

(51) International Patent Classification:
G06F 17/28 (2006.01)(21) International Application Number:
PCT/US2009/036410(22) International Filing Date:
6 March 2009 (06.03.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/042,691 4 April 2008 (04.04.2008) US
12/144,863 24 June 2008 (24.06.2008) US(71) Applicant (for all designated States except US): **MICROSOFT CORPORATION** [US/US]; One Microsoft Way, Redmond, Washington 98052-6399 (US).(72) Inventors: **NICE, Nir**; One Microsoft Way, Redmond, Washington 98052-6399 (US). **WALKER, Lee, F.**; One Microsoft Way, Redmond, Washington 98052-6399 (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, BR, BW, BY, BZ,

CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

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

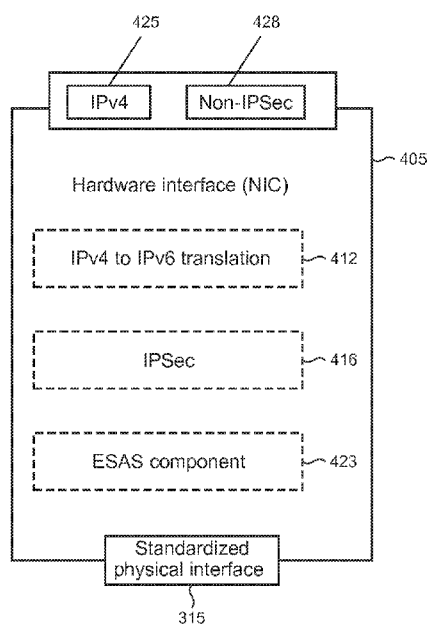
Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

[Continued on next page]

(54) Title: **HARDWARE INTERFACE FOR ENABLING DIRECT ACCESS AND SECURITY ASSESSMENT SHARING**

FIG. 4



(57) **Abstract:** Native IPv6 capabilities are provided to an IPv4 network node, device, or endpoint using a hardware interface that supports network communication under a Direct Access model. The Direct Access model supports IPv6 communication with IPsec and enforces Network Access Protection ('NAP') health requirement policies for endpoints that are network clients. A Direct Access-ready server is enabled using a hardware interface that implements IPv4 to IPv6 translation and optionally IPsec termination capability. A Direct Access-ready client is enabled using a hardware interface that implements IPv4 to IPv6 translation, IPsec termination capability, and which optionally provides NAP (Network Access Protection) capabilities for Direct Access-ready clients that are configured as mobile information appliances. The hardware interface may be implemented as a network interface card ('NIC') (405) or as a chipset (505).



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))

HARDWARE INTERFACE FOR ENABLING DIRECT ACCESS AND SECURITY ASSESSMENT SHARING

BACKGROUND

[0001] While the Internet continues its unprecedented exponential growth, the recent broad adoption of always-on broadband technologies such as Digital Subscriber Line (“DSL”) and cable modems, coupled with the pending integration of personal data assistants (“PDAs”) and mobile phones into always-addressable mobile information appliances, significantly elevates the urgency to expand the address space that Internet-connected systems use to communicate. The address space currently used is defined as part of the Internet Protocol, or the IP (the network layer of the TCP/IP (Transport Control Protocol/Internet Protocol) protocol suite. The version of IP commonly used today is Version 4 (“IPv4”), which has not been substantially changed since RFC 791 (Request for Comments under the Internet Engineering Task Force, or “IETF”) was published in 1981.

Over that time, IPv4 has proven to be robust, easily implemented and interoperable, and has stood the test of scaling an internetwork (a network of networks) to a global utility the size of today’s Internet. While this is a tribute to its initial design, moving forward to an even grander scale requires laying a new foundation.

[0002] IPv6 will continue the tradition of the IPv4 protocol, which gained much of its acceptance by defining mechanisms to tie systems together over a wide variety of disparate networking technologies. Already defined link-layer mappings for transporting IPv6 include Ethernet, Point-to-Point Protocol (“PPP”), Fiber Distributed Data Interface (“FDDI”), Token Ring, Asynchronous Transfer Mode (“ATM”), Frame Relay, IEEE 1394 (Institute of Electrical and Electronics Engineers), and IPv4. From the architectural perspective, an IPv4-based infrastructure appears to IPv6-enabled systems as a single segment non-broadcast multi-access (“NBMA”) network. The capability to send IPv6 traffic over existing IPv4 networks will provide an initial reach as broad as the current Internet, limited only by the endpoints’ ability and readiness to make use of it.

[0003] To address concerns about security and privacy, IPv6 includes IP layer security known as Internet Protocol security (IPsec). IPsec is an industry standard

security technology that provides for data authenticity and integrity as well as data confidentiality across the array of protocols used by the various applications.

Providing the capability at the network layer frees the developer from having to add specific security capabilities to every application.

5 [0004] New capabilities such as scoped addresses (useful for restricting the default range of file and printer sharing), stateless autoconfiguration (lowering the complexity and management burden), and mandatory IP security (permitting end-to-end data authentication and integrity and privacy of connections) are expected to drive rapid adoption. In addition to the new capabilities, the technologies currently
10 used to extend the lifetime of IPv4 – such as Network Address Translators (“NATs”) – frequently break existing applications, and are already restricting the flexibility to deploy new ones. NATs are popular today because they allow multiple systems to share a single scarce public IPv4 address, but in doing so they tend to enforce a client/server usage model where the client uses private address
15 space with only the server existing in public address space. IPv6 brings back the capability of “end-to-end control of communications” making networking applications simpler as the network again becomes transparent.

[0005] The conversion from IPv4 to IPv6 is anticipated to be a larger task for the industry than the preparation for Year 2000. It will affect nearly all networked
20 applications, end-systems, infrastructure systems, and network architectures. It is critical that this change be approached with responsibility to prevent costly unproductive missteps that result from broad premature availability of technologies. Unlike the Year 2000 issue, the conversion to IPv6 has no specific timeline. However, as noted earlier, the rate of IPv4 address consumption is rapidly
25 increasing. Simplicity of deployment will be the key to rapid adoption.

[0006] The migration of IPv4 to IPv6 will not happen overnight. There will be a period of transition when both protocols are in use over the same infrastructure. To address this transition period, the designers of IPv6 have created technologies and address types so that IPv6 nodes can communicate with each other in a mixed
30 environment, even if they are separated by an IPv4-only infrastructure.

[0007] RFC 2893 defines a variety of different node types. An IPv4-only node implements only IPv4 (and has only IPv4 addresses) and does not support IPv6. Most hosts and routers installed today are IPv4-only nodes.

[0008] An IPv6-only node implements only IPv6 (and has only IPv6 addresses) and does not support IPv4. This node is only able to communicate with IPv6 nodes and applications. This type of node is not common today, but might become more prevalent as smaller devices such as cellular phones and handheld computing devices include the IPv6 protocol.

[0010] An IPv6/IPv4 node implements both IPv4 and IPv6.

10 [0011] An IPv4 node implements IPv4. An IPv4 node can be an IPv4-only node or an IPv6/IPv4 node.

[0012] An IPv6 node implements IPv6. An IPv6 node can be an IPv6-only node or an IPv6/IPv4 node.

[0013] For coexistence to occur, the largest number of nodes (IPv4 or IPv6 nodes) can communicate using an IPv4 infrastructure, an IPv6 infrastructure, or an infrastructure that is a combination of IPv4 and IPv6. True migration is achieved when all IPv4 nodes are converted to IPv6-only nodes. However, for the foreseeable future, practical migration is achieved when as many IPv4-only nodes as possible are converted to IPv6/IPv4 nodes. IPv4-only nodes can communicate with IPv6-only nodes only when using an IPv4-to-IPv6 proxy or translation gateway.

[0014] While such gateways can often perform satisfactorily, they often represent an additional expense compared with native IPv6 implementations. And because the IPv4-to-IPv6 proxy or translation gateway needs to terminate the IPsec connection for encrypted traffic before translation can be performed, the link between the gateway and IPv4 infrastructure can pose a security vulnerability in some cases. In addition, use of the gateway typically causes confusion in a given domain with regard to Domain Name System ("DNS") infrastructure because the IPv4 infrastructure will register with DNS servers in the domain as an IPv4 server, for example, even though the gateway supports IPv6. Upgrading DNS

infrastructure to deal with mixed IPv4/IPv6 capabilities is not a trivial undertaking and represents additional costs.

[0015] This Background is provided to introduce a brief context for the Summary and Detailed Description that follow. This Background is not intended to be an aid
5 in determining the scope of the claimed subject matter nor be viewed as limiting the claimed subject matter to implementations that solve any or all of the disadvantages or problems presented above.

SUMMARY

[0016] Native IPv6 capabilities are provided to an IPv4 network node, device, or
10 endpoint (collectively referred to as endpoint) using a hardware interface that supports network communication under a Direct Access model. The Direct Access model supports IPv6 communication with IPsec and enforces Network Access Protection (“NAP”) health requirement policies for endpoints that are network clients. A Direct Access-ready server is enabled using a hardware interface that
15 implements IPv4 to IPv6 translation and optionally IPsec termination capability. A Direct Access-ready client is enabled using a hardware interface that implements IPv4 to IPv6 translation, IPsec termination capability, and that optionally provides NAP (Network Access Protection) capabilities for Direct Access-ready clients that are configured as mobile information appliances. The hardware interface may be
20 implemented as a network interface card (“NIC”) or as a chipset.

[0017] The Direct Access hardware interface advantageously enables non-Direct Access-ready devices including legacy and non-Windows-based devices to be readily upgraded with native IPv6 capabilities at low cost with enhanced security and without modifications or changes to the installed software. In addition, for
25 servers, using the Direct Access hardware interface eliminates the DNS confusion in a domain that is ordinarily generated by the use of an IPv4 to IPv6 gateway.

[0018] In an illustrative example, the Direct Access hardware interface is further configured to provide Enterprise Security Assessment Sharing (“ESAS”) capabilities to an IPv4 endpoint. Here, a semantic abstraction, called a security
30 assessment, is used to enable sharing of security-related information among different ESAS-enabled endpoints. The security assessments existing in a

particular computing environment function to provide a security context that gives an ESAS-enabled endpoint a new way to look at its own locally-available information. The security context enables an ESAS-enabled endpoint to combine or correlate evidence from security assessments received from a variety of different sources, and across object types, in order to significantly enhance the quality of its detection of potential security incidents and reduces the level of false-positive and false-negative identifications of security incidents in the environment. In addition to implementing in hardware some or all of ESAS functionality that is typically provided by software, the Direct Access hardware interface may be configured to send and receive security assessments over a defined channel. The channel may comprise a link or use a defined IP address and may further be handled with a particular quality of service (“QoS”) to guarantee communication of security assessments even in cases where the network is congested. The Direct Access hardware can thus extend the advantages and benefits of ESAS to users who are outside the enterprise network while also increasing the number of ESAS-enabled endpoints that are available to detect potential security threats.

[0019] This Summary is provided to introduce a selection of concepts in a simplified form that are further described below in the Detailed Description. This Summary is not intended to identify key features or essential features of the claimed subject matter, nor is it intended to be used as an aid in determining the scope of the claimed subject matter.

DESCRIPTION OF THE DRAWINGS

[0020] FIG 1 shows an illustrative networked computing environment in which the present hardware interface may operate;

[0021] FIG 2 shows details of a typical implementation of a node in the networked computing environment in which a gateway provides NAT-PT (Network Address Translation-Protocol Translation) and IPsec tunneling functionality;

[0022] FIG 3 shows an illustrative software protocol stack and hardware interface that may be utilized in an endpoint;

[0023] FIG 4 shows the functional components of an illustrative hardware interface that may be implemented as a network interface card;

[0024] FIG 5 shows the functional components of an illustrative hardware interface that may be implemented as a chipset;

5 [0025] FIG 6 shows an illustrative enterprise security assessment sharing (“ESAS”) arrangement in an enterprise network;

[0026] FIG 7 is a diagram of a first illustrative scenario in which a plurality of ESAS-enabled endpoints are coupled to a security assessment channel and a detected incident at one endpoint triggers responses at multiple other endpoints;

10 [0027] FIG 8 is a diagram of a second illustrative scenario in which a low fidelity security assessment is sent over the security assessment channel that triggers the generation of a new high fidelity assessment by a receiving ESAS-enabled endpoint which also performs cross-object mapping;

[0028] FIG 9 is a diagram of a third illustrative scenario that shows the targeted
15 use of remediation techniques;

[0029] FIG 10 shows an illustrative arrangement in which an ESAS security assessment channel may be extended from an enterprise network over a non-secure network such as the Internet to one or more endpoints that are ESAS-enabled through use of the present hardware interface; and

20 [0030] FIG 11 shows an illustrative extended ESAS architecture in which a security assessment is received by a remote endpoint that is ESAS-enabled through the present hardware interface.

[0031] Like reference numerals indicate like elements in the drawings. Elements in the drawings are not drawn to scale unless otherwise indicated.

25 DETAILED DESCRIPTION

[0032] FIG 1 shows an illustrative networked computing environment 100 in which the present hardware interface may operate. In this example, client devices 105_{1, 2 ... N} such as a personal computer (“PC”) 105₁, laptop computer 105₂, mobile information appliance 105₃, and a non-Windows® operating system-based
30 computer 105_N utilize a network such as the Internet 112 to access resources 115 such as web servers 121, or establish remote access to an enterprise network 130.

Users of the client devices 105 may seek remote access to services, files and/or data that is provided by servers in the enterprise network 130 such as a file server 137, an e-mail server 142, and a database server 146, for example.

[0033] FIG 2 shows details of a typical implementation of a node or domain 200 in the networked computing environment in which a gateway 206 supports a NAT-PT (Network Address Translation-Protocol Translation) component 211 and IPsec tunnel endpoint component 215. Such gateway 206 is commonly utilized to provide Direct Access capability to native IPv4 server infrastructure 223 that may be utilized to support the Internet-based resources 115 or enterprise network 130 shown in FIG 1. As noted above, the term “Direct Access” is used to define IPv6 capability using IPsec, including IPsec-NAP in some implementations.

[0034] The NAT-PT component 211 functions as a migration tool to enable the operator of the domain 200 to transition IPv4 networks to IPv6 networks. By placing NAT-PT functionality in the gateway 206, an endpoint in an IPv6-only node can connect with the server infrastructure 223 in the IPv4-only node. The NAT-PT component 211 also supports an Application Layer Gateway (“ALG”) functionality to enable domain name-to-address mapping in the DNS infrastructure 230 that is typically provided in the domain 200. Specifically, the ALG provides the ability to resolve IPv6 addresses into DNS queries and responses into their IPv4 address bindings and vice versa, as DNS packets traverse between the IPv4 and IPv6 networks. This additional complexity is caused by the inability of the server infrastructure 223 to register with the DNS infrastructure 230 as a native IPv6 server.

[0035] The IPsec tunnel endpoint component 215 enables the gateway 206 to terminate an IPsec connection. An IPsec tunnel uses an encrypted IP header and payload during transit. In this way, the tunnel provides protection for the entire packet. An entire IP packet is first encapsulated, for example, with an authentication header or encapsulating security payload header, and then the result is encapsulated with an additional IP header. The additional IP header contains the source and destination of the tunnel endpoints. After the packet reaches the first

destination at the tunnel endpoint, it can be decapsulated and sent to the final destination by reading the IP address.

[0036] NAP functionality will typically be implemented using both client and server components that allow the creation and enforcement of health requirement

5 policies that define the required software and system configurations for computers that connect to a given network. NAP enforces health requirements by inspecting and assessing the health of client computers, limiting network access when client computers are deemed noncompliant, and remediating noncompliant client computers for unlimited network access. NAP enforces health requirements on

10 client computers that are attempting to connect to a network. NAP can also provide ongoing health compliance enforcement while a compliant client computer is connected to a network.

[0037] In some implementations, the server infrastructure 223 will also employ a NAP server-side component that is implemented in this example as a derivative of

15 IPsec known as IPsec with AuthIP, or authenticated IP (as identified by reference numeral 237). This functionality is supported in recent releases of Microsoft Windows operating systems and provides simplified IPsec policy configuration and maintenance in many configurations and additional flexibility for IPsec peer authentication. In particular, the IPsec with AuthIP component 237 is configured to

20 verify the NAP certificate on the server 223.

[0038] FIG 3 shows an illustrative software protocol stack 305 and hardware interface 312 that may be utilized in a non-Direct Access-ready endpoint to enable

it with Direct Access capabilities. An endpoint may include a client computer, mobile information appliance (such as mobile phone, smart phone, PDA, pocket

25 PC, handheld game device, media player, etc.), server, or intermediate network device such as a gateway, router, switch, etc. In this example, the hardware interface 312 may be alternatively implemented as a network interface card

("NIC") or as a chipset. When implemented as a NIC, the hardware interface will typically interface with an endpoint over a standardized physical interface 315 such

30 as those employing a PCI, PCI-X, or PCI Express bus. When implemented as a

chipset, the hardware interface will typically physically interface with an endpoint using a device-specific or proprietary interface 319.

[0039] As shown in FIG 3, the software protocol stack 305 on the endpoint includes an application layer 325 that interacts with a transport layer 332 that supports protocols such as TCP and UDP (User Datagram Protocol). An IPv4 internet layer 336 implements data transport through network interface layer 340. A hardware interface driver 345 provides the necessary abstraction of the hardware interface 312 to the protocol stack 305.

[0040] FIG 4 shows the functional components of an illustrative hardware interface when implemented as a NIC 405. The components may be optionally utilized in various combinations, as indicated by the dashed rectangles, depending on the requirements of a particular implementation. For example, in some implementations, only IPsec is needed if the operating system already supports IPv6. Or in others, direct access may not be needed and the NIC 405 is utilized to provide only ESAS functionality. This could occur, for example, in cases when the NIC 405 is installed in a device like a switch or router.

[0041] The components include a translation component 412 and an IPsec component 416. The translation component 412 provides translation from IPv4 to IPv6 as well as an ALG functionality to make modifications to the DNS registry. The IPsec component 416 enables termination of IPsec connections. In this example, the IPsec component 416 is implemented to include NAP enforcement (i.e., component 416 supports IPsec-NAP). The hardware NIC 405 thus provides non-Direct Access-ready interfaces (i.e., IPv4 and non-IPsec interfaces as respectively indicated by reference numerals 425 and 428) to provide interoperability without modification to the endpoint in which it is installed while enabling native IPv6 capability.

[0042] The NIC 405 further includes an ESAS component 423 which provides Enterprise Security Assessment Sharing capabilities to an endpoint in which the NIC 405 is installed. The ESAS component 423 may implement some or all of the ESAS functionality in hardware that is typically provided by software. Illustrative

ESAS scenarios which utilize an endpoint having an installed NIC with ESAS capability are shown in FIGs 10 – 11 and described in the accompanying text.

[0043] FIG 5 shows the functional components of an illustrative hardware interface when implemented as a chipset 505. As with the components shown in FIG 4, the components in FIG 5 may be optionally utilized in various combinations. The components include a translation component 512 and an IPsec component 516 that are arranged with similar features and functionalities as their counterparts shown in FIG 4 and described in the accompanying text. The chipset 505 also includes a client-side NAP component 521. The client-side NAP component 521 may be used, for example, in client device applications such as with mobile information appliances that are not currently provided with NAP capabilities. As with the hardware NIC 405, the hardware chipset 505 provides non-Direct Access-ready interfaces (i.e., IPv4 and non-IPsec interfaces as respectively indicated by reference numerals 525 and 528) to provide interoperability without modification to the endpoint in which it is installed while enabling native IPv6 capability.

[0044] It is noted that both the NIC 405 and chipset 505 may be alternatively implemented using a “dual stack” arrangement in which both IPv4 and IPv6 are supported. In this implementation, either separate IPv4 and IPv6 network stacks may be used, or more typically, the stacks will share some common code. Dual stack arrangements are described, for example, in RFC 4213 and are often used to provide transition mechanisms between IPv4 and IPv6 so that endpoints in a system can still be accessed using solely IPv4 if needed. It is further noted that the NIC 405 and chipset 505 may be configured to interoperate with either Direct Access clients or Direct Access servers as needed to meet the requirements of a particular implementation.

[0045] The chipset 505 further includes an ESAS component 523 which provides Enterprise Security Assessment Sharing capabilities to an endpoint in which the chipset 505 is installed. The ESAS component 523 may implement some or all of the ESAS functionality in hardware that is typically provided by software.

Illustrative ESAS scenarios which utilize an endpoint having an installed NIC with

ESAS capability are shown in FIGs 10 – 11 and described in the accompanying text.

[0046] An illustrative example in which an ESAS arrangement is implemented using the present hardware interface now presented. In an enterprise computing environment, for example, an office of a business, a number of personal computers, workstations, servers and the like, along with other devices such as mass storage subsystems, internal network interfaces, and external network interfaces, are typically interconnected to provide an integrated environment in which information may be generated, accessed from external sources, and shared among various users. Commonly, users perform a variety of operations including order receipt, manufacturing, shipping, billing, inventory control, document preparation and management, e-mail, web browsing, and other operations in which creation, access, and sharing of data is beneficial.

[0047] Currently, security is typically provided for an enterprise using a variety of different security products that are each normally arranged to monitor only a partial portion of enterprise-wide data. That is, security products are arranged as separate local “islands” where each product monitors, assesses, and takes action with respect to different parts of the data within the enterprise. For example, the host security product, edge firewall product, NIDS product, NAP product, and other discrete security products typically provide security for the various different parts of the enterprise.

[0048] While these security products often perform satisfactorily in many applications, detection of security incidents often suffers from undesirably high levels of false-positive and false-negative occurrences as a result of the monitoring of only partial enterprise security data. It has also been difficult to provide effective common management across all the enterprise security product islands. Current attempts to correlate enterprise-wide security data have high management and maintenance costs and have problems in scaling. Accordingly, ESAS provides a single enterprise-wide view to enable security administrators to define and enforce clear, simple, and unified enterprise-wide policies for automatic responses to security incidents.

[0049] As noted above, ESAS relies upon a semantic abstraction, called a security assessment that enables sharing of security-related information between different security products, called security endpoints, in an enterprise security environment.

A security assessment is defined as a tentative assignment by a security endpoint of
5 broader contextual meaning to information (i.e., data in some context) that is collected about an object of interest in the environment such as a computer, user, service (e.g., a website), data, or the enterprise as a whole. The security assessment utilizes a concise vocabulary for a security endpoint to declare that an object in the environment falls into a particular assessment category such as “compromised” or
10 “under attack” along with the severity (e.g., low, medium, high, critical) of the detected incident.

[0050] A security assessment is tentative because it is subject to some uncertainty and is valid for a limited period of time. The tentative nature of a security assessment is reflected in two of its components: a fidelity field which expresses
15 the level of confidence the security endpoint has in its assignment of contextual meaning, and a time-to-live (“TTL”) field which reflects the security endpoint’s estimate of the time period for which the security assessment is expected to be valid. Thus, for example, a security assessment may be used by a security endpoint to declare, in light of that security endpoint’s current understanding of one or more
20 security incidents, that a particular machine is compromised, with a critical level of severity, with medium fidelity, and having a TTL of 30 minutes. A variety of types of security assessments may be used in any given enterprise security environment having, for example, various combinations of assessment category and object type.

[0051] Security endpoints are enabled with functionality to publish security
25 assessments onto a security assessment channel operating in the environment, as well as subscribe to a subset of available security assessments published by other security endpoints. The security assessments existing in the environment that are active (i.e., those having a TTL which indicates the assessments are still valid) function to provide a security context that gives such an ESAS-enabled endpoint a
30 new way to look at its own locally-available information. That is, the security context enables the ESAS-enabled endpoint to combine or correlate evidence from

security assessments received from a variety of different sources, and across object types, in order to significantly enhance the quality of its detection of potential security incidents. The ESAS-enabled endpoint then makes a decision as to what local action or response is appropriate for each type of security assessment

5 (whether received from another security endpoint or internally generated by the security endpoint itself) in accordance with a set of response policies. Incident detection is both efficient and cost-effective because the security context enables distributed processing of enterprise-wide information, in the form of security assessments, without the burden of sharing large amounts of raw data throughout
10 the enterprise (most of which is completely irrelevant due to the lack of any context). ESAS-enabled endpoints are further arranged to roll back the local action upon expiration of the security assessment that prompted the local action (i.e., when the security assessment exceeds the time-to-live specified in the TTL field).

[0052] In most typical ESAS implementations, a specialized security endpoint
15 called an ESAS central server is utilized. The ESAS central server is coupled to the security assessment channel and performs as a centralized audit point by subscribing to all security assessments, logging the security assessments, and also logging the local actions taken by security endpoints in response to security incidents in the environment. The ESAS central server provides administrators
20 with a comprehensive view of the history and current status of the enterprise as a whole and of each ESAS-enabled endpoint. The utilization of the security assessments enables an administrator to compactly and efficiently configure response policies to incidents that are detected across the entire enterprise. The security assessments function as natural anchors, or starting points, to define
25 enterprise-wide security response policies. A streamlined and consistent management interface is thus enabled to define the desired responses for each type of security assessment across the entire enterprise.

[0053] The ESAS arrangement provides a number of advantages. By employing a security assessment having a concise vocabulary, overall data complexity in the
30 enterprise is drastically reduced and only meaningful information is shared between security endpoints. Use of the security assessment also eliminates the need to

collect large amounts of raw data in a central storage location, and thereby enables highly scalable enterprise security solutions to be built on a very cost effective basis. In addition, a new security endpoint may be readily deployed with on-demand extensibility. Security assessments may be shared between the new security endpoint and existing security endpoints without the need to reconfigure any of the response policies within existing security endpoints. The new security endpoint simply functions as a new source of security assessments using a semantic abstraction that the existing security endpoints already understand. The utilization of security assessments also enables enterprise-wide security policies to be established using a very compact and clear methodology, without needing to understand all of the possible security events that every security endpoint may generate in the enterprise, and then try to describe the responsive action for each event.

[0054] Turning now to FIG 6, an illustrative ESAS arrangement 600 deployed in the enterprise network 130 is shown in which a security assessment channel 602 is provided to enable a security assessment to be shared among multiple security endpoints using a language/protocol that is commonly-utilized at each security endpoint. The security assessment channel 602 facilitates a publish/subscribe model used by the security endpoints for connecting the sources of security assessments (publishers) to the consumers of the security assessments (subscribers). As shown, both the publishers and subscribers on the security assessment channel 602 are security endpoints 605.

[0055] The security endpoints 605 are isolated from the mechanics of the actual transport and management of the publish/subscribe model through a semantic abstraction layer that is arranged to simplify interactions with the security assessment channel 602. The abstraction layer comprises tables describing the security assessment types to which the security endpoints subscribe, and tables describing the security assessment types that security endpoints publish (as described below, not all security endpoints generally subscribe to all security assessment types). In addition, the abstraction layer provides an API (application

programming interface) for reading received security assessments, and an API for generating security assessments.

[0056] A specialized security endpoint, ESAS central server 616, is coupled to the security assessment channel 602 and performs as a centralized audit point for the ESAS arrangement 600. Accordingly, the ESAS central server 616 subscribes to all security assessments and permanently logs them. ESAS central server 616 also receives and logs messages from the security endpoints that indicate the local actions that are taken by a security endpoint. The ESAS central server 616 thus provides administrators with security assessment monitoring functionality that gives a comprehensive view of the history and current status of the enterprise as a whole, as well as each ESAS-enabled endpoint.

[0057] FIG 7 is a diagram of a first illustrative scenario in which a plurality of ESAS-enabled endpoints are coupled to the security assessment channel 602, and a detected incident at one security endpoint triggers responses at multiple other security endpoints. This illustrative scenario is described in three stages. As indicated by reference numeral 710, the edge firewall 605₂ first identifies a potentially compromised client, for example, because it creates so many connections to the perimeter of the enterprise network 130 that the most likely explanation for the behavior is the existence of a security compromise. Second, the edge firewall 605₂ sends a security assessment that indicates the particular client is “compromised” with high severity and high fidelity, as indicated by reference numeral 720, over the security assessment channel 602 to subscribing security endpoints.

[0058] Third, the subscribing security endpoints 605_{1, 2, 3 ... N} and the ESAS central server 616 which receive the security assessment apply their specific security expertise through the application of their own correlation rules and locally-available data to trigger an appropriate action. As collectively indicated by reference numeral 730 in FIG 7, the host security endpoint 605₁ performs an on-demand scan. The NAP endpoint 605₃ revokes the IP security certificate for the identified compromised client and implements a port shutdown. The line-of-business security endpoint 605_N temporarily suspends instant messaging (“IM”)

traffic to the compromised client based on the received security assessment. The ESAS central server 616 raises an alert for a security analyst (e.g., an administrator) and also logs all of the security assessments and actions invoked.

[0059] The first illustrative scenario described above provides a case where the

5 security endpoint detecting the suspicious incident generates a security assessment with high severity and high fidelity (i.e., the security endpoint has a high degree of confidence that it has validly detected a serious incident). By comparison, FIG 8 is a diagram of a second illustrative scenario in which a low fidelity security assessment is sent over the security assessment channel 602 that triggers the
10 generation of a high fidelity assessment by a receiving security endpoint which also performs cross-object mapping.

[0060] This second illustrative scenario is also described in three stages. As indicated by reference numeral 810, the edge firewall 605₂ first detects a large number of client connections to a perimeter of the enterprise network 130.

15 However, unlike the first illustrative scenario shown in FIG 7 and described in the accompanying text, the number of connections being established by the client is not so high that the edge firewall 605₂ can be absolutely certain that the client has been compromised. In current enterprise security systems, when a security endpoint sees such data it generally just drops the data and takes no action as there is not enough
20 evidence to warrant the typically harsh response such as disconnecting the machine. By comparison, in the present scenario, the edge firewall 605₂ in the second stage sends a security assessment 815 over the security assessment channel 602 that indicates that the particular client is compromised with medium severity and low fidelity, as indicated by reference numeral 820.

25 [0061] Here, the subscribing security endpoints to the particular object referenced in the security assessment 815 generated by the edge firewall 605₂ include the host security endpoint 605₁ and the ESAS central server 616. While such a low fidelity data normally does not trigger an action to be taken at a security endpoint in current security products, in accordance with the present enterprise security assessment
30 sharing, the host security endpoint 605₁ looks at its own local data differently in light of the received security assessment from the edge firewall 605₂. In this case,

the local data resulting from an on-demand scan at the host security endpoint 605₁ and the information contained in the security assessment from the edge firewall 605₂ are used to generate new assessments 825 and 828. Thus, the host security endpoint 605₁ has information that, by itself, does not warrant the generation of a new security assessment, but when reinforced with even a low fidelity assessment from another security endpoint, as in this case, there is sufficient evidence to justify the creation of the new security assessments 825 and 828 which each have high fidelity.

[0062] The host security endpoint 605₁ places the new security assessments 825 and 828 onto the security assessment channel 602. The new security assessments 825 and 828 are received over the security assessment channel 602 by the subscribing security endpoints which, in this illustrative scenario, include the edge firewall 605₂, and the ESAS central server 616 for security assessment 825 and line-of-business endpoint 605_N for security assessment 828.

[0063] Note that the line-of-business endpoint 605_N was not a subscriber to the original security assessment 815 produced by the edge firewall 605₂ because the reference object type is a machine and the line-of-business endpoint 605_N, by virtue of its role in protecting e-mail, is typically concerned with the users. However, in this second illustrative scenario the host security endpoint 605₁ maps from a host object type to a user object type when it generates a new security assessment 828. Such cross-object mapping capability may be beneficial in many scenarios as it is contemplated that a high severity incident, such as malware or malicious activity that potentially compromises the data confidentiality or integrity of a host computer, may also potentially compromise the user as well. A security assessment may be generated that cross-maps the high severity incident from the host object type to a user object type with a certain degree of fidelity. Similarly, for a critical severity incident in which malware or malicious activity has actually caused a loss of data integrity on a host computer, a security assessment for a user object type may be generated with even higher fidelity.

[0064] In stage three, the new security assessments 825 and 828 trigger a variety of respective actions at the receiving security endpoints, as collectively indicated by

reference numeral 830. Specifically, the edge firewall 605₂ blocks all access by the compromised client with the exception of software updates and/or mission-critical access. The line-of-business endpoint 605_N temporarily suspends outgoing e-mails. And, as with the first illustrative scenario, the ESAS central server 616 continues to log all assessments and actions. As noted above, such restrictions are enforced only during the period of time for which the TTL associated with the new security assessments 825 and 828 remains valid. When the new security assessments expire, the actions taken by the respective security endpoints are rolled back unless the TTL is extended or a new security assessment which invokes the restrictive actions is received.

[0065] FIG 9 is a diagram of a third illustrative scenario that shows the targeted use of remediation techniques. This third illustrative scenario is described in three stages. As indicated by reference numeral 910, the edge firewall 605₂ first detects a large number of client connections to the perimeter network. Second, the edge firewall 605₂ sends a security assessment 915 that indicates the particular client is “compromised” with high severity and high fidelity, as indicated by reference numeral 920, over the security channel 602 to subscribing security endpoints. The subscribing security endpoints include the host security endpoint 605₁ the NAP endpoint 605₃ and the ESAS central server 616.

[0066] The host security endpoint 605₁ reviews the received security assessment and applies its specific security expertise using correlation rules and any relevant locally-available data. In this illustrative example, the host security endpoint 605₁ responsively generates a new security assessment 925 containing a user object type to which the line-of-business security endpoint 605_N subscribes.

[0067] In the third stage of the scenario, the remediation techniques employed by the security endpoints are considered expensive in terms of their potential impact on business operations within the enterprise network 130. For example, as indicated by reference numeral 930, the line-of-business security endpoint 605_N implements a response policy that entails temporarily suspending outgoing e-mail.

In addition, the host security endpoint 605₁ performs an on-demand scan and if no results are achieved, performs a deep scan. While such remediation techniques can

be very effective in addressing malware, malicious users, and other problems, they typically impart significant expense to the enterprise. For example a user whose outgoing e-mail is suspended will be less productive, and deep scanning typically requires one or more reboots which will remove the machine from service for a
5 period of time.

[0068] The ESAS arrangement advantageously enables these effective, albeit expensive, remediation techniques to be applied in a targeted manner and not merely in a general way or across-the-board which can be unjustified for some machines and/or users. Only objects in the environment that are deemed
10 suspicious, using pre-defined criteria, will be subject to these particular remediation techniques.

[0069] FIG 10 shows an illustrative arrangement in which an ESAS security assessment channel may be extended from the enterprise network 130 over a non-secure network such as the Internet 112 to an endpoint that is ESAS-enabled
15 through use of the present hardware interface. In this example, the PC 105₁ utilizes a Direct Access-ready client NIC 405 while a mobile information appliance 105₃ uses a Direct Access-ready client chipset 505. Both the NIC 405 and chipset 505 use the optionally-utilized ESAS component which implements ESAS capability in hardware in this example. While client devices 105 are shown as being equipped
20 with ESAS capability in FIG 10, it is emphasized that any of a variety of devices in a networking environment may be configured to include the present hardware interface with ESAS including servers and intermediate network devices such as routers, gateways, switches, and the like.

[0070] As shown in FIG 10, security software running on the mobile information
25 appliance 105₃ detects a security incident such as a website that appears to be a phishing site. It can then publish a security assessment 1012 through the extended ESAS security assessment channel (indicated by reference numeral 1022) which is received by subscribing security endpoints 605 in the enterprise network 130. The chipset 505 in the mobile information appliance 105₃ may be configured to send
30 and receive security assessments over a defined channel. For example, the channel may comprise a link or use a defined IP address and may further be handled with a

particular QoS to guarantee communication of security assessments even in cases where the Internet 112 is congested.

[0071] As shown in FIG 11, the extended ESAS security assessment channel 1022 supports the receipt at the devices 105 of security assessments that are published by the security endpoints 605 in the enterprise network 130. As shown, a security assessment 1112 published by the edge firewall 605₂ is received by the PC 105₁ and the mobile information appliance 105₃. The receipt of the security assessment may trigger local responses by the client devices 105 in a manner that is similar to that described above in the text accompanying FIGs 7 – 9.

[0072] Although the subject matter has been described in language specific to structural features and/or methodological acts, it is to be understood that the subject matter defined in the appended claims is not necessarily limited to the specific features or acts described above. Rather, the specific features and acts described above are disclosed as example forms of implementing the claims.

WHAT IS CLAIMED IS:

1. A network interface card (405) arranged for enabling Direct Access when installed in a host endpoint in an enterprise network, comprising:
 - an IPv4 to IPv6 translation component (412) for providing IPv4 to IPv6 translation for data traffic that is incoming to the network interface card;
 - an IPsec component (416) arranged for terminating an IPsec connection; and
 - an enterprise security assessment sharing component (423) arranged for implementing a security assessment publish and subscribe model in hardware for sharing security assessments among network endpoints, a security assessment being arranged to provide contextual meaning to a security incident that occurs within an enterprise network environment.
2. The network interface card of claim 1 further including a standardized physical interface.
3. The network interface card of claim 1 further including a client-side NAP component that provides NAP capabilities to client devices in which the network interface card is installed.
4. The network interface card of claim 1 in which the IPv4 to IPv6 translation component is further arranged with an ALG functionality to perform modifications to a DNS registry.
5. The network interface card of claim 1 in which the enterprise security assessment sharing component is further arranged for defining a time interval over which the security assessment is valid.
6. The network interface card of claim 1 in which the enterprise security assessment sharing component is further arranged for receiving security assessments about security incidents detected by the network endpoints.
7. The network interface card of claim 1 in which the enterprise security assessment sharing component is further arranged for initiating a local response to a received security assessment.
8. The network interface card of claim 7 in which the enterprise security assessment sharing component is further arranged for rolling back a local response when a received security assessment is no longer valid.

9. A chipset (505) arranged for enabling Direct Access when installed in a host device (105), comprising:

an IPv4 to IPv6 translation component (512) for providing IPv4 to IPv6 translation for data traffic that is incoming to the host device (105); and

an enterprise security assessment sharing component (523) arranged for implementing an enterprise security assessment sharing system in hardware, the system being arranged for implementing a security-related information sharing model by which security-related information is shareable among a plurality of endpoints in an enterprise security environment, the model facilitating use of a method comprising the steps of describing an object in the environment using a semantic abstraction of security-related information that is available to an endpoint, the semantic abstraction i) being categorized by type, and ii) being commonly utilizable by the endpoints, and using a publish and subscribe model by which a publishing endpoint publishes the semantic abstraction to which a subscribing endpoint subscribes according to a subscription, the subscription being based on the semantic abstraction type.

10. The chipset of claim 9 in which the semantic abstraction is a security assessment that is arranged for providing an assignment of context by an endpoint to the security-related information using a pre-defined taxonomy which utilizes a schematized vocabulary comprising object types and assessment categories.

11. The chipset of claim 9 further including an IPsec component arranged for terminating an IPsec connection.

12. The chipset of claim 11 in which the IPsec component is an IPsec-NAP component.

13. The chipset of claim 11 in which the IPsec component performs IPsec tunneling.

14. The chipset of claim 11 in which the IPsec component implements an IPsec tunneling endpoint.

15. The chipset of claim 9 further including a device-specific physical interface.

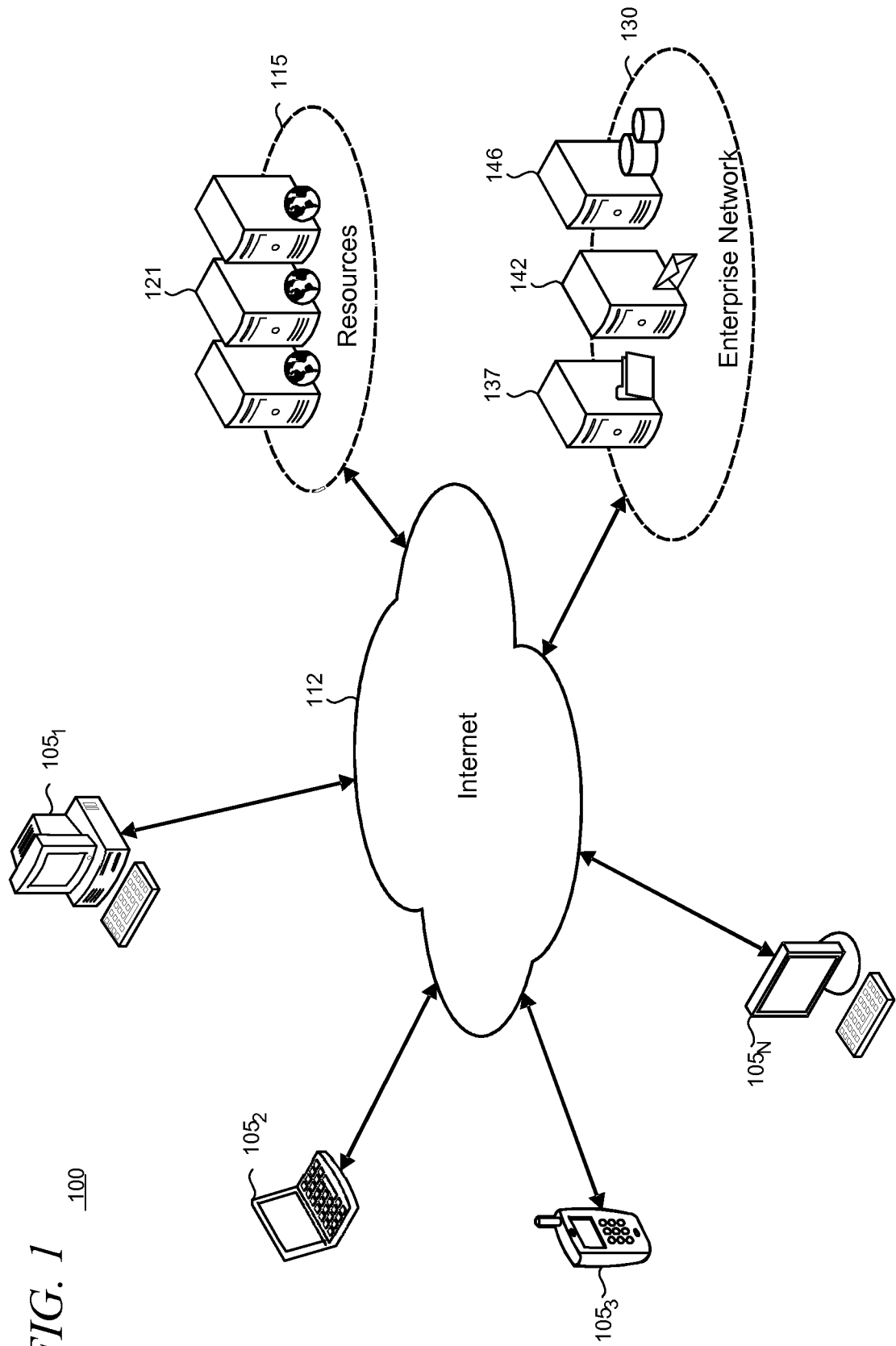


FIG. 1

FIG. 2

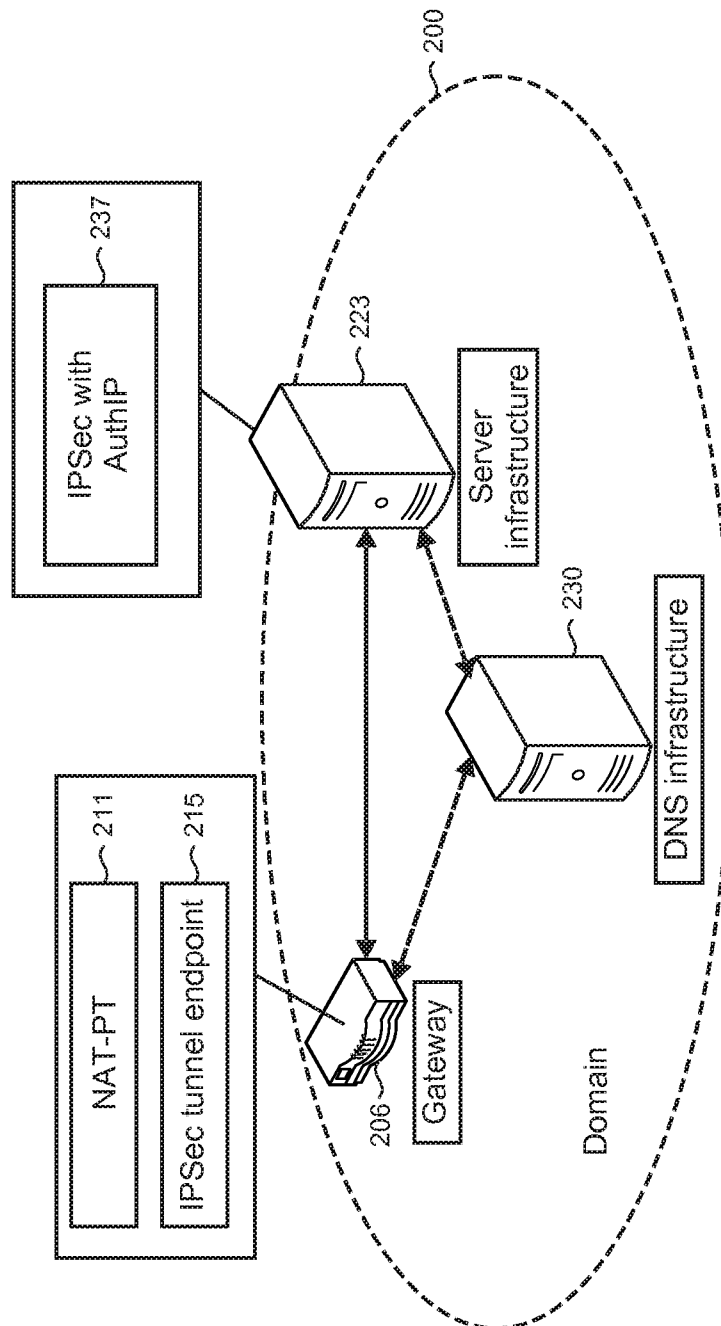


FIG. 3

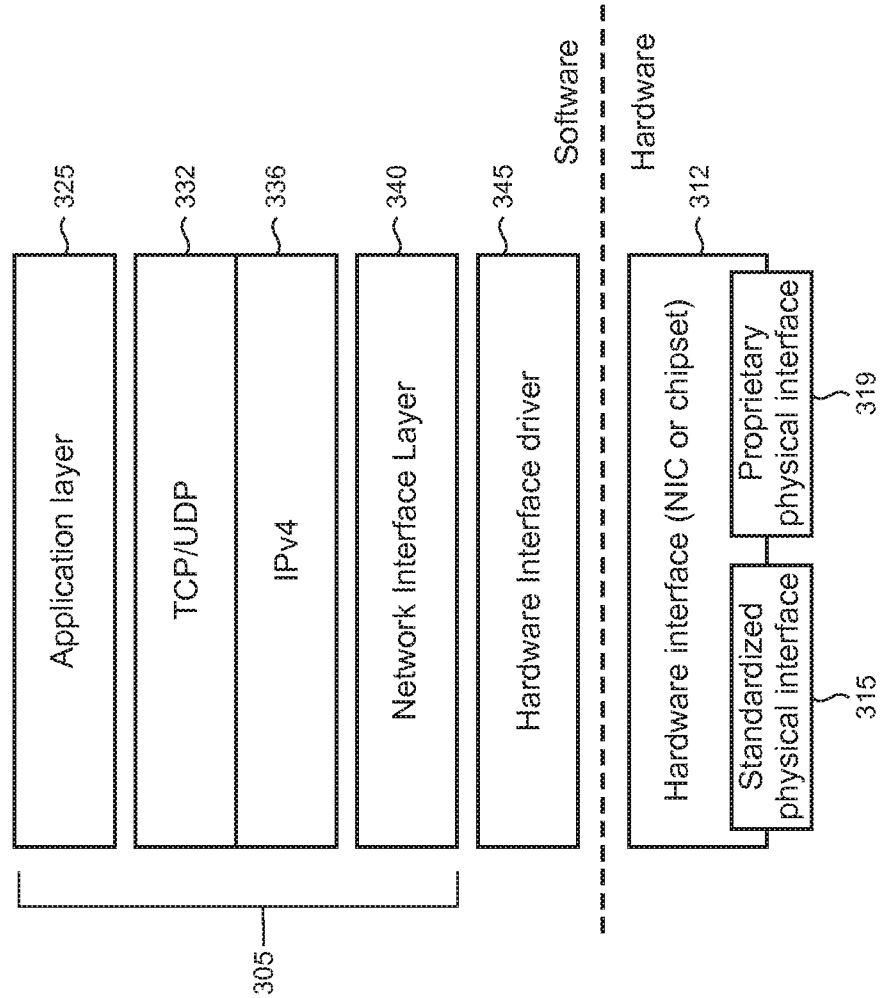


FIG. 4

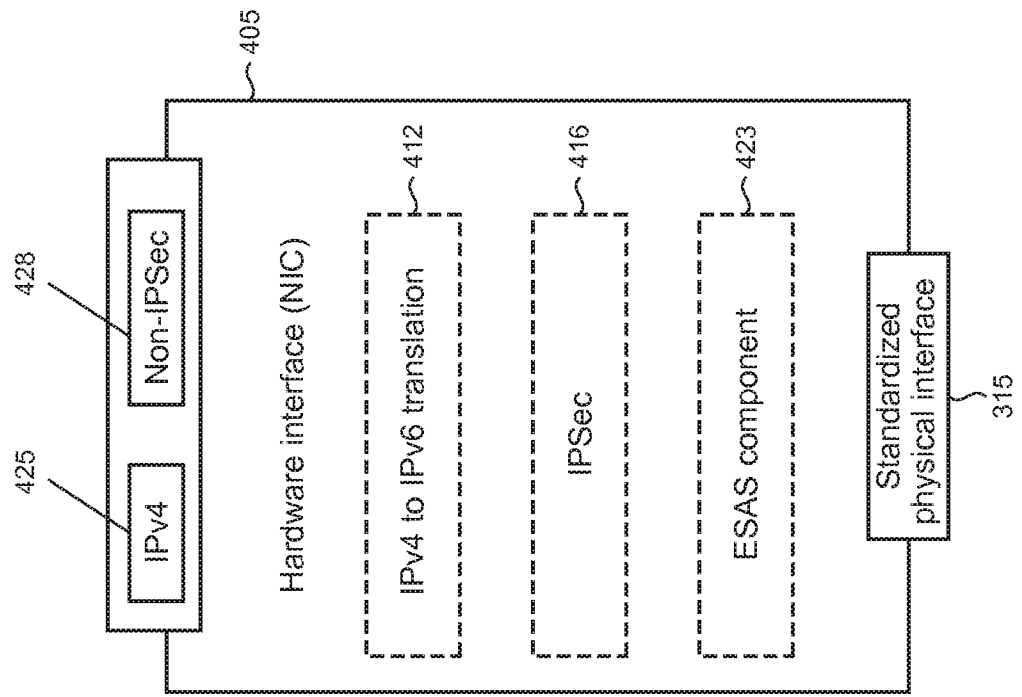


FIG. 5

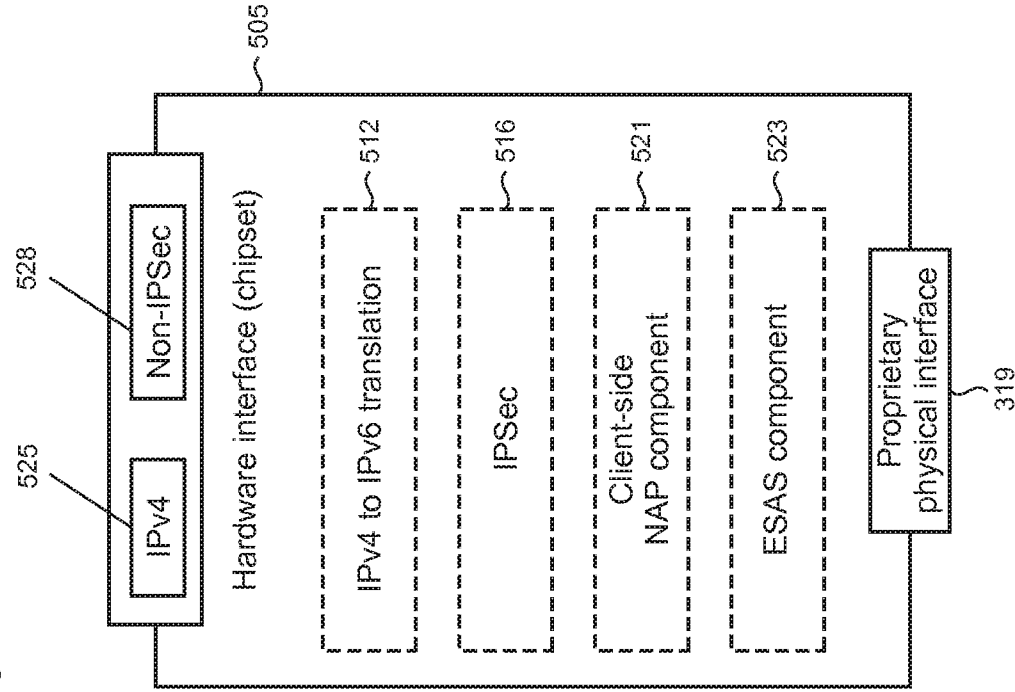
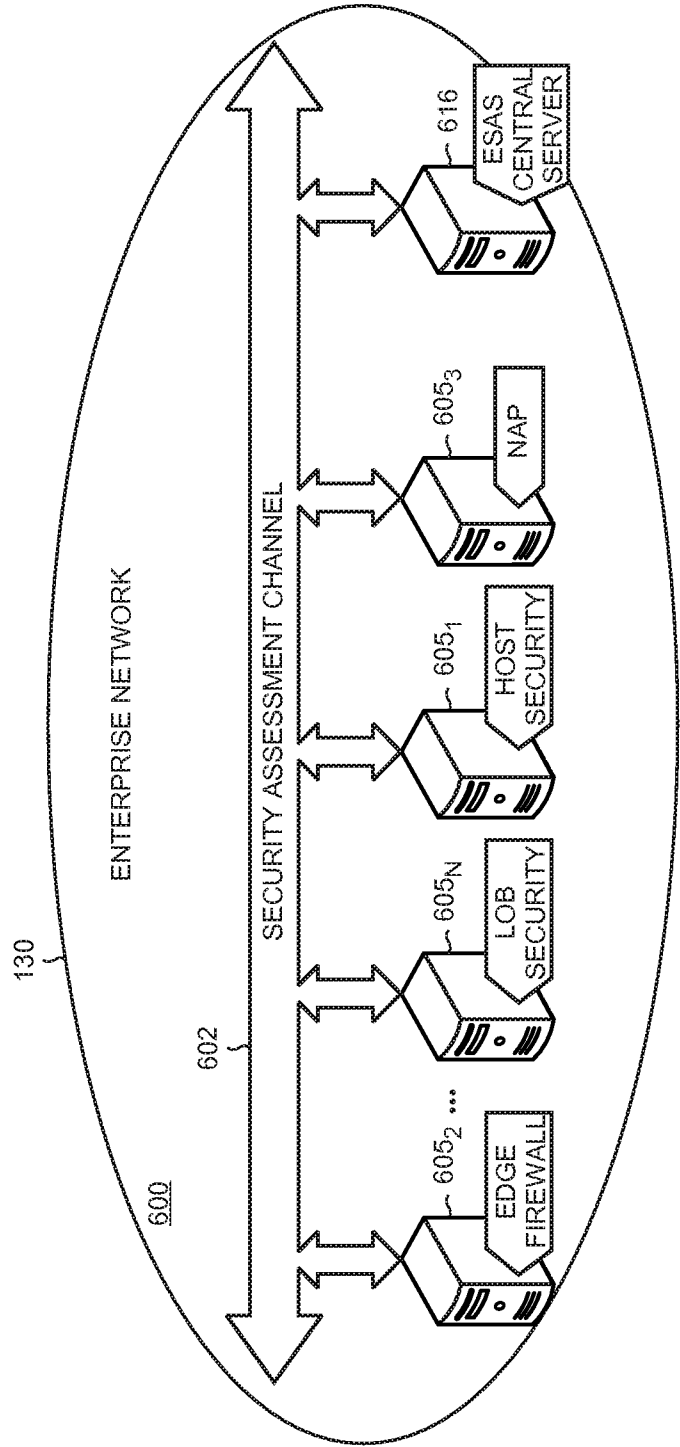
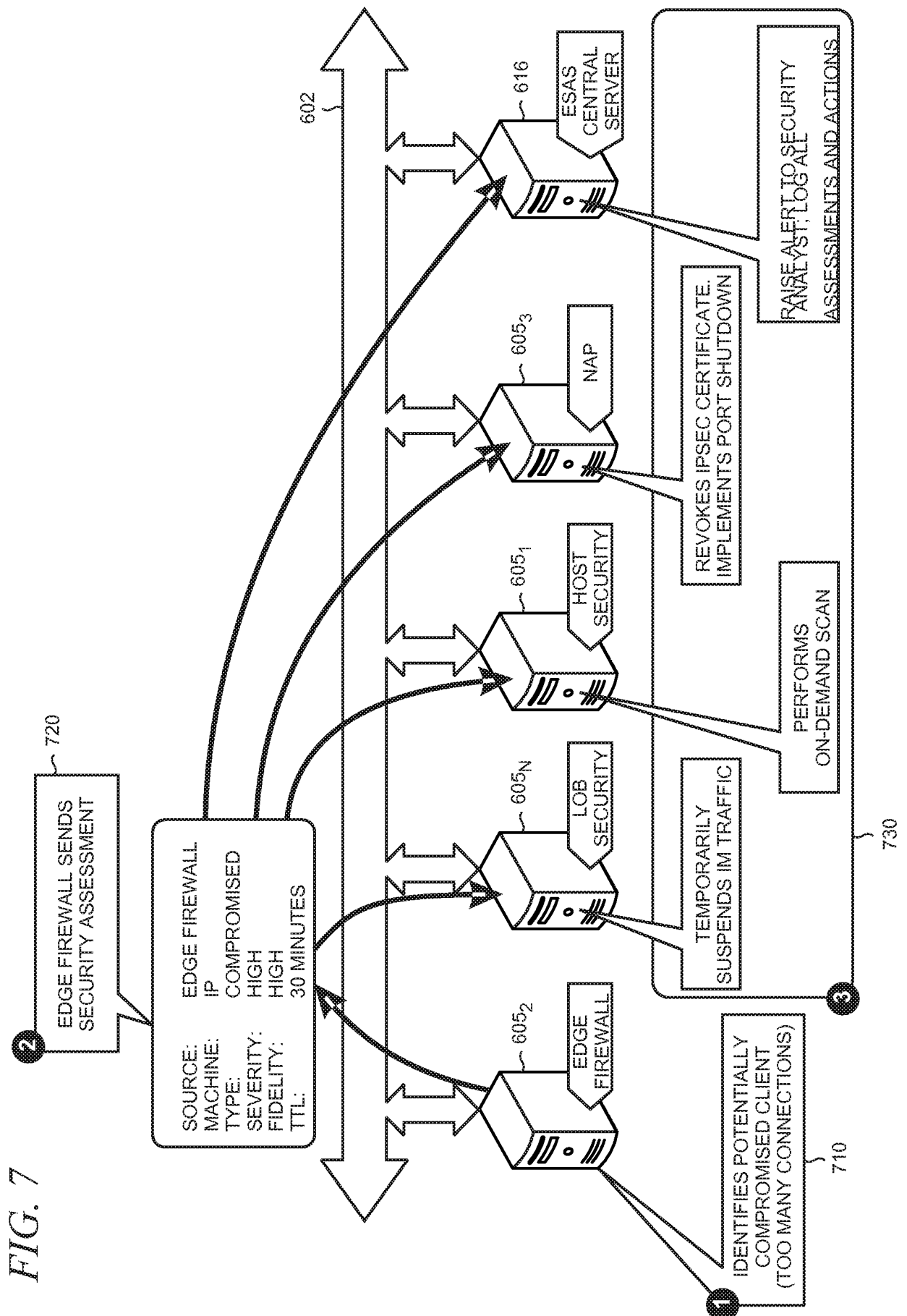
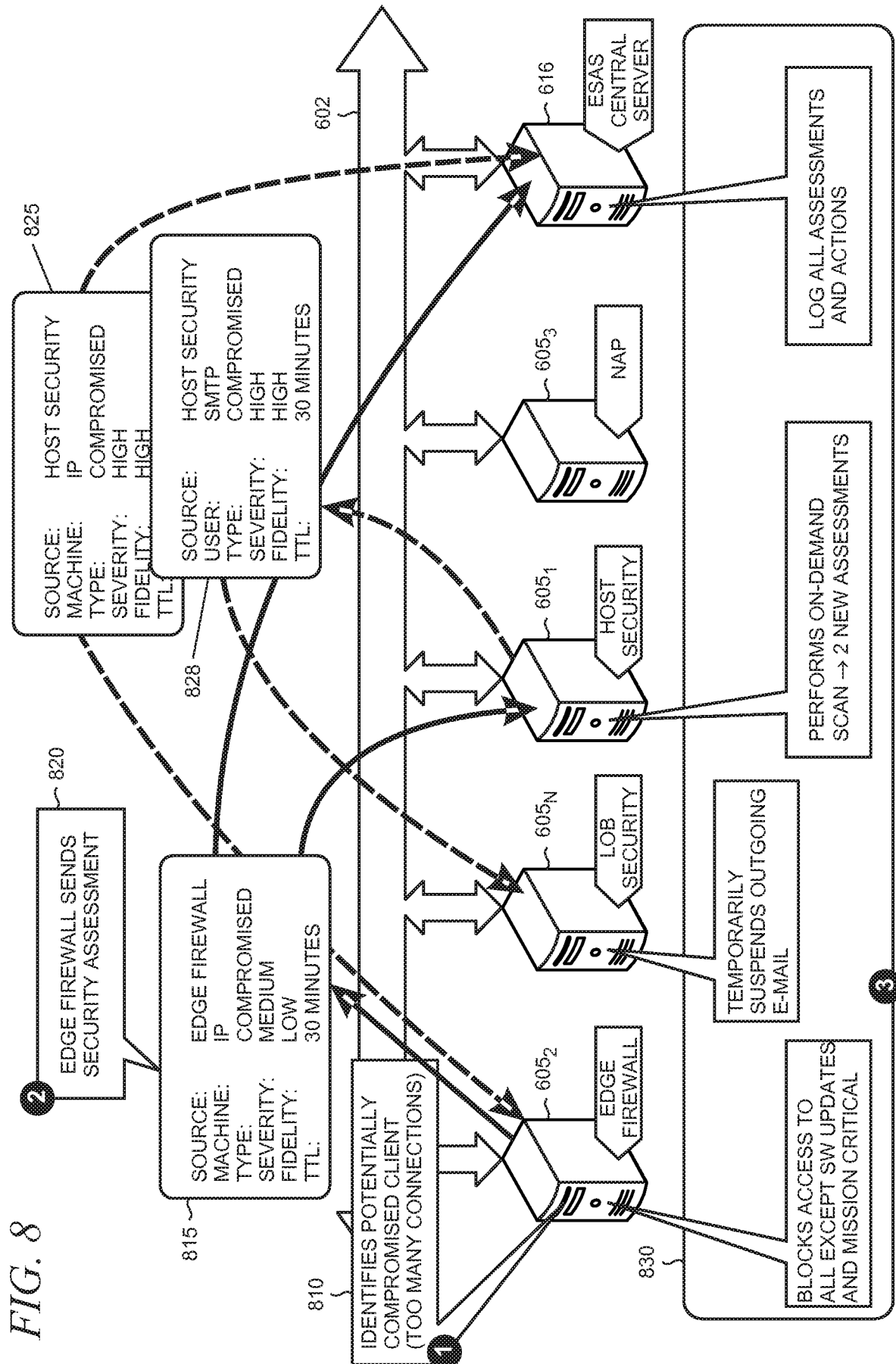


FIG. 6





7/10



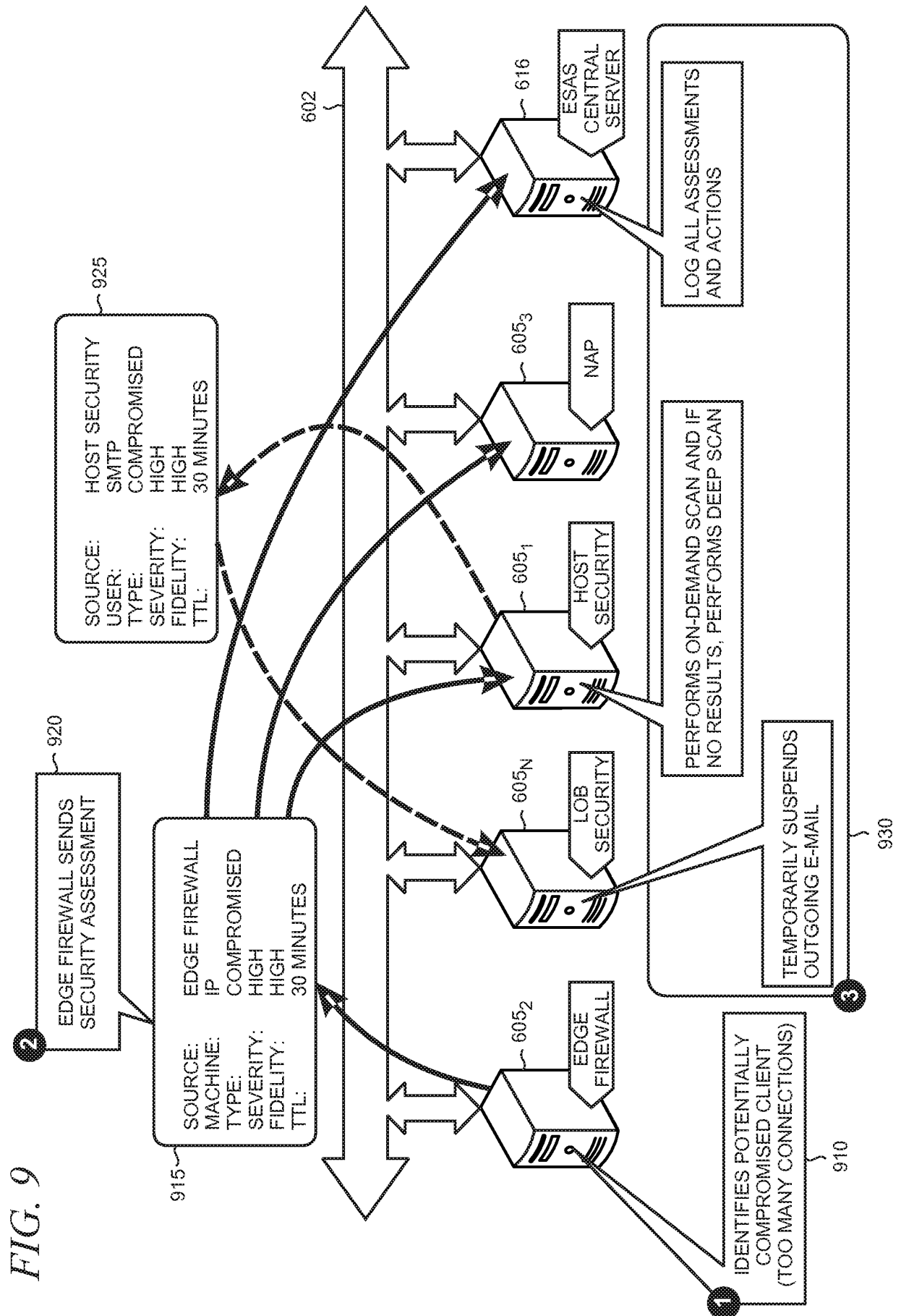
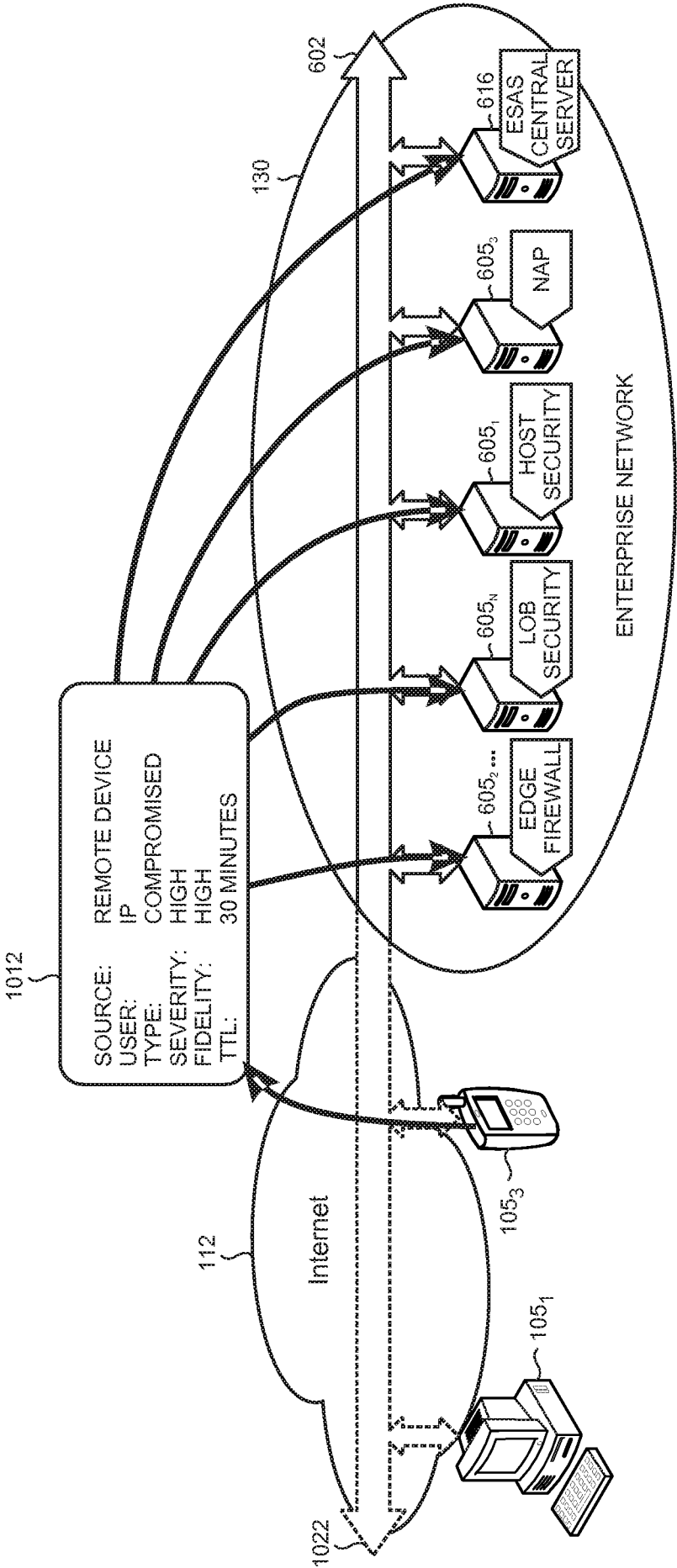
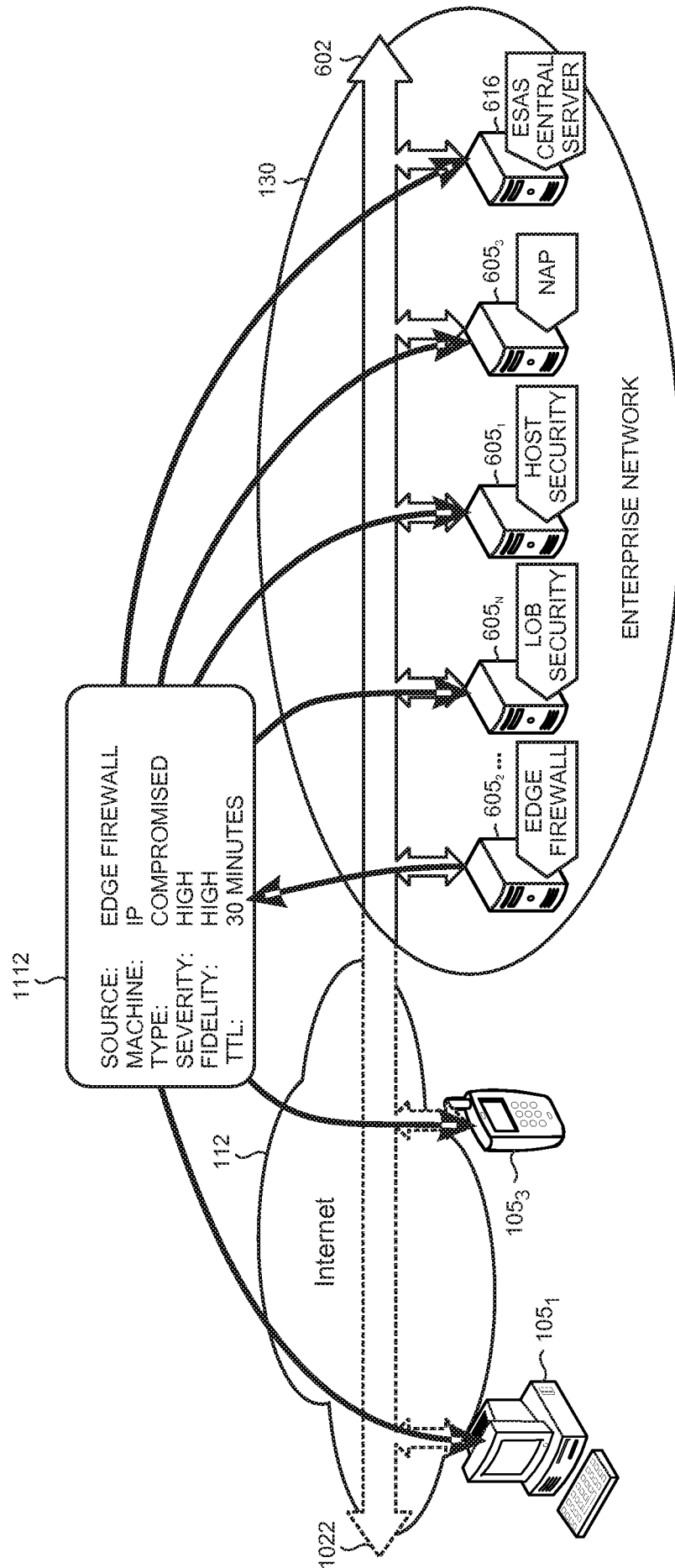


FIG. 10



10/10

FIG. 11



INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2009/036410**A. CLASSIFICATION OF SUBJECT MATTER****G06F 17/28(2006.01)i**

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Korean Utility models and applications for Utility models since 1975

Japanese Utility models and applications for Utility models since 1975

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

eKOMPASS (The internal search database of KIPO)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KR 10-2007-0121323 A (UNIVERSITY-INDUSTRY COOPERATION GROUP OF KYUNG HEE UNIVERSITY) 27 DECEMBER 2007 See abstract, figure 1, page 3, claims 1-4	1, 9
A	US 6,795,917 B1 (YLONEN, T.) 21 SEPTEMBER 2004 See abstract, figures 10 and 12, column 5, line 1-39, claims 1-5 and 9-11	1, 9
A	US 6,708,219 B1 (BORELLA, M. S. et al.) 16 MARCH 2004 See abstract, figure 5, column 4, line 3-19 and 40-47, column 9, line 25-38, column 9, line 59-column 10, line 8 and line 22-58, claims 1-3 and 5-9	1, 9



Further documents are listed in the continuation of Box C.



See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search

27 AUGUST 2009 (27.08.2009)

Date of mailing of the international search report

27 AUGUST 2009 (27.08.2009)

Name and mailing address of the ISA/KR

Korean Intellectual Property Office
Government Complex-Daejeon, 139 Seonsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea

Facsimile No. 82-42-472-7140

Authorized officer

Tae-Geun KIM

Telephone No. 82-42-481-8120



INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.

PCT/US2009/036410

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 10-2007-0121323 A	27. 12. 2007	None	
US 06795917 B1	21.09.2004	AU 1999-18795 A1 CA 2315722 A1 CA 2315722 C EP 1036460 A2 EP 1036460 B1 JP 03-457645 B2 JP 2002-501332 A WO 1999-035799 A2	30. 12. 1998 15.07. 1999 04. 12.2007 20.09.2000 19. 10.2005 01.08.2003 15.01.2002 15.07. 1999
US 06708219 B1	16.03.2004	AU 2001-19673 A1 WO 2001-031888 A1	18. 10.2000 03.05.2001