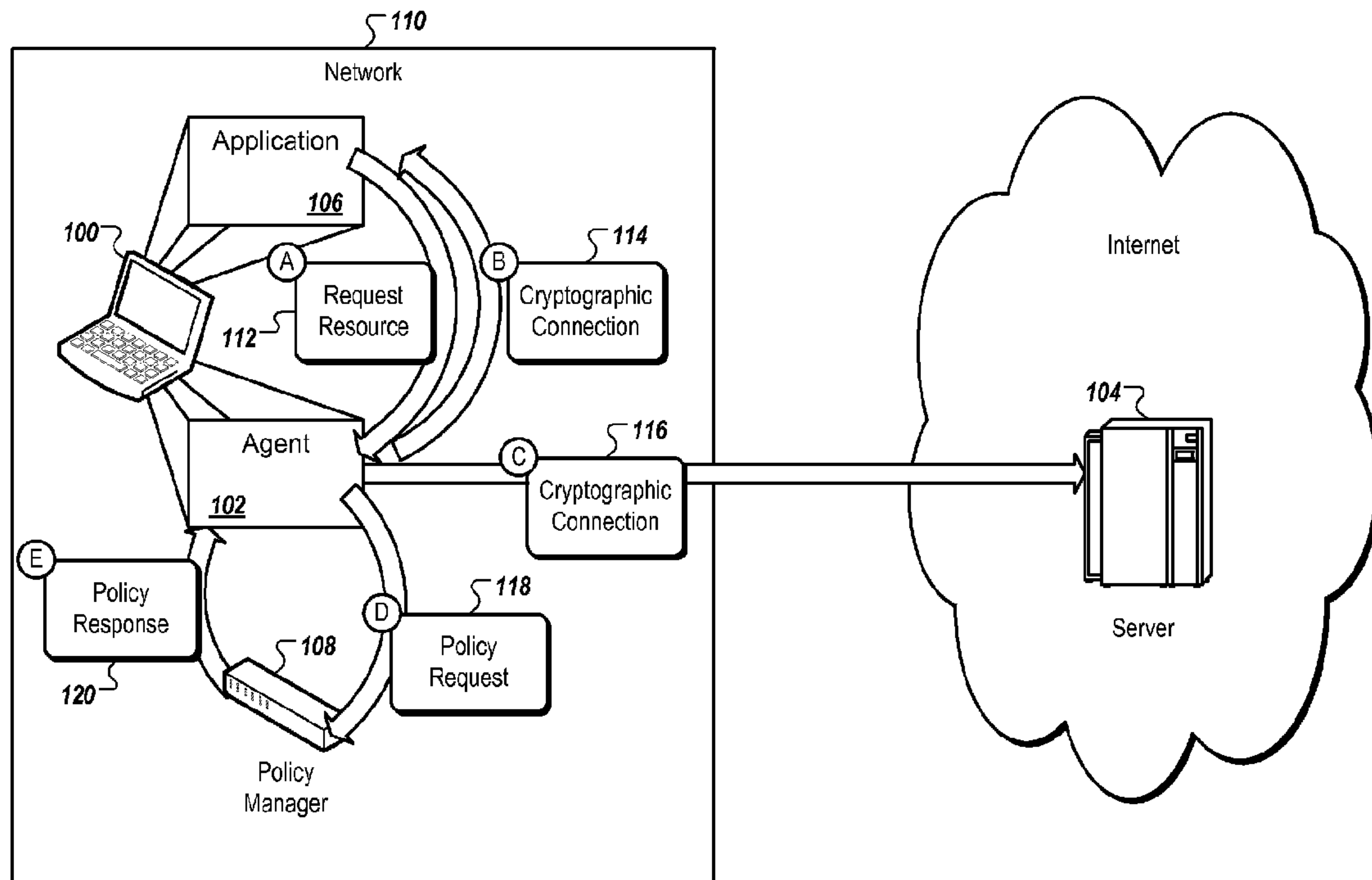




(86) Date de dépôt PCT/PCT Filing Date: 2014/05/06
(87) Date publication PCT/PCT Publication Date: 2014/11/13
(45) Date de délivrance/Issue Date: 2020/01/07
(85) Entrée phase nationale/National Entry: 2015/11/09
(86) N° demande PCT/PCT Application No.: US 2014/037009
(87) N° publication PCT/PCT Publication No.: 2014/182727
(30) Priorité/Priority: 2013/05/08 (US13/890,146)

(51) Cl.Int./Int.Cl. *H04L 9/32* (2006.01)
(72) Inventeur/Inventor:
MARTINI, PAUL MICHAEL, US
(73) Propriétaire/Owner:
IBOSS, INC., US
(74) Agent: SMART & BIGGAR LLP

(54) Titre : REALISATION SELECTIVE D'UN DECHIFFREMENT AVEC INTERVENTION HUMAINE
(54) Title: SELECTIVELY PERFORMING MAN IN THE MIDDLE DECRYPTION



(57) Abrégé/Abstract:

An agent on a device within a network receives a request to access a resource outside the network. A first encrypted connection is established between the device and the agent, and a second encrypted connection is established between the agent and the resource, to facilitate encrypted communication traffic between the device and the resource. The agent sends a policy request to a network appliance within the network, the request specifying the resource. The agent receives a policy response indicating that the resource is associated with one or more security policies of the network. Traffic passing between the device and the resource is selectively decrypted and inspected depending on the security policies.

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

(19) World Intellectual Property
Organization
International Bureau(43) International Publication Date
13 November 2014 (13.11.2014)

WIPO | PCT

(10) International Publication Number
WO 2014/182727 A3

(51) International Patent Classification:

H04L 29/06 (2006.01) *H04L 29/08* (2006.01)

(21) International Application Number:

PCT/US2014/037009

(22) International Filing Date:

6 May 2014 (06.05.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

13/890,146 8 May 2013 (08.05.2013) US

(71) Applicant: **IBOSS, INC.** [US/US]; 9950 Summers Ridge Road, Suite 160, San Diego, California 92121 (US).(72) Inventor: **MARTINI, Paul Michael**; 9950 Summers Ridge Road, Suite 160, San Diego, California 92121 (US).(74) Agent: **PHILLIPS, John C.**; Fish & Richardson P.C., P. O. Box 1022, Minneapolis, Minnesota 55440-1022 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME,

MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

Declarations under Rule 4.17:

— as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))

Published:

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

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

(88) Date of publication of the international search report:

31 December 2014

(54) Title: SELECTIVELY PERFORMING MAN IN THE MIDDLE DECRYPTION

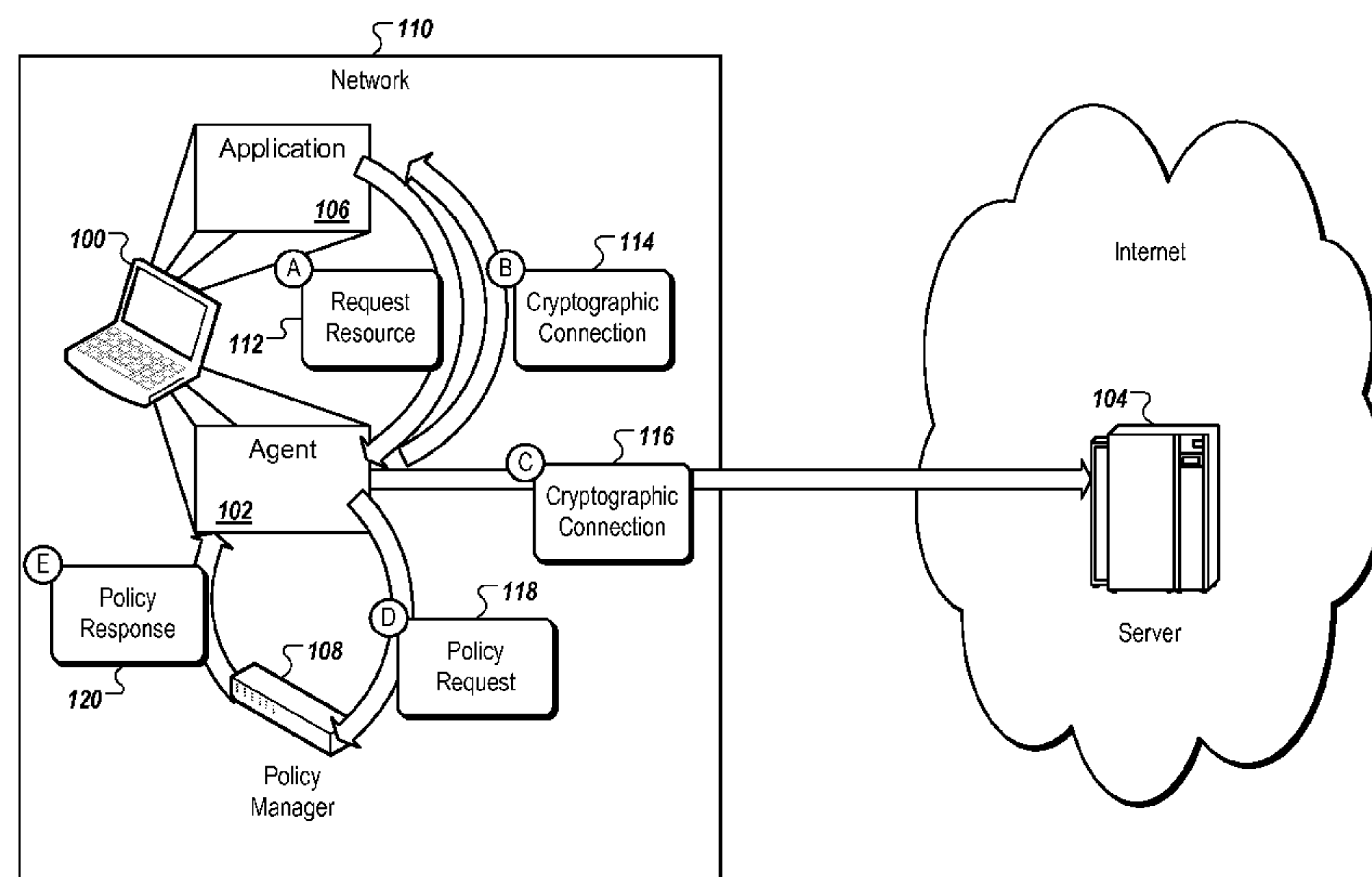


FIG. 1

(57) Abstract: An agent on a device within a network receives a request to access a resource outside the network. A first encrypted connection is established between the device and the agent, and a second encrypted connection is established between the agent and the resource, to facilitate encrypted communication traffic between the device and the resource. The agent sends a policy request to a network appliance within the network, the request specifying the resource. The agent receives a policy response indicating that the resource is associated with one or more security policies of the network. Traffic passing between the device and the resource is selectively decrypted and inspected depending on the security policies.

WO 2014/182727 A3

SELECTIVELY PERFORMING MAN IN THE MIDDLE DECRYPTION

TECHNICAL FIELD

The present document relates to computer networking.

BACKGROUND

[0001] A computer network is a collection of computers and other hardware
5 interconnected by communication channels that allow sharing of resources and
information. Communication protocols define the rules and data formats for exchanging
information in a computer network. Transport Layer Security (TLS) and Secure Socket
Layer (SSL) are two examples of cryptographic communication protocols that provide
communication security by allowing devices to exchange encrypted, as opposed to
10 plaintext, messages.

SUMMARY

[0002] In one aspect, a method is performed by data processing apparatus. The
method includes receiving, by an agent on a device within a network, a request to access
a resource outside the network. The method further includes establishing a first
15 encrypted connection between the device and the agent, and a second encrypted
connection between the agent and the resource, to facilitate encrypted communication
traffic between the device and the resource. The method further includes sending, by the
agent in response to receiving the request to access the resource, a policy request to a
network appliance within the network, the request specifying the resource. The method
20 further includes receiving, by the agent and from the network appliance, a policy
response indicating that the resource is associated with one or more security policies of
the network. The method further includes selectively decrypting and inspecting the

encrypted communication traffic passing between the device and the resource depending on the security policies.

[0003] Implementations can include any, all, or none of the following features.

The device and the network appliance are subject to the same administrative control.

5 Decrypting and inspecting the encrypted communication traffic includes blocking the encrypted communication traffic. The request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request. The method including receiving, by the agent, a second request to access a second resource outside the network; determining that the second recourse is on a
10 whitelist that lists resources for which man-in-middle analysis should not apply; causing the establishment, responsive to determining that the second recourse is on the whitelist, a third encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource. The method including removing the device from the network; receiving, by the agent, a third
15 request to access a third resource outside the network; establishing a fourth encrypted connection between the device the agent, and a fifth encrypted connection between the agent and the third resource, to facilitate encrypted communication traffic between the device and the third resource; sending, by the agent in response to receiving the third request to access the resource, a third policy request to the network appliance, the request
20 specifying the third resource; receiving, by the agent and from the network appliance, a third policy response indicating that the third resource is associated with one or more security policies of the network; and selectively decrypting and inspecting the encrypted communication traffic passing between the device and the third resource depending on

the security policies. The agent is a driver installed in a protocol stack of the device. The agent is configured to receive requests to access resources from a plurality of applications of the device.

[0004] In one aspect, non-transitory computer storage media encoded with
5 computer program instructions that, when executed by one or more processors, cause a computer device to perform operations. The operations include receiving, by an agent on a device within a network, a request to access a resource outside the network. The operations further include establishing a first encrypted connection between the device and the agent, and a second encrypted connection between the agent and the resource, to
10 facilitate encrypted communication traffic between the device and the resource. The operations further include sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource. The operations further include receiving, by the agent and from the network appliance, a policy response indicating that the resource is
15 associated with one or more security policies of the network. The operations further include selectively decrypting and inspecting the encrypted communication traffic passing between the device and the resource depending on the security policies.

[0005] Implementations can include any, all, or none of the following features. The device and the network appliance are subject to the same administrative control.
20 Decrypting and inspecting the encrypted communication traffic includes blocking the encrypted communication traffic. The request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request. The operations further include receiving, by the agent, a second request to

access a second resource outside the network; determining that the second recourse is on
a whitelist that lists resources for which man-in-middle analysis should not apply;
causing the establishment, responsive to determining that the second recourse is on the
whitelist, a third encrypted connection between the device and the second resource to
5 facilitate encrypted communication traffic between the device and the second resource.
The operations further include removing the device from the network; receiving, by the
agent, a third request to access a third resource outside the network; establishing a fourth
encrypted connection between the device the agent, and a fifth encrypted connection
between the agent and the third resource, to facilitate encrypted communication traffic
10 between the device and the third resource; sending, by the agent in response to receiving
the third request to access the resource, a third policy request to the network appliance,
the request specifying the third resource; receiving, by the agent and from the network
appliance, a third policy response indicating that the third resource is associated with one
or more security policies of the network; and selectively decrypting and inspecting the
15 encrypted communication traffic passing between the device and the third resource
depending on the security policies. The agent is a driver installed in a protocol stack of
the device. The agent is configured to receive requests to access resources from a
plurality of applications of the device.

[0006] In one aspect, a system includes one or more processors configured to
20 execute computer program instructions. The system further includes non-transitory
computer storage media encoded with computer program instructions that, when
executed by one or more processors, cause a computer device to perform operations. The
operations include receiving, by an agent on a device within a network, a request to

access a resource outside the network. The operations further include establishing a first encrypted connection between the device and the agent, and a second encrypted connection between the agent and the resource, to facilitate encrypted communication traffic between the device and the resource. The operations further include sending, by
5 the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource. The operations further include receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network. The operations further include selectively decrypting and
10 inspecting the encrypted communication traffic passing between the device and the resource depending on the security policies.

[0007] Implementations can include any, all, or none of the following features. The device and the network appliance are subject to the same administrative control. Decrypting and inspecting the encrypted communication traffic includes blocking the
15 encrypted communication traffic. The request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request. The operations further include, by the agent, a second request to access a second resource outside the network; determining that the second resource is on a whitelist that lists resources for which man-in-middle analysis should not apply; causing the
20 establishment, responsive to determining that the second resource is on the whitelist, a third encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource. The operations further include removing the device from the network; receiving, by the agent,

a third request to access a third resource outside the network; establishing a fourth encrypted connection between the device the agent, and a fifth encrypted connection between the agent and the third resource, to facilitate encrypted communication traffic between the device and the third resource; sending, by the agent in response to receiving the third request to access the
 5 resource, a third policy request to the network appliance, the request specifying the third resource; receiving, by the agent and from the network appliance, a third policy response indicating that the third resource is associated with one or more security policies of the network; and selectively decrypting and inspecting the encrypted communication traffic passing between the device and the third resource depending on the security policies. The
 10 agent is a driver installed in a protocol stack of the device. The agent is configured to receive requests to access resources from a plurality of applications of the device.

[0007a] In another aspect, there is provided a method performed by data processing apparatus, the method involves: receiving, by an agent on a device within a network, a request to access a resource outside the network; determining that the resource is not on a whitelist
 15 that lists resources for which man-in-the-middle analysis should not apply; establishing a device/agent encrypted connection having endpoints at the device and the agent; establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication
 20 traffic between the device and the resource and wherein the device/agent encrypted connection and the agent/resource encrypted connection are in different formats; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource, wherein the network appliance is different than the device; receiving, by the agent and from the network appliance,
 25 a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside of the network; and decrypting and inspecting at
 30 least some of the encrypted communication traffic passing between the device and the resource.

[0007b] In another aspect, there is provided a non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations including: receiving, by an agent on a device within a network, a request to access a resource outside the network; determining that the resource is not on a whitelist that lists resources for which man-in-the-middle analysis should not apply; establishing a device/agent encrypted connection having endpoints at the device and the agent; establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication traffic between the device and the resource and wherein the device/agent encrypted connection and the agent/resource encrypted connection are in different formats; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource, wherein the network appliance is different than the device; receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside of the network; and decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource.

[0007c] In another aspect, there is provided a system including one or more processors configured to execute computer program instructions. The system further includes non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations including: receiving, by an agent on a device within a network, a request to access a resource outside the network; determining that the resource is not on a whitelist that lists resources for which man-in-the-middle analysis should not apply; establishing a device/agent encrypted connection having endpoints at the device and the agent; establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the

agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication traffic between the device and the resource and wherein the device/agent encrypted connection and the agent/resource encrypted connection are in different formats; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource, wherein the network appliance is different than the device; receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside of the network; and decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource.

[0007d] In another aspect, there is provided a method performed by data processing apparatus. The method involves: receiving, by an agent on a device within a network, a request to access a resource outside the network; establishing, by the agent, a device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device; establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource; receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network; decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies; decrypting and selectively inspecting, by the agent, encrypted communication traffic from the resource and address to the device, depending on the security policies; receiving, by the agent, a second request to access a second resource outside the network; determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and causing the establishment, responsive to determining that the second resource is on

the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource; wherein the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource encrypted connection are separate and have
 5 different formats.

[0007e] In another aspect, there is provided a non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations including: receiving, by an agent on a device within a network, a request to access a resource outside the network; establishing, by the
 10 agent, a device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device; establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within
 15 the network, the request specifying the resource; receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network; decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies; decrypting and selectively inspecting, by the agent, encrypted
 20 communication traffic from the resource and address to the device, depending on the security policies; receiving, by the agent, a second request to access a second resource outside the network; determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted
 25 connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource; wherein the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource encrypted connection are separate and have different formats.

[0007f] In another aspect, there is provided a system including one or more processors
 30 configured to execute computer program instructions. The system further includes non-

transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations including: receiving, by an agent on a device within a network, a request to access a resource outside the network; establishing, by the agent, a device/agent encrypted connection between the device

5 and the agent such that the agent is configured to act as a proxy of the resource to the device; establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource; sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource;

10 receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network; decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies; decrypting and selectively inspecting, by the agent, encrypted communication traffic from the resource and address to the

15 device, depending on the security policies; receiving, by the agent, a second request to access a second resource outside the network; determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device and the second resource to

20 facilitate encrypted communication traffic between the device and the second resource; wherein the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource encrypted connection are separate and have different formats.

[0007g] In another aspect, there is provided a device including: memory for storing machine instructions, an agent, and an operating system; and a transceiver configured to enable the

25 device to communicate with a policy manager on a first network, and one or more resources. The system further includes a processor for executing machine instructions stored in the memory, wherein execution of the machine instructions causes the device to perform operations including the following: alternately performing either (a) or (b) depending on whether the device is hosted on the first network or on a second network other than the first

30 network: (a) if a device is hosted on a first network: (i) receiving, by an agent on the device, a

first request to access a resource outside the first network, wherein the first request is transmitted from an operating system of the device to the agent without being transmitted outside of the device; (ii) transmitting, by the agent on the device, a first policy request to a policy manager hosted on the first network in response to the agent's receiving the first request, wherein the first policy request is routed from the agent on the device to the policy manager hosted on the first network without leaving the first network; (iii) receiving, by the agent on the device, a first policy response from the policy manager, the first policy response instructing the agent to monitor communication between the device and the resource; (iv) establishing, by the agent on the device, a device/agent encrypted connection between the device's operating system and the agent such that communication traffic of the device/agent encrypted connection is not transmitted outside the device; (v) establishing, by the agent on the device, an agent/resource encrypted connection between the agent on the device and the resource such that communication traffic of the agent/resource encrypted connection enters and exits the first network at a gateway of the first network; and (vi) monitoring, by the agent on the device, communication between the device's operating system and the resource; wherein monitoring, by the agent, communication between the device's operating system and the resource includes: receiving, from the device's operating system, first encrypted communication traffic from the device/agent encrypted connection; decrypting the first encrypted communication traffic into first decrypted communication traffic; inspecting the first decrypted communication traffic; encrypting the first decrypted communication traffic into second encrypted communication traffic; and transmitting, to the resource, the agent/resource encrypted communication traffic on the agent/resource encrypted connection and (b) alternatively, if the device is hosted on a second network other than the first network: (i) receiving, by the agent on the device, a second request to access the resource, wherein the request is transmitted from the operating system of the device to the agent without being transmitted outside of the device; (ii) transmitting, by the agent on the device, a second policy request to the policy manager hosted on the first network in response to the agent's receiving the second request, wherein the second policy request is routed from the second network to the first network in order to reach the policy manager on the first network; (iii) receiving, by the agent on the device, a second policy response from the policy manager, the policy response

instructing the agent to monitor communication between the device and the resource; (iv) establishing, by the agent on the device, a device/second resource encrypted connection between the device's operating system and the agent such that communication traffic of the device/second resource encrypted connection is not transmitted outside the device; (v) 5 establishing, by the agent on the device, a second device/agent encrypted connection between the agent and the resource such that communication traffic of the second device/agent encrypted connection is routed between the agent on the device and the resource without being routed to the first network; and (vi) monitoring, by the agent, communication between the device's operating system and the resource wherein monitoring, by the agent, communication 10 between the device's operating system and the resource includes: receiving, from the device's operating system, third encrypted communication traffic from the device/second resource encrypted connection; decrypting the third encrypted communication traffic into second decrypted communication traffic; inspecting the second decrypted communication traffic; encrypting the second decrypted communication traffic into fourth encrypted communication 15 traffic; and transmitting, to the resource, the fourth encrypted communication traffic on the second device/agent encrypted connection.

[0007h] In another aspect, there is provided a device including: memory for storing machine instructions, an agent, and an operating system; and means for communicating with a policy manager on a first network, and one or more resources. The device further includes a 20 processor for executing machine instructions stored in the memory, wherein execution of the machine instructions causes the device to perform operations including the following: alternately performing either (a) or (b) depending on whether the device is hosted on the first network or on a second network other than the first network: (a) if a device is hosted on a first network: (i) receiving, by an agent on the device, a first request to access a resource outside 25 the first network, wherein the first request is transmitted from an operating system of the device to the agent without being transmitted outside of the device; (ii) transmitting, by the agent on the device, a first policy request to a policy manager hosted on the first network in response to the agent's receiving the first request, wherein the first policy request is routed from the agent on the device to the policy manager hosted on the first network without leaving 30 the first network; (iii) receiving, by the agent on the device, a first policy response from the

policy manager, the first policy response instructing the agent to monitor communication between the device and the resource; (iv) establishing, by the agent on the device, a device/agent encrypted connection between the device's operating system and the agent such that communication traffic of the device/agent encrypted connection is not transmitted outside the device; (v) establishing, by the agent on the device, an agent/resource encrypted connection between the agent on the device and the resource such that communication traffic of the agent/resource encrypted connection enters and exits the first network at a gateway of the first network; and (vi) monitoring, by the agent on the device, communication between the device's operating system and the resource wherein monitoring, by the agent, communication between the device's operating system and the resource involves: receiving, from the device's operating system, first encrypted communication traffic from the device/agent encrypted connection; decrypting the first encrypted communication traffic into first decrypted communication traffic; inspecting the first decrypted communication traffic; encrypting the first decrypted communication traffic into second encrypted communication traffic; and transmitting, to the resource, the second encrypted communication traffic on the agent/resource encrypted connection; and (b) alternatively, if the device is hosted on a second network other than the first network: (i) receiving, by the agent on the device, a second request to access the resource, wherein the request is transmitted from the operating system of the device to the agent without being transmitted outside of the device; (ii) transmitting, by the agent on the device, a second policy request to the policy manager hosted on the first network in response to the agent's receiving the second request, wherein the second policy request is routed from the second network to the first network in order to reach the policy manager on the first network; (iii) receiving, by the agent on the device, a second policy response from the policy manager, the policy response instructing the agent to monitor communication between the device and the resource; (iv) establishing, by the agent on the device, a device/second resource encrypted connection between the device's operating system and the agent such that communication traffic of the device/second resource encrypted connection is not transmitted outside the device; (v) establishing, by the agent on the device, a second device/agent encrypted connection between the agent and the resource such that communication traffic of the second device/agent encrypted connection is routed between the agent on the device and

the resource without being routed to the first network; and (vi) monitoring, by the agent, communication between the device's operating system and the resource wherein monitoring, by the agent, communication between the device's operating system and the resource involves: receiving, from the device's operating system, third encrypted communication traffic from the device/second resource encrypted connection; decrypting the third encrypted communication traffic into second decrypted communication traffic; inspecting the second decrypted communication traffic; encrypting the second decrypted communication traffic into fourth encrypted communication traffic; and transmitting, to the resource, the fourth encrypted communication traffic on the second device/agent encrypted connection.

10 **[0007i]** In another aspect, there is provided a system including: a network hosting a policy manager and a first plurality of clients each of the first plurality of client including an agent; and a second plurality of clients, each of the second plurality of clients external to the network and communicably coupled with the policy manager, wherein each of the second plurality of clients includes an agent. The policy manager is configured to: receive, from each of the agents, policy requests; and return, responsive to receiving the policy, a corresponding policy response indicating a policy. The agents are configured to: receive, from the agent's client, a resource request; responsive to receiving the resource request, send to the policy manager the policy requests; receive, from the policy manager, the corresponding policy responses; and apply, to the agent's client, the policy indicated by the corresponding policy response to the resource request.

20 **[0007j]** In another aspect, there is provided a method performed by data processing apparatus. The method involves receiving, by a policy manager, policy requests from a first plurality of clients wherein each of the clients includes an agent, at least a first plurality of the clients being hosted on a network that hosts the policy manager, at least a second plurality of clients being external to the network and communicably coupled with the policy manager, and each of the agents are configured to: receive, from the agent's client, a resource request; responsive to receiving the resource request, send to the policy manager the policy request; receive, from the policy manager, a corresponding policy response; and apply, to the agent's client, the policy indicated by the corresponding policy response to the resource request. The

method further involves returning, by the policy manager, the corresponding policy response indicating a policy.

[0008] The systems and processes described here may be used to provide any of a number of potential advantages. By performing man in the middle analysis on the device initiating encrypted traffic, the computational load needed to perform the man in the middle analysis can be handled by the initiating device. Performing the man in the middle on the device also ensures that the plaintext of the message never needs to be generated outside of the device, increasing security. An agent performing man in the middle on the device allows a network security policy to apply to the device, even when the device is not in communication with the network. If the agent is in communication with the network, up-to-date policy changes can be reflected without returning the device to the network.

DESCRIPTION OF DRAWINGS

[0009] FIG. 1 is a block diagram of a computer with a man in the middle agent communicating with a remote resource.

[0010] FIG. 2 is a block diagram of a man in the middle agent on a computer that
5 has moved out of the network.

[0011] FIG. 3 is a swim-lane diagram of an example process for establishing a communication link through a man in the middle agent.

[0012] FIG. 4 is a block diagram showing a device with a man in the middle agent.

10 [0013] FIG. 5 is a schematic diagram that shows an example of a computing device and a mobile computing device.

[0014] Like reference symbols in the various drawings indicate like elements

DETAILED DESCRIPTION

[0015] When data on a network is encrypted (e.g., by SSL or TLS) the data can
15 pose challenges to network security appliances and routines in that it makes it difficult to inspect the data as it is transferred between the end users and servers on the Internet. This can lead to problems such as viruses being transferred over secure connections and entering the network instead of being blocked because the gateway security appliances could not inspect the data. In addition, organizational policies cannot be applied since the
20 data within the encrypted traffic is protected causing security functions to fail as they cannot inspect the data.

[0016] Described in this document is a use of man in the middle (MitM) encryption and decryption performed locally by each computer. Agents residing on each

network device can intercept requests to initiate encrypted communication sessions and insert themselves as men in the middle. The agents can then pass relevant information (e.g., URL) to a policy manager in a side band channel. The policy manager may then indicate blocking or other action based on a centralized policy.

5 [0017] By using an agent on each computer, as opposed to a single network device performing MitM inspection for all traffic on the network, each computer handles their own encryption and decryption. This allows the number of computers to scale without creating a bottleneck on a single piece of hardware dedicated to MitM inspection.

[0018] FIG. 1 is a block diagram of a computer 100 with a man in the middle
10 agent 102 communicating, on behalf of an application 106, with a remote resource on a server 104. The computer 100 represents any appropriate computing device capable of browsing remote resources. Also shown is a policy manager 108 on the same network 110 as the computer 100. While not shown for clarity's sake, the network 110 can include other elements including, but not limited to, wireless and/or wired access points,
15 file and/or application servers, network gateways, routers, and network cables, as well as additional computers 100 and/or policy managers 108.

[0019] The computer 100 can be configured to route all incoming and outgoing messages through the agent 102. For example, the application 106 may generate a request 112 to access a resource on the server 104. The agent 102 can intercept the
20 request 112 and, instead of passing the request to the server 104, can initiate a cryptographic connection 114 with the application 106 and a second cryptographic connection 116 with the server 104. By creating these two cryptographic connections 114 and 116, the agent 102 can in effect inserted itself as a MitM between the application

106 and the server 104. Future messages to be sent from the application 106 to the server 104, or vice versa, are decrypted, optionally inspected and acted upon (modified, dropped, logged), and then re-encrypted by the agent 102. In general, dropping a connection blocks the resource from the application. Modifying a request can be used to, for example, block or redirect a request. A resource can be blocked by redirecting to a website explaining that a requested resource is in violation of a security policy. A redirection can also be used to change where a resource is received from. For example, a request to a web search engine may be redirected to a different search engine that has content filters.

10 [0020] After creating the encrypted connections 114 and 116, the agent 102 can send a policy request 118 to the policy manager 108. The policy request 118 can specify, for example, the name, universal resource locator (URL), or other information of the resource accessed by the application 106. The policy manager can determine if there is one or more network policies associated with the network 110 that apply to the resource.

15 The policy manager 108 can return a policy response 120 to the agent 102. The policy response 120 may include, for example, instruction on actions (e.g. modify, drop, log) to apply to communications between the application 106 and the server 104 and/or a list of the policies that apply to the resource. Based on the policy response 120, the agent 102 can take any appropriate action on the communication between the application 106 and the server 104, including no action.

20

[0021] Inspection, alteration, dropping, or logging of communication by the agent 102 can ensure that encrypted communication into and out of the computer 100 conforms to any number of policies. For example, the network 110 may have a policy of inspecting

incoming messages for computer viruses, malware, or other unwanted content. The agent 102 may apply these policies to the encrypted traffic of the computer 100 inspecting incoming messages in their decrypted state and dropping any messages that fail the same tests as applied by the policy manager 108. In some configurations, plaintext traffic to and from the computer 100 can be inspected by the agent 102, with similar actions taken on the plaintext messages as is taken on encrypted messages. In some configurations, policies can be applied to plaintext messages when they enter or exit the network. For example, a network gateway (not shown) through which network traffic enters and exits the network 100 can examine the plaintext messages and act on the messages as specified by the policies of the network.

[0022] Although only one computer 100 is shown, additional, and different types of, computers may be on the network 110. These computers may have different hardware profiles, operating systems, and installed applications. For example, the network 110 may include a heterogeneous group of laptops, desktop computers, and mobile devices including cell phones and tablet computers. Different versions of the agent 102 may be developed and deployed on these devices, as appropriate. Each agent may be, for example, operating system specific, and may accomplish the actions described using operating system techniques. An agent for one operating system may, for example, be installed as a driver in the network stack of an operating system while an agent for another operating system may be, for example, a service that alters the firewall of the operating system.

[0023] The agent 106 may also perform other actions in addition to those already described. For example, the agent 106 may install one or more public key certificates

into the computer 100. These certificates may, for example, prevent the application 106 from creating warning or error messages that indicate an unknown MitM agent is intercepting the computer's 100 communications.

[0024] Additionally or alternative, the agent 102 may store a whitelist of
5 resources for which no MitM is to be applied. For example, the computer 100 may include a virtual private network (VPN) client used to virtually join other networks (not shown) administered by the same administrator that administrates the network 110. The agent 102 may keep a record of this VPN connection in a whitelist and, when the application 106 initiates the VPN connect, determine that the connection is on the
10 whitelist. When such a connection is identified, the agent 102 may be configured not to intercept the connection request, allowing the connection to be made without the agent 102 acting as a MitM. The agent 102 may be configured to populate and update this whitelist from, for example, the policy manager 108.

[0025] FIG. 2 is a block diagram of the man in the middle agent 102 on the
15 computer 100 after the computer 100 has moved out of the network 110. For example, the user of the computer 100 may have, in FIG. 1, used the computer 100 on a network 110 during the day while at work or school, taken the computer 100 home, and then connected the computer 100 to the user's home network or the network of a coffee shop (not shown). As such, the computer 100 remains under the same administrative control
20 as the network 110 and still subject to the policy determinations of the policy manager 108, even though not on the network 110.

[0026] Similar to as described with respect to FIG. 1, the application 106 can generate a request 212 to access a resource on a server 204. The agent 102 can intercept

the request 212 and initiate cryptographic connections 114 and 116. Once created, the agent 102 can send a policy request 218 to the policy manager and receive a policy response 220. Based on the policy response 220, the agent 102 can perform the appropriate MitM actions on communications between the application 106 and the server 204.

5 [0027] In contrast with FIG 1, in FIG. 2, the computer 100, and thus the agent 102, is not on the network 110. However, the agent 102 can still communicate with the policy manager 108, receiving up to date policy responses 220, even if a policy has changed before the computer 100 is brought back onto the network 110. Additionally, once the agent 102 has created the cryptographic connections 214 and 216, data between the computer 100 and the server 204 need not be routed through the network 110 to have the policies of the network 110 applied.

10 [0028] FIG. 3 is a swim-lane diagram of an example process 300 for establishing a communication link through a man in the middle agent 102. The process 300 is described with reference to the components shown in FIG. 1. However, other components, including and not limited to the components shown in FIG. 2, can be used to perform the process 300 or a similar process.

15 [0029] The application 106 creates a request to access a resource outside the network (302). For example, the application 106 may be a web browser, and a user may have entered a webpage to request. In another example, the application 106 may be an email client configured to request updates to a user's inbox on a regular basis. The request may take the form of any appropriate message defined by any appropriate protocol. Example messages include, but are not limited to, Hypertext Transfer Protocol

20

(HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST requests, File Transfer Protocol (FTP) RETR requests, or a TLS ClientHello message. The request may also include an identifier of the resource, such as a URL or Internet Protocol (IP) address.

5 **[0030]** The agent 102 compares the resource to a whitelist (304). The agent 102 may store a whitelist of resources identified by, for example, name, URL, or IP address. This whitelist lists resources for which the agent 102 should not perform MitM decryption and encryption. Alternatively, the agent 102 can store a blacklist of resources for which MitM decryption and encryption should be applied. If the resource is on the
10 whitelist, or not on the blacklist, the resource server 104 establishes a cryptographic connection with the application 106 (306). Once established, the application 106 and resource server 104 can pass encrypted traffic back and forth.

[0031] If the resource is not on the whitelist, if no whitelist is used, or if the resource is on the blacklist, the agent 102 establishes a first cryptographic connection
15 with the application 106 (308). The agent 102 requests a cryptographic connection with the resource server 104 (310) and the resource server 104 establishes the cryptographic connection with the agent 102 (312). For example, the agent 102 may act as a proxy for the resource server 104, mimicking the interface of the resource server 104 in communications with the application 106. The agent 102 may also act as a proxy for the
20 application 106, mimicking the interface of the application 106 in communication with the resource server 104. The two encryption sessions may be of the same or different formats or types.

[0032] The agent 102 creates a policy request for the resource (102) and the policy manager 108 replies with a policy request (316). For example, once the two encrypted connections are established, the agent 102 can send information about the resource and/or the connections to the policy manager 108. The policy manager 108 can
5 determine if one or more of the policies of the network 110 apply to the resource and or connections.

[0033] If no policies apply, the policy manager 108 can return a policy response to the agent 102 indicating that no policies apply and/or that the agent 102 should perform no or minimal MitM analysis. For example, the resource may be a news website with no
10 history of hosting malicious code. The policy manager 108 may determine that no network policies apply to the news website and return a policy response indicating as such. The agent 102 may then apply only the basic MitM analysis that is to be applied to all traffic (e.g. virus scanning).

[0034] If one or more policies do apply, the policy manager 108 can return a
15 policy response to the agent 102 a policy response indicating that the resource is associated with one or more security policies. For example, the policy response may list the applicable policies, or the MitM actions that the agent 102 should take on the related traffic.

[0035] The application 106 generates traffic, encrypts the traffic into a first
20 encrypted form, and passes the traffic to the agent 102 (318). For example, the application 106 can create a HTTP Get request for the data object. The application 106 can encrypt the HTTP Get request according to the requirements of the encrypted connection with the agent 102 and pass the encrypted HTTP Get request to the agent 102.

[0036] The agent 102 receives the traffic, decrypts the traffic, inspects the traffic, encrypts the traffic into a second encrypted form, and passes the traffic to the resource server 104 (320). For example, the agent 102 can decrypt the encrypted message into plaintext and determine that the message is an HTTP Get request. The agent 102 can
5 compare the HTTP Get request with the actions or rules of policies specified by the policy response from the policy manager 108. If the HTTP Get request does not match any of the actions, the agent 102 can encrypt the HTTP Get request according to the requirements of the encrypted connection with the resource server 104 and pass the encrypted HTTP Get request to the resource server 104. If the HTTP Get request does
10 match, the agent 102 can modify, log, or drop the request, as appropriate.

[0037] The resource server 104 receives the traffic in the second encrypted form (322). For example, the resource server 104 may receive the encrypted HTTP Get request, decrypt the HTTP Get request, and determine that the user of the application 106 has authorization to access the requested data object.

15 [0038] The resource server 104 generates traffic, encrypts the traffic into a third encrypted form, and passes the traffic to the agent 102 (324). For example, the resource server 104 can access the requested data object, format the data object into XML or other appropriate format, and add the XML object to an HTTP reply. The resource server 104 can encrypt the HTTP reply according to the requirements of the encrypted connection
20 with the agent 102 and pass the encrypted HTTP reply to the agent 102

[0039] The agent 102 receives the traffic, decrypts the traffic, inspects the traffic, encrypts the traffic into a fourth form, and passes the traffic to the application 106 (326). For example, the agent 102 can decrypt the encrypted message into plaintext and

determine that the message is an HTTP reply. The agent 102 can compare the HTTP reply with the actions or rules of policies specified by the policy response from the policy manager 108. If the HTTP reply does not match any of the actions, the agent 102 can encrypt the HTTP reply according to the requirements of the encrypted connection with the application 106 and pass the encrypted HTTP reply to the application 106. If the HTTP reply does violate a policy (e.g., contains malicious code, too large), the agent 102 can modify, log, or drop the reply, as appropriate. The application 106 receives the encrypted traffic (328). For example the browser device can decrypt the HTTP reply, extract the XML object, and store the XML object to disk.

10 [0040] Although a particular number, type, and order of operations are shown here, other numbers, types, and orders of operations are possible. For example, the agent 102 may not store a whitelist or blacklist and may never allow an encrypted connection between the application 106 and resource server 104 without MitM analysis. In some cases, the agent 102 can create and send the policy request after creating the

15 cryptographic connections with the application 106 and the resource server 104. In other cases, the agent 102 can create and send the policy request as the cryptographic connections are being made.

[0041] FIG. 4 is a block diagram showing a device 400 with a man in the middle agent. The device 400 may be any sort of device that can host applications that send and receive traffic from an external network. For example, the device 400 may be a personal

20 computer, server, cell phone, tablet computer, or network appliance.

[0042] The device 400 can have installed a number of applications including, but not limited to, a web browser 402, a different web browser 404, and email application

406, and a chat program. The device 400, or, for example, the device's 400 operating system, can provide these application with an interface to access to an external network 410.

[0043] An agent 412 may be installed in this interface. In some cases, the agent 412 may be installed after the device 400 is manufactured. For example, the device 400 may be procured for an employee or student for use in a corporate or university setting. Before giving the device 400 to the user, a network administrator may configure the device 400 so that the device 400 meets the user's needs (e.g. has the applications 402-408 needed) and has the agent 412.

[0044] When installed and set-up, the agent 412 may install one or more certificates in the device 400 to specify that server's in the corporate or university domain are trusted. For example, the agent 412 may install an operating system certificate 414 with the operating system of the device 400. The web browser 404 and email application 406 may be configured to use the operating system's certificates, including the operating system certificate 414, when creating encrypted connections. Additionally or alternatively, the agent 412 can install certificates in application. For example, the web browser 402 may ignore the operating system's certificates and only user certificates installed with the web browser 402. In this case, the agent 412 can install a certificate 416 in the web browser 402.

[0045] FIG. 5 shows an example of a computing device 500 and an example of a mobile computing device that can be used to implement the techniques described here. The computing device 500 is intended to represent various forms of digital computers, such as laptops, desktops, workstations, personal digital assistants, servers, blade servers,

mainframes, and other appropriate computers. The mobile computing device is intended to represent various forms of mobile devices, such as personal digital assistants, cellular telephones, smart-phones, and other similar computing devices. The components shown here, their connections and relationships, and their functions, are meant to be exemplary only, and are not meant to limit implementations of the inventions described and/or claimed in this document.

[0046] The computing device 500 includes a processor 502, a memory 504, a storage device 506, a high-speed interface 508 connecting to the memory 504 and multiple high-speed expansion ports 510, and a low-speed interface 512 connecting to a low-speed expansion port 514 and the storage device 506. Each of the processor 502, the memory 504, the storage device 506, the high-speed interface 508, the high-speed expansion ports 510, and the low-speed interface 512, are interconnected using various busses, and may be mounted on a common motherboard or in other manners as appropriate. The processor 502 can process instructions for execution within the computing device 500, including instructions stored in the memory 504 or on the storage device 506 to display graphical information for a GUI on an external input/output device, such as a display 516 coupled to the high-speed interface 508. In other implementations, multiple processors and/or multiple buses may be used, as appropriate, along with multiple memories and types of memory. Also, multiple computing devices may be connected, with each device providing portions of the necessary operations (e.g., as a server bank, a group of blade servers, or a multi-processor system).

[0047] The memory 504 stores information within the computing device 500. In some implementations, the memory 504 is a volatile memory unit or units. In some

implementations, the memory 504 is a non-volatile memory unit or units. The memory 504 may also be another form of computer-readable medium, such as a magnetic or optical disk.

[0048] The storage device 506 is capable of providing mass storage for the computing device 500. In some implementations, the storage device 506 may be or contain a computer-readable medium, such as a floppy disk device, a hard disk device, an optical disk device, or a tape device, a flash memory or other similar solid state memory device, or an array of devices, including devices in a storage area network or other configurations. A computer program product can be tangibly embodied in an information carrier. The computer program product may also contain instructions that, when executed, perform one or more methods, such as those described above. The computer program product can also be tangibly embodied in a computer- or machine-readable medium, such as the memory 504, the storage device 506, or memory on the processor 502.

[0049] The high-speed interface 508 manages bandwidth-intensive operations for the computing device 500, while the low-speed interface 512 manages lower bandwidth-intensive operations. Such allocation of functions is exemplary only. In some implementations, the high-speed interface 508 is coupled to the memory 504, the display 516 (e.g., through a graphics processor or accelerator), and to the high-speed expansion ports 510, which may accept various expansion cards (not shown). In the implementation, the low-speed interface 512 is coupled to the storage device 506 and the low-speed expansion port 514. The low-speed expansion port 514, which may include various communication ports (e.g., USB, Bluetooth, Ethernet, wireless Ethernet) may be

coupled to one or more input/output devices, such as a keyboard, a pointing device, a scanner, or a networking device such as a switch or router, e.g., through a network adapter.

[0050] The computing device 500 may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a standard server 520, or multiple times in a group of such servers. In addition, it may be implemented in a personal computer such as a laptop computer 522. It may also be implemented as part of a rack server system 524. Alternatively, components from the computing device 500 may be combined with other components in a mobile device (not shown), such as a mobile computing device 550. Each of such devices may contain one or more of the computing device 500 and the mobile computing device 550, and an entire system may be made up of multiple computing devices communicating with each other.

[0051] The mobile computing device 550 includes a processor 552, a memory 564, an input/output device such as a display 554, a communication interface 566, and a transceiver 568, among other components. The mobile computing device 550 may also be provided with a storage device, such as a micro-drive or other device, to provide additional storage. Each of the processor 552, the memory 564, the display 554, the communication interface 566, and the transceiver 568, are interconnected using various buses, and several of the components may be mounted on a common motherboard or in other manners as appropriate.

[0052] The processor 552 can execute instructions within the mobile computing device 550, including instructions stored in the memory 564. The processor 552 may be implemented as a chipset of chips that include separate and multiple analog and digital

processors. The processor 552 may provide, for example, for coordination of the other components of the mobile computing device 550, such as control of user interfaces, applications run by the mobile computing device 550, and wireless communication by the mobile computing device 550.

5 **[0053]** The processor 552 may communicate with a user through a control interface 558 and a display interface 556 coupled to the display 554. The display 554 may be, for example, a TFT (Thin-Film-Transistor Liquid Crystal Display) display or an OLED (Organic Light Emitting Diode) display, or other appropriate display technology. The display interface 556 may comprise appropriate circuitry for driving the display 554
10 to present graphical and other information to a user. The control interface 558 may receive commands from a user and convert them for submission to the processor 552. In addition, an external interface 562 may provide communication with the processor 552, so as to enable near area communication of the mobile computing device 550 with other devices. The external interface 562 may provide, for example, for wired communication
15 in some implementations, or for wireless communication in other implementations, and multiple interfaces may also be used.

[0054] The memory 564 stores information within the mobile computing device 550. The memory 564 can be implemented as one or more of a computer-readable medium or media, a volatile memory unit or units, or a non-volatile memory unit or units.
20 An expansion memory 574 may also be provided and connected to the mobile computing device 550 through an expansion interface 572, which may include, for example, a SIMM (Single In Line Memory Module) card interface. The expansion memory 574 may provide extra storage space for the mobile computing device 550, or may also store

applications or other information for the mobile computing device 550. Specifically, the expansion memory 574 may include instructions to carry out or supplement the processes described above, and may include secure information also. Thus, for example, the expansion memory 574 may be provide as a security module for the mobile computing
5 device 550, and may be programmed with instructions that permit secure use of the mobile computing device 550. In addition, secure applications may be provided via the SIMM cards, along with additional information, such as placing identifying information on the SIMM card in a non-hackable manner.

[0055] The memory may include, for example, flash memory and/or NVRAM
10 memory (non-volatile random access memory), as discussed below. In some implementations, a computer program product is tangibly embodied in an information carrier. The computer program product contains instructions that, when executed, perform one or more methods, such as those described above. The computer program product can be a computer- or machine-readable medium, such as the memory 564, the
15 expansion memory 574, or memory on the processor 552. In some implementations, the computer program product can be received in a propagated signal, for example, over the transceiver 568 or the external interface 562.

[0056] The mobile computing device 550 may communicate wirelessly through the communication interface 566, which may include digital signal processing circuitry
20 where necessary. The communication interface 566 may provide for communications under various modes or protocols, such as GSM voice calls (Global System for Mobile communications), SMS (Short Message Service), EMS (Enhanced Messaging Service), or MMS messaging (Multimedia Messaging Service), CDMA (code division multiple

access), TDMA (time division multiple access), PDC (Personal Digital Cellular), WCDMA (Wideband Code Division Multiple Access), CDMA2000, or GPRS (General Packet Radio Service), among others. Such communication may occur, for example, through the transceiver 568 using a radio-frequency. In addition, short-range communication may occur, such as using a Bluetooth, WiFi, or other such transceiver (not shown). In addition, a GPS (Global Positioning System) receiver module 570 may provide additional navigation- and location-related wireless data to the mobile computing device 550, which may be used as appropriate by applications running on the mobile computing device 550.

10 [0057] The mobile computing device 550 may also communicate audibly using an audio codec 560, which may receive spoken information from a user and convert it to usable digital information. The audio codec 560 may likewise generate audible sound for a user, such as through a speaker, e.g., in a handset of the mobile computing device 550. Such sound may include sound from voice telephone calls, may include recorded sound
15 (e.g., voice messages, music files, etc.) and may also include sound generated by applications operating on the mobile computing device 550.

[0058] The mobile computing device 550 may be implemented in a number of different forms, as shown in the figure. For example, it may be implemented as a cellular telephone 580. It may also be implemented as part of a smart-phone 582, personal digital
20 assistant, or other similar mobile device.

[0059] Various implementations of the systems and techniques described here can be realized in digital electronic circuitry, integrated circuitry, specially designed ASICs (application specific integrated circuits), computer hardware, firmware, software, and/or

combinations thereof. These various implementations can include implementation in one or more computer programs that are executable and/or interpretable on a programmable system including at least one programmable processor, which may be special or general purpose, coupled to receive data and instructions from, and to transmit data and instructions to, a storage system, at least one input device, and at least one output device.

5 [0060] These computer programs (also known as programs, software, software applications or code) include machine instructions for a programmable processor, and can be implemented in a high-level procedural and/or object-oriented programming language, and/or in assembly/machine language. As used herein, the terms machine-readable medium and computer-readable medium refer to any computer program product, apparatus and/or device (e.g., magnetic discs, optical disks, memory, Programmable Logic Devices (PLDs)) used to provide machine instructions and/or data to a programmable processor, including a machine-readable medium that receives machine instructions as a machine-readable signal. The term machine-readable signal refers to 10 any signal used to provide machine instructions and/or data to a programmable processor.

15 [0061] To provide for interaction with a user, the systems and techniques described here can be implemented on a computer having a display device (e.g., a CRT (cathode ray tube) or LCD (liquid crystal display) monitor) for displaying information to the user and a keyboard and a pointing device (e.g., a mouse or a trackball) by which the user can provide input to the computer. Other kinds of devices can be used to provide for interaction with a user as well; for example, feedback provided to the user can be any 20 form of sensory feedback (e.g., visual feedback, auditory feedback, or tactile feedback);

and input from the user can be received in any form, including acoustic, speech, or tactile input.

[0062] The systems and techniques described here can be implemented in a computing system that includes a back end component (e.g., as a data server), or that includes a middleware component (e.g., an application server), or that includes a front end component (e.g., a client computer having a graphical user interface or a Web browser through which a user can interact with an implementation of the systems and techniques described here), or any combination of such back end, middleware, or front end components. The components of the system can be interconnected by any form or medium of digital data communication (e.g., a communication network). Examples of communication networks include a local area network (LAN), a wide area network (WAN), and the Internet.

[0063] The computing system can include clients and servers. A client and server are generally remote from each other and typically interact through a communication network. The relationship of client and server arises by virtue of computer programs running on the respective computers and having a client-server relationship to each other.

EMBODIMENTS IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method performed by data processing apparatus, the method comprising:

5 receiving, by an agent on a device within a network, a request to access a resource outside the network;

determining that the resource is not on a whitelist that lists resources for which man-in-the-middle analysis should not apply;

establishing a device/agent encrypted connection having endpoints at the device and the agent;

10 establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication traffic between the device and the resource and wherein the device/agent encrypted connection and
15 the agent/resource encrypted connection are in different formats;

sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource, wherein the network appliance is different than the device;

20 receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside
25 of the network; and

decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource.

2. The method of claim 1, wherein the device and the network appliance are subject to the same administrative control.
- 5 3. The method of claim 1, wherein decrypting and inspecting the encrypted communication traffic includes blocking the encrypted communication traffic.
4. The method of claim 1, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.
- 10 5. The method of claim 1, the method further comprising:

receiving, by the agent, a second request to access a second resource outside the network;

determining that the second resource is on the whitelist; and

causing the establishment, responsive to determining that the second resource is on

15 the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource.
6. The method of claim 1, the method further comprising:

removing the device from the network;

20 receiving, by the agent, a request to access an other resource outside the network;

establishing a second device/agent encrypted connection between the device and the agent, and an agent/other resource encrypted connection between the agent and

the other resource, to facilitate encrypted communication traffic between the device and the other resource;

5 sending, by the agent in response to receiving the request to access the other resource, a policy request to the network appliance, the request specifying the other resource;

receiving, by the agent and from the network appliance, a third policy response indicating that the other resource is associated with one or more security policies of the network; and

10 selectively decrypting and inspecting the encrypted communication traffic passing between the device and the other resource depending on the security policies.

7. The method of claim 1, wherein the agent is a driver installed in a protocol stack of the device.
8. The method of claim 1, wherein the agent is configured to receive requests to access resources from a plurality of applications of the device.
- 15 9. The method of claim 1, wherein actions for the agent to apply include dropping at least some of the encrypted communication traffic passing between the device and the resource.
10. The method of claim 1, wherein the device/agent encrypted connection and the agent/resource encrypted connection are of different types.
- 20 11. The method of claim 1, wherein the session key for the device/agent encrypted connection is different than the session key for the agent/resource encrypted connection.

12. The method of claim 1, wherein decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource comprises:

receiving, on the device/agent encrypted connection, first traffic that is addressed to the resource and that is encrypted into a first encrypted form;

5 decrypting the first traffic;

encrypting the first traffic into a second encrypted form;

transmitting, on the agent/resource encrypted connection, the first traffic in the second encrypted form;

10 receiving, on the agent/resource encrypted connection, second traffic that is addressed to the device and that is encrypted into a third encrypted form;

decrypting the second traffic;

encrypting the second traffic into a fourth encrypted form; and

transmitting, on the device/agent encrypted connection, the first traffic in the fourth encrypted form.

- 15 13. A non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations comprising:

receiving, by an agent on a device within a network, a request to access a resource outside the network;

20 determining that the resource is not on a whitelist that lists resources for which man-in-the-middle analysis should not apply;

establishing a device/agent encrypted connection having endpoints at the device and the agent;

establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication traffic between the device and the resource and wherein the device/agent encrypted connection and the agent/resource encrypted connection are in different formats;

sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource, wherein the network appliance is different than the device;

receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside of the network; and

decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource.

14. The computer storage media of claim 13, wherein the device and the network appliance are subject to the same administrative control.
15. The computer storage media of claim 13, wherein decrypting and inspecting the encrypted communication traffic includes blocking the encrypted communication traffic.
16. The computer storage media of claim 13, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.

17. The computer storage media of claim **13**, the operations further comprising:

receiving, by the agent, a second request to access a second resource outside the network;

determining that the second resource is on the whitelist; and

5 causing the establishment of, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource.

18. The computer storage media of claim **13**, the operations further comprising:

10 removing the device from the network;

receiving, by the agent, a request to access an other resource outside the network;

15 establishing a second device/agent encrypted connection between the device and the agent, and an agent/other resource encrypted connection between the agent and the other resource, to facilitate encrypted communication traffic between the device and the other resource;

sending, by the agent in response to receiving the request to access the other resource, a policy request to the network appliance, the request specifying the other resource;

20 receiving, by the agent and from the network appliance, a policy response indicating that the other resource is associated with one or more security policies of the network; and

selectively decrypting and inspecting the encrypted communication traffic passing between the device and the other resource depending on the security policies.

19. The computer storage media of claim 13, wherein the agent is a driver installed in a protocol stack of the device.
20. The computer storage media of claim 13, wherein the agent is configured to receive requests to access resources from a plurality of applications of the device.
- 5 21. A system comprising:
- one or more processors configured to execute computer program instructions; and
- non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations comprising:
- 10 receiving, by an agent on a device within a network, a request to access a resource outside the network;
- determining that the resource is not on a whitelist that lists resources for which man-in-the-middle analysis should not apply;
- establishing a device/agent encrypted connection having endpoints at the
- 15 device and the agent;
- establishing, after the device/agent encrypted connection is established, an agent/resource encrypted connection having endpoints at the agent and the resource, wherein the device/agent encrypted connection and the agent/resource encrypted connection facilitate encrypted communication
- 20 traffic between the device and the resource and wherein the device/agent encrypted connection and the agent/resource encrypted connection are in different formats;
- sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the

request specifying the resource, wherein the network appliance is different than the device;

receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network, wherein the security policies of the network include instructions for actions for the agent to apply to the encrypted communication traffic passing between the device and the resource, wherein the security policies of the network are policies designed to apply to traffic associated with a class of resources outside of the network; and

decrypting and inspecting at least some of the encrypted communication traffic passing between the device and the resource.

22. The system of claim **21**, wherein the device and the network appliance are subject to the same administrative control.

23. The system of claim **21**, wherein decrypting and inspecting the encrypted communication traffic includes blocking the encrypted communication traffic.

24. The system of claim **21**, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.

25. The system of claim **21**, the operations further comprising:

receiving, by the agent, a second request to access a second resource outside the network;

determining that the second resource is on the whitelist; and

causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device

and the second resource to facilitate encrypted communication traffic between the device and the second resource.

26. The system of claim **21**, wherein the operations further comprise:

removing the device from the network;

5 receiving, by the agent, a request to access an other resource outside the network;

establishing a second device/agent encrypted connection between the device and the agent, and an agent/other resource encrypted connection between the agent and the other resource, to facilitate encrypted communication traffic between the device and the other resource;

10 sending, by the agent in response to receiving the request to access the other resource, a policy request to the network appliance, the request specifying the other resource;

receiving, by the agent and from the network appliance, a policy response indicating that the other resource is associated with one or more security policies
15 of the network; and

selectively decrypting and inspecting the encrypted communication traffic passing between the device and the other resource depending on the security policies.

27. The system of claim **21**, wherein the agent is a driver installed in a protocol stack of the device.

20 **28.** The system of claim **21**, wherein the agent is configured to receive requests to access resources from a plurality of applications of the device.

29. A method performed by data processing apparatus, the method comprising:

receiving, by an agent on a device within a network, a request to access a resource outside the network;

5 establishing, by the agent, a device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;

establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource;

10 sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource;

15 receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network;

decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies;

20 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the resource and address to the device, depending on the security policies;

receiving, by the agent, a second request to access a second resource outside the network;

25 determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and

causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource; wherein the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource encrypted connection are separate and have different formats.

30. The method of claim 29, wherein the device and the network appliance are subject to the same administrative control.
31. The method of claim 29, wherein inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource includes blocking encrypted communication traffic from the device and addressed to the resource.
32. The method of claim 29, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.
33. The method of claim 29, the method further comprising:
 - removing the device from the network;
 - receiving, by the agent, a third request to access a third resource outside the network;
 - establishing, by the agent, a second device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;
 - establishing, by the agent, an agent/third resource encrypted connection between the agent and the third resource such that the agent is configured to act as a proxy of the device to the third resource;

sending, by the agent in response to receiving the third request to access the resource, a third policy request to the network appliance, the request specifying the third resource;

5 receiving, by the agent and from the network appliance, a third policy response indicating that the third resource is associated with one or more security policies of the network;

decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the third resource, depending on the security policies; and

10 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the third resource and address to the device, depending on the security policies.

34. The method of claim 29, wherein the agent is a driver installed in a protocol stack of the device.

15 35. The method of claim 29, wherein the agent is configured to receive requests to access resources from a plurality of applications of the device.

36. A non-transitory computer storage media encoded with computer program instructions that, when executed by one or more processors, cause a computer device to perform operations comprising:

20 receiving, by an agent on a device within a network, a request to access a resource outside the network;

establishing, by the agent, a device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;

establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource;

5 sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource;

receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network;

10 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies;

15 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the resource and address to the device, depending on the security policies;

receiving, by the agent, a second request to access a second resource outside the network;

determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and

20 causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource; wherein the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource
25 encrypted connection are separate and have different formats.

37. The computer storage media of claim 36, wherein the device and the network appliance are subject to the same administrative control.
38. The computer storage media of claim 36, wherein inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource includes blocking encrypted communication traffic from the device and addressed to the resource.
39. The computer storage media of claim 36, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.
40. The computer storage media of claim 36, the operations further comprising:
- removing the device from the network;
 - receiving, by the agent, a third request to access a third resource outside the network;
 - establishing, by the agent, a second device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;
 - establishing, by the agent, an agent/third resource encrypted connection between the agent and the third resource such that the agent is configured to act as a proxy of the device to the third resource;
 - sending, by the agent in response to receiving the third request to access the resource, a third policy request to the network appliance, the request specifying the third resource;
 - receiving, by the agent and from the network appliance, a third policy response indicating that the third resource is associated with one or more security policies of the network;

decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the third resource, depending on the security policies; and

5 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the third resource and address to the device, depending on the security policies.

41. The computer storage media of claim 36, wherein the agent is a driver installed in a protocol stack of the device.
42. The computer storage media of claim 36, wherein the agent is configured to receive
10 requests to access resources from a plurality of applications of the device.

43. A system comprising:
- one or more processors configured to execute computer program instructions; and
- non-transitory computer storage media encoded with computer program
instructions that, when executed by one or more processors, cause a computer
15 device to perform operations comprising:

receiving, by an agent on a device within a network, a request to access a resource outside the network;

20 establishing, by the agent, a device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;

establishing, by the agent, an agent/resource encrypted connection between the agent and the resource such that the agent is configured to act as a proxy of the device to the resource;

sending, by the agent in response to receiving the request to access the resource, a policy request to a network appliance within the network, the request specifying the resource;

5 receiving, by the agent and from the network appliance, a policy response indicating that the resource is associated with one or more security policies of the network;

decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource, depending on the security policies;

10 decrypting and selectively inspecting, by the agent, encrypted communication traffic from the resource and address to the device, depending on the security policies;

receiving, by the agent, a second request to access a second resource outside the network;

15 determining that the second resource is on a whitelist that lists resources for which man-in-the-middle analysis should not apply; and

causing the establishment, responsive to determining that the second resource is on the whitelist, a device/second resource encrypted connection between the device and the second resource to facilitate encrypted communication traffic between the device and the second resource; wherein
20 the device/agent encrypted connection, the agent/resource encrypted connection, and the device/second resource encrypted connection are separate and have different formats.

44. The system of claim 43, wherein the device and the network appliance are subject to the
25 same administrative control.

45. The system of claim 43, wherein inspecting, by the agent, encrypted communication traffic from the device and addressed to the resource includes blocking encrypted communication traffic from the device and addressed to the resource.
46. The system of claim 43, wherein the request to access the resource is a Hypertext Transfer Protocol (HTTP) or Hypertext Transfer Protocol Secure (HTTPS) GET or POST request.
47. The system of claim 43, wherein the operations further comprising:
- removing the device from the network;
 - receiving, by the agent, a third request to access a third resource outside the network;
 - establishing, by the agent, a second device/agent encrypted connection between the device and the agent such that the agent is configured to act as a proxy of the resource to the device;
 - establishing, by the agent, an agent/third resource encrypted connection between the agent and the third resource such that the agent is configured to act as a proxy of the device to the third resource;
 - sending, by the agent in response to receiving the third request to access the resource, a third policy request to the network appliance, the request specifying the third resource;
 - receiving, by the agent and from the network appliance, a third policy response indicating that the third resource is associated with one or more security policies of the network;
 - decrypting and selectively inspecting, by the agent, encrypted communication traffic from the device and addressed to the third resource, depending on the security policies; and

decrypting and selectively inspecting, by the agent, encrypted communication traffic from the third resource and address to the device, depending on the security policies.

- 5 **48.** The system of claim **43**, wherein the agent is a driver installed in a protocol stack of the device.
- 49.** The system of claim **43**, wherein the agent is configured to receive requests to access resources from a plurality of applications of the device.

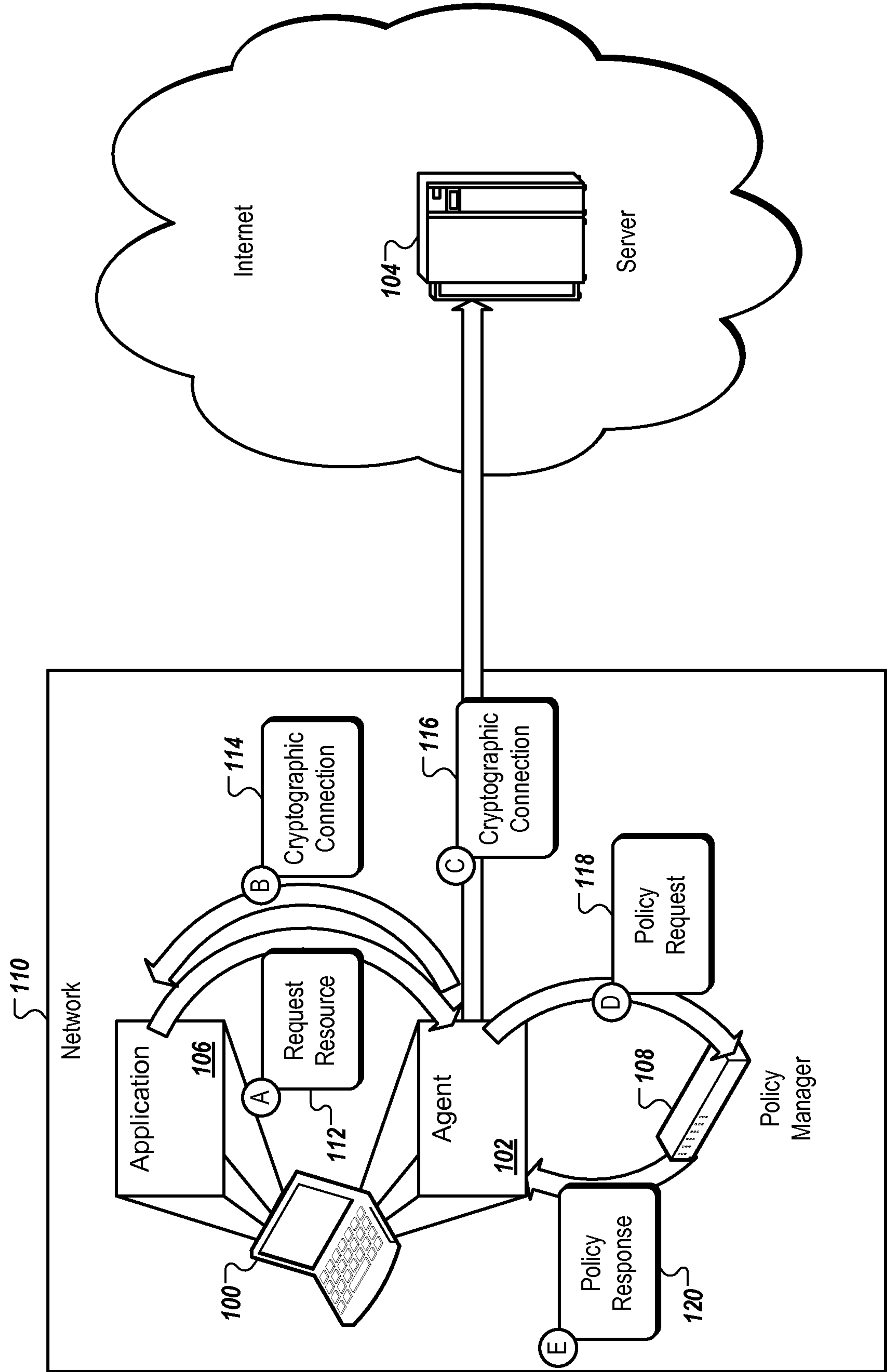


FIG. 1

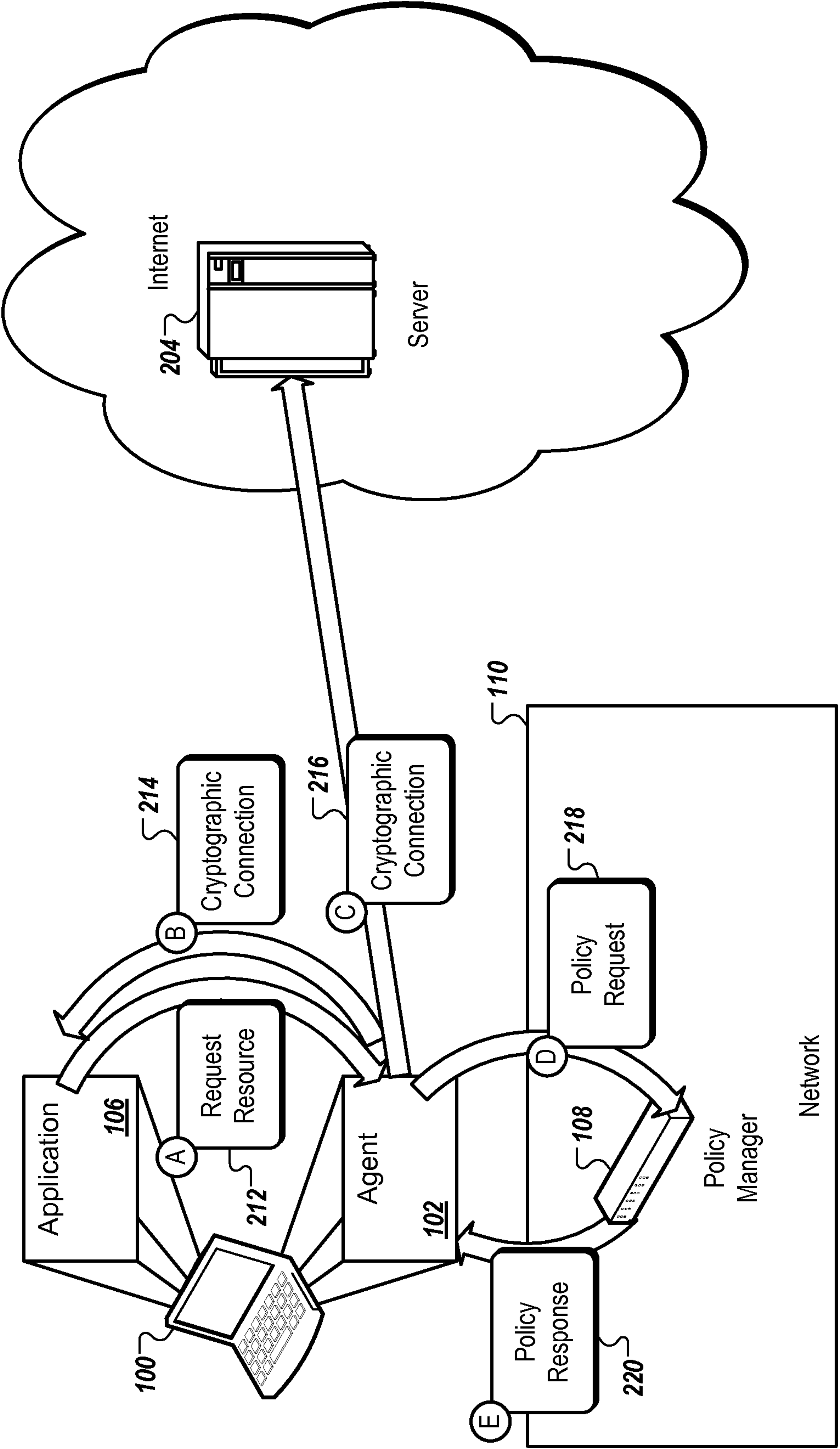


FIG. 2

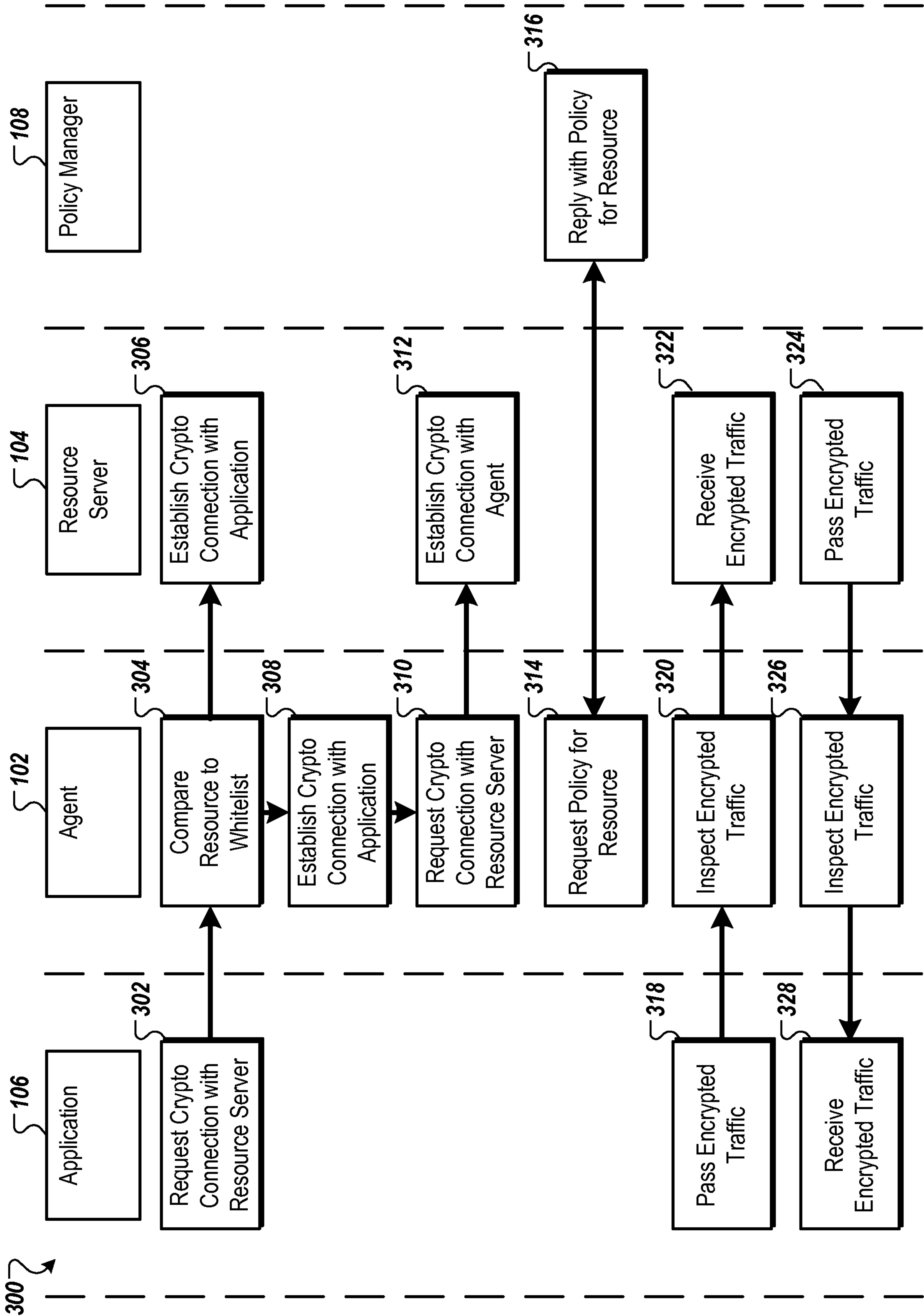
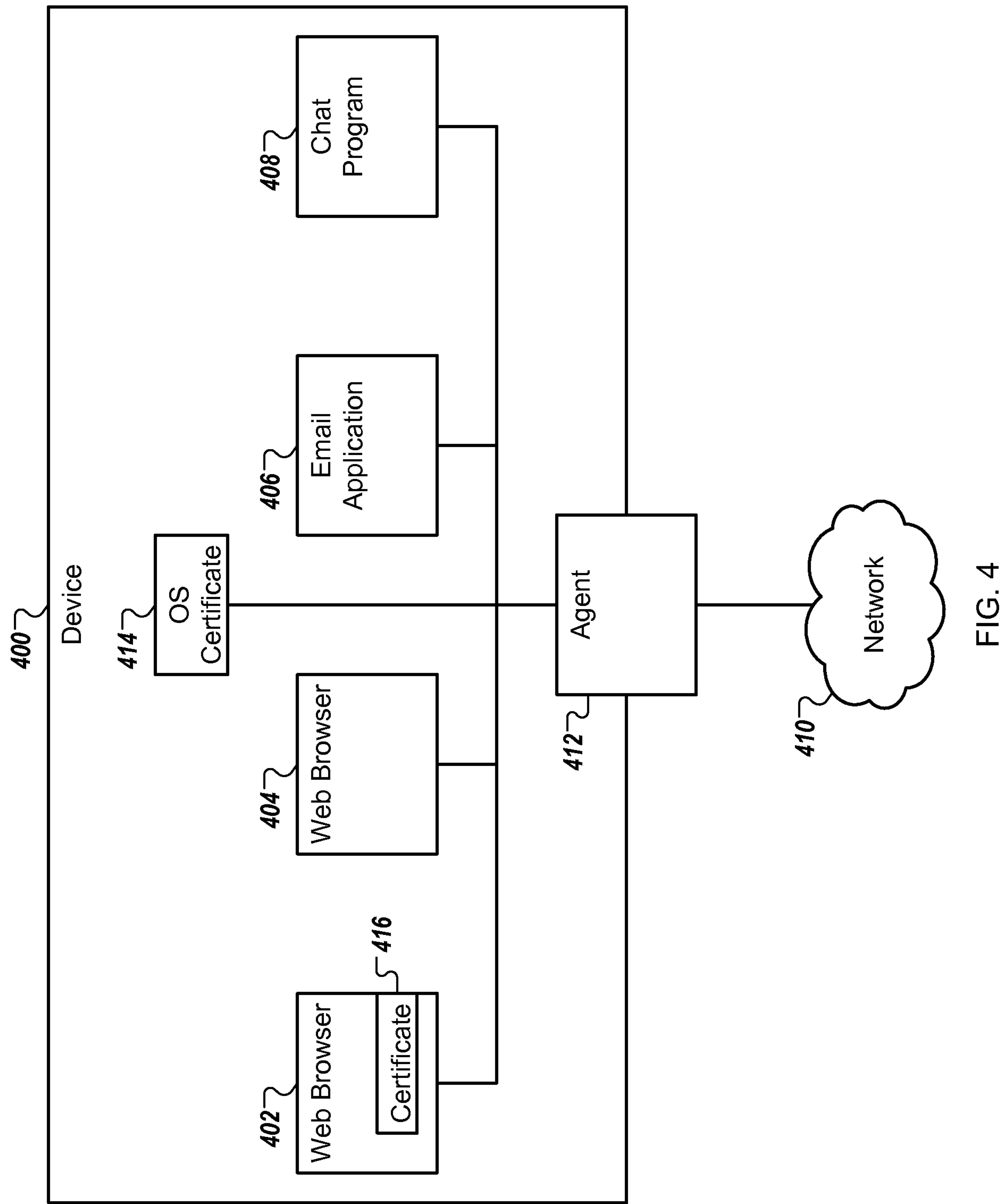


FIG. 3



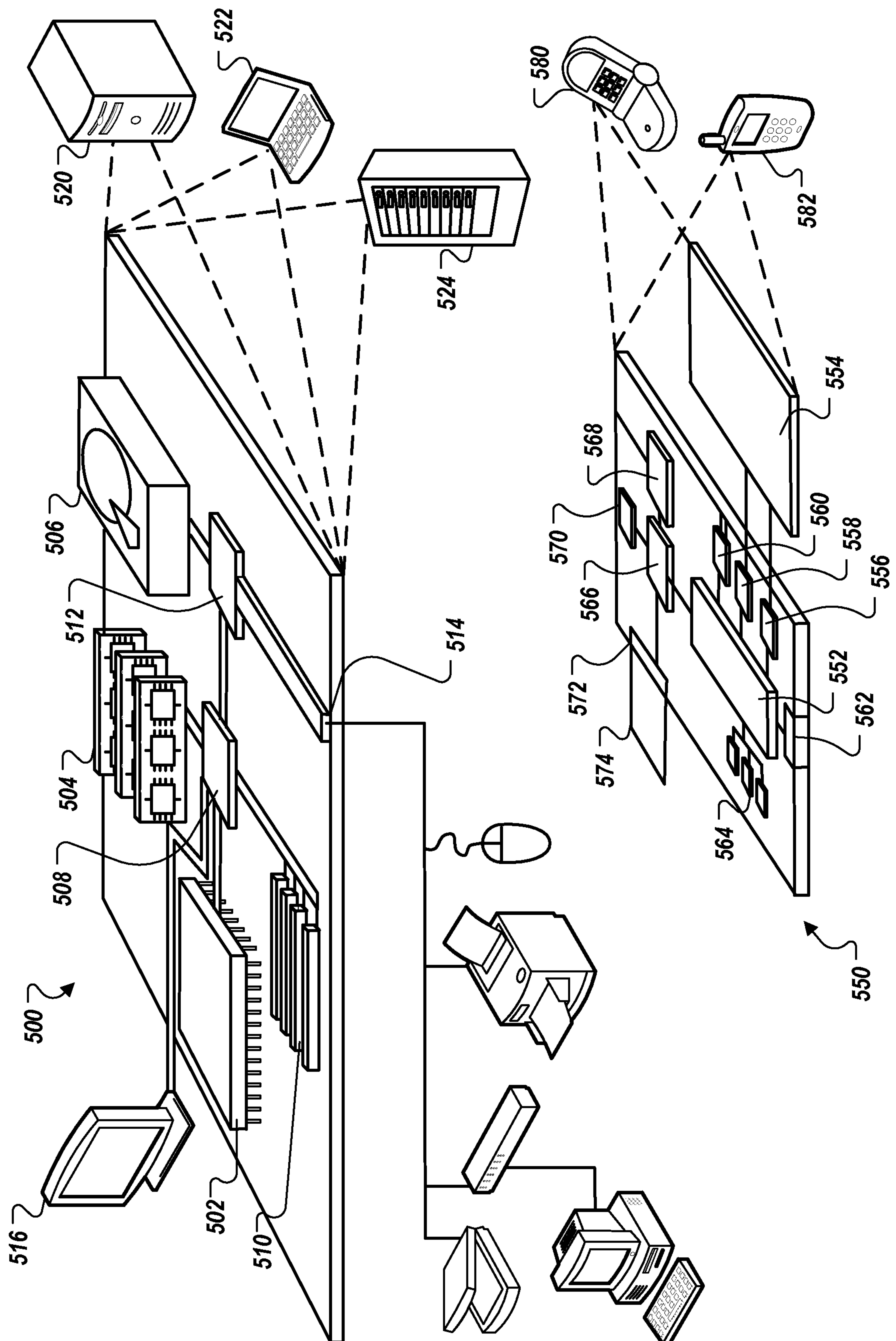


FIG. 5

