1	2006-02-02	AU2005266945
US20060029063	A1	2006-02-09	US20060029063
US20060029062	A1	2006-02-09	US20060029062
US20060029064	A1	2006-02-09	US20060029064
US20060037071	A1	2006-02-16	US20060037071
KR20070037649	A	2007-04-05	KR20070037649
KR20070037648	A	2007-04-05	KR20070037648
KR20070037650	A	2007-04-05	KR20070037650
EP1771979	A1	2007-04-11	EP1771979
KR20070039597	A	2007-04-12	KR20070039597
IL180405	A	2007-06-03	IL-180405
IL180404	A	2007-06-03	IL-180404
IL180403	A	2007-06-03	IL-180403
IL180402	A	2007-06-03	IL-180402
IN3959/KOLNP/2006	A	2007-06-22	IN2006KN03959
JP2007195217	A	2007-08-02	JP2007195217
JP2007202178	A	2007-08-09	JP2007202178
JP2007215201	A	2007-08-23	JP2007215201
EP1853013	A1	2007-11-07	EP1853013
JP2008507929	A	2008-03-13	JP2008507929
CN101199187	A	2008-06-11	CN101199187
US7606902	B2	2009-10-20	US7606902
US20100002693	A1	2010-01-07	US20100002693
EP2264956	A2	2010-12-22	EP2264956
EP2267951	A2	2010-12-29	EP2267951
EP2264956	A3	2011-01-05	EP2264956
EP2267951	A3	2011-01-12	EP2267951



IL180404	B	2011-05-31	IL-180404				
JP4708376	B2	2011-06-22	JP4708376				
US7978714	B2	2011-07-12	US7978714				
US8019868	B2	2011-09-13	US8019868				
EP1771979	B1	2011-11-23	EP1771979				
AT535078	T	2011-12-15	ATE535078				
HK1102727	A1	2012-07-06	HK1102727				
US8291119	B2	2012-10-16	US8291119				
US20130014206	A1	2013-01-10	US20130014206				
US8363650	B2	2013-01-29	US8363650				
US20130128892	A1	2013-05-23	US20130128892				
US8892778	B2	2014-11-18	US8892778				
US8897299	B2	2014-11-25	US8897299				
EP2267951	B1	2016-12-28	EP2267951				
EP2264956	B1	2017-06-14	EP2264956				
IN290234	B	2017-12-08	IN-290234				

Abstract

(EP2267951)

A method for routing packages from an endpoint (110) to a gateway (120) includes receiving a filtering table from a client application. An outbound packet is intercepted and transmitted to the client application, responsive to the filtering table. The client application transmits the outbound packet to a gateway responsive to an application of a policy to the outbound packet and a routing table. Information about the outbound packet is also transmitted to the client application. The outbound packet is also transmitted to a port monitored by the client application. The method further includes, by the application: authentication of the endpoint to the gateway; encrypting the outbound packet; and establishing a secure sockets layer (SSL) tunnel to the gateway (120). The client application resides on a gateway computing device (120), on a client computing device (110), or on a peripheral device.

Inventors

RAO GOUTHAM P

BRUEGGEMANN ERIC

RODRIGUEZ ROBERT

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2006-02-02

2006-02-02

2006-02-02

2006-02-09

2006-02-09

2006-02-09

2006-02-16

2007-04-05

2007-04-05

2007-04-05

2007-04-11

2007-04-12

2007-06-03

2007-06-03

2007-06-03

2007-06-03
2007-06-22
2007-08-02
2007-08-09
2007-08-23
2007-11-07
2008-03-13
2008-06-11
2009-10-20
2010-01-07
2010-12-22
2010-12-29
2011-01-05
2011-01-12
2011-05-31
2011-06-22
2011-07-12
2011-09-13
2011-11-23
2011-12-15
2012-07-06
2012-10-16
2013-01-10
2013-01-29
2013-05-23
2014-11-18
2014-11-25
2016-12-28
2017-06-14
2017-12-08

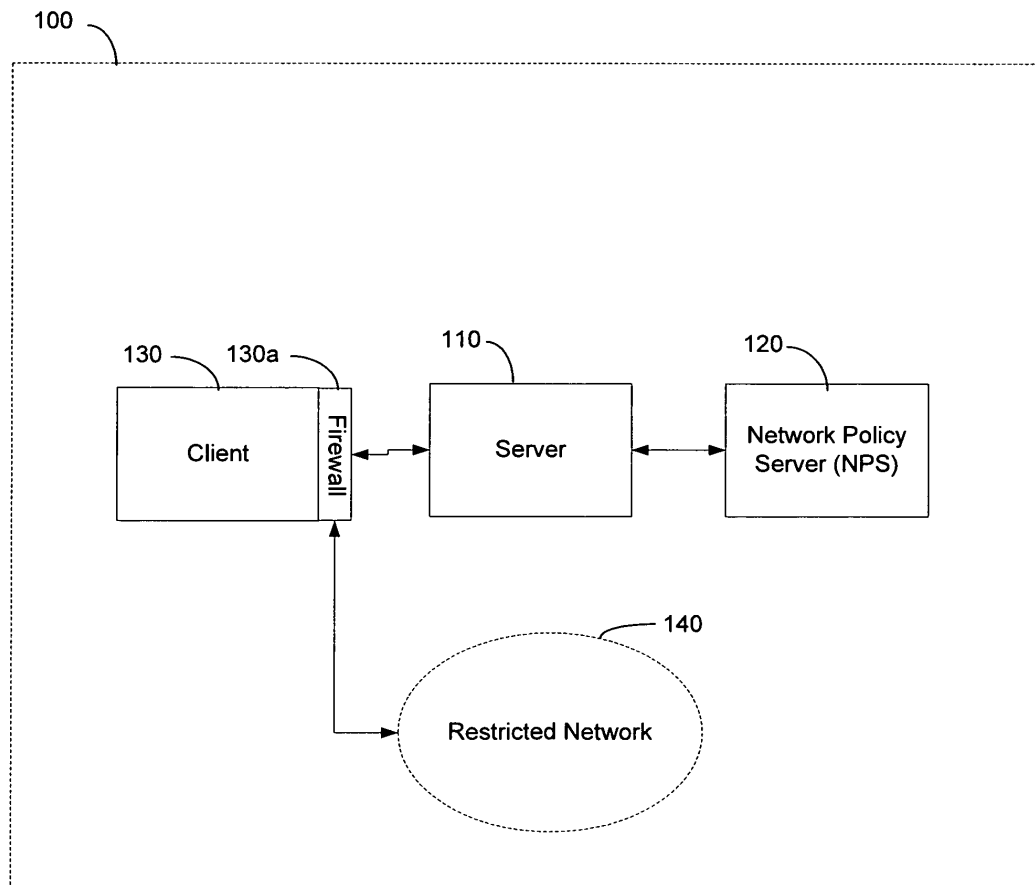
Family 29/50 - FAMPAT - ©Questel

Title

(EP2206291)

Controlling network access

Images



Publication data including kind & date

US20090113540	A1	2009-04-30	US20090113540
WO2009058495	A1	2009-05-07	WO200958495
EP2206291	A1	2010-07-14	EP2206291
CN101843046	A	2010-09-22	CN101843046
IN2288/CHENP/2010	A	2010-10-15	IN2010CN02288
US9225684	B2	2015-12-29	US9225684
EP2206291	A4	2016-12-07	EP2206291



Abstract

(EP2206291)

Systems and methods for controlling network access determine that a client computer on the network is in compliance with administrator-defined network health policy standards before the client computer is granted access to the network. A packet exchange mechanism is defined wherein filtering instructions from a server are converted into firewall rules on the client computer to restrict client access to remediation servers on the network. The client computer obtains update patches from the remediation servers to become compliant with network health policy standards.

Inventors

CHANDWANI SANTOSH

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2009-04-30

2009-05-07

2010-07-14

2010-09-22

2010-10-15

2015-12-29

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2006-03-02

2006-03-09

2006-03-09

2007-06-06

2007-06-28

2007-08-03

2009-10-13

2010-01-28

2014-02-12

2016-05-03

2017-10-04

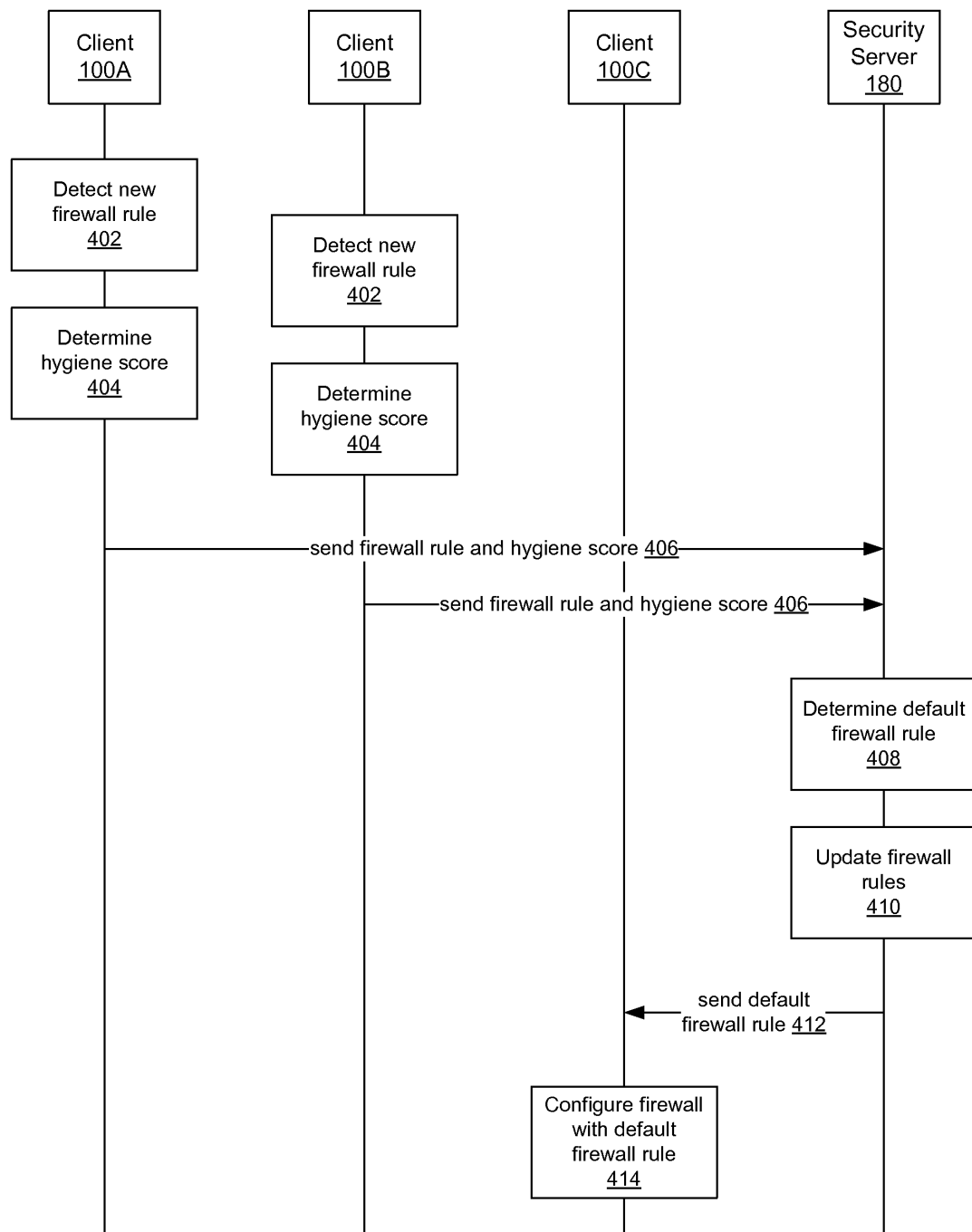
Family 31/50 - FAMPAT - ©Questel

Title

(US8353021)

Determining firewall rules for an application on a client based on firewall rules and reputations of other clients

Images

**Publication data including kind & date**

US8353021

B1 2013-01-08 US8353021

**Abstract**

(US8353021)

A security system monitors the trustworthiness and firewall configurations of a set of clients, where a firewall configuration comprises a set of firewall rules that control access by an application to network communication functionalities of a client. Based on the firewall rules used by other clients and the reputation of those clients, the system determines a set of default firewall rules by selecting one or more rules that are used by the more trustworthy clients. The default firewall rules are made available to other clients, which may use these default rules. This leverages community knowledge about how much network access to allow for a particular application.

Inventors

SATISH SOURABH

SOBEL WILLIAM E

Latest standardized assignees - inventors removed

SYMANTEC

Publication dates

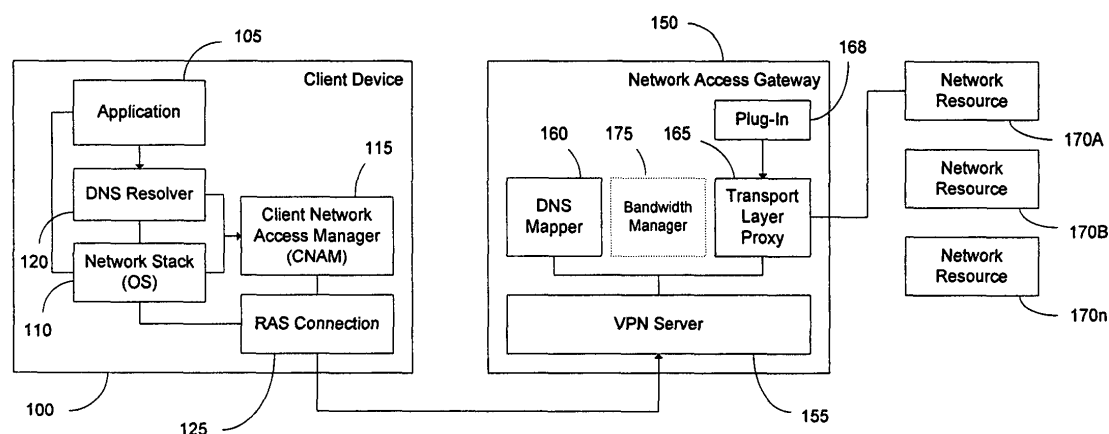
2013-01-08

Family 32/50 - FAMPAT - ©Questel

Title

(EP1902383)

Unified architecture for remote network access

Images**Publication data including kind & date**

US20070011733	A1	2007-01-11	US20070011733
WO2007008856	A2	2007-01-18	WO200708856
CA2611554	A1	2007-01-18	CA2611554
AU2006268313	A1	2007-01-18	AU2006268313
WO2007008856	A3	2007-05-10	WO200708856
WO2007008856	A9	2007-07-05	WO200708856
KR20080026161	A	2008-03-24	KR20080026161
MX2008000175	A	2008-03-26	MX2008000175
EP1902383	A2	2008-03-26	EP1902383
IN10183/DELNP/2007	A	2008-06-20	IN2007DN10183
CN101218577	A	2008-07-09	CN101218577
JP2009500968	A	2009-01-08	JP2009500968
RU2007148416	A	2009-07-10	RU2007148416
CN101218577	B	2010-10-06	CN101218577B
BRPI0612400	A2	2010-11-03	BR200612400
BRPI0612400	A2	2010-11-03	BRPI0612400
US8166538	B2	2012-04-24	US8166538

**Abstract**

(EP1902383)

A unified architecture for enabling remote access to a network is provided. The network may comprise, as examples, a virtual private network (VPN) and/or a peer-to-peer network. In one embodiment, the architecture includes components installed on a client device/node and a gateway/supernode. Components implemented on the client device may facilitate access in a manner similar to that of a traditional VPN, while components on the gateway may facilitate access in a manner similar to an application proxy. Communication between the client device and gateway may occur, as an example, via a Secure Sockets Layer (SSL) communication protocol.

Inventors

GBADEGESIN ABOLADE

THALER DAVID G

MAYFIELD PAUL G

MURCHING ARVIND M

SANDERS HENRY L

GIDWANI NARENDRA C

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2007-01-11

2007-01-18

2007-01-18

2007-01-18

2007-05-10

2007-07-05

2008-03-24

2008-03-26

2008-03-26

2008-06-20

2008-07-09

2009-01-08

2009-07-10

2010-10-06

2010-11-03

2010-11-03

2012-04-24

Family 33/50 - FAMPAT - ©Questel

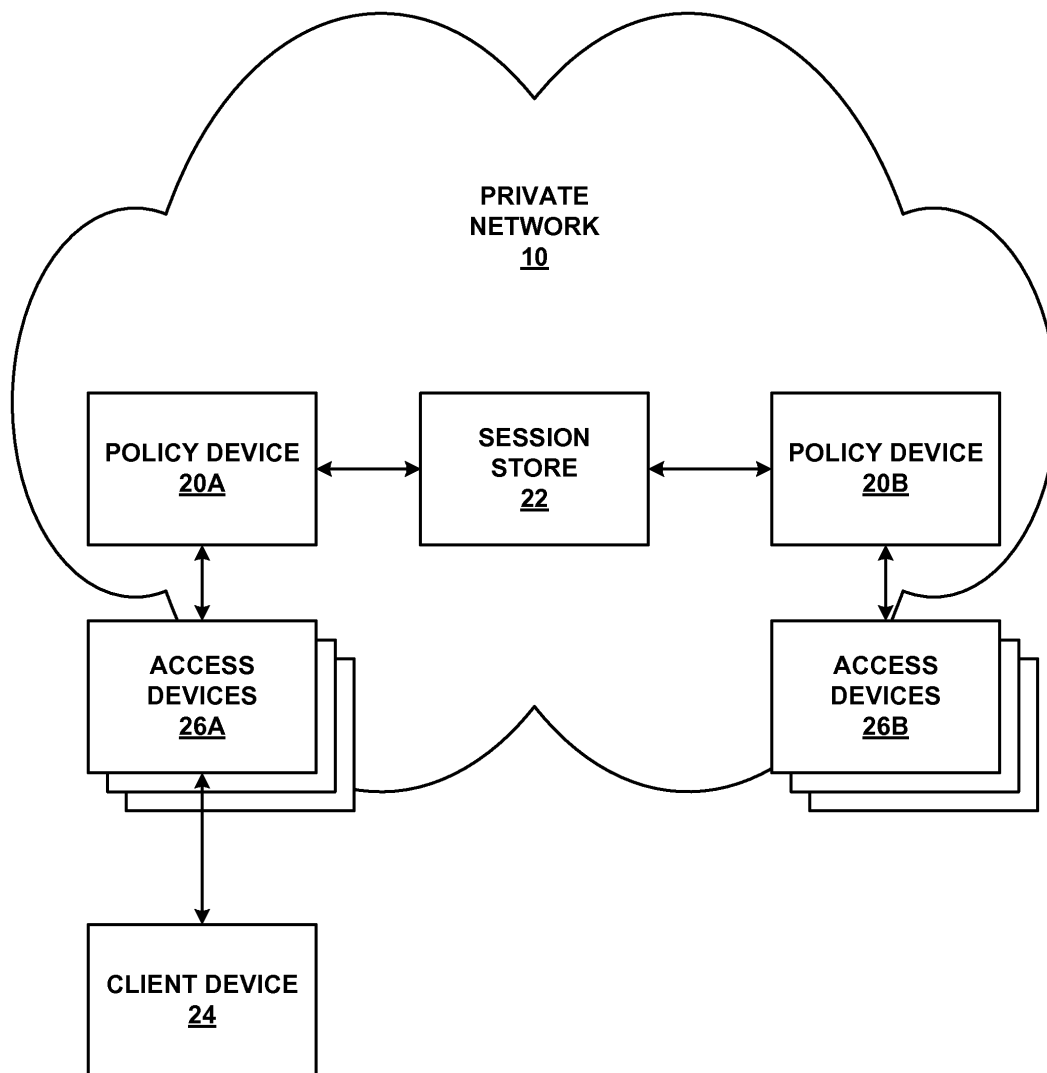
Title

(EP2337296)

Session migration between network policy servers

Images

9



Publication data including kind & date

CN102104592	A	2011-06-22	CN102104592
EP2337296	A1	2011-06-22	EP2337296
US20110153854	A1	2011-06-23	US20110153854
CN102104592	B	2014-08-13	CN102104592B
US10057239	B2	2018-08-21	US10057239



Abstract

(EP2337296)

A policy device grants access to a client device, without authenticating the client device, when the client device provides a session identifier to the policy device that was previously granted to the client device by a second policy device upon authenticating the client device by the second policy device. In one example, a policy device includes a network interface that receives a session identifier from a client device, wherein the policy device comprises an individually administered autonomous policy server, and an authorization module that grants the client device access to a network protected by the policy device based on the session identifier without authenticating the client device by the policy device. In this manner, the client device need not provide authentication information multiple times within a short time span, and the policy device can deallocate resources when a session migrates to a second policy device.

Inventors

CHICKERING ROGER A

Latest standardized assignees - inventors removed

JUNIPER NETWORKS

SMOBIIE SYSTEMS

PULSE SECURE

Publication dates

2011-06-22

2011-06-22

2011-06-23

2014-08-13

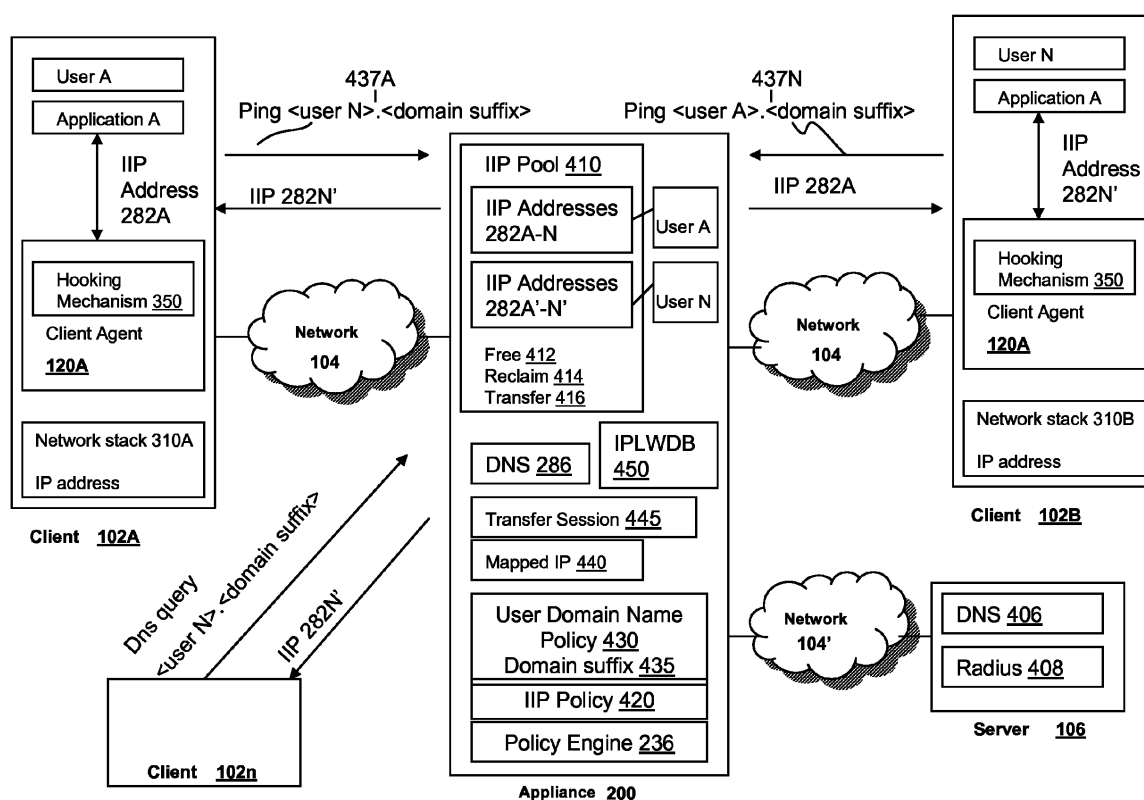
2018-08-21

Family 34/50 - FAMPAT - ©Questel

Title

(US9009327)

Systems and methods for providing IIP address stickiness in an SSL VPN session failover environment

Images**Publication data including kind & date**

US20090037763

A1 2009-02-05

US20090037763

US9009327

B2 2015-04-14

US9009327

**Abstract**

(US9009327)

The SSL VPN session failover solution of the appliance and/or client agent described herein provides an environment for handling IP address assignment and end point re-authorization upon failover. The appliances may be deployed to provide a session failover environment in which a second appliance is a backup to a first appliance when a failover condition is detected, such as failure in operation of the first appliance. The backup appliance takes over responsibility for SSL VPN sessions provided by the first appliance. In the failover environment, the first appliance propagates SSL VPN session information including user IP address assignment and end point authorization information to the backup appliance. The backup appliance maintains this information. Upon detection of failover of the first appliance, the backup appliance activates

the transferred SSL VPN session and maintains the user assigned IP addresses. The backup appliance may also re-authorize the client for the transferred SSL VPN session.

Inventors

ADHYA SAIBAL

CHOUDHARY AKSHAT

NANJUNDASWAMY SHASHI

VERZUNOV SERGEY

KUMAR ARKESH

MULLICK AMARNATH

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2009-02-05

2015-04-14

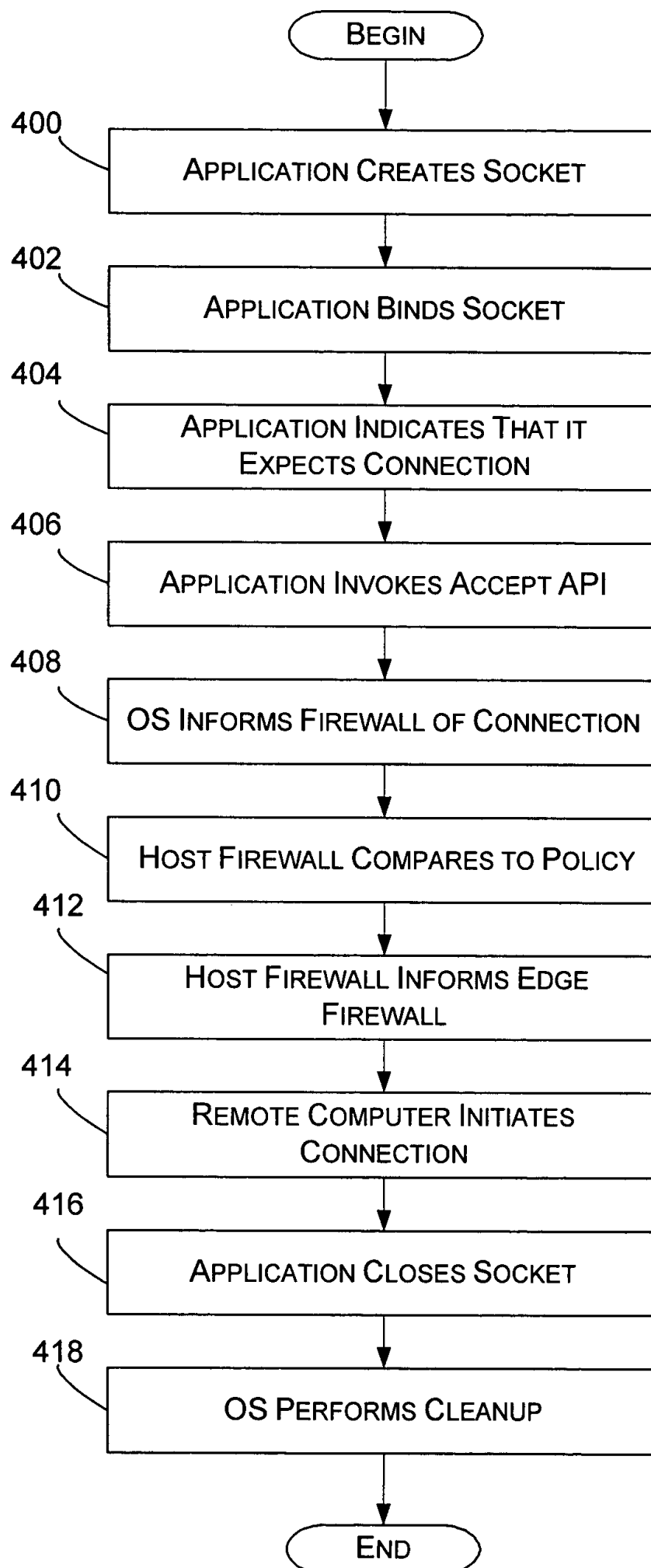
Family 35/50 - FAMPAT - ©Questel

Title

(EP1492299)

Method of assisting an application to traverse a firewall

Images



Publication data including kind & date

EP1492299	A2	2004-12-29	EP1492299
KR20050001397	A	2005-01-06	KR20050001397
US20050005165	A1	2005-01-06	US20050005165
JP2005018769	A	2005-01-20	JP2005018769
CN1578232	A	2005-02-09	CN1578232
IN0778/DEL/2004	A	2006-06-16	IN2004DE00778
CN100499487	C	2009-06-10	CN100499487C
US7559082	B2	2009-07-07	US7559082
EP1492299	A3	2010-07-21	EP1492299

**Abstract**

(EP1492299)

A method for a firewall-aware application to communicate its expectations to a firewall without requiring the firewall to change its policy or compromise network security. An application API is provided for applications to inform a firewall or firewalls of the application's needs, and a firewall API is provided that informs the firewall or firewalls of the application's needs. An interception module watches for connect and listen attempts by applications and services to the network stack on the local computer. The interception module traps these attempts and determines what user is making the attempt, what application or service is making the attempt, and conducts a firewall policy look-up to determine whether the user and/or application or service are allowed to connect to the network. If so, the interception module may instruct the host and/or edge firewall to configure itself for the connection being requested.

Inventors

MORGAN DENNIS

GAVRILESCU ALEXANDRU

BURSTEIN JONATHAN L

SHELEST ART

LEBLANC DAVID

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2004-12-29

2005-01-06

2005-01-06

2005-01-20

2005-02-09

2006-06-16

2009-06-10

2009-07-07

2010-07-21

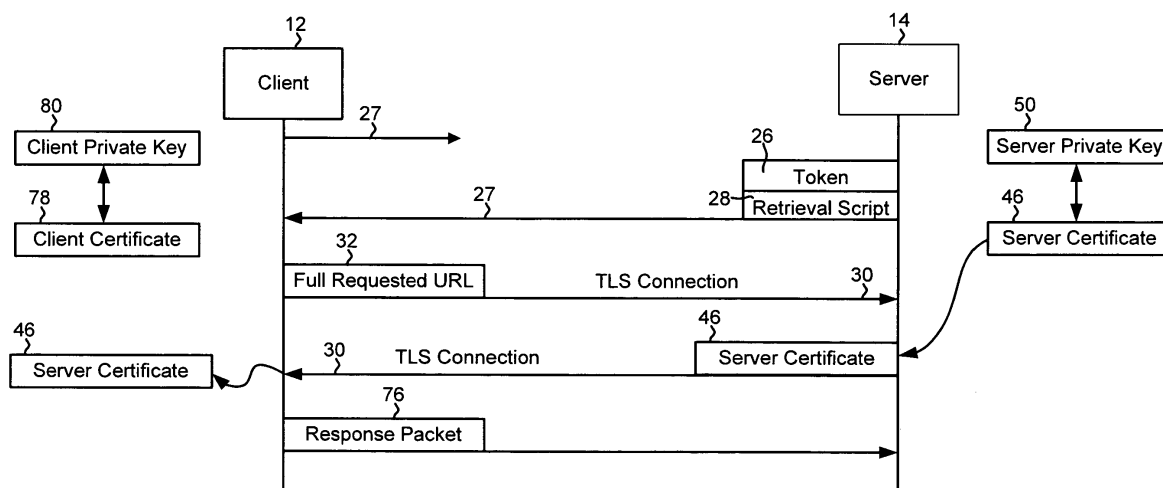
Family 36/50 - FAMPAT - ©Questel

Title

(EP2070248)

System and method for facilitating secure online transactions

Images



Publication data including kind & date

US20080077791	A1	2008-03-27	US20080077791				
US20080077796	A1	2008-03-27	US20080077796				
WO2008039227	A1	2008-04-03	WO200839227				
AU2007300707	A1	2008-04-03	AU2007300707				
US20090025080	A1	2009-01-22	US20090025080				
WO2009014704	A1	2009-01-29	WO200914704				
EP2070248	A1	2009-06-17	EP2070248				
JP2010505334	A	2010-02-18	JP2010505334				
EP2070248	A4	2011-09-21	EP2070248				
AU2007300707	B2	2011-11-17	AU2007300707				
US8327142	B2	2012-12-04	US8327142				
US20130091358	A1	2013-04-11	US20130091358				
JP5186648	B2	2013-04-17	JP5186648				
US8700901	B2	2014-04-15	US8700901				
US20140215213	A1	2014-07-31	US20140215213				
US9294288	B2	2016-03-22	US9294288				
US20160308682	A1	2016-10-20	US20160308682				
US9900163	B2	2018-02-20	US9900163				
EP2070248	B1	2018-10-10	EP2070248				

Abstract

(EP2070248)

A method and system for mutually authenticating a client and a server is provided in accordance with an aspect of the present invention. The method commences with transmitting a token from the server to the client. Thereafter, the method continues with establishing a secure data transfer link between the server and the client. A server certificate is transmitted to the client during the establishment of the secure data transfer link. The method continues with transmitting a response packet to the server, which is validated thereby upon receipt. The system includes a client authentication module that initiates the secure data transfer link and transmits the response packet, and a server authentication module that transmits the token and validates the response packet.

Inventors

LUND CRAIG

GRAJEK GARRET

MOORE STEPHEN

Latest standardized assignees - inventors removed

SECUREAUTH

Publication dates

2008-03-27
2008-03-27
2008-04-03
2008-04-03
2009-01-22
2009-01-29
2009-06-17
2010-02-18
2011-09-21
2011-11-17
2012-12-04
2013-04-11
2013-04-17
2014-04-15
2014-07-31
2016-03-22
2016-10-20
2018-02-20
2018-10-10

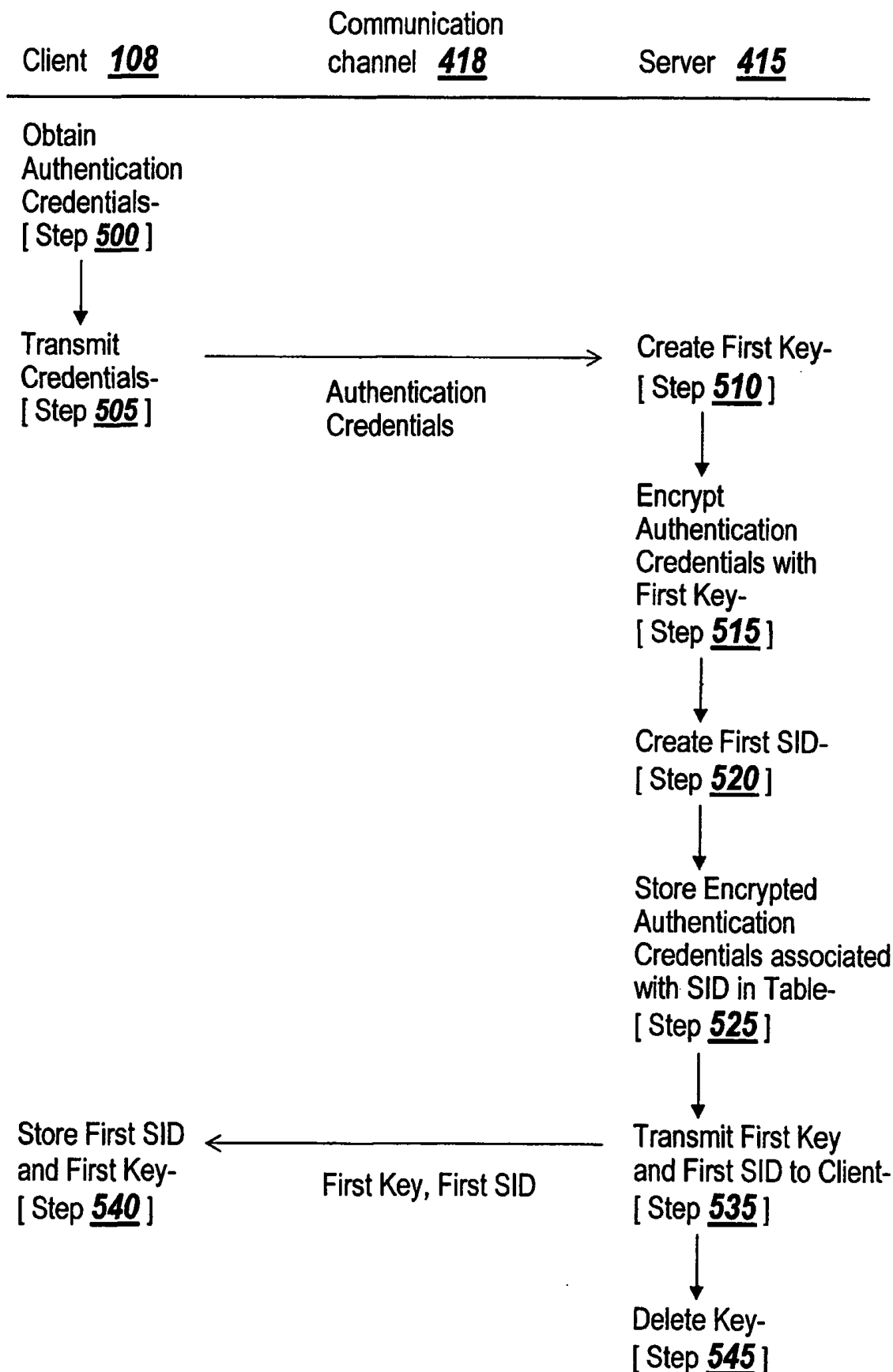
Family 37/50 - FAMPAT - ©Questel

Title

(EP1678918)

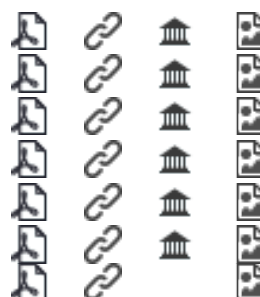
A persistent and reliable session securely traversing network components using an encapsulating protocol

Images



Publication data including kind & date

WO03072903	A2	2003-09-04	WO200372903
CA2477102	A1	2003-09-04	CA2477102
AU2003212449	A1	2003-09-09	AU2003212449
AU2003212449	A8	2003-09-09	AU2003212449
WO03072903	A3	2004-07-01	WO200372903
NO20043708	A	2004-09-03	NO200403708



GB0418714	D0	2004-09-22	GB200418714				
MXPA04008316	A	2004-11-26	MX2004PA008316				
GB2402417	A	2004-12-08	GB2402417				
GB2402417	A8	2004-12-08	GB2402417				
US20050080907	A1	2005-04-14	US20050080907				
WO2005036832	A1	2005-04-21	WO200536832				
CA2541137	A1	2005-04-21	CA2541137				
AU2004306787	A1	2005-04-21	AU2004306787				
WO2005036858	A1	2005-04-21	WO200536858				
WO2005036857	A1	2005-04-21	WO200536857				
CA2541151	A1	2005-04-21	CA2541151				
CA2542139	A1	2005-04-21	CA2542139				
AU2004306772	A1	2005-04-21	AU2004306772				
AU2004306771	A1	2005-04-21	AU2004306771				
EA200401116	A1	2005-06-30	EA200401116				
CN1650140	A	2005-08-03	CN1650140				
US20050198380	A1	2005-09-08	US20050198380				
US20050198379	A1	2005-09-08	US20050198379				
GB2402417	B	2005-10-05	GB2402417				
US20050246445	A1	2005-11-03	US20050246445				
US20050267974	A1	2005-12-01	US20050267974				
US20050273513	A1	2005-12-08	US20050273513				
GB2402417	A8	2005-12-14	GB2402417				
EA006694	B1	2006-02-24	EA---6694				
CO5611223	A2	2006-02-28	CO5611223				
IN1230/KOLNP/2004	A	2006-05-05	IN2004KN01230				
EP1678885	A1	2006-07-12	EP1678885				
EP1678918	A1	2006-07-12	EP1678918				
EP1678917	A1	2006-07-12	EP1678917				
IL174816	A	2006-08-20	IL-174816				
IL174815	A	2006-08-20	IL-174815				
IL174814	A	2006-08-20	IL-174814				
KR20060120035	A	2006-11-24	KR20060120035				
KR20060120032	A	2006-11-24	KR20060120032				
KR20060126952	A	2006-12-11	KR20060126952				
JP2007509521	A	2007-04-12	JP2007509521				
IN0869/KOLNP/2006	A	2007-04-13	IN2006KN00869				
IN0929/KOLNP/2006	A	2007-04-20	IN2006KN00929				
IN0909/KOLNP/2006	A	2007-04-20	IN2006KN00909				
JP2007514337	A	2007-05-31	JP2007514337				
JP2007515852	A	2007-06-14	JP2007515852				
EP1678918	B1	2007-12-12	EP1678918				
AT381196	T	2007-12-15	ATE381196				
DE602004010703	D1	2008-01-24	DE602004010703				
US7340772	B2	2008-03-04	US7340772				
ES2298835	T3	2008-05-16	ES2298835				
HK1096213	A1	2008-06-06	HK1096213				
EP1678917	B1	2008-08-27	EP1678917				

AT406751	T	2008-09-15	ATE406751				
DE602004016200	D1	2008-10-09	DE602004016200				
DE602004010703	T2	2008-11-27	DE602004010703				
EP1678885	B1	2008-12-10	EP1678885				
AT417437	T	2008-12-15	ATE417437				
DE602004018365	D1	2009-01-22	DE602004018365				
US7502726	B2	2009-03-10	US7502726				
HK1096212	A1	2009-04-09	HK1096212				
HK1096211	A1	2009-06-19	HK1096211				
US7562146	B2	2009-07-14	US7562146				
CN100523689	C	2009-08-05	CN100523689C				
IN240601	B	2010-05-21	IN-240601				
CA2477102	C	2010-07-20	CA2477102				
NO330318	B1	2011-03-28	NO-330318				
US20110113247	A1	2011-05-12	US20110113247				
US7984157	B2	2011-07-19	US7984157				
US8090874	B2	2012-01-03	US8090874				
CA2541151	C	2013-06-11	CA2541151				
US8874791	B2	2014-10-28	US8874791				
CA2542139	C	2014-11-25	CA2542139				
CA2541137	C	2016-06-14	CA2541137				

Abstract

(EP1678918)

The invention relates to systems and methods for reestablishing client communications by securely traversing network components using an encapsulating communication protocol to provide session persistence and reliability. A first protocol that encapsulates a plurality of secondary protocols is used to communicate over a network to provide session persistence and a reliable connection between a client and a host service via a first protocol service. A ticket authority generates a first ticket and a second ticket associated with the client. The first ticket is provided to the client and the client uses the first ticket to establish a communication session with the first protocol service. The second ticket is provided to the first protocol service and the first protocol service uses the second ticket to establish a communication session with the host service.

Inventors

PANASYUK ANATOLIY

KRAMER ANDRE

PEDERSEN BRADLEY JAY

STONE DAVID SEAN

TREDER TERRY

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2003-09-04

2003-09-04

2003-09-09

2003-09-09

2004-07-01

2004-09-03

2004-09-22

2004-11-26

2004-12-08

2004-12-08
2005-04-14
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-04-21
2005-06-30
2005-08-03
2005-09-08
2005-09-08
2005-10-05
2005-11-03
2005-12-01
2005-12-08
2005-12-14
2006-02-24
2006-02-28
2006-05-05
2006-07-12
2006-07-12
2006-07-12
2006-08-20
2006-08-20
2006-08-20
2006-11-24
2006-11-24
2006-12-11
2007-04-12
2007-04-13
2007-04-20
2007-04-20
2007-05-31
2007-06-14
2007-12-12
2007-12-15
2008-01-24
2008-03-04
2008-05-16
2008-06-06
2008-08-27
2008-09-15
2008-10-09
2008-11-27
2008-12-10

2008-12-15

2009-01-22

2009-03-10

2009-04-09

2009-06-19

2009-07-14

2009-08-05

2010-05-21

2010-07-20

2011-03-28

2011-05-12

2011-07-19

2012-01-03

2013-06-11

2014-10-28

2014-11-25

2016-06-14

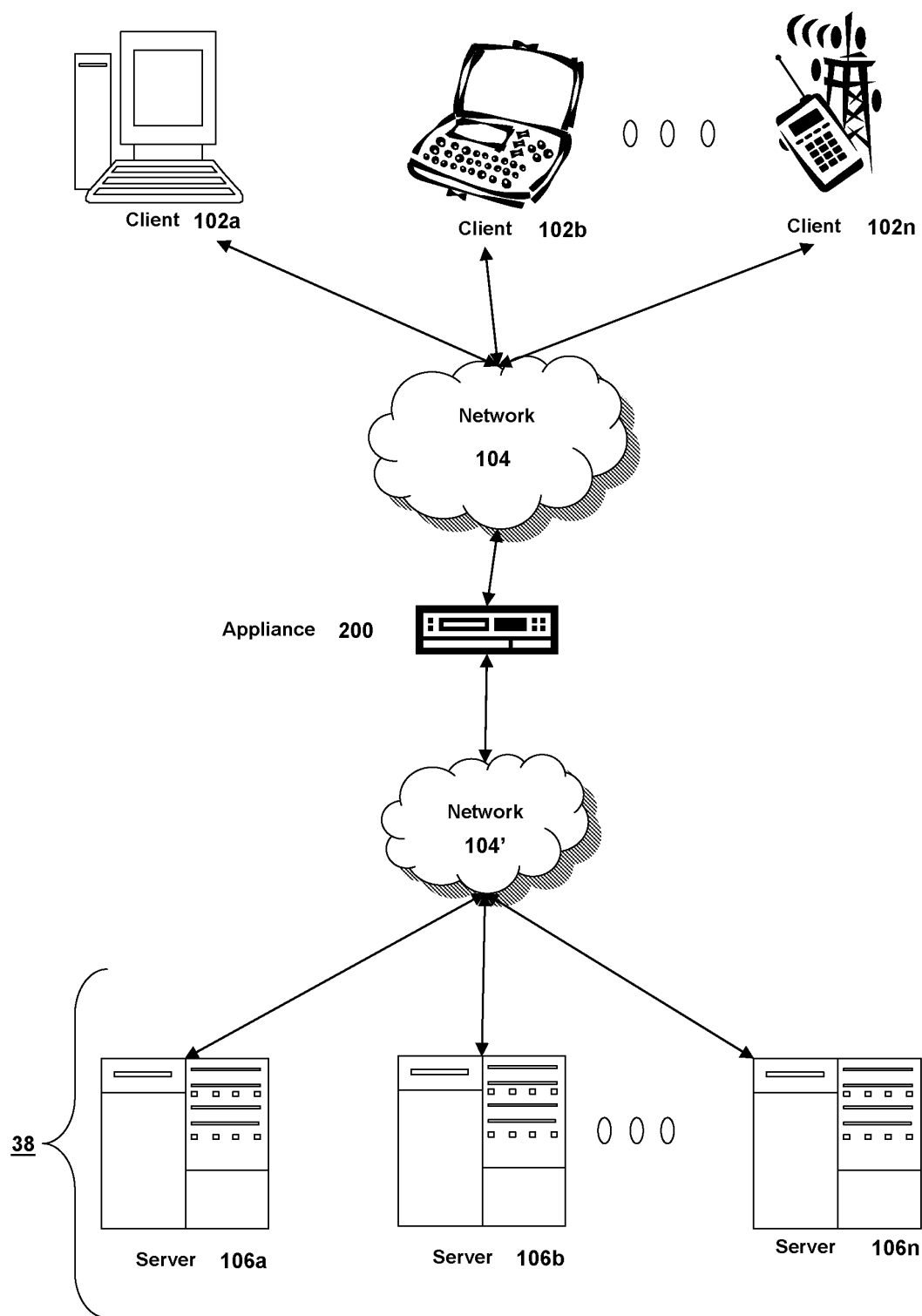
Family 38/50 - FAMPAT - ©Questel

Title

(US9407608)

Systems and methods for enhanced client side policy

Images



Publication data including kind & date

US20080046993	A1	2008-02-21	US20080046993
US8397287	B2	2013-03-12	US8397287
US20130152162	A1	2013-06-13	US20130152162
US20140344891	A1	2014-11-20	US20140344891
US8904475	B2	2014-12-02	US8904475
US9407608	B2	2016-08-02	US9407608



Abstract

(US9407608)

An appliance and method for authorizing a level of access of a client to a virtual private network connection, based on a client-side attribute includes the step of establishing, by an appliance, a control connection with a client upon receiving a

client request to establish a virtual private network connection with a network. The appliance transmits, via the control connection, a request to the client to evaluate at least one clause of a security string, the at least one clause including an expression associated with a client-side attribute. The client transmits, via the control connection, a response to the appliance comprising a result of evaluating the at least one clause by the client. The appliance assigns the client to an authorization group based on the result of evaluation of the at least one clause.

Inventors

MULLICK AMARNATH

VENKATRAMAN CHARU

NANJUNDASWAMY SHASHI

HE JUNXIAO

SONI AJAY

STAVRAKOS NICHOLAS

KOOPMANS CHRIS

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2008-02-21

2013-03-12

2013-06-13

2014-11-20

2014-12-02

2016-08-02

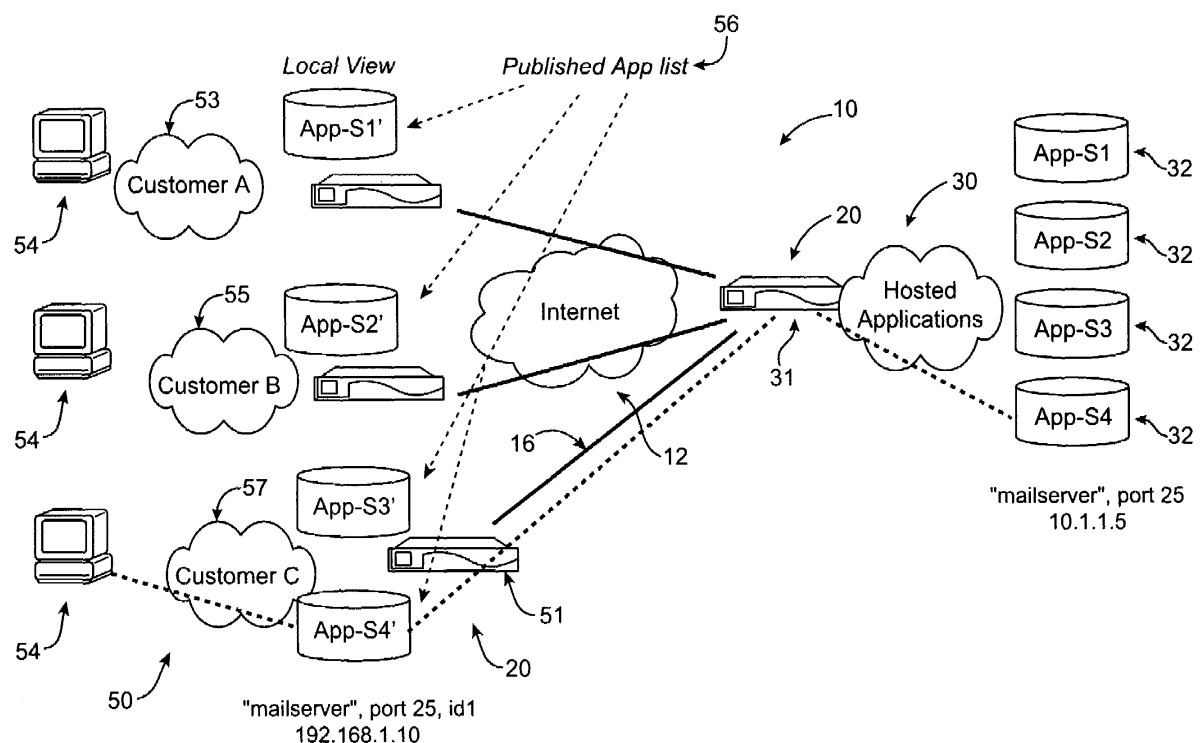
Family 39/50 - FAMPAT - ©Questel

Title

(US8249081)

Dynamic virtual private network (VPN) resource provisioning using a dynamic host configuration protocol (DHCP) server, a domain name system (DNS) and/or static IP assignment

Images



Publication data including kind & date

US20080082640

A1 2008-04-03

US20080082640



[CN101184015](#)

A 2008-05-21 CN101184015

[US8249081](#)

B2 2012-08-21 US8249081

[CN101184015](#)

B 2013-03-20 CN101184015B

Abstract

(US8249081)

A method of provisioning resources, which includes hosting at least one resource at a first site. A secure connection is established between the first site and a second site, and a listing of available resources is exported to the second site. The second site publishes the listing of available resources to at least one client and at least one resource from the first site to second site is provisioned by providing the at least one client with an IP address of the at least one resource.

Inventors

CHANG ARTHUR

HSU NAI-TING

WU MICHAEL

YEN LEEMAY

ZHAO LINGYAN

Latest standardized assignees - inventors removed

ARRAY NETWORKS

Publication dates

2008-04-03

2008-05-21

2012-08-21

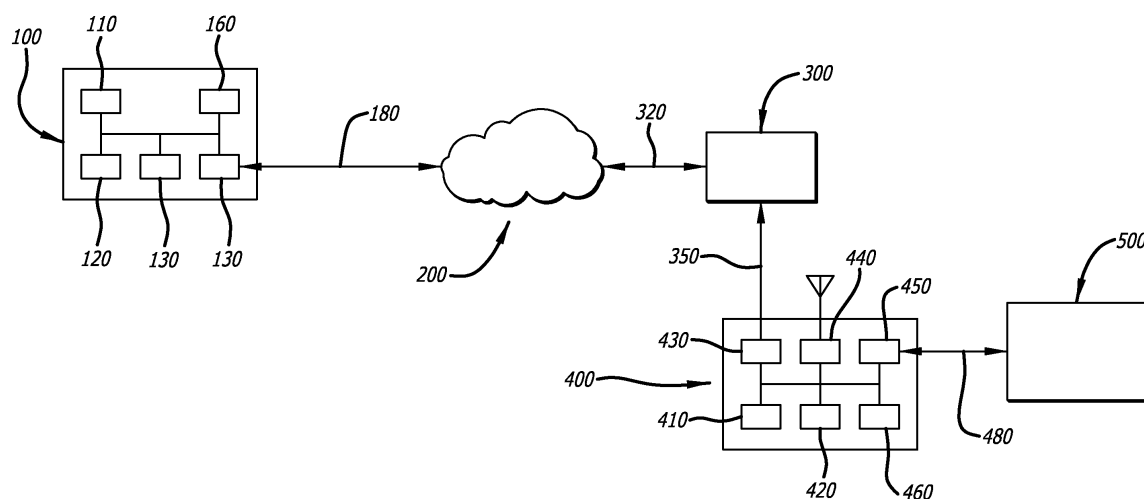
2013-03-20

Family 40/50 - FAMPAT - ©Questel

Title

(US9509746)

Provisioning remote access points

Images**Publication data including kind & date**[US20100313262](#)

A1 2010-12-09 US20100313262

[US20140082060](#)

A1 2014-03-20 US20140082060

[US9509746](#)

B2 2016-11-29 US9509746

[US20170078277](#)

A1 2017-03-16 US20170078277

Abstract

(US9509746)

Provisioning remote access points for use in a telecommunication network. A remote access point contains identity information established during manufacturing; this identity information may be in the nature of a digital certificate. The identity information is stored in the remote access point, and may be stored in a Trusted Platform Module if present. When the remote access node is powered up in unprovisioned state, outside the manufacturing environment, it attempts to establish an internet connection via a first wired interface, and queries a user for information representing the TCP/IP address of its controller via a second wired interface. Once an internet connection is present, and a TCP/IP address has been provided, the remote access point attempts to connect to the controller at that address. Once a connection is established, controller and access point exchange and verify each other's identities.

Inventors

MEHTA MANISH

KSHIRSAGAR SHEKHAR

PALCHAUDHURI SANTASHIL

Latest standardized assignees - inventors removed

HEWLETT PACKARD ENTERPRISE DEVELOPMENT

Publication dates

2010-12-09

2014-03-20

2016-11-29

2017-03-16

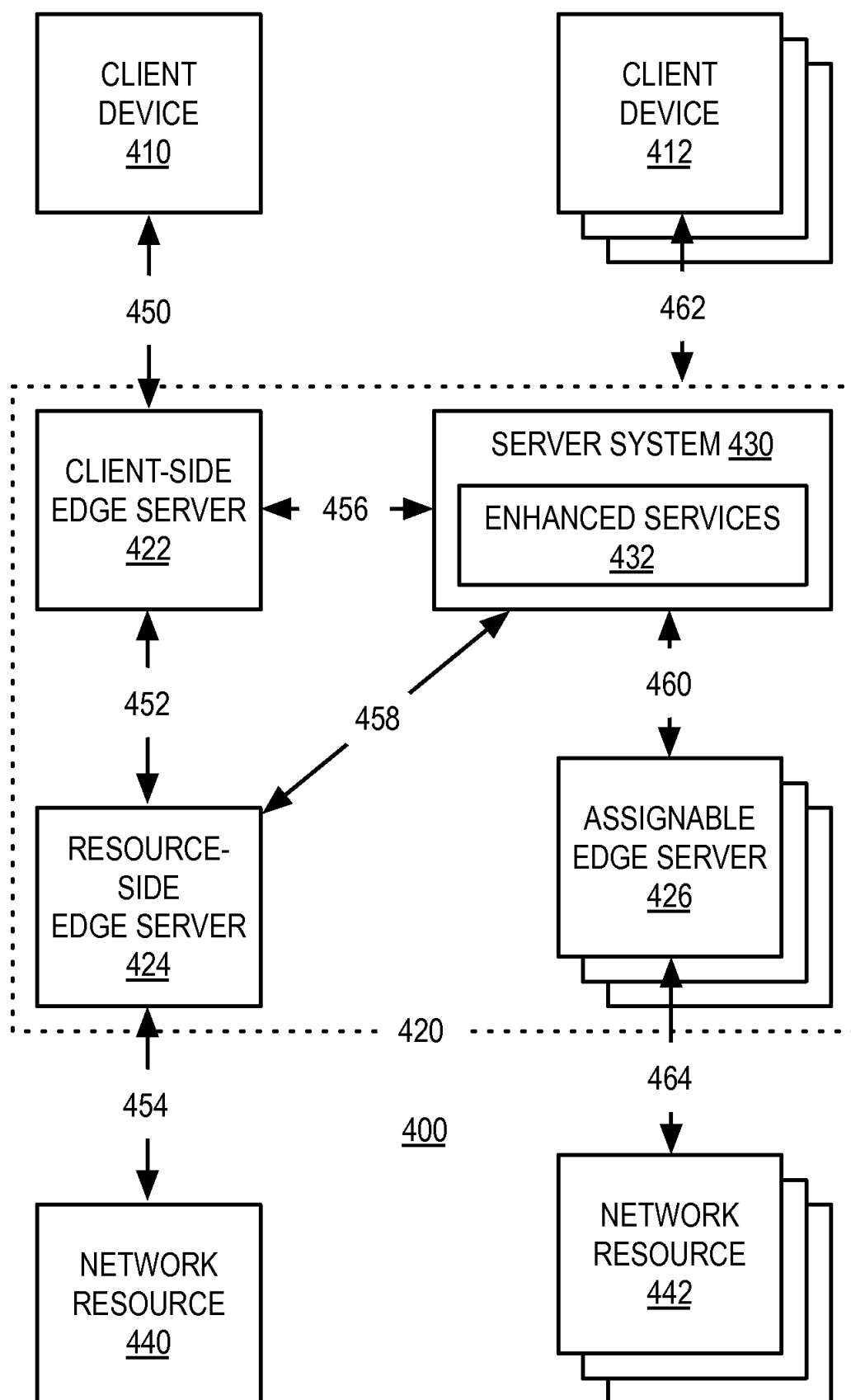
Family 41/50 - FAMPAT - ©Questel

Title

(US9923897)

Edge server selection for enhanced services network

Images

**Publication data including kind & date**[US20140259109](#)

A1 2014-09-11

US20140259109

[US9923897](#)

B2 2018-03-20

US9923897

**Abstract**

(US9923897)

An enhanced services network provides enhanced privacy and/or security over public networks to client subscribers of the service. Client devices access the enhanced services network over a public communications network (e.g., the Internet, cellular network, etc.) via a client-side edge server of the enhanced services network. The enhanced services network interfaces with client-requested network resources hosted by third-party server devices via a resource-side edge server. The particular client-side edge server and/or resource-side edge server that is utilized for a particular client session may be selected by the enhanced services network according to a rule set. The rule set may seek to achieve one or more target goals, such as: (1) limit discoverability of the enhanced services network, (2) minimize or reduce geographic/network distance between an edge server and a target computing device, and/or (3) establish connections that are more secure than the connections originally requested by the client.

Inventors

HOUSTON CHRIS

NUAIMI ATHIR

GROSS JOSH

Latest standardized assignees - inventors removed

SURFEASY

Publication dates

2014-09-11

2018-03-20

Family 42/50 - FAMPAT - ©Questel

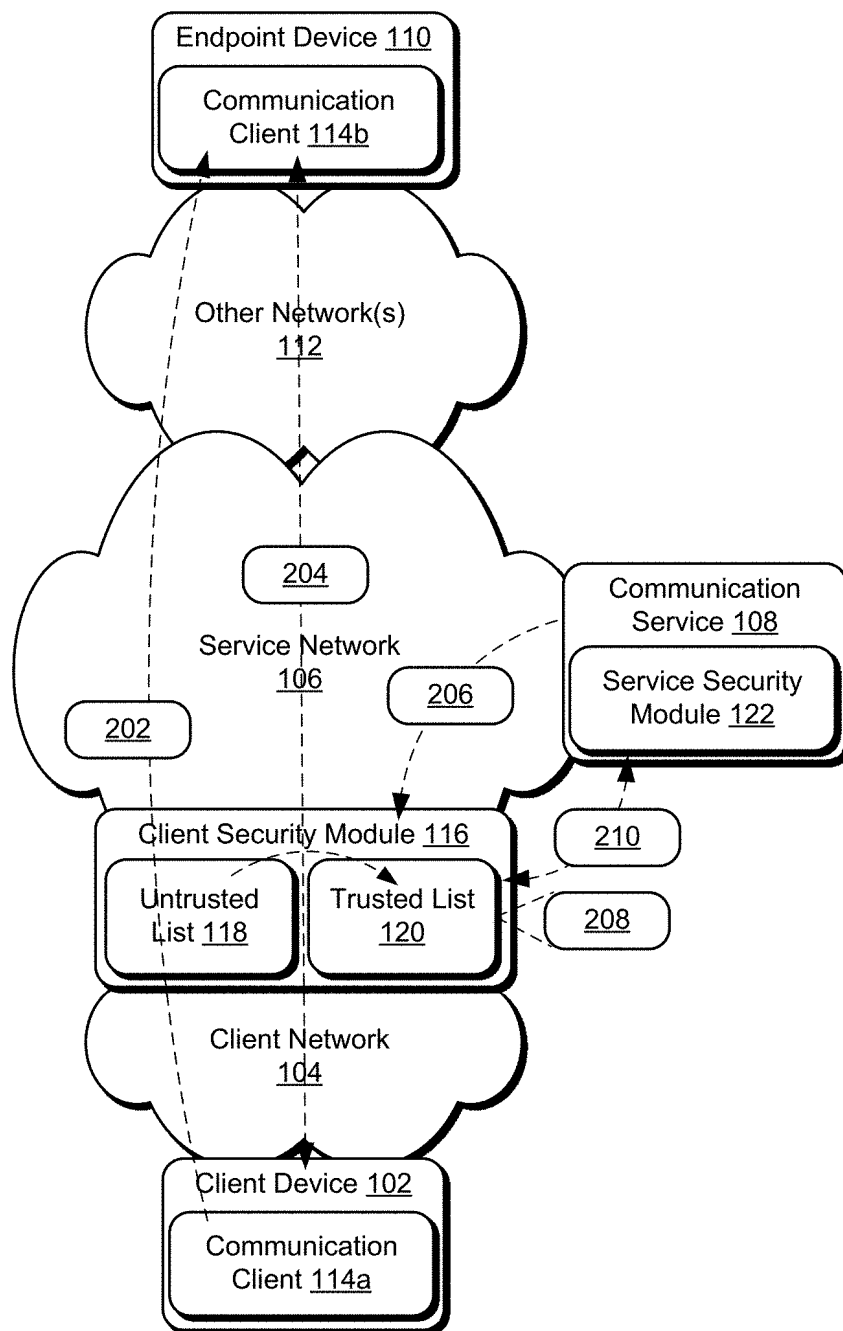
Title

(WO201744510)

Trust status of a communication session

Images

200

**Publication data including kind & date**

US20170070479	A1	2017-03-09	US20170070479
WO2017044510	A1	2017-03-16	WO201744510
US9942202	B2	2018-04-10	US9942202
US20180234391	A1	2018-08-16	US20180234391

**Abstract**

(WO201744510)

Techniques for trust status of a communication session are described. According to various embodiments, different networks cooperate to facilitate routing of communication sessions between different devices. According to various embodiments, a network involved in routing a communication session ascertains whether an authentication status of a communication session is received, and categorizes a trust status of the communication session accordingly.

Inventors

MENEZES PASCAL FRANCIS

LEEB GUNTER

HASSAN AMER AREF

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2017-03-09

2017-03-16

2018-04-10

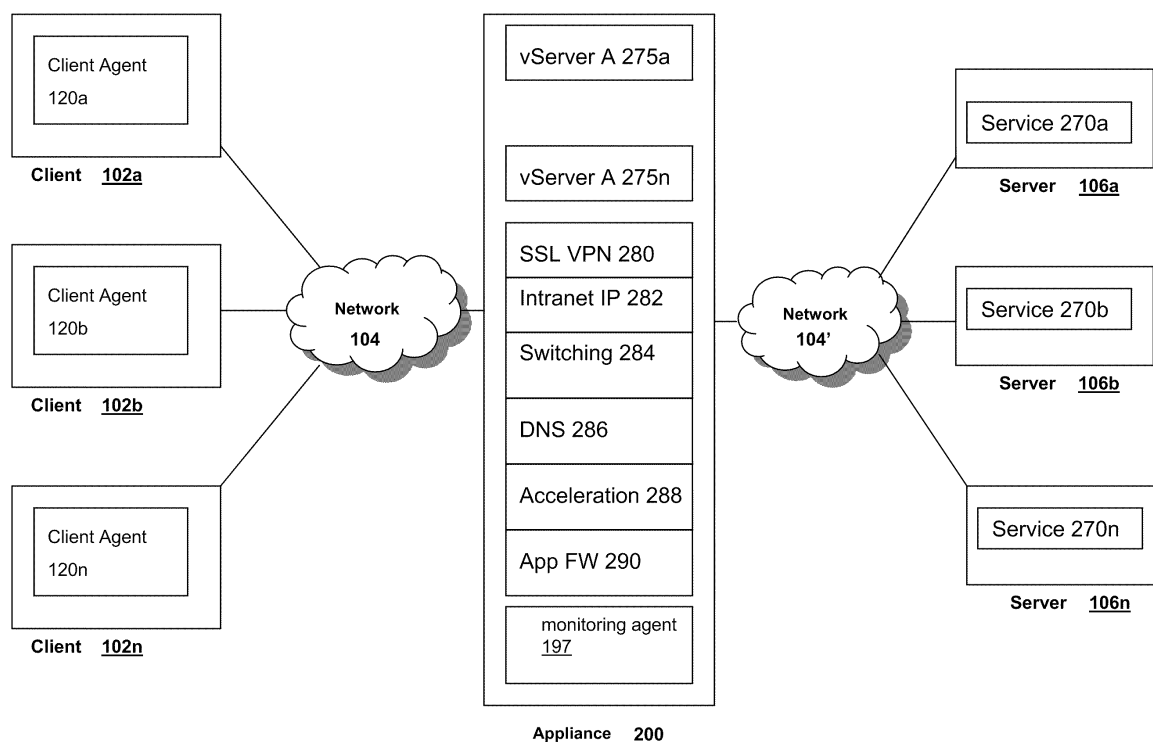
2018-08-16

Family 43/50 - FAMPAT - ©Questel

Title

(EP2241081)

Systems and methods for fine grain policy driven cookie proxying

Images**Publication data including kind & date**

WO2009094657	A1	2009-07-30	WO200994657
US20090193129	A1	2009-07-30	US20090193129
US20090199285	A1	2009-08-06	US20090199285
IN2658/KOLNP/2010	A	2010-09-24	IN2010KN02658
EP2241081	A1	2010-10-20	EP2241081
CN101984778	A	2011-03-09	CN101984778
US8090877	B2	2012-01-03	US8090877
US8769660	B2	2014-07-01	US8769660
CN101984778	B	2014-08-13	CN101984778B
US20140298410	A1	2014-10-02	US20140298410
US9059966	B2	2015-06-16	US9059966
EP2241081	B1	2018-05-02	EP2241081



IN296286

B 2018-05-04 IN-296286

Abstract

(EP2241081)

The present application enables the enterprise to configure various policies to address various subsets of the traffic based on various information relating the client, the server, or the details and nature of the interactions between the client and the server. An intermediary deployed between clients and servers may establish an SSL VPN session between a client and a server. The intermediary may receiving a response from a server to a request of a client via the clientless SSL VPN session. The response may comprise one or more cookies. The intermediary may identify an access profile for the clientless SSL VPN session. The access profile may identify one or more policies for proxying cookies. The intermediary may determine, responsive to the one or more policies of the access profile, whether to proxy or bypass proxying for the client the one or more cookies.

Inventors

AGARWAL PUNEET

ADHYA SAIBAL KUMAR

THIRUNARAYANAN SRINIVASAN

HARRIS JAMES

Latest standardized assignees - inventors removed

CITRIX SYSTEMS

Publication dates

2009-07-30

2009-07-30

2009-08-06

2010-09-24

2010-10-20

2011-03-09

2012-01-03

2014-07-01

2014-08-13

2014-10-02

2015-06-16

2018-05-02

2018-05-04

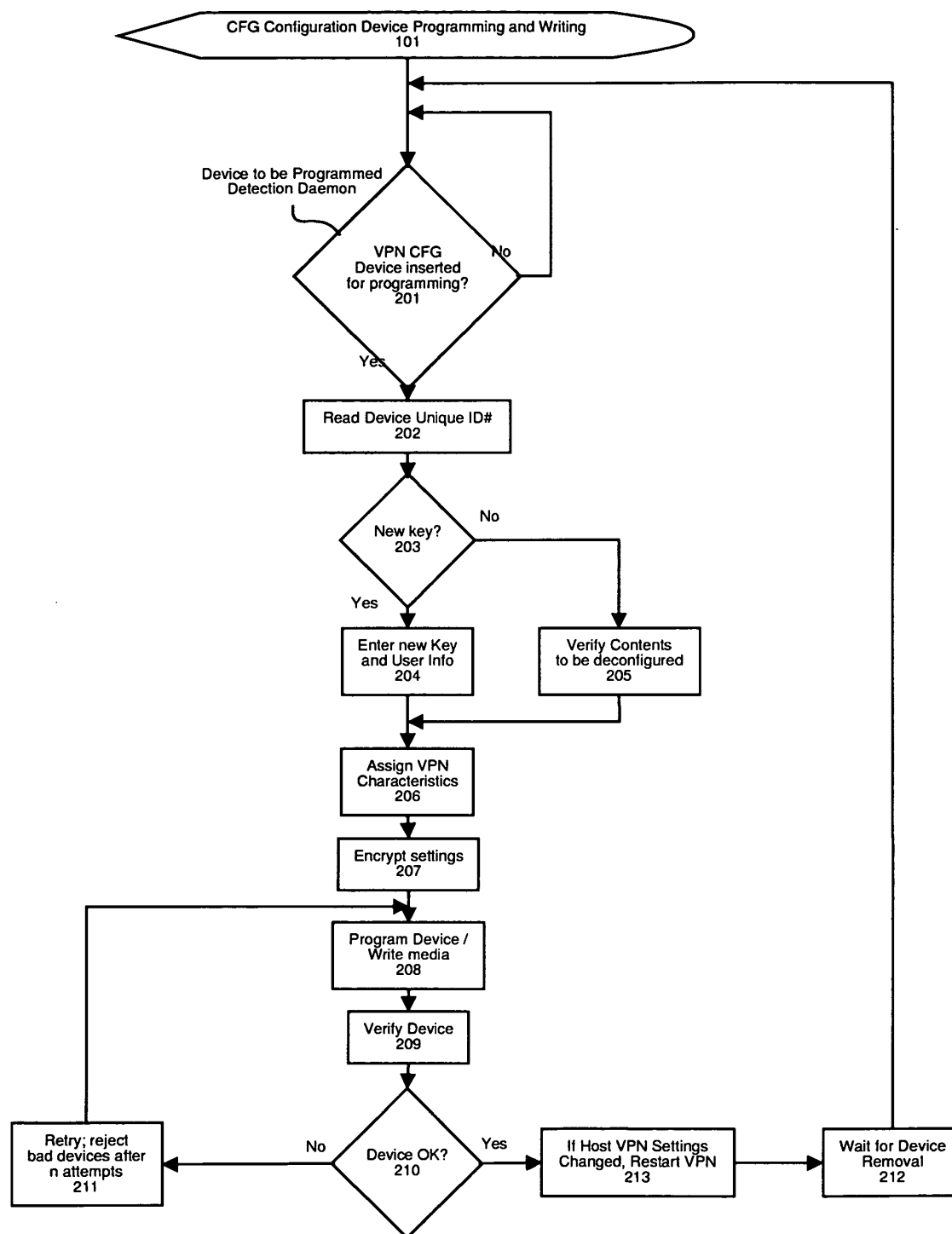
Family 44/50 - FAMPAT - ©Questel

Title

(US20050193103)

Method and apparatus for automatic configuration and management of a virtual private network

Images

**Publication data including kind & date**

US20050193103

A1 2005-09-01

US20050193103

**Abstract**

(US20050193103)

The present invention provides a method and apparatus for automatic configuration and management of a virtual private network operating over a public data network, and a method and apparatus for delivery of the configuration parameters to client interface equipment participating in the virtual private network. The system defines allowed connections between client and server gateway devices, and the parameters associated with the virtual private network. The system defines methods and apparatus for automatic startup, configuration, and shutdown of nodes of the resulting virtual private network based on factors such as the presence of a configuration carrier device. The present invention also describes a class of pseudo-interface mechanism that can hide the complexity of the underlying system from client devices incorporating the present invention, via a conventional network device interface.

Inventors

DRABIK JOHN

Publication dates

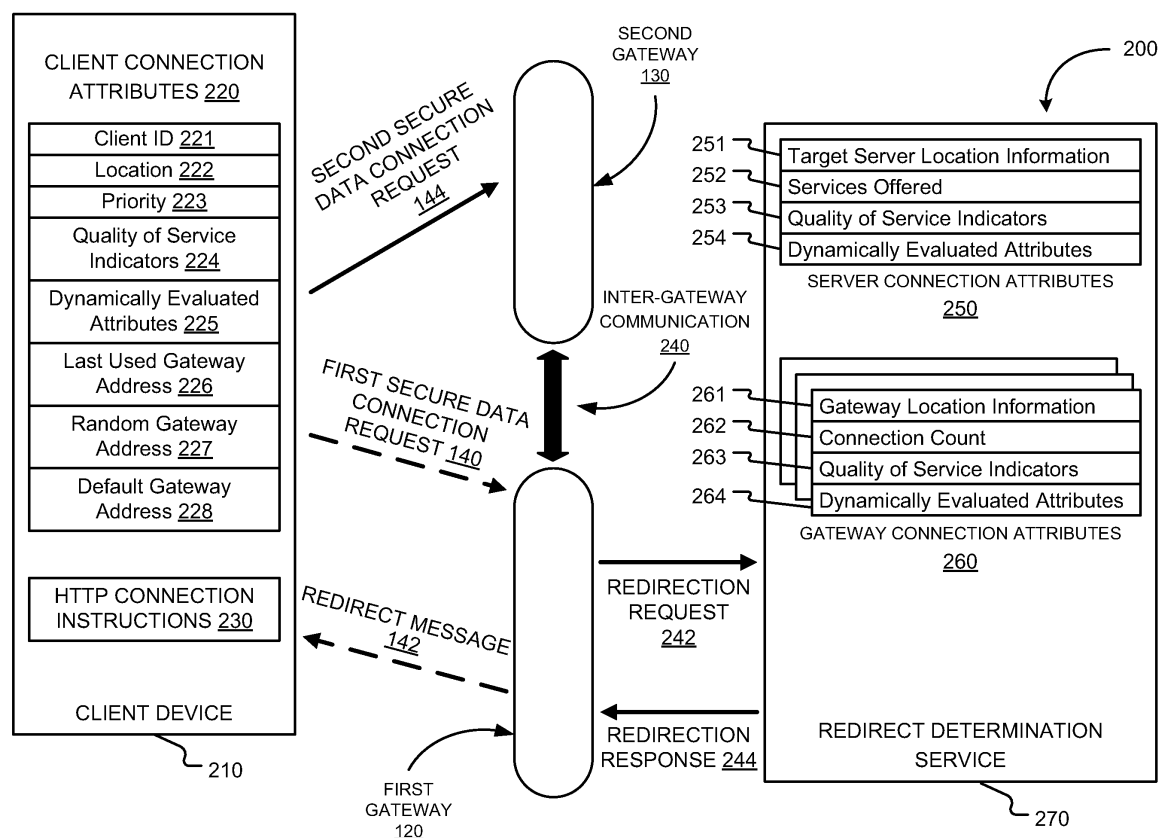
2005-09-01

Family 45/50 - FAMPAT - ©Questel

Title

(EP2401842)

Redirection of secure data connection requests

Images**Publication data including kind & date**

US20100218248	A1	2010-08-26	US20100218248
WO2010098960	A2	2010-09-02	WO201098960
WO2010098960	A3	2010-12-02	WO201098960
EP2401842	A2	2012-01-04	EP2401842
CN102334311	A	2012-01-25	CN102334311
JP2012519416	A	2012-08-23	JP2012519416
US8613072	B2	2013-12-17	US8613072
CN102334311	B	2014-05-07	CN102334311B
JP5540021	B2	2014-07-02	JP5540021
EP2401842	A4	2017-04-05	EP2401842

**Abstract**

(EP2401842)

Methods, systems, and computer-readable media are disclosed for processing a secure data connection request. A particular method receives, at a first gateway, a secure data connection request from a client identifying a server to connect to. The first gateway sends the client device a redirect message instructing the client device to attempt alternate connection via a second gateway. The client sends a secure data connection request to the second gateway and the second gateway facilitates the secure data connection between the client and the server.

Inventors

NICE NIR

SCHULTZ BENJAMIN M

VENKATARAMAIAH NARASIMHAN A

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2010-08-26

2010-09-02

2010-12-02

2012-01-04

2012-01-25

2012-08-23

2013-12-17

2014-05-07

2014-07-02

2017-04-05

Family 46/50 - FAMPAT - ©Questel

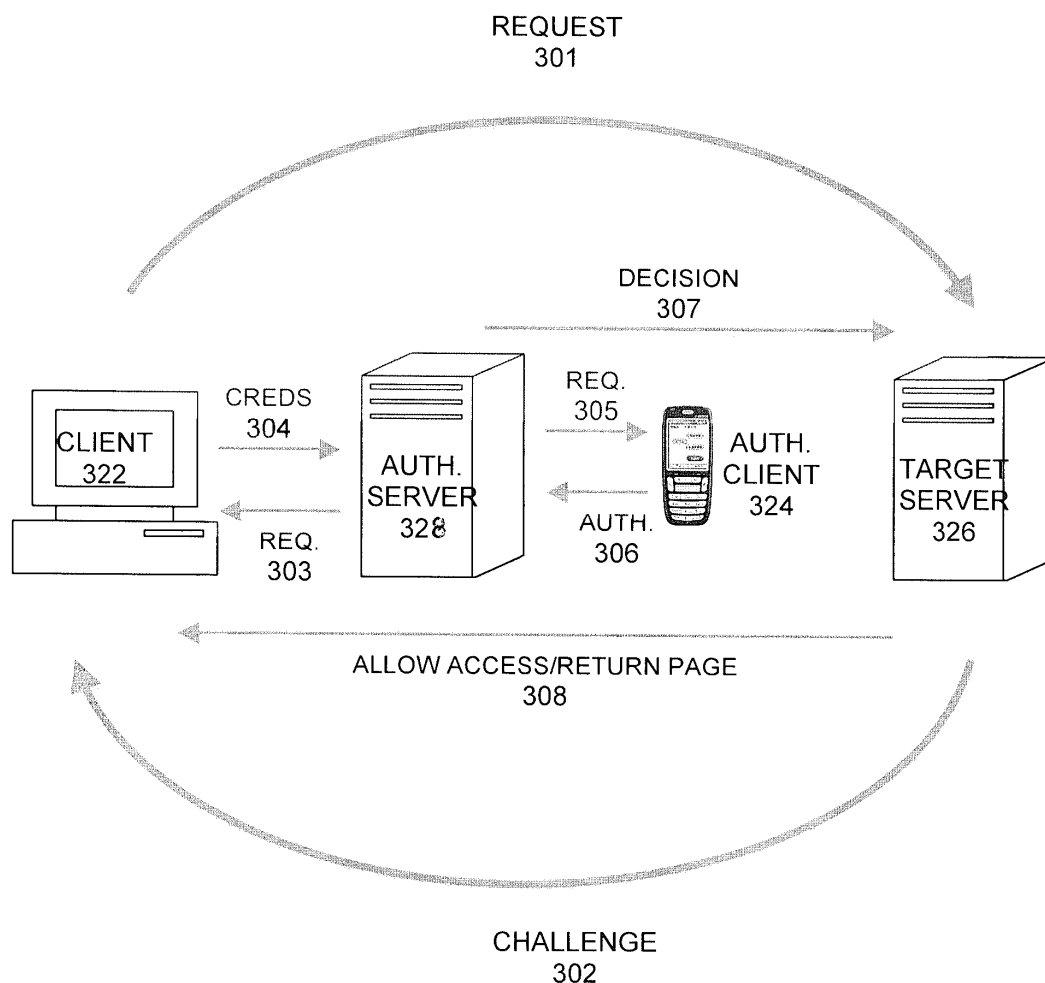
Title

(WO2014105263)

Multi-factor authentication and comprehensive login system for client-server networks

Images

300

**Publication data including kind & date**

US20140189808	A1	2014-07-03	US20140189808
WO2014105263	A1	2014-07-03	WO2014105263
GB201511914	D0	2015-08-19	GB201511914
GB2523710	A	2015-09-02	GB2523710
US9374369	B2	2016-06-21	US9374369

**Abstract**

(WO2014105263)

Embodiments are directed to a system and method for authenticating a user of a client computer making a request to a server computer providing access to a network resource through an authentication platform that issues a challenge in response to the request requiring authentication of the user identity through a reply from the client computer, determining one or more items of context information related to at least one of the user, the request, and the client computer, and determining a disposition of the request based on the reply and the one or more items of context information. The reply includes a user password and may be provided by an authorizing client device coupled to the client computer over a wireless communications link.

Inventors

MAHAFFEY KEVIN PATRICK
 RICHARDSON DAVID LUKE
 SALOMON ARIEL
 CROY R TYLER

WALKER SAMUEL ALEXANDER

BUCK BRIAN JAMES

MARCIN GORRINO SERGIO IVAN

GOLOMBEK DAVID

Latest standardized assignees - inventors removed

LOOKOUT

Publication dates

2014-07-03

2014-07-03

2015-08-19

2015-09-02

2016-06-21

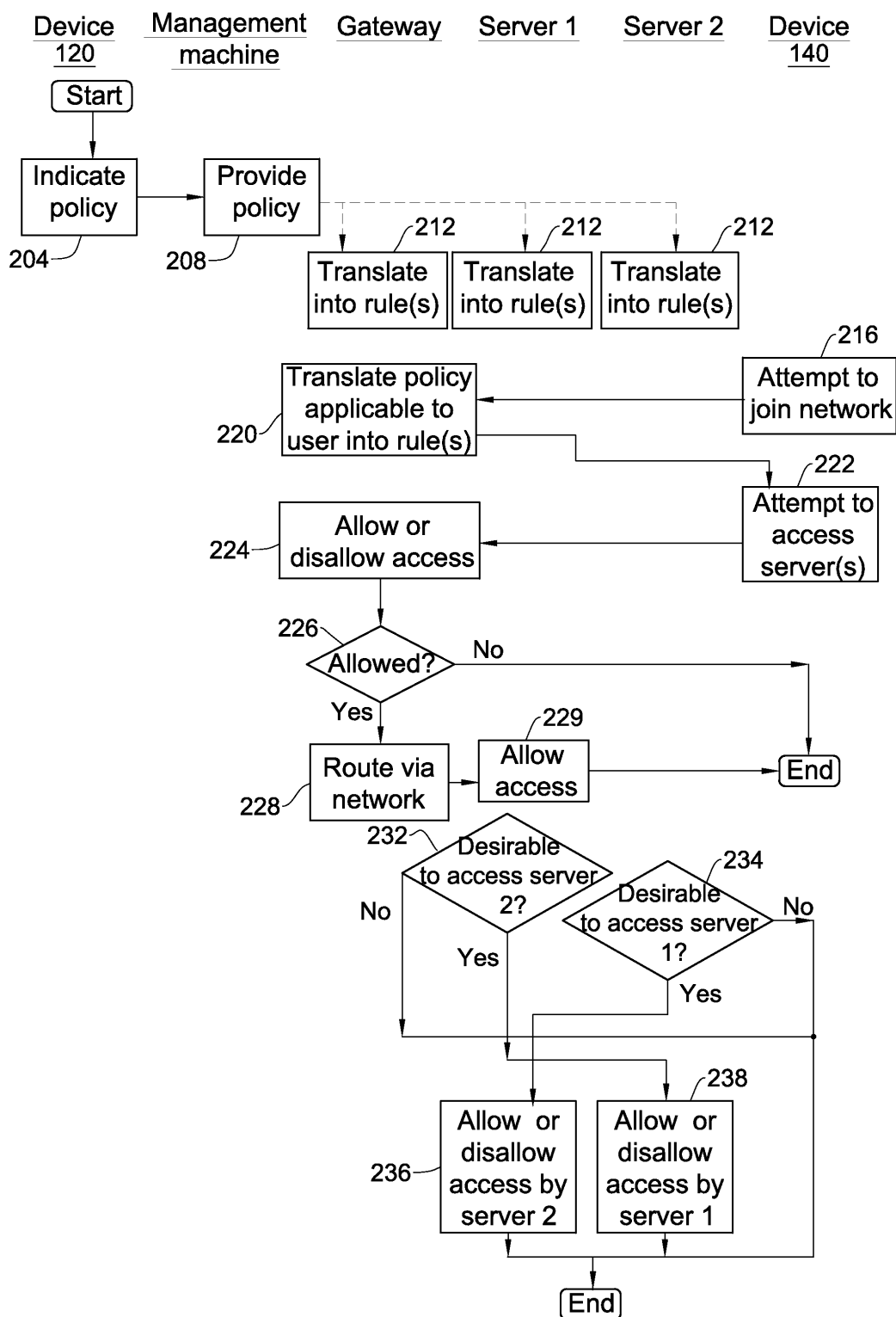
Family 47/50 - FAMPAT - ©Questel

Title

(WO2014141283)

Access control in a secured cloud environment

Images



Publication data including kind & date

US20140282818	A1	2014-09-18	US20140282818
WO2014141283	A1	2014-09-18	WO2014141283



Abstract

(WO2014141283)

The disclosure presents systems, methods and computer program products relating to access control in a secured network. An access control policy may be indicated which at least includes a first entity being allowed to access a second entity, by way of at least one protocol via a secured network. The policy may be translated by at least one gateway or server in the secured network into firewall rule(s) to control access in the secured network.

Inventors

SINGER NOAM

NAFTALI AMIR

Latest standardized assignees - inventors removed

FORTYCLOUD

Publication dates

2014-09-18

2014-09-18

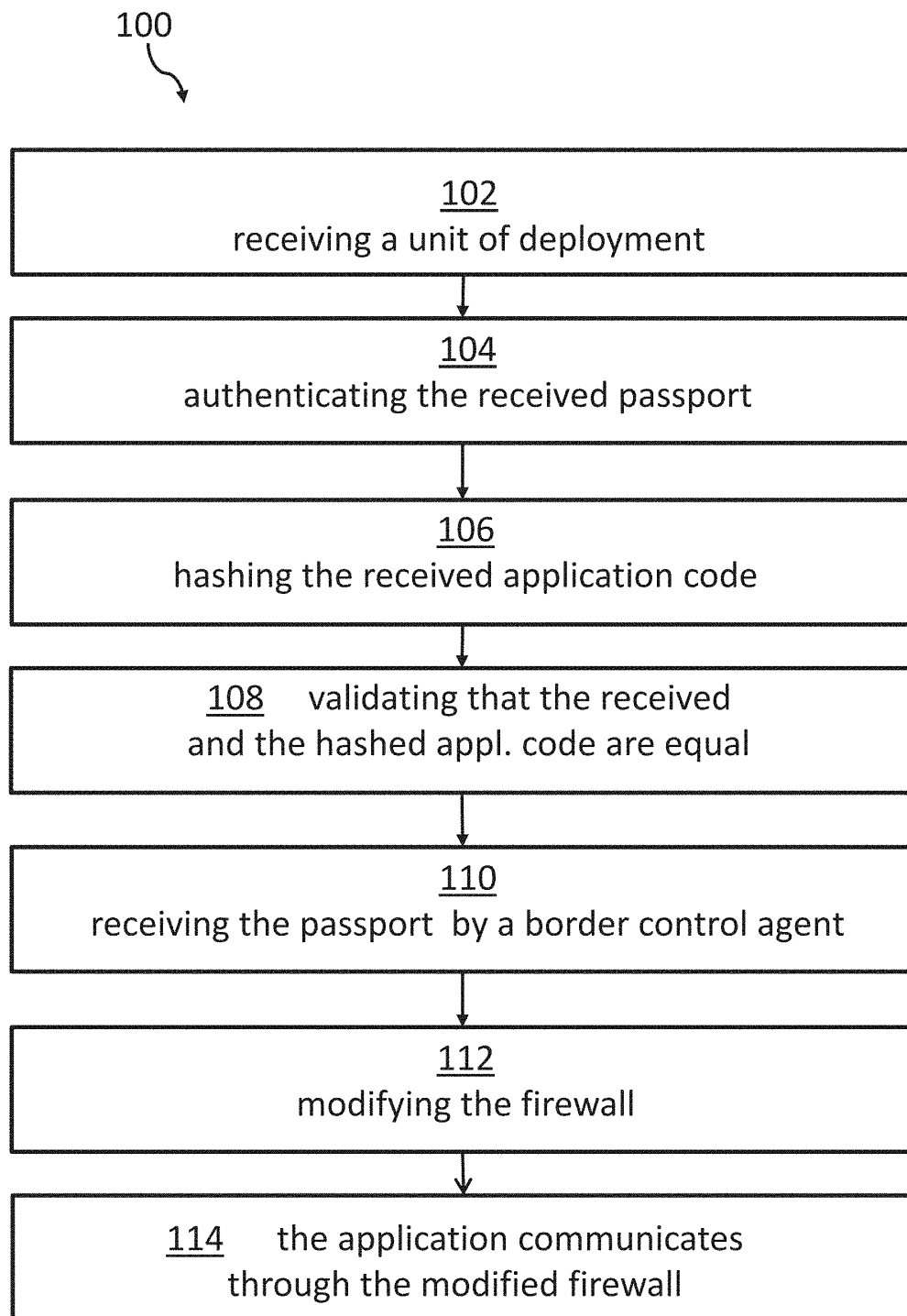
Family 48/50 - FAMPAT - ©Questel

Title

(US9900285)

Passport-controlled firewall

Images



Publication data including kind & date

US20170048198	A1	2017-02-16	US20170048198
US9900285	B2	2018-02-20	US9900285
US20180139182	A1	2018-05-17	US20180139182
US10069798	B2	2018-09-04	US10069798
US20180288003	A1	2018-10-04	US20180288003



Abstract

(US9900285)

A method, and associated system and computer program product, for dynamically modifying rules in a firewall infrastructure. A unit of deployment is received at a requestor module at a server. The unit of deployment includes the

application code and a signed passport. The passport includes a firewall rule and a first application hash value. The received passport is authenticated, the received application code is hashed resulting in a second application hash value, and it is validated that the received first application hash value and the generated application hash value are equal. In response to the validation, the passport is received by a border control agent of the firewall from the server, a firewall is modified in the firewall infrastructure according to the received firewall rule, and communicating with the application is enabled through the modified firewall.

Inventors

FRANK JOACHIM H

KARN HOLGER

Latest standardized assignees - inventors removed

IBM

Publication dates

2017-02-16

2018-02-20

2018-05-17

2018-09-04

2018-10-04

Family 49/50 - FAMPAT - ©Questel

Title

(EP1958093)

Peer-to-peer remediation

Images

Abstract

(EP1958093)

A network in which peer-to-peer remediation is provided to keep clients in the network up-to-date. As network clients establish peer-to-peer connections, they exchange status information. The status information allows the clients to mutually identify whether one client is more out-of-date than another. The more up-to-date client provides update information to the more out-of-date client. To preserve the integrity of the update process, updates are provided as signed binary files and are only applied by the client receiving the update if the binary file may be authenticated by the recipient.

Inventors

CHOE CALVIN CHOON-HWAN

Latest standardized assignees - inventors removed

MICROSOFT TECHNOLOGY LICENSING

Publication dates

2007-06-14

2007-06-14

2008-08-20

2008-09-09

2008-12-17

2009-05-21

2012-08-22

2012-10-16

2013-01-03

2013-01-17

2013-03-06

2014-03-12

2014-12-30

2015-07-22

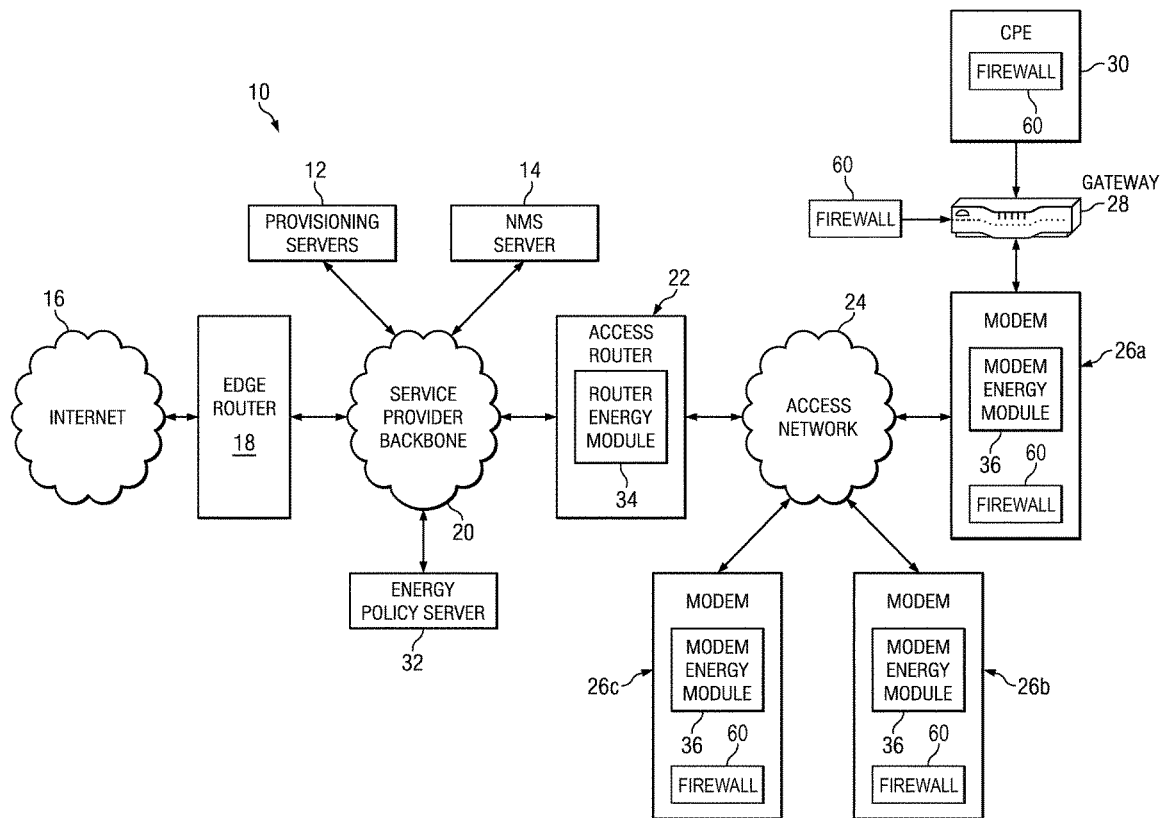
Family 50/50 - FAMPAT - ©Questel

Title

(US9958924)

Configuration of energy savings

Images

**Publication data including kind & date**

US20150067815	A1	2015-03-05	US20150067815
US9958924	B2	2018-05-01	US9958924
US20180239411	A1	2018-08-23	US20180239411

**Abstract**

(US9958924)

According to one example embodiment, a modem or other network device include an energy module configured to enter a low-power, low-bandwidth state when not in active use by a user. The low-power state may be maintained under certain conditions where network activity is not present, and or when only non-bandwidth-critical traffic is present. The network device may include a user interface for configuring firewall rules, and the user may be able to concurrently designate particular types of traffic as important or unimportant. The energy module may also be integrated with a firewall, and power saving rules may be inferred from firewall rules.

Inventors

OVERCASH MICHAEL

Latest standardized assignees - inventors removed

CISCO TECHNOLOGY

Publication dates

2015-03-05

2018-05-01

2018-08-23