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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 March 2004 (18.03.2004)

PCT

(10) International Publication Number
WO 2004/023307 A1

(51) International Patent Classification[7]: G06F 11/30, 12/14, H04L 9/00, 9/32

(21) International Application Number: PCT/US2003/028065

(22) International Filing Date: 8 September 2003 (08.09.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/408,856 6 September 2002 (06.09.2002) US

(71) Applicant *(for all designated States except US)*: **O2MICRO, INC.** [US/US]; 3118 Patrick Henry Drive, Santa Clara, CA 95054 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **CHEN, Jyshyang** [US/US]; 1454 Poppy Way, Cupertino, CA 95014 (US).

(74) Agents: **PFLEGER, Edmund, P.** et al.; Grossman Tucker Perreault & Pfleger, PLLC, 55 South Commercial Street, Manchester, NH 03101 (US).

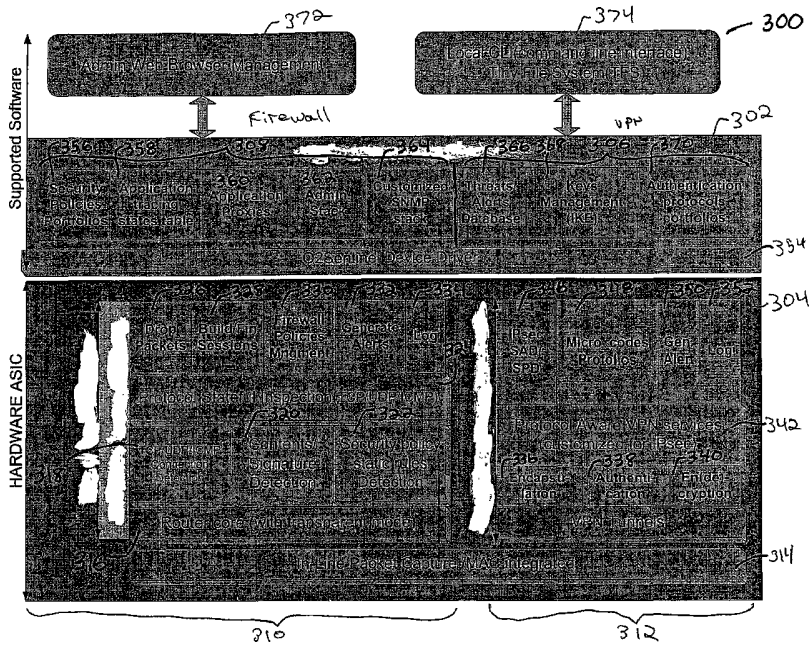
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: VPN AND FIREWALL INTEGRATED SYSTEM



(57) Abstract: The present invention provides an integrated VPN/Firewall system (300) that uses bath hardware (firmware) (304) and software (302, 372, 374) to optimize the efficiency of both VPN (306) and firewall (308) functions. The hardware (304) portions of the VPN (306) and firewall (308) are designed in flexible and scalable layers to permit high-speed processing without sacrificing system security. The software portions (302, 372, 374) are adapted to provide interfacing with hardware components (304), report and rules management control.

WO 2004/023307 A1

VPN AND FIREWALL INTEGRATED SYSTEM

This application claims priority to U.S. Provisional Application Serial No. 60/408,856, filed September 6, 2003, the teachings of which are hereby incorporated by reference in its entirety.

Field of the Invention

The present invention relates to networking systems, and more particularly, to an integrated firewall and VPN system. Utility for the present invention can be found in any LAN/WAN environment where VPN and/or firewall capabilities are utilized.

SUMMARY OF THE INVENTION

In one aspect, the present invention provides an integrated firewall/VPN system that includes at least one wide area network (WAN) and at least one local area network (LAN). An integrated firewall/VPN chipset is provided that is adapted to send and receive data packets between the WAN and said LAN. The chipset includes a firewall portion and to provide access control between the WAN and the LAN and a VPN portion adapted to provide security functions for data between the LAN and the WAN. The firewall includes firewall hardware and software portions wherein at least the firewall hardware portion is adapted to provide iterative functions associated with said access control. The VPN potion includes VPN hardware and software portions wherein at least VPN hardware portion is adapted to provide iterative functions associated with the security functions.

In another aspect, the present invention provides firewall/VPN integrated circuit (IC) the includes a router core adapted to interface between at least one untrusted network and at least one trusted network to send and receive data packets between the untrusted and the trusted networks. The IC also includes a firewall system adapted to provide access control between the untrusted and trusted networks, and includes firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with access control. The IC further includes a VPN engine adapted to provide security functions for data between the untrusted and trusted networks, and includes VPN hardware and software wherein at least said VPN hardware portion is adapted to provide iterative functions associated with the security functions.

One exemplary method according to the present invention includes a method of providing firewall access control functions, comprising the steps of defining one or more access control protocols; receiving a data packet; selecting a certain number of bytes of said data packet; and processing said selected bytes using said access control protocols.

The integrated firewall and VPN of the present invention is adapted to deliver complete suits of Internet security solutions, consolidated network management and comprehensive accounting loggings report based on traffic flow. In addition, the present invention offers protection from Internet threats since the VPN tunnel connection receives inherent firewall protection. Common DOS (denial of service) attacks that might compromise a stand-alone VPN gateway are detected and properly handled with the integrated firewall.

The present invention includes embedded concurrent policies to provide fine granular security to be applied to VPN traffic, thereby providing access control for all traffic. Both firewall and VPN can share the same user identification, and therefore individuals and predefined groups can have the same level of security services to access the resources they entitled.

Database updates and security policy management can be simultaneously applied to both VPN and firewall, which can reduce the impact latency in complicated network environment and provide centralized management and simpler configuration of the system. Therefore, network management does not have to maintain user identification across multiple systems.

The present invention firewall /VPN integrated system can control bandwidth management by every individual policy. By adjusting firewall policies the present invention also can efficiently effect the VPN channel bandwidth management.

Further security can be implemented by integrating the policy based NAPT with tunnel mode of encapsulation in IPsec VPN.

It will be appreciated by those skilled in the art that although the following Detailed Description will proceed with reference being made to preferred embodiments, the present invention is not intended to be limited to these embodiments. It should be understood from the outset that the present invention shall make use of the terms "software" or "modular processes", and the such terms shall be construed broadly as

encompassing one or more program processes, data structures, source code, program code, etc., and/or other stored data on one or more conventional general purpose and/or proprietary processors, that may include memory storage means (e.g. RAM, ROM) and storage devices (e.g. computer-readable memory, disk array, direct access storage). Alternatively, or additionally, such methods or modular processors may be implemented using custom and/or off-the-shelf circuit components arranged in a manner well-understood in the art to achieve the functionality stated herein.

Other features and advantages of the present invention will become apparent as the following Detailed Description proceeds, and upon reference to the Drawings, wherein like numerals depict like parts, and wherein:

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a generalized block diagram of the firewall/VPN integrated system according to the present invention;

Figure 2 is a functional block diagram of the firewall/VPN integrated system according to the present invention;

Figure 3 is an exemplary block diagram of the software and firmware components of the firewall/VPN integrated system according to the present invention;

Figure 4 is a detailed network-level block diagram of an exemplary implementation of the firewall/VPN integrated system according to the present invention.

Detailed Description of Exemplary Embodiments

Figure 1 depicts a generalized block diagram of the firewall/VPN integrated system 100 according to the present invention. In one exemplary embodiment, the system 100 includes a VPN portion 102 and a firewall portion 104 that operate to monitor traffic between the WAN 106 and LAN 108. The VPN portion 102 generally operates to provide secure encryption/decryption of packet data between gateways on the WAN side. The VPN portion includes hardware 110 and software 112 to provide encryption/decryption using conventional and/or proprietary encryption/decryption algorithms (processes), as is well understood in the art. The firewall portion 104 monitors traffic between the LAN and WAN (in a manner well understood in the art) and generally includes both hardware 114 and software 116 to monitor traffic. The present invention optimizes hardware and software to achieve both integrated functionality of

VPN and firewall functions, and to increase performance of the data flow on a system-wide level.

Figure 2 depicts a functional block diagram 200 of the firewall/VPN integrated system according to the present invention. The diagram 200 depicts data flow and processes for booth the VPN portion and the firewall portion. Incoming data (in the form of a packet stream) 202 from the LAN or WAN is received by the network interface 204. In the exemplary embodiment, the interface 104 is adapted to interface with the protocols used in the particular LAN/WAN environment, as is understood in the art. The interface 204 receives a packet stream and places the data into a packet buffer memory 206. Additionally, the system may be configured with additional and/or external memory 208 (e.g., Flash memory, SDRAM, etc.) which is adapted to temporarily store the packet data. In the exemplary embodiment, the external memory 208 is adapted top store IP data packets.

The interface 204 determines if the incoming data is plain text (from the LAN) or cipher text (from the WAN). If the data is plain text (meaning the data has come in from the LAN side), then the interface 204 is adapted to forward (along data path 222) a preselected number of bytes to the firewall 220. In the exemplary embodiment, the first 144 bytes of data from the packet stream are selected since these bytes contain Layer 2 through Layer 7 headers and content information. However, 144 bytes is only exemplary and may be some other preselected value, depending on, for example, the desired level of security or efficiency of the firewall. If the interface 204 determines that the incoming data 202 is cipher text (i.e., encrypted data coming in from the WAN side), then the incoming data stream is sent to the inbound VPN engine 210.

The inbound VPN engine 210 generally includes decryption and decapsulation processing to convert cipher text into a plain text IP packet. As will be described more fully below with reference to Figure 3, the VPN portion of the present invention utilizes both hardware and software to enhance the efficiency of the VPN engine. The incoming data along path 224 is placed into a conventional buffer 212. An inbound VPN processor 214 processes the data to decrypt and decapsulate the data. An inbound security associate database 216 is provided that includes a database of tunnels that associate two gateways on the WAN side, in a manner known in the art. The processor 214 uses the

tunnel information the database 216 to decrypt and decapsulate the incoming data. Also, protocol instructions 218 may be provided that includes microcodes to instruct the processor 214 to decrypt and/or decapsulate the data according to conventional and or user-defined security procedures. Once the message is decrypted and/or decapsulated, the resultant plain text (IP Packet) data is sent to the interface 204 along data path 225. In a manner described above, preselected bytes (e.g., the first 144 bytes) of the data are forwarded to the firewall 220 along path 222.

The firewall 220 receives the preselected number of bytes from the interface 204 to begin the process of packet filtering and routing. As will be described more fully below with reference to Figure 3, the firewall portion of the present invention utilizes both hardware and software to enhance the efficiency of the firewall. The firewall operates in a conventional manner to analyze incoming data according to preset or user-defined security policies. Such security policies are well understood in the art and may include conventional and/or proprietary security policies. The firwewall essentially operates to provide access control between an untrusted network (WAN) and a trusted network (LAN).

In the present invention, the firewall 220 is adapted with appropriate hardware and software to analyze the preselected data instead of having to operate on the entire data packet. This can increase the overall speed and efficiency of the firewall. Those skilled in the art will recognize that larger portions of preselected data will increase security, but may tend to slow down the firewall processing. Therefore, the present invention permits users to "tune" the firewall settings to meet desired security and/or speed requirements.

Once the data has passed the security policies, the present invention may also be adapted with quality management 224 and quality of service 226 processing. The quality management processing manages the packet buffer 206 to maintain the links between queued packets stored in the memory. Quality of services 226 operates as a packet priority scheduler and will receive information from the quality of service mapping and processor 228. Essentially, and as understood in the art, quality of service analyzes the type of data coming in to determine which goes out first, based on, for example, data type

(voice, IP, video, etc.) or bandwidth considerations on the network. Quality of service may also be adapted to determine the best path across the network for the data.

As a general matter, if data leaving the firewall is destined for the LAN, then the quality service process proceeds as described above and upon completion transmits a control signal 227 to the output interface 238 to instruct the packet buffer 208 to release the data. If data leaving the firewall is destined for the WAN, it may require encryption/encapsulation before being forwarded along to the WAN. In that event, an outbound VPN engine 230 is provided that provides encryption and/or encapsulation of WAN outbound data. The engine 230 includes an outbound VPN processor 232 that encrypts and encapsulates the data based on instructions from the protocol 234 and the outbound security associate database 236, in a manner similar to the inbound VPN engine 210 (described above). In one exemplary embodiment, the security policies in place in the outbound security associate database may be adapted to match the security policies of the firewall 220. Once the data is encrypted it is sent to the transmission interface 230 and leaves out onto the WAN 240.

Figure 3 is an exemplary block diagram 300 of the software and firmware components of the firewall/VPN integrated system according to the present invention. Generally, the software portions are set out at 302 and the hardware (ASIC) portions are set out at 304. The hardware and software associated with the firewall are set out at 310 and 308, respectively, while the hardware and software associated with the VPN are set out at 312 and 306, respectively. As set out above, the present invention utilizes hardware and software to increase overall efficiency. As a general matter, processes that are highly repetitive and/or mathematically intensive are formed in hardware, while other processes are performed using software. Each of the processes in the hardware platform 304 may comprise one or more distributed RISC-type processors adapted to perform the stated tasks, although other processor implementations are equally contemplated herein. It should be understood at the outset that the present invention provides a layered approach to both hardware and software functionality, as indicated by the different layers depicted in Figure 3. Of course, those skilled in the art will recognize that Figure 3 represents only one exemplary approach, and that other layered arrangements can be

made without departing from the spirit and scope of the present invention. Each of the blocks of Figure 3 is described more fully below.

Firewall Hardware Platform

The In-Line Packet Capture/MAC integrated block 314 is operable to receive traffic from the network, where the frame is the unit in this level. The router core 316 ensures that the packets will be forwarded according to different destination addresses and associated security measures, based upon either Firewall or VPN (virtual private network). The TCP/UDP/ICMP connection detection block 318 is adapted to determine the connection has been state fully traced. It can be adapted to make hash approach, then search if the coming packet has been in the traced and registered connection. It can be assumed the packets are save proven if they are within these state fully traced connection, then forward those packets to expedite this security measure.

The Contents/Signature detection block 320 is adapted to perform real time analysis of the 144 bytes of information of incoming data packet to determine if a limited number of patterns exists within incoming packets, which may be recognized codes of viruses or worms. The Security Policy static rules detection block 322 is adapted to provide static packet filtering function. The static feature means this packet filtering investigates the current single packet instead of looking the correlation or context of preceding packets or afterward. The Protocol Stateful Inspection (TCP/UDP/ICMP) block 324 is adapted to recognize the connection by inspecting its protocol's dynamics, so different applications using TCP or UDP, or ICMP can use this block to analyze incoming data. After the analysis contribution of this component, it will communicate with TCP/UDP/ICMP connection detection component to work out the speed connection check.

The drop packets block 326 receives results from the lower layers (324, 318, 320 and 322) to generate pass or deny decisions according to the security policies. The Build/Fin Sessions block 328 parses and tracks the beginning and ending of connection or session. Since the starting of TCP connection has states transition for two ends of connection, thus the security of TCP connection can rely on these states transition to close state to trade off for the performance. By this stateful tracking, the present invention utilizes hardware speed to monitor and lookup these connection building, lookup and

tearing down status. The Firewall Policies Management block 330 generally defines the hardware storage of security policies, which may include internal memory storage. The generate alerts block 332 generates specific events for the alerts by creating associated Interrupt events to software stack. The stores data according to different security policies or rules setup and individual statistic the packets for the software generated log reports.

VPN Hardware Platform

The Protocol Aware VPN engine 342 includes several hardware-core embedded function parts, including the Encapsulation function block 336, Authentication block 338, and En(de)cryption block 340. For flexibility and security concerns, distributed RISC-oriented proprietary cores may be used in this VPN engine. By changing the micro-codes for each individual micro-processor, the different tasks executed in this VPN engine will be different according to different protocols required, for example higher performance of IPsec protocol for IPv4 or IPv6.

The IPsec SADB/SPD block 346 includes hardware storage of IPsec tunnel attributes data base, and rule selectors. Every packet within tunnel needs to reference this data base to come out actions employ into this packet for IPsec protocol. This component may be optimized for IPsec protocol purpose. The contents of this database are from the tunnel negotiating via an IKE process. The Microcodes profiles block 348 holds different micro-codes for different security protocols. The Generate Alert block 350 is adapted to create Alerts based upon selected criteria, for example, the live time expiring of tunnel, an encounter with malicious encrypted packets, unsuccessful processing packets due to tunnel synchronization, etc. The Log 352 hardware statistics supports general logs VPN related and by every tunnel base.

Software Platform

The Device Driver 354 provides the interface between software 302 and hardware 304. The securities policies portfolios block 356 provides the management software for the deployment of security policies. The Application tracing states table block 358 is the software component to provide detailed investigation to see which applications use the TCP/UDP/
ICMP protocol. Then according to different application requirements and its stateful inspection, this software component may create associated gates in the firewall system

for secure protection purpose. The Application Proxies block 360 is generally located at the Kernel level to provide more detailed investigation according to application level. This process can re-assembly the flows and contexts of in-line network traffics to make more detailed content analysis or pattern searching for the database of virus or worms, or filter unwanted commands. The Administrative software stack 362 executes the administration tasks for the system. These tasks include firewall systems and VPN engine systems. The SNMP (small network management protocol) stack 364 is provided to execute the SNMP according to general RFC requirement. This component is the interface for the general network device or network software stack to get the status or any statistics or logs in the system.

The Threats/Alerts database 366 is provided to collect threats or alerts from hardware and software. These events can be stored in database form, to permit easy interface with a database application deployed above this kernel. The-7 Auto Keys/SA Management (IKE/ISAMP) block 368 provides the main protocols of IPsec to manually or auto negotiate keys and SA (security attribution) according to RFC2408 requirement. This component is associated with IPsec functions. The Authentication protocols portfolios 370 is provided to support IPsec authentication requirement. It may include message authentication protocol (HMAC-96) [RFC-2104] within ESP (Encapsulating Security Payload) and AH (Authentication Header). The goal of authentication algorithm is to ensure that the packet is authentic and can not be modified in transit.

The Administrative Web Browser Management provides Web based management GUI (graphic user interface) component. In the exemplary system, the system general CPU will host web server under HTTPS protocol, the management web page will stored in this web server. All configuration and management process for the system can be collaborated within this page point. By using socket layer SSL (Secure Sockets Layer), the management web page can be browsed remotely (in WAN host), or local secure LAN host with the encrypted connection.(i.e. the connection uses the chosen encryption algorithm to provide high degree privacy). The Local CLI(command line interface)/Tiny File System(TFS) 374 is adapted to provide local access with command line and configuration files interaction.

Figure 4 is a detailed network-level block diagram 400 of an exemplary implementation of the firewall/VPN integrated system according to the present invention. The firewall/VPN system 402, as described above, is employed as the access control module between the public network (WAN) 414 and one ore more LAN networks 408 and/or 410. In this example, the system is employed on a proxy server 406 via a conventional PCI bus 404. The router and other portions of this figure are self-explanatory to those skilled in the art.

System Overview And Specific Exemplary Implementations

As a summary, the following description details the present invention with reference some specific embodiments as depicted in Figures 2, 3 and 4. These embodiments are only exemplary and not intended to limit the present invention. The present invention provides a system-on-chip solution for high performance Firewall with integrated VPN. The firewall portion may be implemented as a coded system to provide multiple layers of static/dynamic packer filtering engines with different granularity of real-time policies inspection and flexible rule policies management. Besides the static/dynamic packet filtering for the sophisticated rule inspection, it has "Statefull Inspected" TCP/UDP connection match engine. The present invention can therefore be adapted to specifically expedite packet Filtering functions for the packets within established TCP/UDP connection.

For the rare virus or worms with deep dangerous content over the 144 bytes range that the hardware packet filtering system can not cover, the system then routes packets, along with the pre-analysis results, to Protection Proxies run on a CPU (or NPU). The protection proxies use a hardware engine to analyze the header and contents and includes pre-analysis processing, thereby reducing the working load of CPU (or NPU) in the analysis or processing of individual packets.

Using hardware, the firewall of the present invention can be adapted to include 3 Gbs Ethernet link wire-speed and ~ 200 Mbs 3DES VPN and IPsec to fit all aspects of high security demands in the modern network infrastructures.

Exemplary functionality of various components of the hardware and software are described below:

1. Router core and configure ports.

This router core 316 provides the basic routing function to multiple logic ports in response to different packets. For example, as depicted in Figure 4, the system 402 can be connected to four different ports: one is an untrusted port which is connected to Internet router, one is a trusted port, one is a DMZ port, one is a CPU host port and one optional NPU port. Every port has its own IP level subnets (except the NPU port which may be configured in routing table manually). To make use of the high processing bandwidth of the present invention, the port structure may be adapted to provide two configure settings, for example, one Gbs port or multiple 10/100 Mbs ports. There are two kinds of ports adapted to handle untrusted traffic and trusted traffic. If these two flexible ports are configured as 10/100 Mbs, the ingress ports will be in aggregated by the router and processed as a single logical port. Likewise for egress condition, the ports will be logically aggregated as one port, where the choice of output port may be according to the addresses of the egress packets.

2. Flexible and Scalable Four Layer Firewall System. The firewall includes three layers of hardware oriented static/dynamic packet filtering engines, and one layer of customized virus or worms detection proxies. Every layer of this protection system has its own features and contributes different level security shields.

The first layer is Header Match packet filtering Engine (HME for short) which mainly handles the pattern match for header contribution and their combination from L2, L3, L4 headers. Since the header fields have some degree of granularity and expectation in header pattern, this layer of packet filtering is generally more straight-forward. Therefore, rules compilation and management in this layer can be implemented in a simple fashion, thereby reducing the efforts of the IT user. Without sacrificing the high bandwidth performance for this simplicity, this layer is adapted to handle traffic in a sustained Gbs (giga bits per second) bandwidth state.

The first layer (HME) may not be able to be effectively identify suspect virus or worms. Accordingly, the present invention includes a second layer in the firewall embedded with a Contents Match hardware packet filtering Engine (CME for short). This engine analyzes the scope of the 144 bytes.

The third layer in firewall system is different sets of application proxies run in the CPU (or NPU). For the intimate limitation of pure hardware packet filtering engines, it

can not cover the rare pattern detection need to locate the patterns over 144 bytes. Even this deep layer protection provided in CPU software proxies, the results of these first layer and second layer contents analyzing still can make much contribution when the packet needs to forward to CPU port and comes along with this "pre-analysis" results. This architect approach can tremendously off-load the processing demands from general CPU running different proxies in the case of deeper layer virus detection.

A Session Match Engine (SME) is provided as the fourth layer in firewall system. The SME includes an embedded Session Look Up Table which stores the TCP/UDP connections setup by the "stateful inspection" logic. The connection setup procedure in TCP/ UDP goes through 3 way handshaking, those TCP/ UDP handshaking control message packets will be caught by the system's SME, then forward to the general CPU for tracking the setup progress. After the procedure of setup connection is performed and recorded by CPU, this layer can program the connection socket address into Session Look Up Table for future packets received on this connection. The TCP/UDP packets flowing through this layer may only be hashed and searched in this Session LookUp Table to check if within the setup connections (sessions) to decide pass or drop to speed TCP/UDP connection checking.

All these four firmware blocks are integrated to provide high security while permitting the system to be flexible and fully scalable.

3. Protocol Aware VPN Engine

In this VPN engine, an array of micro-coded uPs are the foundation to provide the flexibility of different security protocols (in addition to Ipsec). The microprocessors include programmable instruction memory to permit updates of multi-protocol functions.

For this, high bandwidth performance is designed into the VPN engine. There are two independent pipelines for processing inbound and outbound VPN traffics. Every pipeline used array of micro-coded IPs to execute the tasks assigned. Every pipe has one independent programmable IP for executing specific tasks assigned in this pipe and task done within the work period to provide sustaining bandwidth. This VPN engine executes all kinds of VPN security functions include data integrity and data origin by different micro-code programming. Its primary authentication provided by the hardware

specialized HMAC-MD5-96, and HMAC-SHA- 1-96. The primary algorithm of data confidentiality will rely on the hardware core of DES/3 DES, AES, so the latency of processing can be positively predicable. For the flexibility concern, one pipe IP will provide one external system bus which can interface with external proprietary en(de)cryption chips without any public system bus overhead.

Also, the system may include an integrated smartcard reader, which can efficiently provide the storage of seeds for periodically generating shared keys or key pairs while establishing VPN channels phase.

The present invention features an Input Buffered Output Queued Architecture, which can eliminate the head of line blocking problem in the router services. Input Buffer Management Unit stores the received IP packets in a modern Linked List Structure, which allows for easy access, modification by the forwarding modules. The Output Queuing scheme also provides support for per port bandwidth management functions. These Bandwidth Management Functions are implemented as an integral part of the Output Queuing Function module.

The policy-based NA(P)T also gets the action from matched-policy to execute the relative NAT translation of the IP source address, as well as TCP/UDP ports translation and recovery.

The present invention also provides QoS (Quality of Service) supports. This quality of services ability will depend on the policies setup and matched in Policy Engine and the TOS field of packet header acting as DiffServ stamp and the VLAN tag priority changes the queuing priority for every egress packet. Through the policy classification process and DiffServ mapping, the packet will get different queuing strategies for its necessary bandwidth arranged to meet its traffic management requirement.

The system supports both redundant failover and load balancing by a ports mirroring scheme and parts of BGP/OSPF route protocol. A secure tunnel requires that certain states of information be maintained and synchronized in a periodic manner. Port Mirroring communicates the state information with the alternative gateway by using one of Ethernet ports and BGP/OSPF messages transit so the switching over time needed will be kept to a minimum.

The modular software stacks of the present invention permits the system to operate at high efficiency. In balancing security and optimum performance trade-off, the embedded software stacks provide several primitive proxies in its Lunix based kernel. The software can also include the "transparent proxying" or "hybrid proxying" features which automatically starts packet filtering by hardware and redirects the packets to an associated proxy. One advantage of this approach is that it is not visible from the user's perspective and they do not have to configure the system to communicate with the external services. Instead, the system intercepts the packets, and redirects to the system proxy stacks by the user who configured it. With this versatile structure, the system can have the more sophisticated security measures offered by proxy with the speed performance of the hardware packet filter. Exemplary proxies included in system proxy stacks are FTP proxy, Telnet proxy, and mail proxy (POP, POP3, etc.) providing high application-aware ability with virus-preventive protection.

In the configuration management aspects, the software has centralized management control, which can access all components of the distributed system. For example, the software may include a Command Line Interface to provide the scripting form accommodating multiple
Commands, Web-based Interface that may comprise an illustrative and intuitive GUI, a configuration file which can be created in a central controlled management station and upload to VPN gateway when needed, and an Application Programming Interface(API) to enable third-party vendors to develop management software for the network provisioning system.

Integrated features of the present invention include Hardware Firewall/VPN integrated ASIC chip, configuring 1 Gbs port for Enterprise level link or flexible 10/100 Mbs Ethernet ports, flexible external interface with proprietary en(de)crytion ASIC chip if applicable, PCI-66/33 MHz interface with general CPU, proprietary interface bus with NPU if applicable.

Exemplary performance features of the present invention include a Firewall throughput of sustained 2.1 Gbs Ethernet line speed and real-time header or content analysis, two layers of hardware packet-filtering engines adapted to use deterministic 12 clocks per packet (both Hardware packet filtering engines support dynamic packet

filtering scheme), TCP/UDP Connection filtering system operating at 800 Mbs, VPN throughput - 630 Mbs/3DES, 1 Gbs/DES.

Exemplary Firewall system features:

On-chip 1000 policies and scalable amount of policies supported with external SRAM array. Packet filtering analysis 14-4 bytes contents of packet starting from IP layer in line speed to provide no-overhead contents-aware security. All packet filtering engines support policies change dynamically according to received packets contents. Connection filtering engine provides stateful inspection of TCP/UDP handshake establishment to 25,000 connections, offered by the hardware searching in Session LookUp Table. MAC-address and ingress port ID engagement for detection topology changes. Policy based NAPT(network address/port translation) to support many to one IP address for extranet VPN application and internal address hidden. Transparent switch mode in disengaged NAT. Traffic flow and rate shaping controlled by individual policy granularity. Fine granularity and flexible policy setup prevent unlawful attacks with ICMP coven channel. High speed Denial of Service protection -defend against attacks with TCP-SYNFLOOD, Ping of Death, TearDrop, etc.

Exemplary VPN features:

Full support IPsec security services for IPv4 traffics. Support L2TP within IPsec. Support around 1000 on chip tunnels delivering high speed and diverse business-class capabilities for cross-abroad managed security. Authentication services with HMAC-MD5-96, and HMAC-SHA- 1-96 in 800 Mbs. Data confidentiality with DES/3DES, and external interface bus with proprietary en(de)cryption ASIC chip. Can accommodate VLANs implemented by 801.1 Q for increased security measures.

Exemplary QoS traffic management features:

Traffic shape control, Guaranteed bandwidth, and Voice over IP. Priority bandwidth

DiffServ Stamp.

Other Exemplary features of the system:

Stateful backup failover capability for mission-critical applications. Configure Gbs port or 10/100 Mbs ports, which can offer the enterprise-class bandwidth link. The multi-l0/100 Mbs ports can be adapted to provide link aggregation and automatic

failover for defective physical links. .15 urn advanced CMOS technology.

Of course, other features and advantages will be apparent to those skilled in the art. The forgoing system overview represents some exemplary implementations, but other implementations will be apparent to those skilled in the art, and all such alternatives are deemed equivalent and within the spirit and scope of the present invention, only as limited by the claims.

Claims:

1. An integrated firewall/VPN system, comprising:

at least one wide area network (WAN);

at least one local area network (LAN); and

an integrated firewall/VPN chipset adapted to send and receive data packets between said WAN and said LAN, said chipset comprising a firewall portion and to provide access control between said WAN and said LAN and a VPN portion adapted to provide security functions for data between said LAN and said WAN; said firewall including firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control; said VPN potion including VPN hardware and software portions wherein at least VPN hardware portion is adapted to provide iterative functions associated with said security functions.

2. A system as claimed in claim 1, wherein said chipset further comprises a router adapted to route data between said LAN and said LAN.

3. A system as claimed in claim 1, wherein said firewall hardware portion comprising circuitry to provide static and/or dynamic data packet filtering.

4. A system as claimed in claim 3, wherein said circuitry includes a header match packet filtering circuit to provide pattern matching in selected headers of said data.

5. A system as claimed in claim 1, wherein said chipset further adapted to analyze access control functions based on preselected bytes of said data packets.

6. A system as claimed in claim 5, wherein said preselected bytes comprise the first 144 bytes of said data packet.

7. A system as claimed in claim 1, wherein said VPN security functions comprise, encryption, decryption, encapsulation, and decapsulation of said data packets.

8. A system as claimed in claim 1, wherein said firewall access control functions comprise user-defined access control protocols.

9. A firewall/VPN integrated circuit (IC), comprising:

a router core adapted to interface between at least one untrusted network and at least one trusted network to send and receive data packets between said untrusted and said trusted networks;

a firewall system adapted to provide access control between said untrusted and said trusted networks, and comprising firewall hardware and software portions wherein at least said firewall hardware portion is adapted to provide iterative functions associated with said access control; and

a VPN engine adapted to provide security functions for data between said untrusted and said trusted networks, and comprising VPN hardware and software wherein at least said VPN hardware portion is adapted to provide iterative functions associated with said security functions.

10. An IC system as claimed in claim 9, wherein said firewall hardware portion comprising circuitry to provide static and/or dynamic data packet filtering.

11. An IC as claimed in claim 10, wherein said circuitry includes a header match packet filtering circuit to provide pattern matching in selected headers of said data.

12. An IC as claimed in claim 9, wherein said firewall system further adapted to analyze access control functions based on preselected bytes of said data packets.

13. An IC as claimed in claim 12, wherein said preselected bytes comprise the first 144 bytes of said data packet.

14. A system as claimed in claim 9, wherein said VPN security functions comprise, encryption, decryption, encapsulation, and decapsulation of said data packets.

15. A system as claimed in claim 9, wherein said firewall access control functions comprise user-defined access control protocols.

16. A method of providing firewall access control functions, comprising the steps of:

defining one or more access control protocols;

receiving a data packet;

selecting a certain number of bytes of said data packet;

processing said selected bytes using said access control protocols.

17. A method as claimed in claim 16, further comprising the steps of:

providing hardware implementation of static and/or dynamic packet data filtering using said access control protocols.

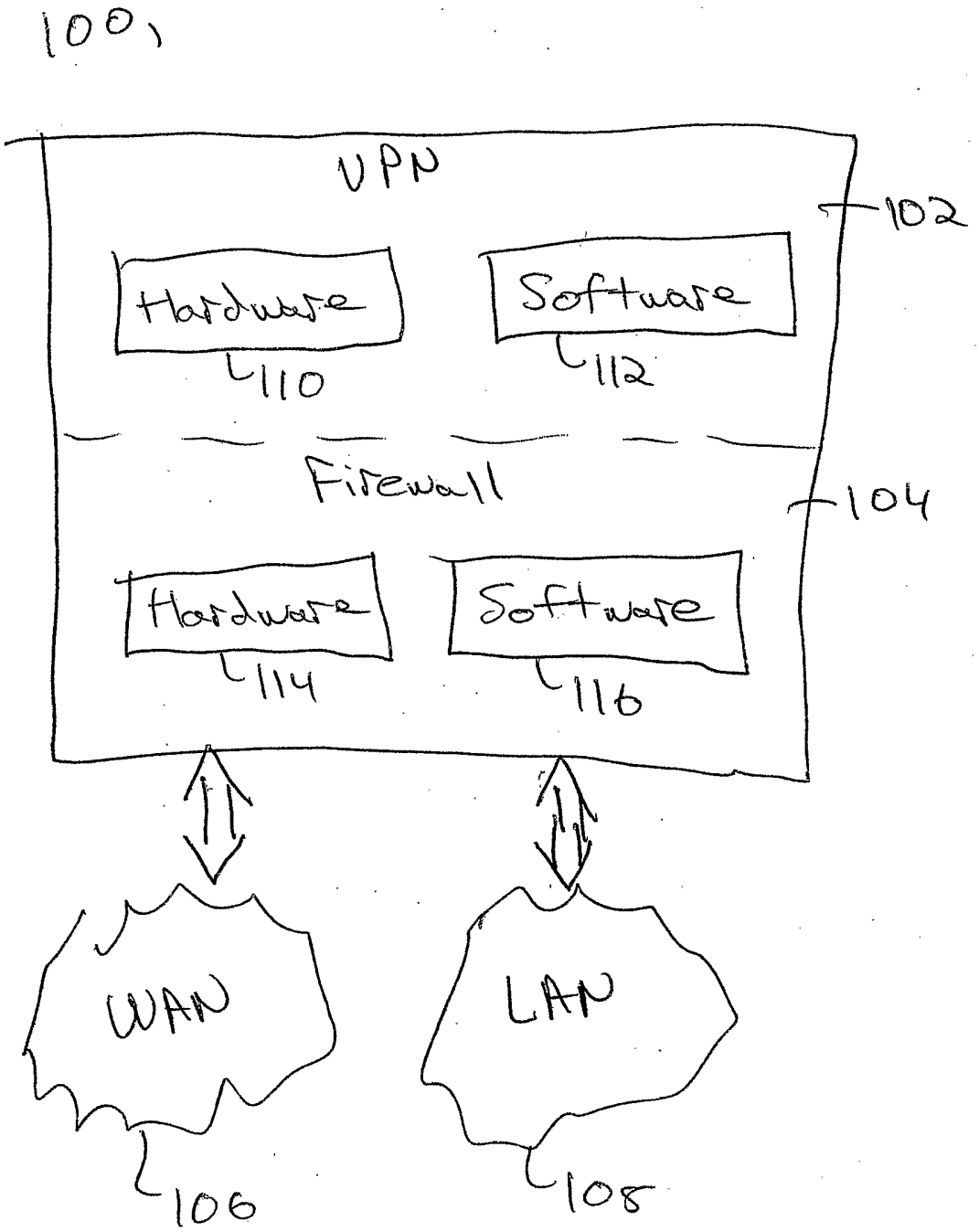

100
VPN
102
Hardware
110
Software
112
Firewall
104
Hardware
114
Software
116
WAN
106
LAN
108

Figure 1

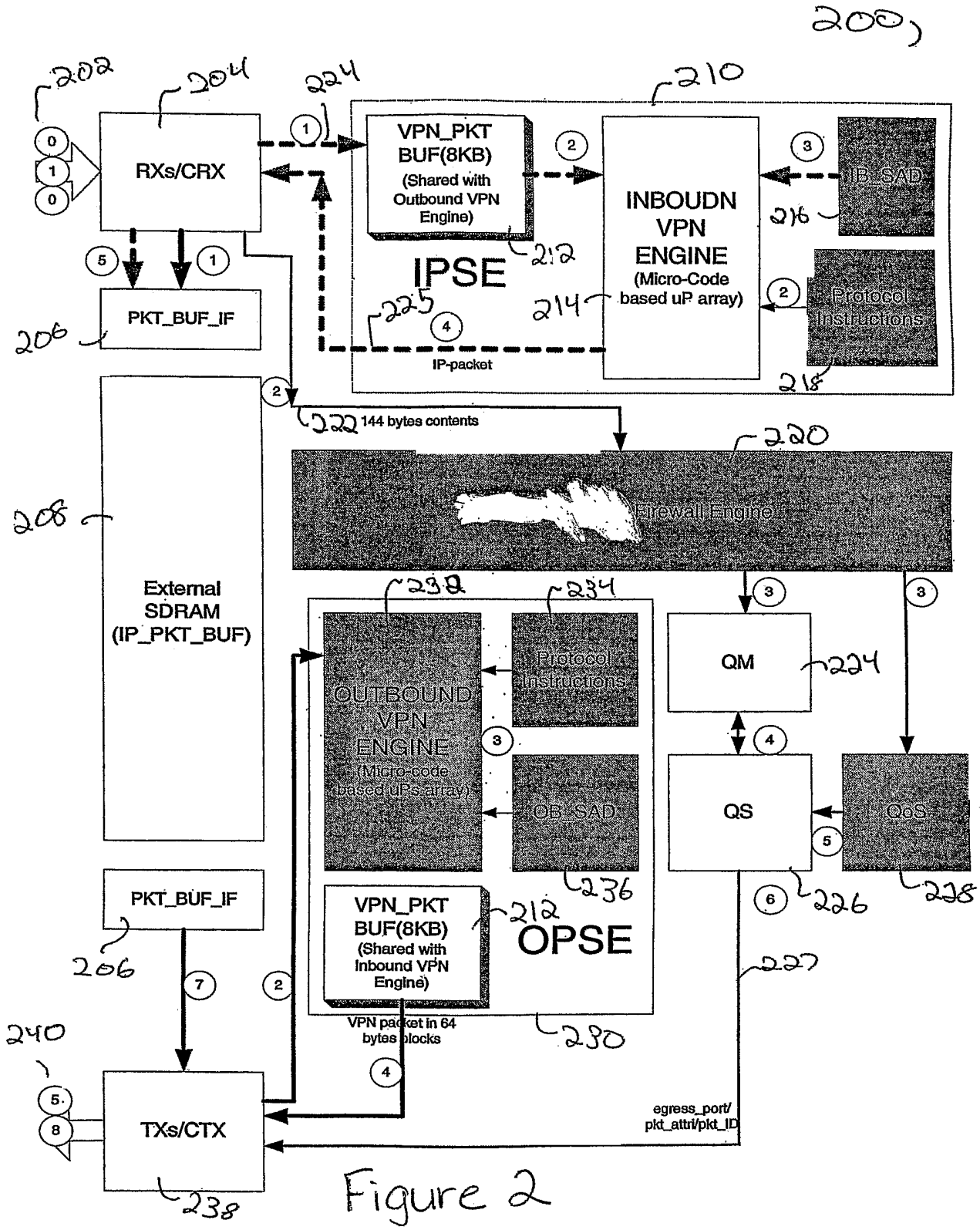

200
202
204
224
210
RXs/CRX
VPN_PKT BUF(8KB) (Shared with Outbound VPN Engine)
IPSE
212
INBOUDN VPN ENGINE (Micro-Code based uP array)
214
IB_SAD
216
Protocol Instructions
218
PKT_BUF_IF
206
225
IP-packet
222 144 bytes contents
220
Firewall Engine
208
External SDRAM (IP_PKT_BUF)
232
234
OUTBOUND VPN ENGINE (Micro-code based uPs array)
Protocol Instructions
OB_SAD
236
QM
224
QS
QoS
226
228
VPN_PKT BUF(8KB) (Shared with Inbound VPN Engine)
OPSE
230
227
VPN packet in 64 bytes blocks
egress_port/ pkt_attri/pkt_ID
240
TXs/CTX
238

Figure 2

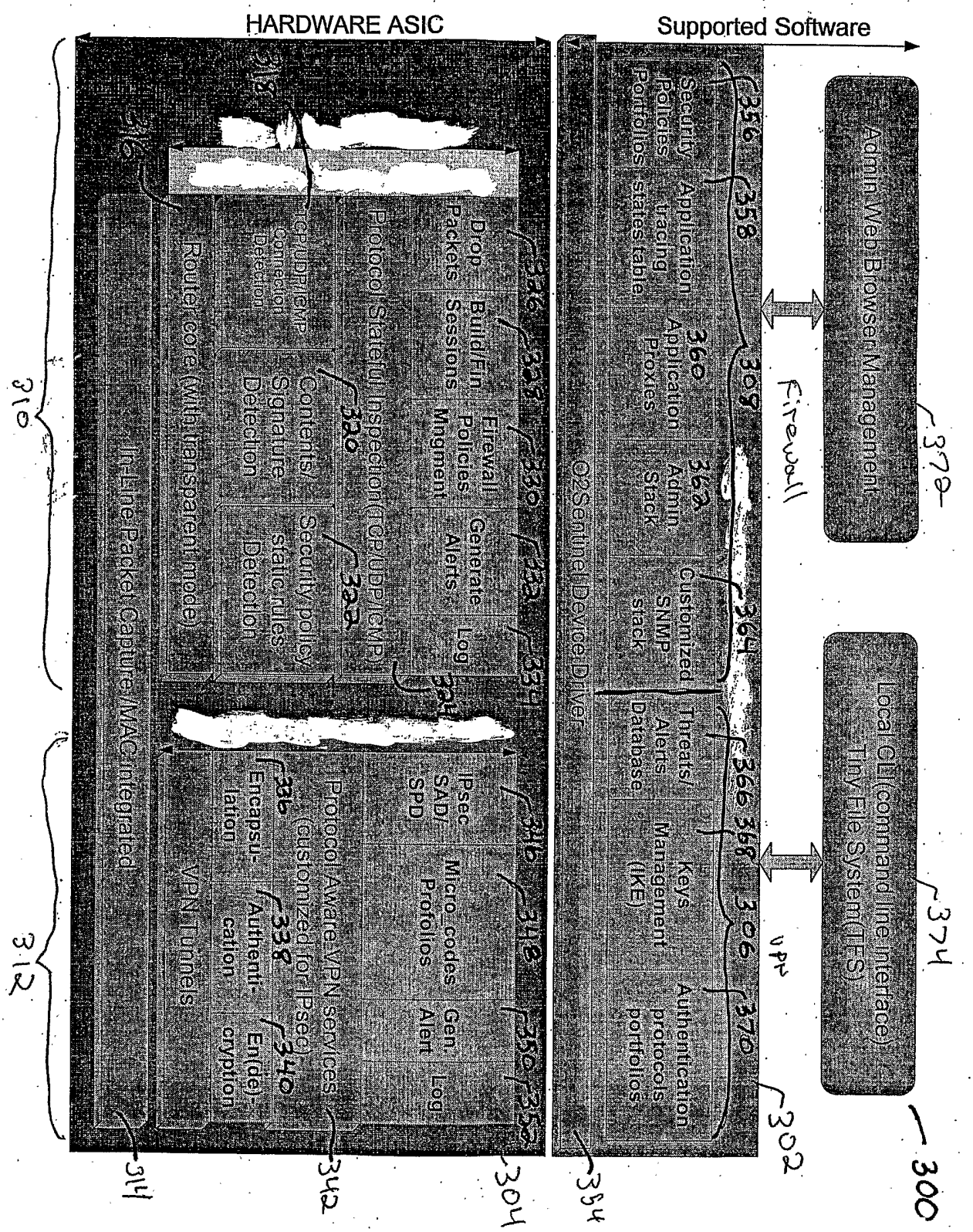

HARDWARE ASIC
Supported Software
Admin Web Browser Management
Local CLI (command line interface) Tiny File System (TFS)
Firewall
VPN
Security Policies Portfolios
Application tracing
Application Proxies
Admin Stack
Customized SNMP Stack
Threats/ Alerts Database
Keys Management (IKE)
Authentication protocols portfolios
O2Sentinel Device Driver
Drop Packets
Build/Fin Sessions
Firewall Policies
Generate Alerts
Log Mngment
TCP/UDP/ICMP Connection Detection
Router core (with transparent mode)
Protocol Stateful Inspection (TCP/UDP/ICMP)
Contents/ Signature Detection
Security policy static rules Detection
In-Line Packet Capture/MAC integrated
IPsec SAD/ SPD
Micro codes Protocols
Gen. Alert
Log
Protocol Aware VPN services (customized for IPsec)
Encapsu-lation
Authenti-cation
En(de)-cryption
VPN Tunnels
310
312
314
316
318
302
304
306
308
342
356
358
360
362
364
366
368
370
372
374
380
382
384

Figure 3

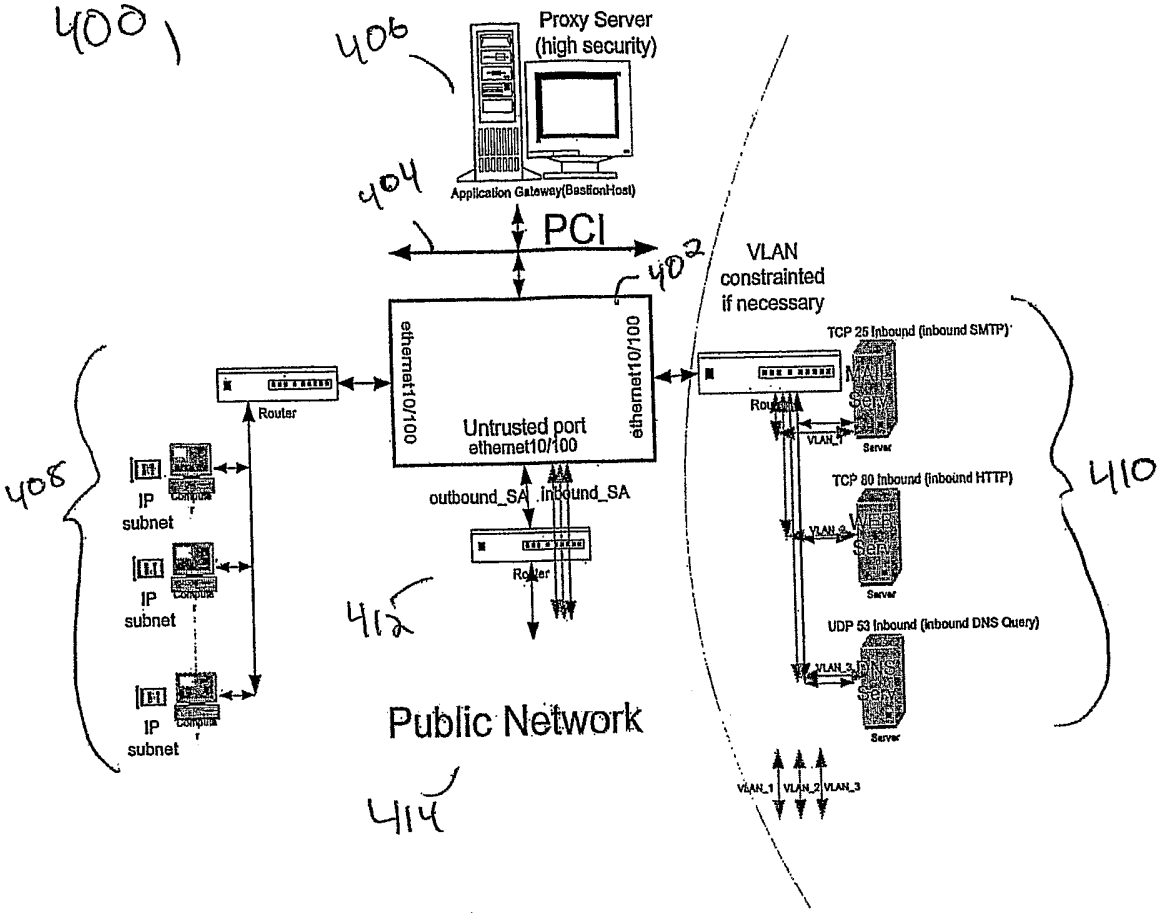

400
406
Proxy Server
(high security)
404
Application Gateway(BastionHost)
PCI
402
VLAN
constrainted
if necessary
ethernet10/100
ethernet10/100
Untrusted port
ethernet10/100
Router
Router
outbound_SA
inbound_SA
408
IP
subnet
IP
subnet
IP
subnet
412
Public Network
414
TCP 25 Inbound (inbound SMTP)
TCP 80 Inbound (inbound HTTP)
UDP 53 Inbound (inbound DNS Query)
Server
Server
Server
VLAN_1
VLAN_2
VLAN_3
410

Figure 4

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/28065

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 11/30, 12/14; H04L 9/00, 9/32
US CL : 713/201

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)
U.S. : 713/201

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y,P	US 6,550,012 B1 (VILLA et al.) 15 April 2003 (15.04.2003) Figures 3a, 3b, 3c; column 3, lines 21-31; column 9, line 40 to column 11 line 58.	1-17
Y,P	US 6,453,419 B1 (FLINT et al.) 17 September 2002 (17.09.2002) Figures 1a, 1b, 2, 3; column 3, lines 15-31.	1-17
A	US 6,154,839 (ARROW et al.) 28 November 2000 (28.11.2000). column 2, line 62 to column 3, line 23.	1-17
A	US 6,304,973 B1 (WILLIAMS) 16 October 2001 (16.10.2001). column 4, line 23 to column 5, line 67.	1-17
A	US 6,182,226 B1 (REID et al.) 30 January 2001 (30.01.2001). column 1, line 58 to column 2, line 27.	1-17
A	US 5,870,744 (SPRAGUE) 09 February 1999 (09.02.1999), column 1, lines 37-48.	1-17
A	US 6,226,748 B1 (BOTS et al.) 01 May 2001 (01.05.2001), column 2, line 37 to column 3, line 22.	1-17
A,P	US 6,609,148 B1 (SALO et al.) 19 August 2003 (19.08.2003), column 3, line 57 to column 4, line 33.	1-17
A,T	US 6,625150 B1 (YU) 23 September 2003 (23.09.2003), column 1, line 27 to column 2, line 28; column 2, line 46 to column 3, line 46.	1-17

☒ 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 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 another 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	Date of mailing of the international search report
24 November 2003 (24.11.2003)	11 DEC 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Ayaz Sheikh Telephone No. (703)305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/28065

Continuation of B. FIELDS SEARCHED Item 3:
EAST, IEEE, ACM
search terms: VPN, firewall, router