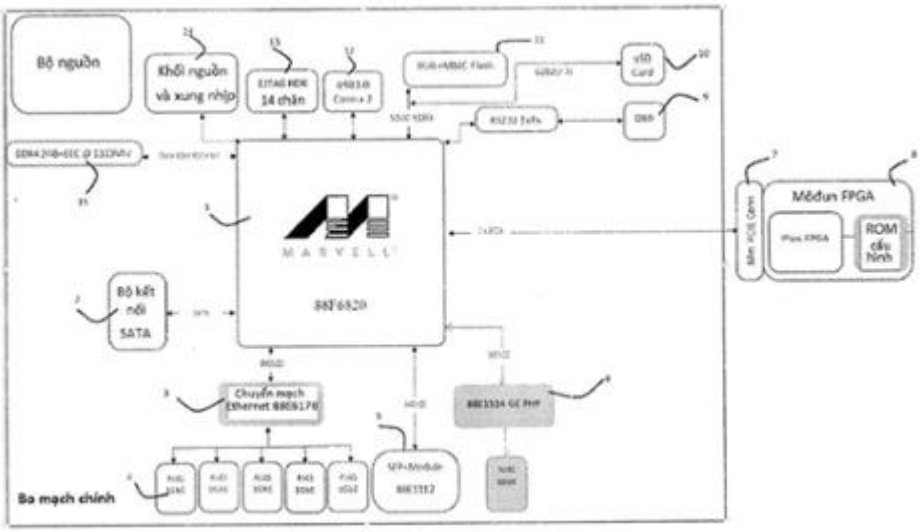
(12) BẢN MÔ TẢ SÁNG CHẾ THUỘC BẰNG ĐỘC QUYỀN SÁNG CHẾ
(19) **Cộng hòa xã hội chủ nghĩa Việt Nam (VN)**
CỤC SỞ HỮU TRÍ TUỆ
(11) **1-0037864**
(51)[2020.01] **H04L 12/00**
(13) **B**

(21) 1-2020-04923
(22) 26/08/2020
(45) 25/12/2023 429
(43) 25/11/2020 392A
(73) TRƯỜNG ĐẠI HỌC BÁCH KHOA - ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH (VN)
268 Lý Thường Kiệt, phường 14, quận 10, thành phố Hồ Chí Minh
(72) Hoàng Trang (VN); Bùi Quốc Bảo (VN); Trần Hoàng Linh (VN).

(54) THIẾT BỊ ĐỊNH TUYẾN TĂNG TỐC BẢO MẬT DÙNG PHẦN CỨNG MẢNG PHẦN TỬ LOGIC NGƯỜI DÙNG CÓ THỂ LẬP TRÌNH ĐƯỢC (FPGA)

(57) Sáng chế đề cập đến thiết bị định tuyến tăng tốc bảo mật dùng phần cứng dùng mảng phần tử logic người dùng có thể lập trình được (FPGA), thiết bị theo sáng chế có khả năng cung cấp kết nối bảo mật trên nền tảng mạng riêng ảo (VPN) với tốc độ cao. Thiết bị định tuyến tăng tốc bảo mật này cung cấp nhiều cổng giao tiếp LAN (Local Network Area - Mạng cục bộ), một cổng giao tiếp WAN (Wide Area Network - Mạng diện rộng) và một cổng giao tiếp quang, tất cả đều hỗ trợ tốc độ Gigabit. Bo mạch chính của thiết bị gồm vi xử lý Marvell 88F6820 đảm nhiệm các tác vụ chính; chip chuyển mạch 88E6176 cho phép mở rộng 05 cổng LAN. Các thiết bị ngoại vi khác gồm một cổng nối tiếp và EJTAG để gỡ rối chương trình; hai cổng USB để kết nối thiết bị ngoại vi. Bộ nhớ lưu trữ chính là eMMC có dung lượng 8 Gbit. Ngoài ra, bo mạch chính có giao tiếp SATA (Serial Advanced Technology Attachment) để kết nối ổ đĩa cứng; giao tiếp SDIO (Secure Digital Input Output) để kết nối với SD CARD (Secure Digital Card). Để tăng tốc cho thiết bị, toàn bộ quá trình tính toán bảo mật theo chuẩn IPsec được đưa vào một môđun FPGA, kết nối với bo mạch chính qua giao tiếp mini PCIe.



Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập đến thiết kế của một thiết bị định tuyến tăng tốc bảo mật có khả năng cung cấp kết nối bảo mật trên nền tảng mạng riêng ảo (VPN) với tốc độ cao. Để tăng tốc cho quá trình tính toán bảo mật và cung cấp khả năng cập nhật, cấu hình lại, toàn bộ quá trình tính toán bảo mật theo chuẩn IPsec được đưa vào phần cứng FPGA (Mảng phần tử logic người dùng có thể lập trình được). CPU chuyên dụng sẽ đảm nhận các tác vụ mạng như định tuyến, phân tách mạng. Để đảm bảo tốc độ xử lý, dữ liệu được trao đổi giữa chip vi xử lý và FPGA thông qua giao tiếp tốc độ cao mini PCIe.

Tình trạng kỹ thuật của sáng chế

Cùng với sự phát triển của internet, kỹ thuật Internet kết nối vạn vật (IoT), hiện nay vấn đề bảo mật kết nối là vấn đề cực kỳ quan trọng.

Đối với các công ty lớn, các giải pháp chuyên nghiệp được sử dụng như tường lửa, thiết bị phát hiện xâm nhập, thiết bị tạo mạng riêng ảo chuyên dụng. Các thiết bị này cung cấp khả năng bảo mật cao, ổn định. Tuy nhiên, giá thành các thiết bị này rất cao và đòi hỏi đội ngũ kỹ sư vận hành, bảo trì có tay nghề cao, do đó chi phí cho việc lắp đặt, vận hành các hệ thống này là rất cao.

Đối với người dùng cá nhân, cũng như các công ty cỡ nhỏ, việc bảo mật đường truyền ít được chú trọng. Đối với các máy tính cá nhân, việc bảo vệ thường được giới hạn bởi các phần mềm chống virus. Các phần mềm này chỉ hiệu quả để phòng chống các mã độc xâm nhập vào máy tính, nhưng không có tác dụng bảo vệ đối với các phương thức tấn công, nghe lén trên đường truyền vì dữ liệu gửi đi không được mã hóa. Ngoài ra, các phần mềm này chỉ có tác dụng với từng máy riêng lẻ được cài đặt, không thể cung cấp khả năng bảo vệ với các thiết bị kết nối Internet khác trong mạng.

Để cung cấp khả năng bảo mật cho toàn bộ các thiết bị trong mạng, phương pháp hiệu quả nhất là thiết lập một kết nối mạng riêng ảo (VPN) như được minh họa trên Hình 1. Với thiết lập mô hình mạng như vậy, tất cả các luồng dữ liệu trong mạng đều được mã hóa trước khi đi ra internet, tránh được nguy cơ người tấn công nghe lén, bắt gói dữ liệu trên đường truyền.

Tuy nhiên hiện nay, đối với đa số người dùng cá nhân và các công ty nhỏ, thiết bị định tuyến được sử dụng thường là các thiết bị thông dụng do nhà cung cấp mạng lắp đặt kèm khi cung cấp dịch vụ mạng, hoặc là các thiết bị thông dụng có trên thị trường như các thiết bị định tuyến của D-Link, TP-Link. Các thiết bị này sử dụng các bộ vi xử lý có tốc độ tính toán thấp, cấu hình phần cứng yếu. Khi lưu lượng dữ liệu lớn, thiết bị không có đủ sức mạnh để mã hóa cũng như giải mã luồng dữ liệu đủ nhanh, từ đó làm giảm băng thông đường truyền xuống quá thấp. Vì vậy, các thiết bị trong mạng không thể kết nối Internet một cách hiệu quả. Vì lý do đó, các thiết bị định tuyến thông thường không thể sử dụng để thiết lập kết nối VPN mà không làm ảnh hưởng đến hoạt động của các thiết bị mạng.

Đã có rất nhiều sáng chế cũng như các bài báo khoa học liên quan xử lý vấn đề nêu trên bằng cách sử dụng các phần cứng có khả năng tính toán mã hóa/giải mã độc lập với CPU. Một trong những giải pháp liên quan gần nhất được thể hiện trong bài báo "An FPGA-based reconfigurable IPSec AH core with efficient implementation of SHA-3 for high speed IoT applications", trong đó tác giả đề xuất một thiết kế dùng FPGA để tạo một lõi xác thực IPsec tốc độ cao. Thiết kế này cung cấp khả năng xác thực nguồn gốc dữ liệu (data origin authentication), kiểm tra tính toàn vẹn dữ liệu (data integrity), và dịch vụ chống phát lại (anti-replay service). Hai thiết bị IPsec được kết nối với nhau, và xác thực các luồng dữ liệu đi vào trước khi cho phép các dữ liệu này đi vào mạng nội bộ phía sau qua bộ định tuyến. Trong mô hình này cũng như các mô hình tương tự, các thiết bị IPsec là các thiết bị hoàn toàn độc lập với bộ định tuyến, hoạt động trước bộ định tuyến. Chúng được dùng chuyên biệt để kết nối hai mạng nội bộ với nhau qua đường truyền mạng riêng ảo.

Với mô hình mạng trên, hai mạng nội bộ nói trên chỉ có thể kết nối với nhau, không thể kết nối với các mạng khác. Các thiết bị trong mạng nội bộ muốn truy cập các dịch vụ mạng khác phải thông qua một giao tiếp mạng khác. Vì vậy, thiết kế nói

trên chỉ phù hợp để chế tạo thiết bị tạo mạng VPN chuyên biệt, sử dụng trong hệ thống mạng của các công ty lớn có nhiều mạng con đặt ở các địa điểm khác nhau. Để có thể chế tạo với giá thành thấp và thuận tiện cho sử dụng rộng rãi, thiết bị này phải được chế tạo để tích hợp cả chức năng kết nối mạng riêng ảo và khả năng định tuyến.

Tài liệu sáng chế CN2565211Y đề xuất một mô hình, trong đó một bo mạch (board) có các chip chuyên xử lý mã hóa/giải mã được lắp đặt trên khe mở rộng của một bo mạch chủ. Bo mạch mã hóa/giải mã sẽ đảm nhận xử lý các giải thuật tính toán để xử lý các gói tin IPsec. Luồng dữ liệu được xử lý trên CPU, khi nào cần tính toán thì CPU sẽ ghi dữ liệu xuống chip mã hóa/giải mã và chờ lấy kết quả lên. Nhờ đó, tốc độ xử lý gói tin được tăng lên đáng kể.

Tuy nhiên, hướng tiếp cận theo mô hình này có nhược điểm là dữ liệu truyền giữa CPU và bo mạch mở rộng chỉ để tính toán mã hóa/giải mã, các thao tác khác như xác thực, đóng gói đều phải làm trên CPU, vì vậy không tối ưu được hiệu năng của hệ thống.

Bản chất kỹ thuật của sáng chế

Mục đích của sáng chế là khắc phục nhược điểm của các giải pháp nêu trên, và giải quyết các vấn đề kỹ thuật còn tồn tại.

Để đạt được mục đích nêu trên, sáng chế sử dụng phần cứng FPGA mà có khả năng thiết lập các phần cứng tính toán nhanh, cũng như có khả năng tạo cấu hình lại để tính toán xử lý toàn bộ các gói tin theo chuẩn IPsec. Môđun FPGA không chỉ hỗ trợ tăng tốc các phép toán mã hóa/giải mã, mà còn xử lý toàn bộ gói tin, bao gồm cả các phần xử lý khung truyền. Điều này sẽ làm giảm thời gian vi xử lý phải sao chép dữ liệu vào/ra môđun phần cứng, do đó làm tốc độ xử lý được tăng lên đáng kể. Vi xử lý sẽ làm nhiệm vụ tạo cấu hình, lưu giữ các bản định tuyến và các dịch vụ khác không đòi hỏi tốc độ cao.

Môđun FPGA và vi xử lý giao tiếp qua chuẩn truyền PCIe, cung cấp tốc độ truyền dữ liệu lên đến 2,5 Gbps. Tốc độ này là đủ để không làm ảnh hưởng băng thông cho các thiết bị định tuyến thông thường, vì đường truyền Ethernet tốc độ cao nhất chỉ là 1Gbps.

Theo một phương án ưu tiên của sáng chế, thiết bị định tuyến tăng tốc bảo mật dùng phần cứng mảng phần tử logic người dùng có thể lập trình được (FPGA) gồm hai phần chính:

bo mạch chính, có nhiệm vụ xử lý các tác vụ định tuyến, chuyển tiếp các gói trong mạng nội bộ và xử lý các gói tin theo các lớp trong mô hình TCP/IP (Transmission Control Protocol/ Internet Protocol - Giao thức điều khiển truyền nhận/ Giao thức internet), bo mạch chính gồm vi xử lý, ưu tiên là bộ vi xử lý Marvell 88F6820 để đảm nhiệm các tác vụ chính; chip chuyển mạch 88E6176 cho phép mở rộng nhiều cổng LAN (Local Network Area - Mạng cục bộ); một cổng WAN (Wide Area Network - Mạng diện rộng) và một cổng giao tiếp quang; các thiết vị ngoại vi khác gồm một cổng nối tiếp và EJTAG để gỡ rối chương trình; các cổng USB để kết nối thiết bị ngoại vi; bộ nhớ lưu trữ chính là eMMC có dung lượng 8 Gbit; ngoài ra, bo mạch chính có giao tiếp SATA để kết nối ổ đĩa cứng; giao tiếp SDIO để kết nối với SD CARD;

môđun FPGA được thiết kế theo chuẩn giao tiếp mini PCIe, gồm có 1 chip, ưu tiên là chip Xilinx Artix 7 FPGA và một bộ nhớ ROM MT25QL01GBBB8E12, khác biệt ở chỗ, môđun này kết nối với bo mạch chính qua giao tiếp mini PCIe.

Mô tả vắn tắt các hình vẽ

Hình 1 minh họa mô hình mạng thiết lập mạng riêng ảo sử dụng thiết bị định tuyến theo sáng chế.

Hình 2 minh họa chi tiết sơ đồ khối thiết kế của thiết bị định tuyến theo sáng chế.

Hình 3 minh họa quá trình hệ thống sử dụng FPGA để tăng tốc luồng dữ liệu qua kết nối bảo mật VPN sử dụng IPsec.

Mô tả chi tiết sáng chế

Sau đây, sáng chế sẽ được mô tả chi tiết dựa vào các hình vẽ kèm theo. Trong đó, các số chỉ dẫn giống nhau sẽ được dùng để tham chiếu đến các chi tiết giống nhau hoặc tương đương.

Hình 2 minh họa sơ đồ khối thiết kế của thiết bị định tuyến theo sáng chế. Thiết bị định tuyến được thiết kế gồm hai phần chính là bo mạch chính (main board) và một môđun FPGA, giao tiếp qua chuẩn mini PCIe.

Theo một phương án ưu tiên của sáng chế, thiết bị định tuyến tăng tốc bảo mật dùng phần cứng mảng phần tử logic người dùng có thể lập trình được (FPGA) theo sáng chế bao gồm các thành phần sau. Bo mạch chính có vi xử lý trung tâm của thiết bị là vi xử lý 1, tốt hơn nếu là vi xử lý 88F6820 của hãng Marvell. Vi xử lý 1 kết nối với IC bộ nhớ DRAM (Dynamic Random Access Memory - Bộ nhớ truy nhập ngẫu nhiên động) 15 có dung lượng 2Gbyte. Bo mạch chính sử dụng bộ kết nối SATA 2 để kết nối với ổ đĩa cứng, cho phép mở rộng khả năng lưu trữ. Chip chuyển mạch 3 kết nối vào giao tiếp RGMII của vi xử lý 1, cho phép mở rộng ra 5 cổng LAN 4 với tốc độ Gigabit. Môđun giao tiếp quang 5 được kết nối vào vi xử lý 1 qua giao tiếp SGMII. IC điều khiển vật lý PHY 6 giao tiếp với vi xử lý 1 thông qua giao diện RMII, cung cấp đường truyền WAN cho thiết bị định tuyến. Cổng nối tiếp 9 kết nối vào vi xử lý 1 qua giao tiếp UART. SD CARD 10 và bộ nhớ eMMC 11 có dung lượng 8Gbit cho phép lưu trữ phần mềm hệ thống. Hai cổng USB 12 cho phép kết nối các thiết bị ngoại vi vào thiết bị. Bộ kết nối EJTAG 13 cho phép lập trình và gỡ rối thiết bị. Khối nguồn và xung nhịp 14 cung cấp các nguồn điện và xung nhịp cho CPU.

Môđun FPGA 8 được thiết kế theo chuẩn giao tiếp mini PCIe, ưu tiên là môđun này gồm có 1 chip Xilinx Artix 7 FPGA và một bộ nhớ ROM MT25QL01GBBB8E12 chứa cấu hình của thiết kế. Môđun này kết nối với vi xử lý qua cổng giao tiếp PCIe 7.

Quá trình tăng tốc tính toán của thiết bị định tuyến tăng tốc bảo mật sử dụng phần cứng FPGA:

Bo mạch chính sẽ làm nhiệm vụ xử lý các tác vụ định tuyến, chuyển tiếp các gói trong mạng nội bộ và xử lý các gói tin theo các lớp trong mô hình TCP/IP. Phần tính toán xử lý IPsec, vốn đòi hỏi nhiều tài nguyên và khả năng tính toán của vi xử lý sẽ được đưa xuống FPGA.

Hình 3 minh họa chi tiết quá trình hệ thống sử dụng FPGA để tăng tốc luồng dữ liệu qua kết nối bảo mật VPN sử dụng IPsec. Ở lớp ứng dụng 20 trong mô hình

TCP/IP, ứng dụng StrongSwan 16 làm nhiệm vụ khởi tạo kết nối VPN. Các gói tin đi qua các lớp TCP/UDP 21 và lớp IP 22, được đóng gói thành gói tin TCP/IP 26. Tuy nhiên, các thông tin trong các gói tin như địa chỉ IP, dữ liệu được đóng gói đều không được mã hóa, vì vậy sẽ có nguy cơ rất cao là các gói tin này bị ngăn chặn, nghe lén hoặc thay đổi nội dung trên đường truyền.

Vì vậy, các gói tin này sẽ được mã hóa và đóng gói lại ở lớp IPsec. Ở các bộ định tuyến thông thường, quá trình này sẽ được thực thi hoàn toàn bằng vi xử lý, do đó tiêu tốn phần lớn sức mạnh tính toán của vi xử lý. Ở các bộ định tuyến có bộ tăng tốc mã hóa phần cứng theo sáng chế, các phép tính mã hóa, giải mã sẽ được xử lý trên bộ tăng tốc, tuy nhiên quá trình tính toán IPsec cần nhiều phép tính mã hóa cho một gói tin, do đo vi xử lý cần phải di chuyển dữ liệu vào và ra khỏi bộ nhớ của bộ tăng tốc nhiều lần, làm tăng thời gian xử lý và làm giảm hiệu năng của thiết bị.

Bộ định tuyến theo sáng chế sẽ thực thi toàn bộ quá trình xử lý IPsec trên FPGA 23, toàn bộ quá trình mã hóa và giải mã dữ liệu và thông tin trong khung truyền sẽ được xử lý toàn bộ trong FPGA, sau khi có được gói tin đã mã hóa 27 thì truyền về xi xử lý để đưa xuống các lớp liên kết 24 và vật lý 25 để truyền đi.

Vì phần cứng FPGA nằm độc lập với CPU nên phần cứng này cần có một giao tiếp để truyền nhận dữ liệu. Giao tiếp này phải có tốc độ cao hơn Gbit để không làm giảm tốc độ xử lý của hệ thống. Trên các CPU thông dụng để thiết kế thiết bị định tuyến, chỉ có giao tiếp theo chuẩn mini PCIe là đạt tốc độ yêu cầu. Các giao tiếp USB 2.0 chỉ đạt tốc độ tối đa 480 Mbit/s. Giải pháp theo sáng chế đã lựa chọn giao tiếp mini PCIe để truyền thông giữa CPU và FPGA để thích hợp nhất với nhiệm vụ này.

Ngoài giao tiếp mini PCIe, USB 3.0 cũng có thể đạt tốc độ yêu cầu, tuy nhiên giao tiếp USB 3.0 không thông dụng trên các CPU chuyên dùng. Để sử dụng được giao tiếp USB 3.0 ta cần có các lõi IP trên FPGA, tuy nhiên các lõi này không được nhà sản xuất hỗ trợ mà phải bỏ chi phí bản quyền với giá rất cao. Vì các lý do trên, sáng chế lựa chọn giao tiếp mini PCIe để truyền thông giữa CPU và FPGA.

Hiệu quả đạt được của sáng chế

Sáng chế nhắm đến các thiết bị định tuyến có người dùng phổ thông hoặc các công ty có qui mô nhỏ. Với các đối tượng này, đường truyền nhanh nhất có tốc độ lên đến 1 Gbit/s, vì vậy thiết kế hệ thống được tối ưu với tốc độ này.

Sáng chế sử dụng một lõi IP làm toàn bộ các công việc trong lớp IPsec. Toàn bộ gói dữ liệu sẽ được đưa xuống FPGA. FPGA xử lý toàn bộ lớp IPsec và truyền gói tin lên lớp trên trong mô hình mạng, giải phóng hoàn toàn CPU khỏi việc xử lý IPsec.

YÊU CẦU BẢO HỘ

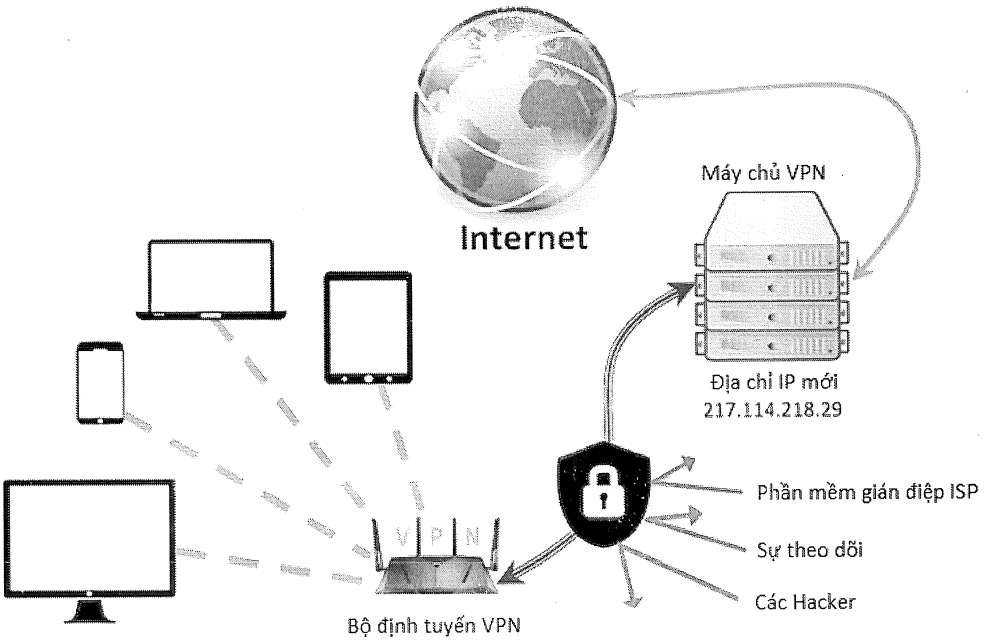
1. Thiết bị định tuyến tăng tốc bảo mật dùng phần cứng mảng phần tử logic người dùng có thể lập trình được (FPGA), thiết bị này gồm hai phần chính:

bo mạch chính, có nhiệm vụ xử lý các tác vụ định tuyến, chuyển tiếp các gói trong mạng nội bộ và xử lý các gói tin theo các lớp trong mô hình TCP/IP (Transmission Control Protocol/ Internet Protocol - Giao thức điều khiển truyền nhận/ Giao thức internet), bo mạch chính gồm vi xử lý, ưu tiên là bộ vi xử lý Marvell 88F6820 để đảm nhiệm các tác vụ chính; chip chuyển mạch, ưu tiên là chip 88E6176 cho phép mở rộng nhiều cổng LAN (Local Network Area - Mạng cục bộ); một cổng WAN (Wide Area Network - Mạng diện rộng) và một cổng giao tiếp quang; các thiết vị ngoại vi khác gồm một cổng nối tiếp và EJTAG để gỡ rối chương trình; các cổng USB để kết nối thiết bị ngoại vi; bộ nhớ lưu trữ chính là eMMC có dung lượng 8 Gbit; ngoài ra, bo mạch chính có giao tiếp SATA (Serial Advanced Technology Attachment) để kết nối ổ đĩa cứng; giao tiếp SDIO (Secure Digital Input Output) để kết nối với SD CARD (Secure Digital Card);

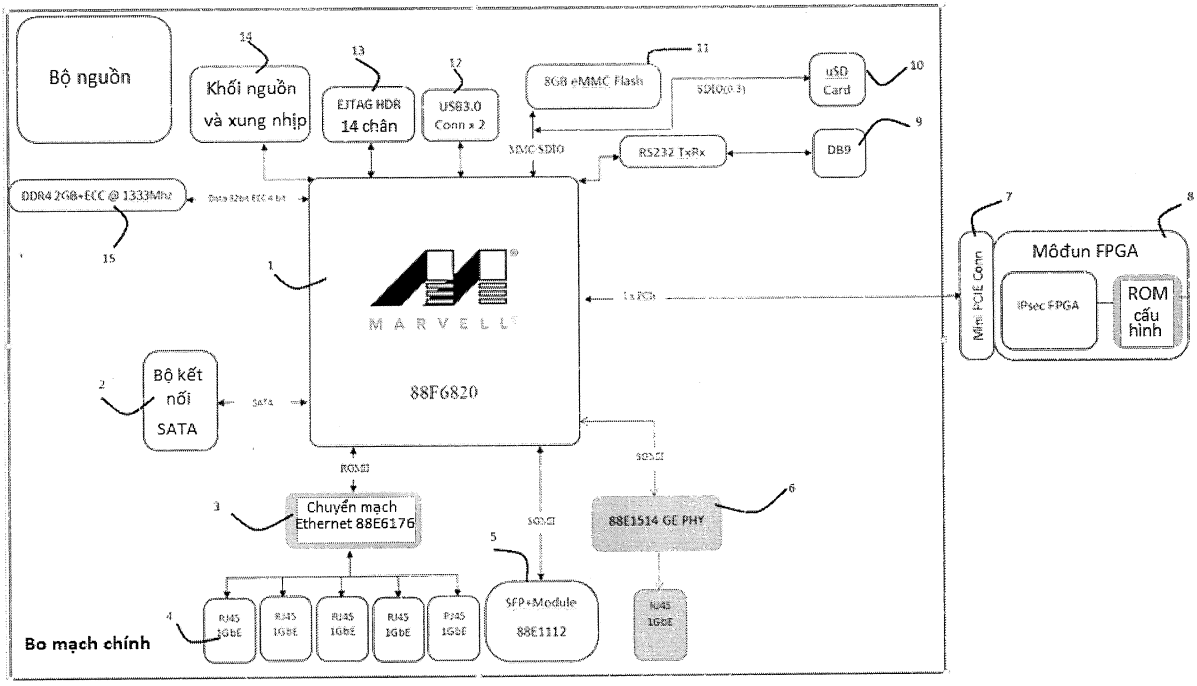
môđun FPGA được thiết kế theo chuẩn giao tiếp mini PCIe, gồm có 1 chip, ưu tiên là chip Xilinx Artix 7 FPGA và một bộ nhớ ROM, ưu tiên là bộ MT25QL01GBBB8E12, khác biệt ở chỗ:

môđun FPGA này có khả năng thiết lập các phần cứng tính toán nhanh, và có khả năng tạo cấu hình lại để tính toán xử lý toàn bộ các gói tin theo chuẩn IPsec, môđun FPGA này không chỉ hỗ trợ tăng tốc các phép toán mã hóa/giải mã, mà còn xử lý toàn bộ gói tin, bao gồm cả các phần xử lý khung truyền, và

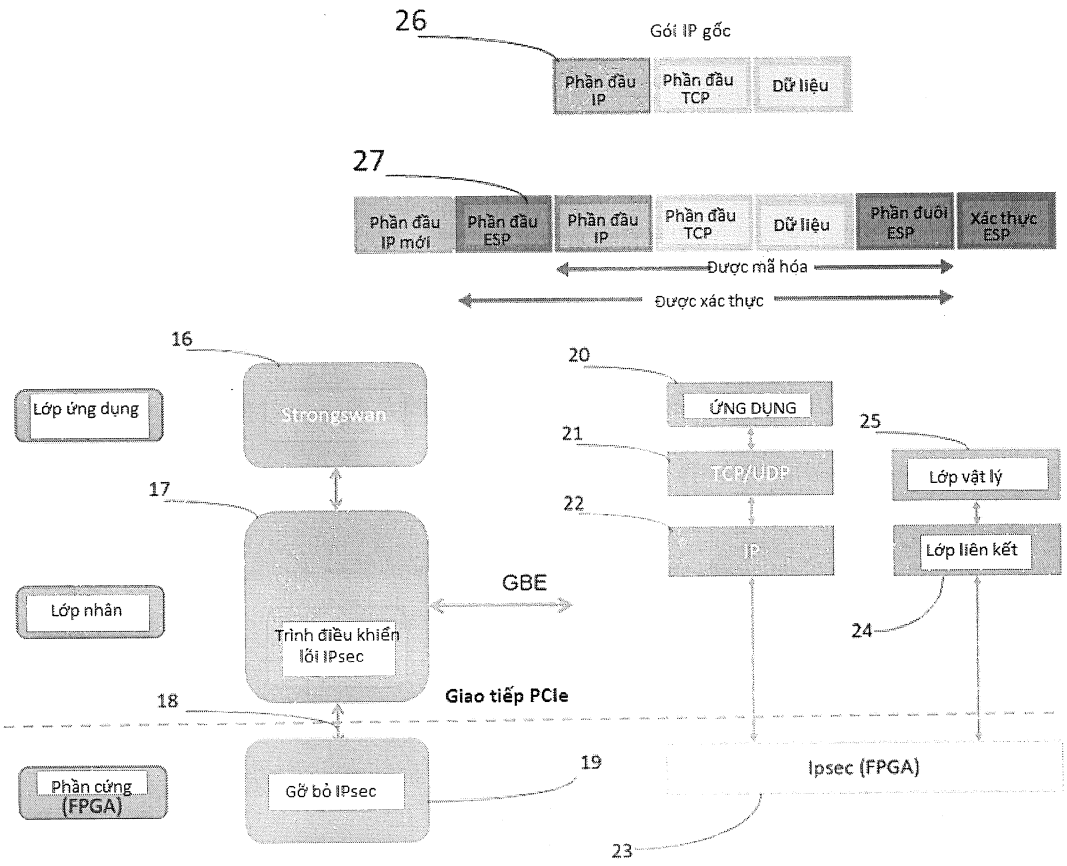
môđun FPGA này kết nối với bo mạch chính qua giao tiếp mini PCIe.


Internet
Máy chủ VPN
Địa chỉ IP mới
217.114.218.29
Phần mềm gián điệp ISP
Sự theo dõi
Các Hacker
V P N
Bộ định tuyến VPN

Hình 1


Bộ nguồn
Khối nguồn và xung nhịp
EJTAG HDR 14 chân
USB3.0 Conn x 2
8GB eMMC Flash
uSD Card
DB9
RS232 TxRx
DDR4 2GB+ECC @ 1333Mhz
MARVELL
88F6820
Bộ kết nối SATA
Chuyển mạch Ethernet 88E6176
88E1514 GE PHY
SFP+Module 88E1112
RJ45 1GbE
Bo mạch chính
Môđun FPGA
IPsec FPGA
ROM cấu hình

Hình 2


26
Gói IP gốc
Phần đầu IP
Phần đầu TCP
Dữ liệu
27
Phần đầu IP mới
Phần đầu ESP
Phần đầu IP
Phần đầu TCP
Dữ liệu
Phần đuôi ESP
Xác thực ESP
Được mã hóa
Được xác thực
16
Strongswan
Lớp ứng dụng
17
Trình điều khiển lõi IPsec
Lớp nhân
GBE
18
Giao tiếp PCIe
Phần cứng (FPGA)
Gỡ bỏ IPsec
19
20
ỨNG DỤNG
21
TCP/UDP
22
IP
25
Lớp vật lý
Lớp liên kết
24
Ipsec (FPGA)
23

Hình 3