(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) **1-0032445**

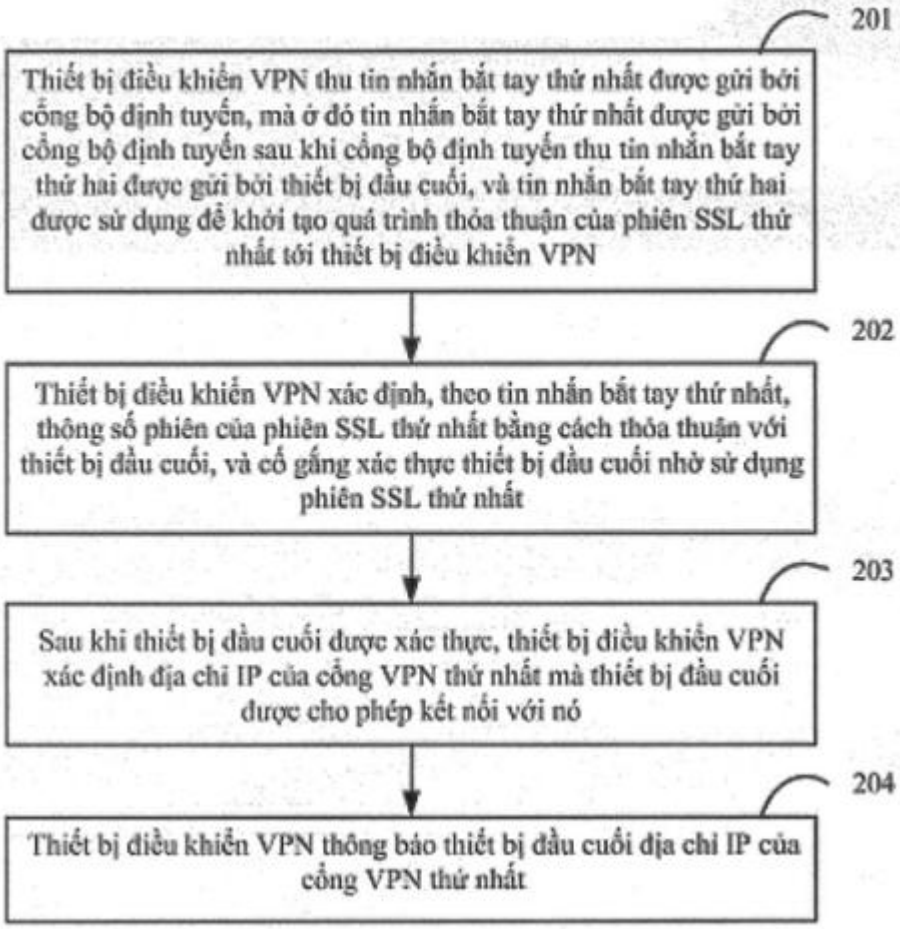
(51)[8] **H04L 12/46**

(13) **B**

(21) 1-2018-05082
(22) 12/04/2017
(86) PCT/CN2017/080310 12/04/2017
(87) WO 2017/181894 A1 26/10/2017
(30) 201610242556.0 18/04/2016 CN
(45) 25/07/2022 412
(43) 25/09/2019 378A
(73) HUAWEI TECHNOLOGIES CO., LTD. (CN)
Huawei Administration Building, Bantian, Longgang District, Shenzhen, Guangdong 518129, China
(72) YANG, Yancheng (CN); CHEN, Xiangrong (CN).
(74) Công ty TNHH một thành viên Sở hữu trí tuệ VCCI (VCCI-IP CO.,LTD)

(54) PHƯƠNG PHÁP ĐƯỢC SỬ DỤNG BỞI THIẾT BỊ ĐẦU CUỐI ĐỂ KẾT NỐI VỚI MẠNG RIÊNG ẢO, HỆ THỐNG ĐƯỢC SỬ DỤNG BỞI THIẾT BỊ ĐẦU CUỐI ĐỂ KẾT NỐI VỚI MẠNG RIÊNG ẢO VÀ THIẾT BỊ ĐIỀU KHIỂN MẠNG RIÊNG ẢO

(57) Sáng chế đề cập đến phương pháp được sử dụng biết bởi thiết bị đầu cuối để kết nối với mạng riêng ảo (VPN), hệ thống được sử dụng bởi thiết bị đầu cuối để kết nối với VPN và thiết bị điều khiển VPN, để giải quyết vấn đề tải làm việc lớn và lỗi dễ xảy ra hiện thời trong suốt quá trình tạo cấu hình địa chỉ giao thức Internet (IP) của cổng VPN đối với thiết bị đầu cuối. Phương pháp này bao gồm các bước: thu, bởi thiết bị điều khiển VPN, tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên lớp ổ bảo mật (SSL) thứ nhất tới thiết bị điều khiển VPN; xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất; sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.


201
Thiết bị điều khiển VPN thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN
202
Thiết bị điều khiển VPN xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất
203
Sau khi thiết bị đầu cuối được xác thực, thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó
204
Thiết bị điều khiển VPN thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất

Lĩnh vực kỹ thuật được đề cập

Sáng chế đề cập tới lĩnh vực các kỹ thuật truyền thông, và cụ thể là, tới phương pháp và hệ thống được sử dụng bởi thiết bị đầu cuối để kết nối với mạng riêng ảo (tiếng anh: Virtual Private Network, VPN), và thiết bị liên quan.

Tình trạng kỹ thuật của sáng chế

Các thiết bị đầu cuối camera giao thức Internet (tiếng Anh: IP camera, IPC) đang rất phổ biến. Để ngăn chặn luồng viđeo được truyền bởi thiết bị đầu cuối IPC tới mạng khỏi việc bị theo dõi với mục đích xấu, và để ngăn chặn việc báo hiệu điều khiển được truyền bởi mạng tới thiết bị đầu cuối IPC khỏi việc bị giả mạo với mục đích xấu trong quá trình truyền, kỹ thuật VPN lớp ổ bảo mật (tiếng Anh: Secure Sockets Layer, SSL) được ứng dụng cho thiết bị đầu cuối IPC, sao cho luồng viđeo và báo hiệu điều khiển được mã hóa để được truyền giữa thiết bị đầu cuối IPC và mạng.

Kỹ thuật SSL VPN có nghĩa là người dùng từ xa được kết nối với máy chủ SSL VPN nhờ sử dụng trình duyệt web. Gói dữ liệu được truyền giữa người dùng từ xa và máy chủ SSL VPN được mã hóa nhờ sử dụng giao thức SSL hoặc giao thức bảo mật lớp truyền tải (tiếng Anh: Transport Layer Security, TLS) (phần tử kế tiếp của giao thức SSL). Cả giao thức SSL và giao thức TLS dưới đây được gọi là "SSL" hoặc "giao thức SSL".

Máy khách kết nối bảo mật được bố trí trước trong thiết bị đầu cuối IPC. Địa chỉ IP của cổng VPN được tạo cấu hình trước trong thiết bị đầu cuối IPC. Máy khách kết nối bảo mật khởi tạo quá trình xác thực. Sau khi quá trình xác thực thành công, phiên SSL được thiết lập giữa thiết bị đầu cuối IPC và cổng VPN. Luồng dữ liệu (ví dụ, luồng viđeo) và luồng báo hiệu có thể được mã hóa nhờ sử dụng phiên SSL để truyền.

Thiết bị đầu cuối IPC ngoài trời không được giám sát, và do đó nảy sinh vấn đề bảo mật đối với thiết bị đầu cuối. Sau khi thiết bị đầu cuối IPC được điều khiển với mục đích xấu, dữ liệu độc hại được truyền tới mạng khó có thể phát hiện do sự bảo vệ bảo mật bởi VPN. Do đó, để đảm bảo sự kết nối bảo mật của IPC tới mạng, cổng VPN có thể không được triển khai quanh mạng lõi, và cổng VPN thường được triển khai trên cổng bộ định tuyến.

Cổng VPN được triển khai trên cổng bộ định tuyến trong chế độ nối tắt. "Chế độ nối tắt" có nghĩa là cổng VPN được kết nối trực tiếp với cổng bộ định tuyến nhờ sử dụng cáp mạng, và cổng VPN và cổng bộ định tuyến từ mạng con độc lập. Cổng VPN chịu trách nhiệm về việc xác thực truy cập và thiết lập phiên SSL của thiết bị đầu cuối IPC trong vùng được quản lý bởi cổng VPN, và chuyển tiếp luồng dữ liệu và luồng báo hiệu tới mạng riêng viđeo. Mạng riêng viđeo là mạng lớp trên mà bao gồm cổng bộ định tuyến, thiết bị giám sát viđeo, và tương tự. Các cổng VPN khác nhau có các địa chỉ IP khác nhau, và các cổng VPN khác nhau chịu trách nhiệm quản lý các vùng khác nhau. Thiết bị đầu cuối IPC không được cho phép kết nối với mạng và thiết lập phiên SSL mà không có sự cho phép của cổng VPN. Thiết bị đầu cuối IPC cần phối hợp với cổng VPN mà quản lý vùng trong đó thiết bị đầu cuối IPC được bố trí cho sự sử dụng thông thường. Địa chỉ IP mà là của cổng VPN và được tạo cấu hình cho thiết bị đầu cuối IPC có thể chỉ là địa chỉ IP của cổng VPN mà quản lý vùng trong đó thiết bị đầu cuối IPC được bố trí. Thường có hàng ngàn thiết bị đầu cuối IPC, và các địa chỉ IP khác nhau của các cổng VPN được tạo cấu hình cho các thiết bị đầu cuối IPC được bố trí trong các vùng quản lý khác nhau. Do đó, tải làm việc là lớn và lỗi dễ dàng xảy ra trong suốt quá trình tạo cấu hình địa chỉ IP của cổng VPN dùng cho thiết bị đầu cuối IPC.

Bản chất kỹ thuật của sáng chế

Sáng chế đề xuất phương pháp và hệ thống được sử dụng bởi thiết bị đầu cuối để kết nối với mạng riêng ảo, và thiết bị liên quan, để giải quyết vấn đề tải làm việc lớn và lỗi dễ xảy ra hiện thời trong suốt quá trình tạo cấu hình địa chỉ IP của cổng VPN đối với thiết bị đầu cuối.

Theo khía cạnh thứ nhất, phương pháp được sử dụng bởi thiết bị đầu cuối để kết nối với VPN được đề xuất, phương pháp này bao gồm các bước:

thu, bởi thiết bị điều khiển VPN, tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

xác định, bởi thiết bị điều khiển VPN theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất;

sau khi thiết bị đầu cuối được xác thực, xác định, bởi thiết bị điều khiển VPN, địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và

thông báo, bởi thiết bị điều khiển VPN, cho thiết bị đầu cuối của địa chỉ IP của cổng VPN thứ nhất.

Theo khía cạnh này, thiết bị điều khiển VPN chịu trách nhiệm về việc xác thực truy cập của thiết bị đầu cuối, và xác định cổng VPN mà thiết bị đầu cuối được cho phép kết nối với nó. Khi địa chỉ IP của thiết bị điều khiển VPN được tạo cấu hình cho tất cả các thiết bị đầu cuối trong hệ thống, sự xác thực bảo mật thiết bị đầu cuối có thể được thực hiện. Cụ thể là, nếu có số lượng lớn các thiết bị đầu cuối, tải làm việc của việc tạo cấu hình đối với các thiết bị đầu cuối có thể được giảm nhiều, nhờ đó nâng cao hiệu quả tạo cấu hình.

Trong sự thực hiện tùy chọn, tin nhắn bắt tay thứ nhất mang mục nhập định tuyến trực tiếp của cổng bộ định tuyến, và mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt; và

bước xác định, bởi thiết bị điều khiển VPN, địa chỉ IP của cổng VPN thứ nhất bao gồm bước:

thu được, bởi thiết bị điều khiển VPN từ danh sách các địa chỉ IP được tạo

cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

Theo sự thực hiện này, thiết bị điều khiển VPN xác định cổng VPN mà thiết bị đầu cuối được cho phép kết nối với nó. Điều này tránh sự phụ thuộc của thiết bị đầu cuối và thiết bị điều khiển VPN, và nâng cao tính linh hoạt truy cập của thiết bị đầu cuối.

Trong sự thực hiện tùy chọn, phương pháp này còn bao gồm bước:

thông báo, bởi thiết bị điều khiển VPN, cổng VPN thứ nhất của địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, mà ở đó cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa.

Trong sự thực hiện tùy chọn, phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, tin nhắn bắt tay thứ ba tới cổng VPN thứ nhất, mà ở đó tin nhắn bắt tay thứ ba được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ hai tới cổng VPN thứ nhất, tin nhắn bắt tay thứ ba mang ký hiệu nhận dạng phiên và văn bản mã hóa, và văn bản mã hóa được tạo bằng cách mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên và thuật toán mã hóa.

Theo sự thực hiện này, thông số phiên của phiên SSL thứ nhất được thiết lập giữa thiết bị đầu cuối và thiết bị điều khiển VPN được sử dụng lại trực tiếp cho phiên SSL thứ hai được thiết lập giữa thiết bị đầu cuối và cổng VPN.

Trong sự thực hiện tùy chọn, bước cố gắng, bởi thiết bị điều khiển VPN, xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất bao gồm các bước:

thu, bởi thiết bị điều khiển VPN nhờ sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối, mà ở đó tin nhắn xác thực mang ký hiệu nhận dạng phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã

hóa ký hiệu nhận dạng của thiết bị đầu cuối nhờ sử dụng thuật toán mã hóa và khóa phiên;

phân tích cú pháp, bởi thiết bị điều khiển VPN, tin nhắn xác thực để thu được ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực; sau khi xác định rằng thiết bị điều khiển VPN lưu trữ ký hiệu nhận dạng phiên, giải mã dữ liệu xác thực nhờ sử dụng khóa phiên và thuật toán mã hóa, để thu được ký hiệu nhận dạng của thiết bị đầu cuối; và gửi ký hiệu nhận dạng của thiết bị đầu cuối tới máy chủ xác thực; và

nếu bước thu tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, xác định, bởi thiết bị điều khiển VPN, rằng sự truy cập của thiết bị đầu cuối được cho phép, mà ở đó tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực sau khi máy chủ xác thực xác định rằng ký hiệu nhận dạng của thiết bị đầu cuối hiện có; hoặc nếu bước thu tin nhắn lỗi xác thực được phản hồi bởi máy chủ xác thực, xác định, bởi thiết bị điều khiển VPN, rằng sự truy cập của thiết bị đầu cuối không được cho phép.

Trong sự thực hiện tùy chọn, phương pháp này còn bao gồm các bước:

thu, bởi cổng VPN thứ nhất, tin nhắn bắt tay thứ ba, và phân tích cú pháp tin nhắn bắt tay thứ ba để thu được ký hiệu nhận dạng phiên và văn bản mã hóa; và

nếu xác định rằng cổng VPN thứ nhất lưu trữ cục bộ ký hiệu nhận dạng phiên, và kết quả thu được bằng cách giải mã văn bản mã hóa nhờ sử dụng khóa phiên được lưu trữ cục bộ và thuật toán mã hóa là địa chỉ IP của thiết bị đầu cuối, thiết lập, bởi cổng VPN thứ nhất, phiên SSL thứ hai với thiết bị đầu cuối, và sử dụng thông số phiên của phiên SSL thứ nhất làm thông số phiên của phiên SSL thứ hai.

Theo khía cạnh thứ hai, hệ thống được sử dụng bởi thiết bị đầu cuối để kết nối với VPN được đề xuất, hệ thống này bao gồm:

thiết bị đầu cuối, được tạo cấu hình để gửi tin nhắn bắt tay thứ hai tới cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo

quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

cổng bộ định tuyến, được tạo cấu hình để gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN sau khi thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối; và

thiết bị điều khiển VPN, được tạo cấu hình để: thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất; sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, cổng bộ định tuyến được tạo cấu hình riêng biệt để:

bổ sung mục nhập định tuyến trực tiếp vào tin nhắn bắt tay thứ hai để thu được tin nhắn bắt tay thứ nhất, mà ở đó mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt; và

thiết bị điều khiển VPN được tạo cấu hình riêng biệt để:

thu được, từ danh sách các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, thiết bị điều khiển VPN còn được tạo cấu hình để:

thông báo cho cổng VPN thứ nhất địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất; và

cổng VPN thứ nhất được tạo cấu hình riêng biệt để:

lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, mà ở đó thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên,

và thuật toán mã hóa.

Trong sự thực hiện tùy chọn, thiết bị đầu cuối còn được tạo cấu hình để:

gửi tin nhắn bắt tay thứ ba tới cổng VPN thứ nhất, mà ở đó tin nhắn bắt tay thứ ba được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ hai tới cổng VPN thứ nhất, tin nhắn bắt tay thứ ba mang ký hiệu nhận dạng phiên và văn bản mã hóa, và văn bản mã hóa được tạo bằng cách mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên và thuật toán mã hóa.

Trong sự thực hiện tùy chọn, thiết bị đầu cuối được tạo cấu hình riêng biệt để:

gửi tin nhắn xác thực tới thiết bị điều khiển VPN nhờ sử dụng phiên SSL thứ nhất, mà ở đó tin nhắn xác thực mang ký hiệu nhận dạng phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã hóa ký hiệu nhận dạng của thiết bị đầu cuối nhờ sử dụng thuật toán mã hóa và khóa phiên;

thiết bị điều khiển VPN được tạo cấu hình riêng biệt để:

thu, nhờ sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối; phân tích cú pháp tin nhắn xác thực để thu được ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực; sau khi xác định rằng thiết bị điều khiển VPN lưu trữ ký hiệu nhận dạng phiên, giải mã dữ liệu xác thực nhờ sử dụng khóa phiên và thuật toán mã hóa, để thu được ký hiệu nhận dạng của thiết bị đầu cuối; và gửi ký hiệu nhận dạng của thiết bị đầu cuối tới máy chủ xác thực;

máy chủ xác thực được tạo cấu hình riêng biệt để:

thu ký hiệu nhận dạng của thiết bị đầu cuối được gửi bởi thiết bị điều khiển VPN, và nếu xác định rằng máy chủ xác thực lưu trữ ký hiệu nhận dạng của thiết bị đầu cuối, phản hồi tin nhắn thành công xác thực tới thiết bị điều khiển VPN; hoặc nếu xác định rằng máy chủ xác thực không lưu trữ ký hiệu nhận dạng của thiết bị đầu cuối, phản hồi tin nhắn lỗi xác thực tới thiết bị điều khiển VPN; và

thiết bị điều khiển VPN được tạo cấu hình riêng biệt để:

nếu bước thu tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối được cho phép; hoặc nếu bước thu tin nhắn lỗi xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối không được cho phép.

Trong sự thực hiện tùy chọn, cổng VPN thứ nhất được tạo cấu hình riêng biệt để:

thu tin nhắn bắt tay thứ ba, và phân tích cú pháp tin nhắn bắt tay thứ ba để thu được ký hiệu nhận dạng phiên và văn bản mã hóa; và

nếu xác định rằng cổng VPN thứ nhất lưu trữ ký hiệu nhận dạng phiên, và kết quả thu được bằng cách giải mã văn bản mã hóa nhờ sử dụng khóa phiên được lưu trữ cục bộ và thuật toán mã hóa là địa chỉ IP của thiết bị đầu cuối, thiết lập phiên SSL thứ hai với thiết bị đầu cuối, và sử dụng thông số phiên của phiên SSL thứ nhất làm thông số phiên của phiên SSL thứ hai.

Theo khía cạnh thứ ba, thiết bị điều khiển VPN được đề xuất, thiết bị này bao gồm:

môđun thu, được tạo cấu hình để thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

môđun xác thực, được tạo cấu hình để: xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất;

môđun xác định, được tạo cấu hình để: sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và

môđun thông báo, được tạo cấu hình để thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, tin nhắn bắt tay thứ nhất mang mục nhập

định tuyến trực tiếp của cổng bộ định tuyến, và mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt; và

môđun xác định được tạo cấu hình riêng biệt để:

thu được, từ danh sách các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, môđun thông báo còn được tạo cấu hình để:

thông báo cho cổng VPN thứ nhất địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, mà ở đó cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa.

Trong sự thực hiện tùy chọn, môđun thu được tạo cấu hình riêng biệt để:

thu, nhờ sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối, mà ở đó tin nhắn xác thực mang khóa phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã hóa ký hiệu nhận dạng của thiết bị đầu cuối nhờ sử dụng thuật toán mã hóa và khóa phiên; và

môđun xác thực được tạo cấu hình riêng biệt để:

phân tích cú pháp tin nhắn xác thực để thu được ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực, sau khi xác định rằng môđun xác thực lưu trữ cục bộ ký hiệu nhận dạng phiên, giải mã dữ liệu xác thực nhờ sử dụng khóa phiên và thuật toán mã hóa, để thu được ký hiệu nhận dạng của thiết bị đầu cuối, và gửi ký hiệu nhận dạng của thiết bị đầu cuối tới máy chủ xác thực; và nếu thu, nhờ sử dụng môđun thu, tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối được cho phép, mà ở đó tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực sau khi máy chủ xác thực xác định rằng ký hiệu nhận dạng của thiết bị đầu cuối hiện có; hoặc nếu thu, nhờ sử dụng môđun thu,

tin nhắn lỗi xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối không được cho phép.

Theo khía cạnh thứ tư, thiết bị điều khiển VPN được đề xuất, bao gồm bộ xử lý và giao diện truyền thông, trong đó

bộ xử lý được tạo cấu hình để: thu, nhờ sử dụng giao diện truyền thông, tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN; xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất; sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và thông báo, nhờ sử dụng giao diện truyền thông, thiết bị đầu cuối của địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, tin nhắn bắt tay thứ nhất mang mục nhập định tuyến trực tiếp của cổng bộ định tuyến, và mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt; và

bộ xử lý được tạo cấu hình riêng biệt để:

thu được, từ danh sách các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

Trong sự thực hiện tùy chọn, bộ xử lý còn được tạo cấu hình để: thông báo, nhờ sử dụng giao diện truyền thông, cho cổng VPN thứ nhất địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, mà ở đó cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và

thuật toán mã hóa.

Theo khía cạnh thứ năm, cổng bộ định tuyến được đề xuất, bao gồm bộ xử lý và giao diện truyền thông, trong đó

bộ xử lý được tạo cấu hình để: thu, nhờ sử dụng giao diện truyền thông, tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN; tạo tin nhắn bắt tay thứ nhất theo tin nhắn bắt tay thứ hai; và gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN nhờ sử dụng giao diện truyền thông.

Theo khía cạnh thứ sáu, thiết bị đầu cuối còn được đề xuất, thiết bị này bao gồm bộ xử lý và giao diện truyền thông, trong đó

bộ xử lý được tạo cấu hình để: gửi tin nhắn bắt tay thứ hai tới cổng bộ định tuyến nhờ sử dụng giao diện truyền thông, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN, và cổng bộ định tuyến gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN sau khi thu tin nhắn bắt tay thứ hai; xác định, theo tin nhắn bắt tay thứ hai, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị điều khiển VPN, và yêu cầu, nhờ sử dụng phiên SSL thứ nhất, thiết bị điều khiển VPN cố gắng xác thực thiết bị đầu cuối; và thu, nhờ sử dụng giao diện truyền thông, địa chỉ IP mà là của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó và được thông báo bởi thiết bị điều khiển VPN, mà ở đó địa chỉ IP của cổng VPN thứ nhất được xác định bởi thiết bị điều khiển VPN sau khi thiết bị đầu cuối được xác thực.

Mô tả vắn tắt các hình vẽ

Fig.1 là sơ đồ giản lược của cấu trúc hệ thống trong đó thiết bị đầu cuối được kết nối với VPN theo một phương án của sáng chế;

Fig.2 là lưu đồ giản lược của phương pháp được sử dụng bởi thiết bị đầu cuối để kết nối với VPN theo một phương án của sáng chế;

Fig.3 là sơ đồ cấu trúc giản lược của mục nhập định tuyến trực tiếp được

mang trong tùy chọn mở rộng của tin nhắn ClientHello theo một phương án của sáng chế;

Fig.4 là sơ đồ giản lược của quá trình trong đó thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất theo một phương án của sáng chế;

Fig.5 là sơ đồ giản lược của quá trình trong đó cổng VPN thứ nhất thiết lập phiên SSL với thiết bị đầu cuối theo một phương án của sáng chế;

Fig.6 là sơ đồ giản lược của lôgic chức năng của sự xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo một phương án của sáng chế;

Fig.7A, Fig.7B, và Fig.7C là lưu đồ giản lược của phương pháp xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo một phương án của sáng chế;

Fig.8A, Fig.8B, Fig.8C, và Fig.8D là sơ đồ giản lược của chuỗi thời gian làm việc của quá trình xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo một phương án của sáng chế;

Fig.9 là sơ đồ cấu trúc giản lược của thiết bị điều khiển VPN theo một phương án của sáng chế;

Fig.10 là sơ đồ cấu trúc giản lược của cổng bộ định tuyến theo một phương án của sáng chế;

Fig.11 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối theo một phương án của sáng chế;

Fig.12 là sơ đồ cấu trúc giản lược của thiết bị điều khiển VPN khác theo một phương án của sáng chế;

Fig.13 là sơ đồ cấu trúc giản lược của cổng bộ định tuyến khác theo một phương án của sáng chế; và

Fig.14 là sơ đồ cấu trúc giản lược của thiết bị đầu cuối khác theo một phương án của sáng chế.

Mô tả chi tiết sáng chế

Trong một phương án của sáng chế, Fig.1 thể hiện cấu trúc hệ thống trong

đó thiết bị đầu cuối được kết nối với VPN. Cấu trúc hệ thống chủ yếu bao gồm thiết bị đầu cuối 101, cổng VPN 102, cổng bộ định tuyến 103, thiết bị điều khiển VPN 104, và máy chủ xác thực 105. Các chi tiết như sau đây:

Thiết bị đầu cuối 101 có thể là thiết bị đầu cuối mà hỗ trợ ngăn xếp giao thức IP, chẳng hạn như IPC. Phần mềm máy khách được cài đặt trên thiết bị đầu cuối 101. Thiết bị đầu cuối khởi tạo quá trình xác thực. Thiết bị đầu cuối có thể là, ví dụ, điện thoại di động, máy tính cá nhân (chẳng hạn như máy tính xách tay hoặc máy tính để bàn), máy tính, điện thoại IP, hoặc máy chiếu.

Cổng VPN 102 được tạo cấu hình để thiết lập phiên SSL với thiết bị đầu cuối. Cổng VPN 102 thực hiện đóng gói đường hầm trên luồng dịch vụ và dòng báo hiệu mà được gửi nhờ sử dụng phiên SSL, mở gói luồng dịch vụ và dòng báo hiệu mà được thu nhờ sử dụng phiên SSL, và chuyển tiếp luồng dịch vụ tới bước nhảy tiếp theo.

Cổng bộ định tuyến 103 được bố trí giữa thiết bị mạng lớp 2 và thiết bị mạng lớp 3, và được tạo cấu hình để thực hiện truy cập lớp 2 và chuyển tiếp lớp 2 với thiết bị mạng lớp 2. Thiết bị mạng lớp 3 được kết nối với cổng VPN và thiết bị điều khiển VPN, và cổng bộ định tuyến 103 thực hiện định tuyến và chuyển tiếp với thiết bị mạng lớp 3.

Thiết bị điều khiển VPN 104 là bộ xác thực của tất cả các thiết bị đầu cuối 101 trong hệ thống, và truyền thông với máy chủ xác thực 105 để hoàn thành việc xác thực trên các thiết bị đầu cuối. Thiết bị điều khiển VPN 104 gửi kết quả xác thực và địa chỉ của cổng VPN tới thiết bị đầu cuối 101. Thiết bị điều khiển VPN 104 gửi, tới cổng VPN 102, ký hiệu nhận dạng của thiết bị đầu cuối 101 mà được xác thực.

Máy chủ xác thực 105 được tạo cấu hình để cố gắng xác thực thiết bị đầu cuối 101.

Thiết bị điều khiển VPN là thiết bị cổng mà làm việc độc lập, hoặc chức năng của thiết bị điều khiển VPN được hoàn thành bởi nhiều thiết bị cổng bằng cách phối hợp.

Cổng VPN là thiết bị cổng mà làm việc độc lập, hoặc chức năng của cổng VPN được hoàn thành bởi nhiều thiết bị cổng bằng cách phối hợp.

Trong ví dụ trong đó thiết bị đầu cuối 101 là thiết bị đầu cuối IPC, hệ thống có thể còn bao gồm thiết bị giám sát viđeo 106. Thiết bị giám sát viđeo 106 được tạo cấu hình để gửi báo hiệu tới thiết bị đầu cuối 101 trong vùng được quản lý bởi cổng VPN 102. Thiết bị giám sát viđeo 106 có thể hiển thị viđeo được gửi bởi thiết bị đầu cuối 101. Một cách tùy chọn, thiết bị giám sát viđeo 106 có thể lưu trữ viđeo được gửi bởi thiết bị đầu cuối 101.

Thiết bị điều khiển VPN và máy chủ xác thực có thể được tích hợp thành một thiết bị.

Dựa trên cấu trúc hệ thống nêu trên, theo một phương án của sáng chế, Fig.2 thể hiện quá trình cụ thể trong đó thiết bị đầu cuối được kết nối với VPN. Các chi tiết như sau đây:

Bước 201: thiết bị điều khiển VPN thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN.

Trước khi thiết bị đầu cuối gửi tin nhắn bắt tay thứ hai, địa chỉ IP của thiết bị điều khiển VPN cần được tạo cấu hình cho thiết bị đầu cuối. Các địa chỉ IP của tất cả các cổng VPN trong hệ thống được tạo cấu hình trong thiết bị điều khiển VPN. Mục nhập định tuyến trực tiếp được tạo cấu hình trong cổng bộ định tuyến. Mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt, hoặc mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con và mặt lạ mà là của cổng VPN mà được bố trí trên cổng bộ định tuyến trong chế độ nối tắt. "Chế độ nối tắt" có nghĩa là cổng bộ định tuyến được kết nối với cổng VPN nhờ sử dụng cáp mạng. Cổng bộ định tuyến và cổng VPN trong chế độ nối tắt thuộc về cùng mạng con.

Địa chỉ IP của tất cả cổng VPN trong hệ thống, hoặc các mặt lạ và các địa

chỉ IP của tất cả các cổng VPN trong hệ thống được tạo cấu hình trong thiết bị điều khiển VPN. Các địa chỉ IP mà là của tất cả các cổng VPN và mà được tạo cấu hình trong thiết bị điều khiển VPN là khác nhau, và các tiền tố mạng con của tất cả các cổng VPN là khác nhau, để đảm bảo tính duy nhất toàn cầu của các cổng VPN.

Sau khi thu tin nhắn bắt tay thứ hai từ thiết bị đầu cuối, và trước khi gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN, cổng bộ định tuyến bổ sung mục nhập định tuyến trực tiếp của cổng bộ định tuyến tới tin nhắn bắt tay thứ hai, để thu được tin nhắn bắt tay thứ nhất.

Bước 202: thiết bị điều khiển VPN xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất.

Thông số phiên của phiên SSL thứ nhất bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa, và thiết bị đầu cuối và thiết bị điều khiển VPN lưu trữ riêng rẽ thông số phiên của phiên SSL thứ nhất.

Thiết bị điều khiển VPN thu, nhờ sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối. Tin nhắn xác thực mang ký hiệu nhận dạng phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã hóa ký hiệu nhận dạng của thiết bị đầu cuối nhờ sử dụng thuật toán mã hóa và khóa phiên.

Thiết bị điều khiển VPN thu được ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực. Sau khi xác định rằng thiết bị điều khiển VPN lưu trữ ký hiệu nhận dạng phiên, thiết bị điều khiển VPN giải mã dữ liệu xác thực nhờ sử dụng khóa phiên và thuật toán mã hóa, để thu được ký hiệu nhận dạng của thiết bị đầu cuối, và gửi ký hiệu nhận dạng của thiết bị đầu cuối tới máy chủ xác thực.

Nếu bước thu tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, thiết bị điều khiển VPN xác định rằng việc xác thực trên thiết bị đầu cuối thành công. Nếu bước thu tin nhắn lỗi xác thực được phản hồi bởi máy chủ

xác thực, thiết bị điều khiển VPN xác định rằng việc xác thực trên thiết bị đầu cuối không thành công.

Sau khi xác định rằng sự truy cập của thiết bị đầu cuối không được cho phép, thiết bị điều khiển VPN hủy phiên SSL thứ nhất.

Bước 203: sau khi thiết bị đầu cuối được xác thực, thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó.

Sau khi thiết bị đầu cuối được xác thực, thiết bị điều khiển VPN xác định, theo mục nhập định tuyến trực tiếp của cổng bộ định tuyến mà gửi tin nhắn bắt tay thứ nhất, cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó.

Ví dụ, thiết bị đầu cuối khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN theo địa chỉ IP được tạo cấu hình của thiết bị điều khiển VPN. Đó là, thiết bị đầu cuối gửi tin nhắn bắt tay thứ hai, đó là, tin nhắn ClientHello nhờ sử dụng địa chỉ IP của thiết bị điều khiển VPN làm địa chỉ đích. Cổng bộ định tuyến thu tin nhắn ClientHello được gửi bởi thiết bị đầu cuối, và bổ sung mục nhập định tuyến trực tiếp của cổng bộ định tuyến tới tùy chọn mở rộng trống của tin nhắn ClientHello, để thu được tin nhắn bắt tay thứ nhất. Cụ thể là, Fig.3 thể hiện cấu trúc của tùy chọn mở rộng của tin nhắn ClientHello, và trường tùy chọn (tiếng Anh: option) tương ứng với loại 60 mang mục nhập định tuyến trực tiếp của cổng bộ định tuyến. Loại mở rộng của tùy chọn mở rộng của tin nhắn ClientHello có thể là trị số không được sử dụng bất kỳ trong khoảng từ 36 đến 65280.

Fig.4 thể hiện quá trình trong đó thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất. Thiết bị điều khiển VPN thu được, từ danh sách các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN trong hệ thống, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp được mang trong tin nhắn bắt tay thứ nhất, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ

nhất. Nếu nhiều hơn một địa chỉ IP của các cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp được mang trong tin nhắn bắt tay thứ nhất được thu, một địa chỉ IP được chọn ngẫu nhiên từ các địa chỉ IP thích hợp thu được làm địa chỉ IP của cổng VPN thứ nhất.

Một cách tùy chọn, địa chỉ IP của cổng VPN thứ nhất được xác định trong các bước sau đây. Bước a: thiết bị điều khiển VPN thu được tiền tố mạng con M và mặt lạ N mà là của cổng VPN và nằm trong mục nhập định tuyến trực tiếp được mang trong tin nhắn bắt tay thứ nhất, và thực hiện phép toán AND trên tiền tố mạng con M và mặt lạ N mà là của cổng VPN để thu được X. Bước b: dùng cho địa chỉ IP mà là của cổng VPN và mà được tạo cấu hình trong thiết bị điều khiển VPN và mặt lạ B tương ứng với địa chỉ IP A, thực hiện phép toán AND trên địa chỉ IP và mặt lạ B để thu được Y. Bước c: xác định xem X có bằng Y hay không, và nếu X bằng Y, xác định rằng địa chỉ IP là địa chỉ IP của cổng VPN thứ nhất; hoặc nếu X không bằng Y, thu được địa chỉ IP mà là của cổng VPN tiếp theo và được tạo cấu hình trong thiết bị điều khiển VPN và mặt lạ tương ứng, và thực hiện lặp lại bước b và bước c đến khi danh sách của các địa chỉ IP mà là của tất cả các cổng VPN trong hệ thống và được tạo cấu hình trong thiết bị điều khiển VPN được đi qua.

Thiết bị điều khiển VPN tìm kiếm danh sách của các địa chỉ IP của tất cả các cổng VPN trong hệ thống theo mục nhập định tuyến trực tiếp. Ví dụ, nếu mỗi mục nhập trong mục nhập định tuyến trực tiếp thể hiện tiền tố mạng con của cổng VPN, tiền tố mạng con của cổng VPN được sử dụng để tìm kiếm danh sách của các địa chỉ IP của tất cả các cổng VPN trong hệ thống, và địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con của cổng VPN được xác định làm địa chỉ IP của cổng VPN thứ nhất mà ở đó thiết bị đầu cuối cần kết nối tới.

Bước 204: thiết bị điều khiển VPN thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.

Thiết bị điều khiển VPN thông báo cổng VPN thứ nhất của địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ

nhất.

Thiết bị đầu cuối và cổng VPN thứ nhất sử dụng lại thông số phiên của phiên SSL thứ nhất để thiết lập phiên SSL thứ hai. Quá trình trong đó thiết bị đầu cuối thiết lập phiên SSL thứ hai với cổng VPN thứ nhất như sau đây:

Thiết bị đầu cuối mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên và thuật toán mã hóa của phiên SSL thứ nhất, để tạo văn bản mã hóa, và bổ sung ký hiệu nhận dạng phiên của phiên SSL thứ nhất và văn bản mã hóa tới tin nhắn bắt tay thứ ba, và gửi tin nhắn bắt tay thứ ba tới cổng VPN thứ nhất. Tin nhắn bắt tay thứ ba được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ hai tới cổng VPN thứ nhất.

Cụ thể là, tin nhắn bắt tay thứ ba là tin nhắn ClientHello. Văn bản mã hóa được tạo bằng cách mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên và thuật toán mã hóa, và văn bản mã hóa được mang tới tùy chọn mở rộng của tin nhắn ClientHello. Loại tùy chọn mở rộng của tin nhắn ClientHello có thể là trị số không được sử dụng bất kỳ trong khoảng từ 36 đến 65280, và loại 61 thể hiện rằng trường tùy chọn của tùy chọn mở rộng mang văn bản mã hóa A.

Cổng VPN thứ nhất thu tin nhắn bắt tay thứ ba, và thu được ký hiệu nhận dạng phiên và văn bản mã hóa mà được mang trong tin nhắn bắt tay thứ ba. Nếu xác định rằng cổng VPN thứ nhất lưu trữ cục bộ ký hiệu nhận dạng phiên, và kết quả thu được bằng cách giải mã văn bản mã hóa nhờ sử dụng khóa phiên được lưu trữ cục bộ và thuật toán mã hóa là địa chỉ IP của thiết bị đầu cuối, cổng VPN thứ nhất thiết lập phiên SSL thứ hai với thiết bị đầu cuối, và sử dụng thông số phiên của phiên SSL thứ nhất làm thông số phiên của phiên SSL thứ hai.

Cụ thể là, Fig.5 thể hiện quá trình trong đó cổng VPN thứ nhất thiết lập phiên SSL thứ hai với thiết bị đầu cuối theo ký hiệu nhận dạng phiên và văn bản mã hóa mà được mang trong tin nhắn bắt tay thứ ba. Các chi tiết như sau đây:

Cổng VPN thứ nhất lưu trữ cục bộ địa chỉ IP của thiết bị đầu cuối mà được cho phép kết nối với cổng VPN thứ nhất, và lưu trữ ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất. Cổng VPN thứ

nhất phân tích cú pháp tin nhắn ClientHello được gửi bởi thiết bị đầu cuối, để thu được ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello, và trích văn bản mã hóa theo tùy chọn mở rộng 61 của tin nhắn ClientHello. Cổng VPN thứ nhất xác định xem ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello có giống như ký hiệu nhận dạng phiên được trữ cục bộ hay không. Nếu ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello khác với ký hiệu nhận dạng phiên được trữ cục bộ, cổng VPN thứ nhất từ chối thiết lập phiên SSL thứ hai. Nếu ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello giống như ký hiệu nhận dạng phiên được trữ cục bộ, cổng VPN thứ nhất giải mã văn bản mã hóa nhờ sử dụng thuật toán mã hóa được lưu trữ cục bộ và khóa phiên của phiên SSL thứ nhất, để thu được trị số X. Cổng VPN thứ nhất xác định xem trị số X có giống như địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu hay không. Nếu trị số X khác với địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu, cổng VPN thứ nhất từ chối thiết lập phiên SSL thứ hai. Nếu trị số X giống như địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu, cổng VPN thứ nhất còn xác định xem địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu có là địa chỉ IP được lưu trữ cục bộ của thiết bị đầu cuối mà được cho phép kết nối với cổng VPN thứ nhất hay không. Nếu địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu không phải là địa chỉ IP được lưu trữ cục bộ của thiết bị đầu cuối mà được cho phép kết nối với cổng VPN thứ nhất, cổng VPN thứ nhất từ chối thiết lập phiên SSL thứ hai; hoặc nếu địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu là địa chỉ IP được lưu trữ cục bộ của thiết bị đầu cuối mà được cho phép kết nối với cổng VPN thứ nhất, cổng VPN thứ nhất thiết lập thành công phiên SSL thứ hai với thiết bị đầu cuối, và sử dụng lại ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất.

Phần mô tả sau đây sử dụng phương án cụ thể để mô tả chi tiết quá trình cố gắng xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL được sử dụng để truyền luồng dịch vụ.

Fig.6 là sơ đồ giản lược của lôgic chức năng của sự xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo phương án cụ thể. Fig.7A, Fig.7B, và

Fig.7C là lưu đồ giản lược của phương pháp xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo phương án cụ thể. Fig.8A, Fig.8B, Fig.8C, và Fig.8D là sơ đồ giản lược của chuỗi thời gian làm việc của sự xác thực truy cập thiết bị đầu cuối và thiết lập phiên SSL theo phương án cụ thể.

Quá trình cụ thể như sau đây:

1. Pha chuẩn bị

Bước 1: tạo cấu hình ba thành phần mạng: thiết bị điều khiển VPN, cổng bộ định tuyến, và thiết bị đầu cuối, và cụ thể là, tải danh sách các địa chỉ IP của tất cả các cổng VPN trong hệ thống trong thiết bị điều khiển VPN, tạo cấu hình mục nhập định tuyến trực tiếp dùng cho cổng bộ định tuyến, và tạo cấu hình địa chỉ IP của thiết bị điều khiển VPN dùng cho thiết bị đầu cuối.

2. Pha xác thực

Bước 2: thiết bị đầu cuối khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN theo địa chỉ IP được tạo cấu hình của thiết bị điều khiển VPN, và cụ thể là, thiết bị đầu cuối gửi tin nhắn ClientHello nhờ sử dụng địa chỉ IP của thiết bị điều khiển VPN làm địa chỉ đích, và tin nhắn ClientHello được định tuyến tới cổng bộ định tuyến.

Bước 3: cổng bộ định tuyến trích tin nhắn ClientHello, bổ sung mục nhập định tuyến trực tiếp tới tùy chọn mở rộng của tin nhắn ClientHello, và gửi, tới thiết bị điều khiển VPN, tin nhắn ClientHello mang mục nhập định tuyến trực tiếp.

Bước 4: thiết bị điều khiển VPN thu tin nhắn ClientHello được gửi bởi cổng bộ định tuyến, thu được mục nhập định tuyến trực tiếp được mang trong tin nhắn ClientHello, và lưu trữ cục bộ mục nhập định tuyến trực tiếp.

Bước 5: thiết bị điều khiển VPN thực hiện quá trình thỏa thuận tiếp theo của phiên SSL thứ nhất với thiết bị đầu cuối theo giao thức SSL tiêu chuẩn, tạo khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa của phiên SSL thứ nhất, và thiết lập thành công phiên SSL thứ nhất; và thiết bị đầu cuối và thiết bị điều khiển VPN lưu trữ riêng rẽ khóa phiên, ký hiệu nhận dạng phiên, và thuật

toán mã hóa, và tất cả các tin nhắn tiếp theo mà được truyền nhờ sử dụng phiên SSL thứ nhất được mã hóa nhờ sử dụng khóa phiên và thuật toán mã hóa, và mang ký hiệu nhận dạng phiên.

Bước 6: thiết bị đầu cuối gửi yêu cầu xác thực tới thiết bị điều khiển VPN, và yêu cầu xác thực mang ký hiệu nhận dạng của thiết bị đầu cuối.

Bước 7: thiết bị điều khiển VPN chuyển tiếp ký hiệu nhận dạng của thiết bị đầu cuối tới máy chủ xác thực, và máy chủ xác thực kiểm tra xem ký hiệu nhận dạng của thiết bị đầu cuối có hiện có cục bộ hay không, và nếu ký hiệu nhận dạng của thiết bị đầu cuối hiện có, máy chủ xác thực phản hồi tin nhắn thành công xác thực tới thiết bị điều khiển VPN, hoặc nếu ký hiệu nhận dạng của thiết bị đầu cuối không hiện có, máy chủ xác thực phản hồi tin nhắn lỗi xác thực tới thiết bị điều khiển VPN; và nếu việc xác thực không thành công, bước 8 được thực hiện, hoặc nếu quá trình xác thực thành công, bước 9 được thực hiện.

Bước 8: thiết bị điều khiển VPN xác định rằng sự xác thực truy cập trên thiết bị đầu cuối không thành công, từ chối sự truy cập của thiết bị đầu cuối, và hủy phiên SSL thứ nhất được thiết lập giữa thiết bị điều khiển VPN và thiết bị đầu cuối.

Bước 9: thiết bị điều khiển VPN xác định rằng sự xác thực truy cập trên thiết bị đầu cuối thành công, và thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó, và thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.

Bước 10: thiết bị điều khiển VPN thông báo tới cổng VPN thứ nhất nội dung sau đây: địa chỉ IP của thiết bị đầu cuối mà được cho phép thiết lập phiên SSL thứ hai, và khóa phiên, thuật toán mã hóa, và ký hiệu nhận dạng phiên của phiên SSL thứ nhất.

Bước 11: cổng VPN thu và lưu trữ nội dung được thông báo bởi thiết bị điều khiển VPN: địa chỉ IP của thiết bị đầu cuối mà được cho phép thiết lập phiên SSL thứ hai, và khóa phiên, thuật toán mã hóa, và ký hiệu nhận dạng phiên của phiên SSL thứ nhất.

3. Pha thiết lập phiên SSL được sử dụng để chuyển tiếp luồng dịch vụ

Bước 12: thiết bị đầu cuối mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên được lưu trữ và thuật toán mã hóa của phiên SSL thứ nhất, để tạo văn bản mã hóa mà được ký hiệu là A=Encrypt (khóa phiên và địa chỉ IP của thiết bị đầu cuối).

Bước 13: thiết bị đầu cuối khởi tạo quá trình thỏa thuận của phiên SSL thứ hai tới cổng VPN, và cụ thể là, thiết bị đầu cuối gửi tin nhắn ClientHello tới cổng VPN, tin nhắn ClientHello mang ký hiệu nhận dạng phiên của phiên SSL thứ nhất và văn bản mã hóa A, và văn bản mã hóa được mang trong tùy chọn mở rộng của tin nhắn ClientHello.

Bước 14: cổng VPN phân tích cú pháp tin nhắn ClientHello để trích ký hiệu nhận dạng phiên và văn bản mã hóa trong tin nhắn ClientHello.

Bước 15: cổng VPN xác định xem có cho phép thiết bị đầu cuối thiết lập phiên SSL thứ hai hay không, và hai điều kiện xác định là như sau đây: điều kiện 1: cổng VPN xác định xem cổng VPN có lưu trữ ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello hay không, và nếu cổng VPN lưu trữ ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello, điều kiện xác định thứ hai được thực hiện, hoặc nếu cổng VPN không lưu trữ ký hiệu nhận dạng phiên được mang trong tin nhắn ClientHello, thiết bị đầu cuối không được cho phép thiết lập phiên SSL thứ hai, và bước 16 được thực hiện. Điều kiện 2: cổng VPN giải mã văn bản mã hóa được thu nhờ sử dụng khóa phiên được lưu trữ và thuật toán mã hóa của phiên SSL thứ nhất, để thu được trị số X, và xác định xem trị số X có giống như địa chỉ IP của thiết bị đầu cuối, hoặc xem trị số X có hiện có trong danh sách được lưu trữ của các địa chỉ IP của các thiết bị đầu cuối hay không, và nếu trị số X giống như địa chỉ IP của thiết bị đầu cuối hoặc trị số X hiện có trong danh sách được lưu trữ của các địa chỉ IP của các thiết bị đầu cuối, thiết bị đầu cuối được cho phép thiết lập phiên SSL thứ hai, và bước 17 được thực hiện, hoặc nếu trị số X khác với địa chỉ IP của thiết bị đầu cuối hoặc trị số X không hiện có trong danh sách được lưu trữ của các địa chỉ IP của các thiết bị đầu cuối, thiết bị đầu cuối không được cho phép thiết lập phiên SSL thứ hai, và

bước 16 được thực hiện.

Bước 16: thiết bị đầu cuối cố gắng thiết lập phiên SSL thứ hai với cổng VPN.

Bước 17: thiết bị đầu cuối và cổng VPN thiết lập thành công phiên SSL thứ hai, và sử dụng lại trực tiếp ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất được thiết lập giữa thiết bị đầu cuối và thiết bị điều khiển VPN.

Bước 18: thiết bị đầu cuối và cổng VPN thực hiện đóng gói dịch vụ và chuyển tiếp nhờ sử dụng phiên SSL thứ hai được thiết lập.

Phương án của sáng chế đề xuất thiết bị điều khiển VPN. Đối với sự thực hiện cụ thể của thiết bị điều khiển VPN, tham chiếu tới một số phần mô tả của phương án cho phương pháp nêu trên. Các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.9, thiết bị điều khiển VPN chủ yếu bao gồm bộ xử lý 901 và giao diện truyền thông 902. Cụ thể là, bộ xử lý 901 thực hiện các quá trình sau đây:

thu, nhờ sử dụng giao diện truyền thông, tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất;

sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và

thông báo, nhờ sử dụng giao diện truyền thông, thiết bị đầu cuối của địa chỉ IP của cổng VPN thứ nhất.

Phương án của đơn sáng chế này còn đề xuất cổng bộ định tuyến. Đối với sự thực hiện cụ thể của cổng bộ định tuyến, tham chiếu tới một số phần mô tả

của phương án cho phương pháp nêu trên. Các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.10, cổng bộ định tuyến bao gồm bộ xử lý 1001 và giao diện truyền thông 1002. Bộ xử lý 1001 thực hiện các quá trình sau đây theo chương trình:

thu, nhờ sử dụng giao diện truyền thông, tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

tạo tin nhắn bắt tay thứ nhất theo tin nhắn bắt tay thứ hai; và

gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN nhờ sử dụng giao diện truyền thông.

Phương án của sáng chế còn đề xuất thiết bị đầu cuối. Đối với sự thực hiện cụ thể của thiết bị đầu cuối, tham chiếu tới một số phần mô tả của phương án cho phương pháp nêu trên. Các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.11, thiết bị đầu cuối bao gồm bộ xử lý 1101 và giao diện truyền thông 1102. Cụ thể là, bộ xử lý 1101 thực hiện các quá trình sau đây:

gửi tin nhắn bắt tay thứ hai tới cổng bộ định tuyến nhờ sử dụng giao diện truyền thông, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN, và cổng bộ định tuyến gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN sau khi thu tin nhắn bắt tay thứ hai;

xác định, theo tin nhắn bắt tay thứ hai, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị điều khiển VPN, và yêu cầu, nhờ sử dụng phiên SSL thứ nhất, thiết bị điều khiển VPN để cố gắng xác thực thiết bị đầu cuối; và

thu, nhờ sử dụng giao diện truyền thông, địa chỉ IP mà là của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó và được thông báo bởi thiết bị điều khiển VPN, mà ở đó địa chỉ IP của cổng VPN thứ nhất được xác định bởi thiết bị điều khiển VPN sau khi thiết bị đầu cuối được xác thực.

Nếu thiết bị đầu cuối là thiết bị đầu cuối IPC, thiết bị đầu cuối còn bao

gồm môđun thu thập viđeo.

Phương án của sáng chế đề xuất thiết bị điều khiển VPN. Đối với sự thực hiện cụ thể của thiết bị điều khiển VPN, tham chiếu tới một số phần mô tả của phương án cho phương pháp nêu trên. các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.12, thiết bị điều khiển VPN bao gồm:

môđun thu 1201, được tạo cấu hình để thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

môđun xác thực 1202, được tạo cấu hình để: xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất;

môđun xác định 1203, được tạo cấu hình để: sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó; và

môđun thông báo 1204, được tạo cấu hình để thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất.

Cụ thể là, các chức năng của môđun thu 1201 và môđun thông báo 1204 có thể được thực hiện bởi giao diện truyền thông 902 của thiết bị điều khiển VPN, và các chức năng của môđun xác thực 1202 và môđun xác định 1203 có thể được thực hiện bởi bộ xử lý 901 của thiết bị điều khiển VPN.

Phương án của sáng chế đề xuất cổng bộ định tuyến. Đối với sự thực hiện cụ thể của cổng bộ định tuyến, tham chiếu tới một số phần mô tả của phương án cho phương pháp nêu trên. Các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.13, cổng bộ định tuyến bao gồm:

môđun thu 1301, được tạo cấu hình để thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi

tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN;

môđun xử lý 1302, được tạo cấu hình để tạo tin nhắn bắt tay thứ nhất theo tin nhắn bắt tay thứ hai; và

môđun gửi 1303, được tạo cấu hình để gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN.

Cụ thể là, các chức năng của môđun thu 1301 và môđun gửi 1303 được thực hiện bởi giao diện truyền thông 1002 của cổng bộ định tuyến, và chức năng của môđun xử lý 1302 được thực hiện bởi bộ xử lý 1001 của cổng bộ định tuyến.

Phương án của sáng chế đề xuất thiết bị đầu cuối. Đối với sự thực hiện cụ thể của thiết bị đầu cuối, tham chiếu tới một số phần mô tả của phương án cho phương pháp nêu trên. Các phần lặp lại không được mô tả lại. Như được thể hiện trên Fig.14, thiết bị đầu cuối bao gồm:

môđun gửi 1401, được tạo cấu hình để: gửi tin nhắn bắt tay thứ hai tới cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN, và cổng bộ định tuyến gửi tin nhắn bắt tay thứ nhất tới thiết bị điều khiển VPN sau khi thu tin nhắn bắt tay thứ hai;

môđun xử lý 1402, được tạo cấu hình để: xác định, theo tin nhắn bắt tay thứ hai, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị điều khiển VPN, và yêu cầu, nhờ sử dụng phiên SSL thứ nhất, thiết bị điều khiển VPN để cố gắng xác thực thiết bị đầu cuối; và

môđun thu 1403, được tạo cấu hình để thu địa chỉ IP mà là của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó và được thông báo bởi thiết bị điều khiển VPN, mà ở đó địa chỉ IP của cổng VPN thứ nhất được xác định bởi thiết bị điều khiển VPN sau khi thiết bị đầu cuối được xác thực.

Cụ thể là, các chức năng của môđun gửi 1401 và môđun thu 1403 được thực hiện bởi giao diện truyền thông 1102 của thiết bị đầu cuối, và chức năng của môđun xử lý 1402 được thực hiện bởi bộ xử lý 1101 của thiết bị đầu cuối.

Chuyên gia trong lĩnh vực kỹ thuật sẽ hiểu rằng các phương án của sáng chế có thể được đề xuất làm phương pháp, hệ thống, hoặc sản phẩm chương trình máy tính. Do đó, sáng chế có thể sử dụng dạng phương án chỉ dùng phần cứng, phương án chỉ dùng phần mềm, hoặc các phương án dưới dạng kết hợp của phần mềm và phần cứng. Hơn nữa, sáng chế có thể sử dụng dạng sản phẩm chương trình máy tính mà được thực hiện trên một hoặc nhiều hơn một phương tiện lưu trữ sử dụng được bằng máy tính (bao gồm nhưng không giới hạn ở bộ nhớ dạng đĩa, CD-ROM, bộ nhớ quang, và tương tự) mà bao gồm mã chương trình sử dụng được bằng máy tính.

Sáng chế được mô tả có viện dẫn tới các lưu đồ và/hoặc các sơ đồ khối của phương pháp, thiết bị (hệ thống), và sản phẩm chương trình máy tính theo các phương án của sáng chế. Được hiểu rằng các lệnh chương trình máy tính có thể được sử dụng để thực hiện mỗi quá trình và/hoặc mỗi khối trong các lưu đồ và/hoặc các sơ đồ khối và dạng kết hợp của quá trình và/hoặc khối trong các lưu đồ và/hoặc các sơ đồ khối. Các lệnh chương trình máy tính này có thể được tạo ra cho máy tính thông dụng hoặc bộ xử lý thiết bị xử lý dữ liệu lập trình được khác bất kỳ để tạo ra máy tính, sao cho các lệnh được thực hiện bởi máy tính hoặc bộ xử lý của thiết bị xử lý dữ liệu lập trình được khác bất kỳ tạo ra thiết bị dùng để thực hiện chức năng cụ thể trong một hoặc nhiều hơn một quá trình trong các lưu đồ và/hoặc trong một hoặc nhiều hơn một khối trong các sơ đồ khối.

Các lệnh chương trình máy tính này có thể được tải vào máy tính hoặc thiết bị xử lý dữ liệu lập trình được khác, sao cho chuỗi thao tác và các bước được thực hiện trên máy tính hoặc thiết bị lập trình được khác, nhờ đó tạo ra xử lý được thực hiện bằng máy tính. Do đó, các lệnh được thực hiện trên máy tính hoặc thiết bị lập trình được khác tạo ra các bước dùng để thực hiện chức năng cụ thể trong một hoặc nhiều hơn một quá trình trong các lưu đồ và/hoặc trong một hoặc nhiều hơn một khối trong các sơ đồ khối.

Hiển nhiên là, chuyên gia trong lĩnh vực kỹ thuật có thể tạo ra các cải biến và các sự điều chỉnh cho sáng chế mà không chệch khỏi phạm vi của sáng chế.

Sáng chế có mục đích bao gồm các cải biến và các điều chỉnh này miễn là chúng nằm trong phạm vi bảo hộ được xác định bởi yêu cầu bảo hộ sau đây.

YÊU CẦU BẢO HỘ

1. Phương pháp được sử dụng bởi thiết bị đầu cuối để kết nối với mạng riêng ảo (Virtual Private Network, viết tắt là VPN) bao gồm các bước:

thu (201), bởi thiết bị điều khiển VPN, tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, trong đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quy trình thỏa thuận của phiên lớp ổ bảo mật (Secure Sockets Layer, viết tắt là SSL) thứ nhất đến thiết bị điều khiển VPN;

xác định (202), bởi thiết bị điều khiển VPN theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối bằng cách sử dụng phiên SSL thứ nhất;

sau khi thiết bị đầu cuối được xác thực, xác định (203), bởi thiết bị điều khiển VPN, địa chỉ giao thức Internet (Internet Protocol, viết tắt là IP) của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối; và

thông báo (204), bởi thiết bị điều khiển VPN, cho thiết bị đầu cuối về địa chỉ IP của cổng VPN thứ nhất, trong đó tin nhắn bắt tay thứ nhất mang mục nhập định tuyến trực tiếp của cổng bộ định tuyến, và mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được đặt trên cổng bộ định tuyến trong chế độ nối tắt; và

bước xác định, bởi thiết bị điều khiển VPN, địa chỉ IP của cổng VPN thứ nhất bao gồm bước:

thu nhận, bởi thiết bị điều khiển VPN từ danh sách của các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

2. Phương pháp theo điểm 1, trong đó phương pháp này còn bao gồm các bước: thông báo, bởi thiết bị điều khiển VPN, cho cổng VPN thứ nhất của địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, trong đó cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa.

3. Phương pháp theo điểm 1 hoặc 2, trong đó phương pháp này còn bao gồm bước:

gửi, bởi thiết bị đầu cuối, tin nhắn bắt tay thứ ba đến cổng VPN thứ nhất, trong đó tin nhắn bắt tay thứ ba được sử dụng để khởi tạo quy trình thỏa thuận của phiên SSL thứ hai đến cổng VPN thứ nhất, tin nhắn bắt tay thứ ba mang ký hiệu nhận dạng phiên và văn bản mã hóa, và văn bản mã hóa được tạo ra bằng cách mã hóa địa chỉ IP của thiết bị đầu cuối bằng cách sử dụng khóa phiên và thuật toán mã hóa.

4. Phương pháp theo điểm bất kỳ trong số các điểm từ 1 đến 3, trong đó bước cố gắng, bởi thiết bị điều khiển VPN, để xác thực thiết bị đầu cuối bằng cách sử dụng phiên SSL thứ nhất bao gồm các bước:

thu, bởi thiết bị điều khiển VPN bằng cách sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối, trong đó tin nhắn xác thực mang ký hiệu nhận dạng phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã hóa ký hiệu nhận dạng của thiết bị đầu cuối bằng cách sử dụng thuật toán mã hóa và khóa phiên;

phân tích, bởi thiết bị điều khiển VPN, tin nhắn xác thực để thu nhận ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực; sau khi xác định rằng thiết bị điều khiển VPN lưu trữ ký hiệu nhận dạng phiên, giải mã dữ liệu xác thực bằng cách sử dụng khóa phiên và thuật toán mã hóa, để thu nhận ký hiệu nhận dạng của thiết bị đầu cuối; và gửi ký hiệu nhận dạng của thiết bị đầu cuối đến máy chủ xác thực; và

nếu bước thu tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, xác định, bởi thiết bị điều khiển VPN, rằng sự truy cập của thiết bị đầu cuối

được cho phép, trong đó tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực sau khi máy chủ xác thực xác định rằng ký hiệu nhận dạng của thiết bị đầu cuối tồn tại; hoặc nếu thu tin nhắn lỗi xác thực được phản hồi bởi máy chủ xác thực, xác định, bởi thiết bị điều khiển VPN, rằng sự truy cập của thiết bị đầu cuối không được cho phép.

5. Hệ thống được sử dụng bởi thiết bị đầu cuối để kết nối với mạng riêng ảo (VPN) bao gồm:

thiết bị đầu cuối (101), được tạo cấu hình để gửi tin nhắn bắt tay thứ hai đến cổng bộ định tuyến (103), trong đó tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quy trình thỏa thuận của phiên lớp ổ bảo mật (SSL) thứ nhất đến thiết bị điều khiển VPN (104);

cổng bộ định tuyến, được tạo cấu hình để gửi tin nhắn bắt tay thứ nhất đến thiết bị điều khiển VPN sau khi thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối; và

thiết bị điều khiển VPN, được tạo cấu hình để: thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối bằng cách sử dụng phiên SSL thứ nhất; sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ giao thức Internet (IP) của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối; và thông báo cho thiết bị đầu cuối về địa chỉ IP của cổng VPN thứ nhất, trong đó cổng bộ định tuyến được tạo cấu hình cụ thể để:

bổ sung mục nhập định tuyến trực tiếp đến tin nhắn bắt tay thứ hai để thu nhận tin nhắn bắt tay thứ nhất, trong đó mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được đặt trên cổng bộ định tuyến trong chế độ nối tắt; và

thiết bị điều khiển VPN được tạo cấu hình cụ thể để:

thu nhận, từ danh sách của các địa chỉ IP được tạo cấu hình của tất cả các

cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

6. Hệ thống theo điểm 5, trong đó thiết bị điều khiển VPN còn được tạo cấu hình để:

thông báo cho cổng VPN thứ nhất về địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất; và

cổng VPN thứ nhất được tạo cấu hình cụ thể để:

lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, trong đó thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa.

7. Hệ thống theo điểm 5 hoặc 6, trong đó thiết bị đầu cuối còn được tạo cấu hình để:

gửi tin nhắn bắt tay thứ ba đến cổng VPN thứ nhất, trong đó tin nhắn bắt tay thứ ba được sử dụng để khởi tạo quy trình thỏa thuận của phiên SSL thứ hai đến cổng VPN thứ nhất, tin nhắn bắt tay thứ ba mang ký hiệu nhận dạng phiên và văn bản mã hóa, và văn bản mã hóa được tạo ra bằng cách mã hóa địa chỉ IP của thiết bị đầu cuối bằng cách sử dụng khóa phiên và thuật toán mã hóa.

8. Hệ thống theo điểm bất kỳ trong số các điểm từ 5 đến 7, trong đó thiết bị đầu cuối được tạo cấu hình cụ thể để:

gửi tin nhắn xác thực đến thiết bị điều khiển VPN bằng cách sử dụng phiên SSL thứ nhất, trong đó tin nhắn xác thực mang ký hiệu nhận dạng phiên và dữ liệu xác thực, và dữ liệu xác thực thu được bằng cách mã hóa ký hiệu nhận dạng của thiết bị đầu cuối bằng cách sử dụng thuật toán mã hóa và khóa phiên;

thiết bị điều khiển VPN được tạo cấu hình cụ thể để:

thu, bằng cách sử dụng phiên SSL thứ nhất, tin nhắn xác thực được gửi bởi thiết bị đầu cuối; phân tích tin nhắn xác thực để thu nhận ký hiệu nhận dạng phiên và dữ liệu xác thực mà được mang trong tin nhắn xác thực; sau khi xác định rằng

thiết bị điều khiển VPN lưu trữ ký hiệu nhận dạng phiên, giải mã dữ liệu xác thực bằng cách sử dụng khóa phiên và thuật toán mã hóa, để thu nhận ký hiệu nhận dạng của thiết bị đầu cuối; và gửi ký hiệu nhận dạng của thiết bị đầu cuối đến máy chủ xác thực;

máy chủ xác thực được tạo cấu hình cụ thể để:

thu ký hiệu nhận dạng của thiết bị đầu cuối được gửi bởi thiết bị điều khiển VPN, và nếu xác định rằng máy chủ xác thực lưu trữ ký hiệu nhận dạng của thiết bị đầu cuối, phản hồi tin nhắn thành công xác thực đến thiết bị điều khiển VPN; hoặc nếu xác định rằng máy chủ xác thực không lưu trữ ký hiệu nhận dạng của thiết bị đầu cuối, phản hồi tin nhắn lỗi xác thực đến thiết bị điều khiển VPN; và

thiết bị điều khiển VPN được tạo cấu hình cụ thể để:

nếu bước thu tin nhắn thành công xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối được cho phép; hoặc nếu thu tin nhắn lỗi xác thực được phản hồi bởi máy chủ xác thực, xác định rằng sự truy cập của thiết bị đầu cuối không được cho phép.

9. Thiết bị điều khiển mạng riêng ảo (VPN) bao gồm:

môđun thu (1201), được tạo cấu hình để thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, trong đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quy trình thỏa thuận của phiên lớp ổ bảo mật (SSL) thứ nhất đến thiết bị điều khiển VPN;

môđun xác thực (1202), được tạo cấu hình để: xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối bằng cách sử dụng phiên SSL thứ nhất;

môđun xác định (1203), được tạo cấu hình để: sau khi thiết bị đầu cuối được xác thực, xác định địa chỉ giao thức Internet (IP) của cổng VPN thứ nhất mà thiết

bị đầu cuối được cho phép kết nối; và

môđun thông báo (1204), được tạo cấu hình để thông báo cho thiết bị đầu cuối về địa chỉ IP của cổng VPN thứ nhất, trong đó tin nhắn bắt tay thứ nhất mang mục nhập định tuyến trực tiếp của cổng bộ định tuyến, và mục nhập định tuyến trực tiếp bao gồm tiền tố mạng con của cổng VPN mà được đặt trên cổng bộ định tuyến trong chế độ nối tắt; và

môđun xác định có cấu trúc cụ thể để:

thu nhận, từ danh sách của các địa chỉ IP được tạo cấu hình của tất cả các cổng VPN, địa chỉ IP của cổng VPN mà thuộc về tiền tố mạng con, của cổng VPN, được bao gồm trong mục nhập định tuyến trực tiếp, và xác định địa chỉ IP thu được của cổng VPN làm địa chỉ IP của cổng VPN thứ nhất.

10. Thiết bị điều khiển VPN theo điểm 9, trong đó môđun thông báo còn được tạo cấu hình để:

thông báo cho cổng VPN thứ nhất về địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, trong đó cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối và thông số phiên của phiên SSL thứ nhất, và thông số phiên bao gồm khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa.

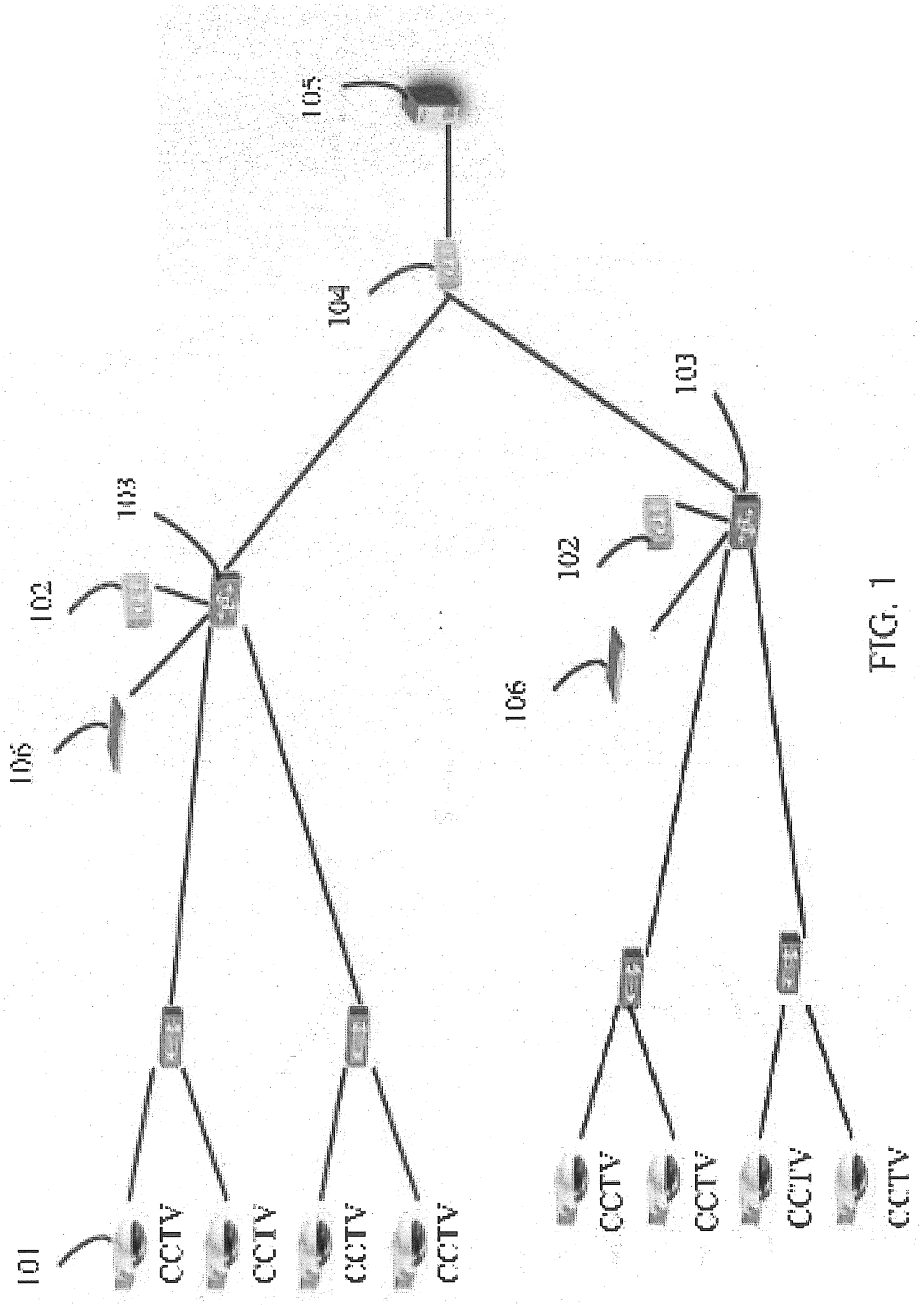

105
104
103
102
106
101
CCTV
CCTV
CCTV
CCTV
CCTV
CCTV
CCTV
CCTV

FIG. 1

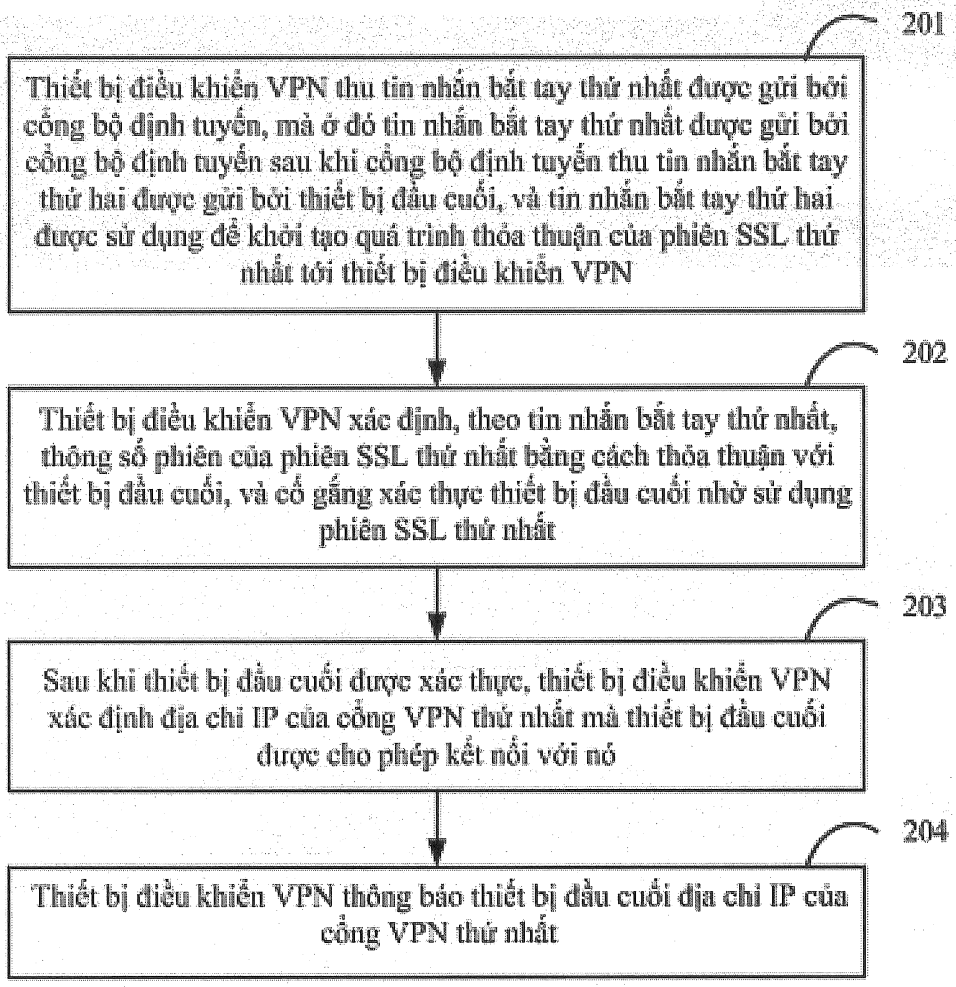

201
Thiết bị điều khiển VPN thu tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến, mà ở đó tin nhắn bắt tay thứ nhất được gửi bởi cổng bộ định tuyến sau khi cổng bộ định tuyến thu tin nhắn bắt tay thứ hai được gửi bởi thiết bị đầu cuối, và tin nhắn bắt tay thứ hai được sử dụng để khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN
202
Thiết bị điều khiển VPN xác định, theo tin nhắn bắt tay thứ nhất, thông số phiên của phiên SSL thứ nhất bằng cách thỏa thuận với thiết bị đầu cuối, và cố gắng xác thực thiết bị đầu cuối nhờ sử dụng phiên SSL thứ nhất
203
Sau khi thiết bị đầu cuối được xác thực, thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó
204
Thiết bị điều khiển VPN thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất

FIG. 2

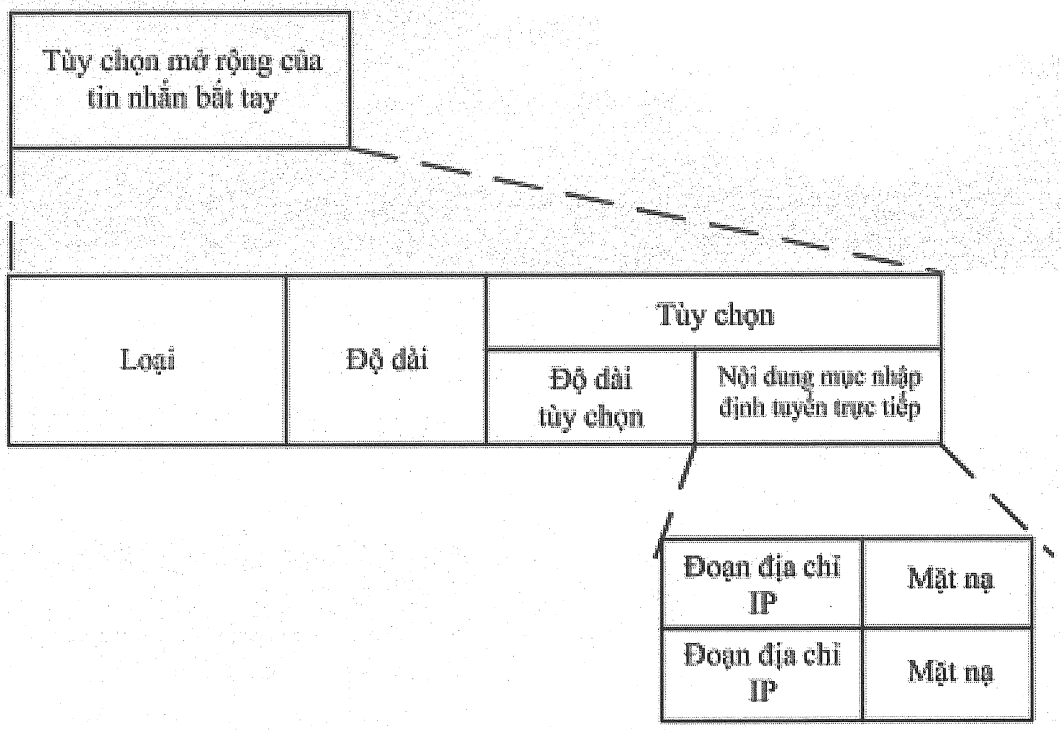

Tùy chọn mở rộng của tin nhắn bắt tay
Loại
Độ dài
Tùy chọn
Độ dài tùy chọn
Nội dung mục nhập định tuyến trực tiếp
Đoạn địa chỉ IP
Mặt nạ
Đoạn địa chỉ IP
Mặt nạ

FIG. 3

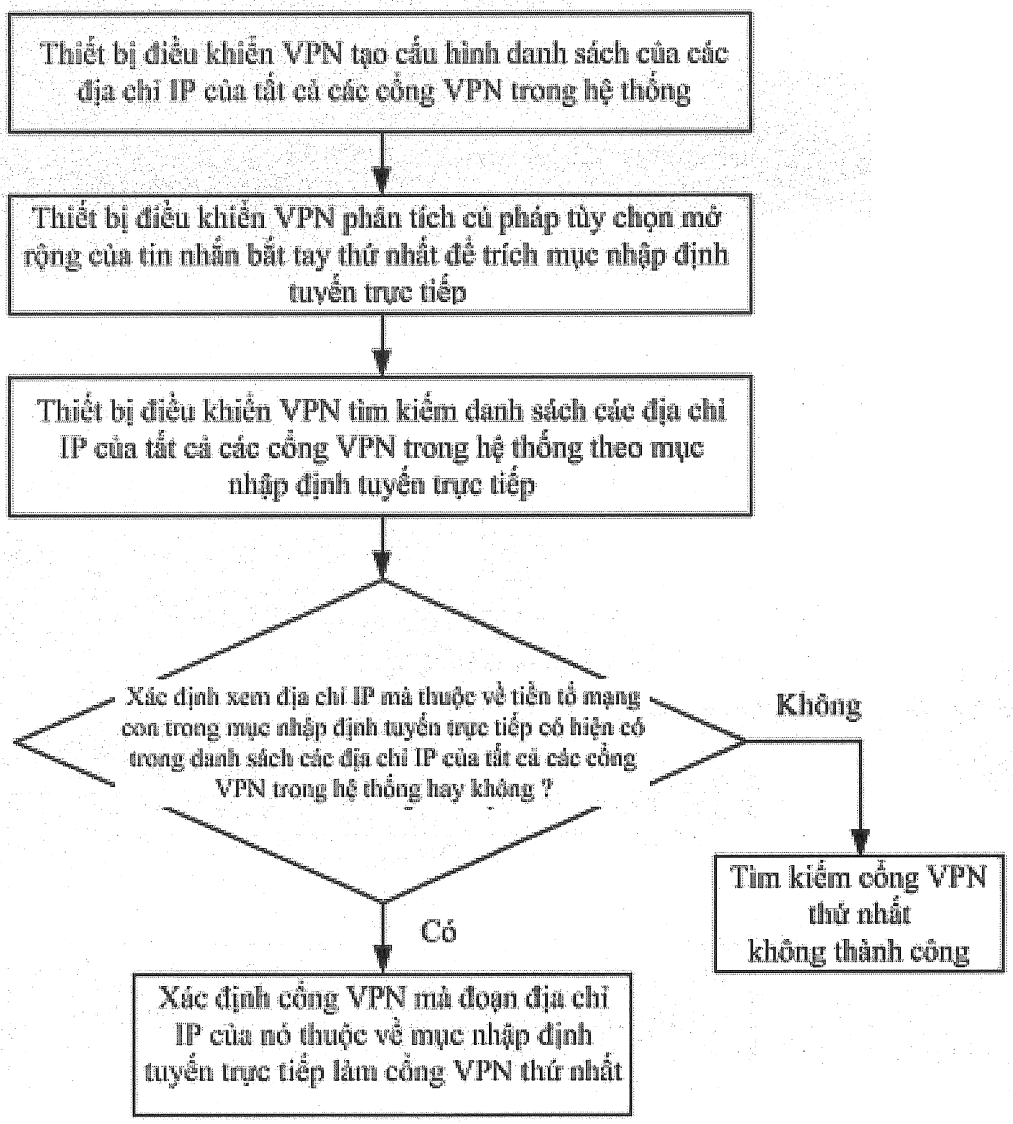

Thiết bị điều khiển VPN tạo cấu hình danh sách của các địa chỉ IP của tất cả các cổng VPN trong hệ thống
Thiết bị điều khiển VPN phân tích cú pháp tùy chọn mở rộng của tin nhắn bắt tay thứ nhất để trích mục nhập định tuyến trực tiếp
Thiết bị điều khiển VPN tìm kiếm danh sách các địa chỉ IP của tất cả các cổng VPN trong hệ thống theo mục nhập định tuyến trực tiếp
Xác định xem địa chỉ IP mà thuộc về tiền tố mạng con trong mục nhập định tuyến trực tiếp có hiện có trong danh sách các địa chỉ IP của tất cả các cổng VPN trong hệ thống hay không ?
Không
Tìm kiếm cổng VPN thứ nhất không thành công
Có
Xác định cổng VPN mà đoạn địa chỉ IP của nó thuộc về mục nhập định tuyến trực tiếp làm cổng VPN thứ nhất

FIG. 4

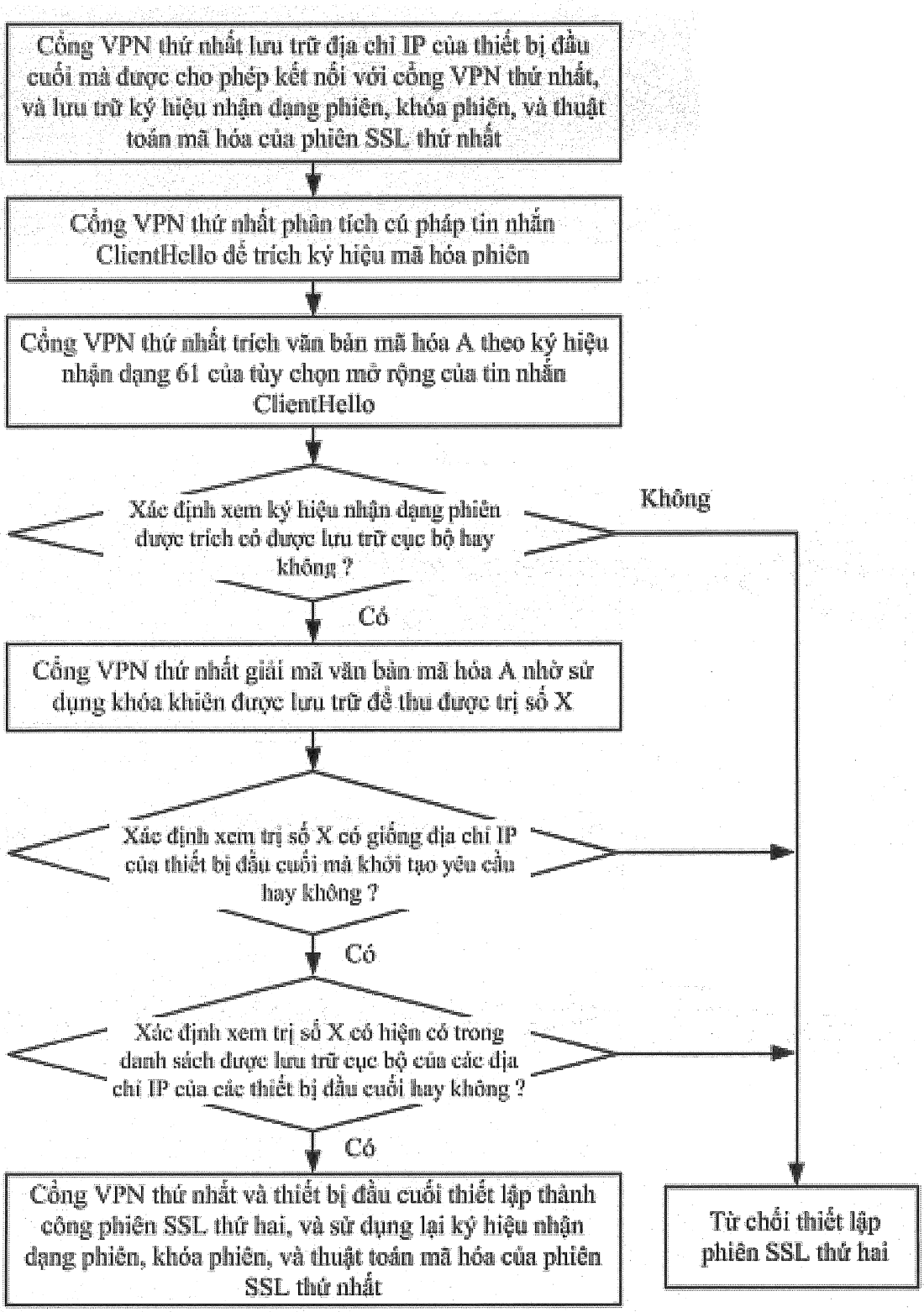

Cổng VPN thứ nhất lưu trữ địa chỉ IP của thiết bị đầu cuối mà được cho phép kết nối với cổng VPN thứ nhất, và lưu trữ ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất
Cổng VPN thứ nhất phân tích cú pháp tin nhắn ClientHello để trích ký hiệu mã hóa phiên
Cổng VPN thứ nhất trích văn bản mã hóa A theo ký hiệu nhận dạng 61 của tùy chọn mở rộng của tin nhắn ClientHello
Xác định xem ký hiệu nhận dạng phiên được trích có được lưu trữ cục bộ hay không ?
Không
Có
Cổng VPN thứ nhất giải mã văn bản mã hóa A nhờ sử dụng khóa khiên được lưu trữ để thu được trị số X
Xác định xem trị số X có giống địa chỉ IP của thiết bị đầu cuối mà khởi tạo yêu cầu hay không ?
Có
Xác định xem trị số X có hiện có trong danh sách được lưu trữ cục bộ của các địa chỉ IP của các thiết bị đầu cuối hay không ?
Có
Cổng VPN thứ nhất và thiết bị đầu cuối thiết lập thành công phiên SSL thứ hai, và sử dụng lại ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất
Từ chối thiết lập phiên SSL thứ hai

FIG. 5

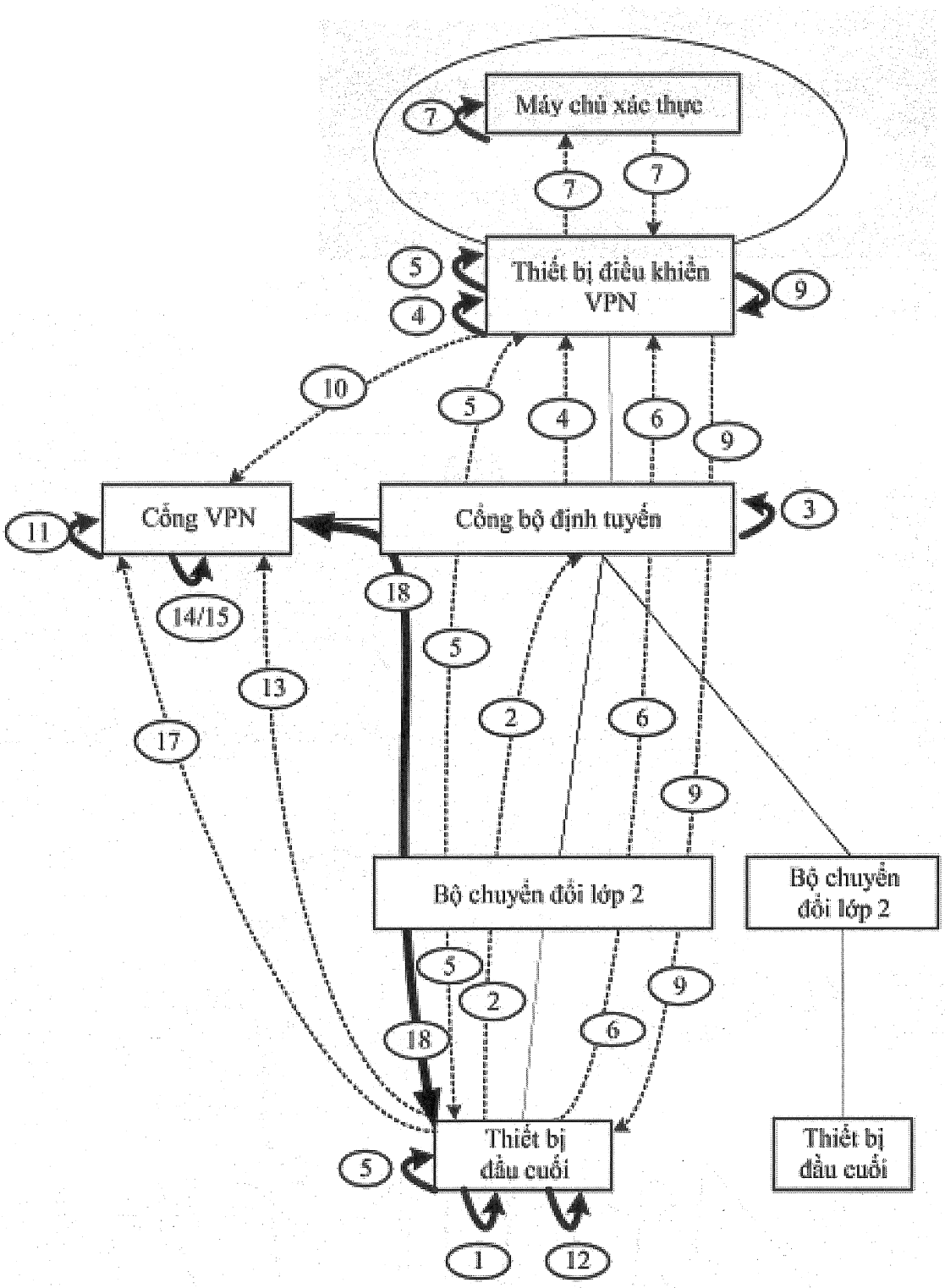

Máy chủ xác thực
Thiết bị điều khiển VPN
Cổng VPN
Cổng bộ định tuyến
Bộ chuyển đổi lớp 2
Bộ chuyển đổi lớp 2
Thiết bị đầu cuối
Thiết bị đầu cuối
1
2
3
4
5
6
7
9
10
11
12
13
14/15
17
18

FIG. 6

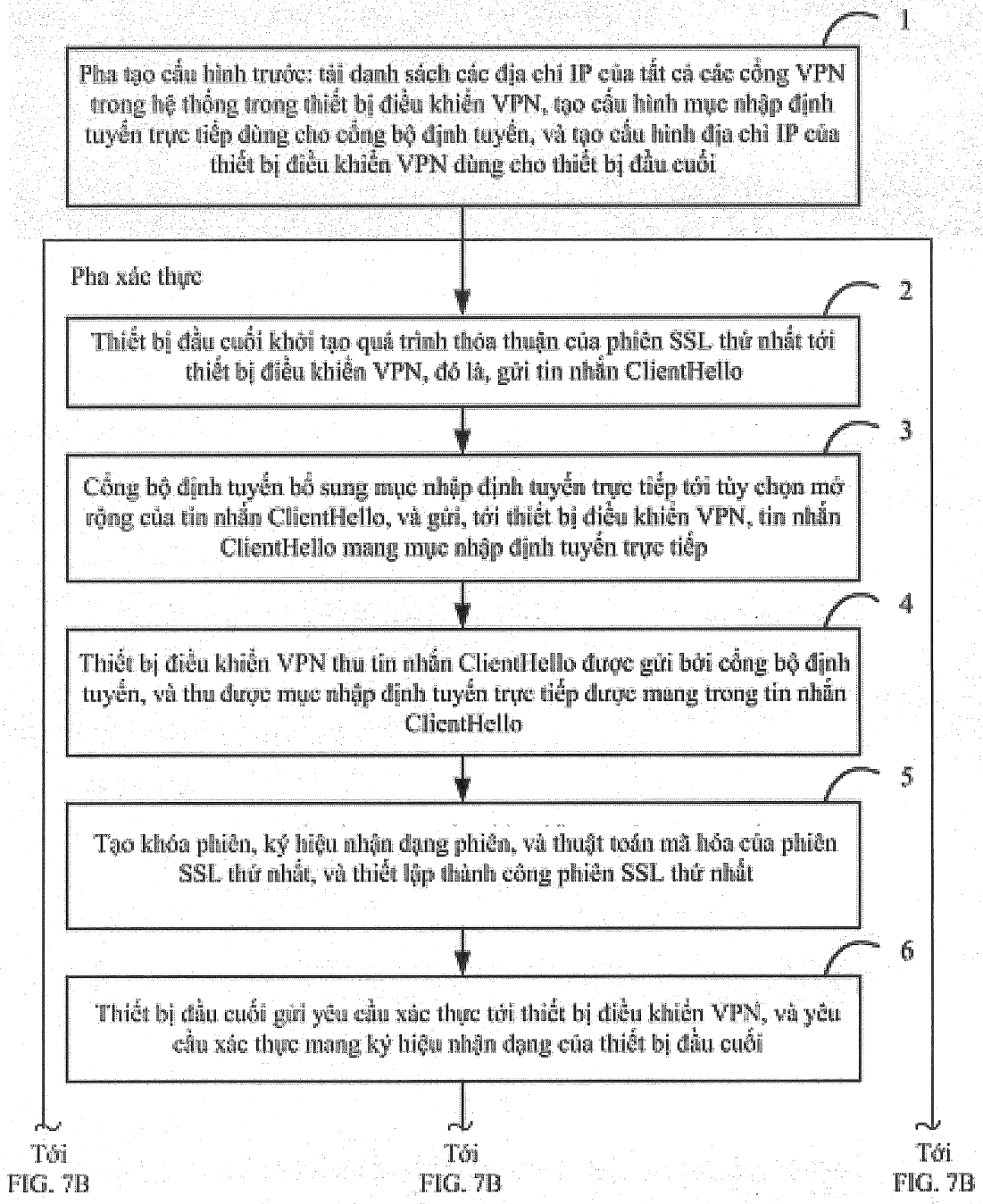

1
Pha tạo cấu hình trước: tải danh sách các địa chỉ IP của tất cả các cổng VPN trong hệ thống trong thiết bị điều khiển VPN, tạo cấu hình mục nhập định tuyến trực tiếp dùng cho cổng bộ định tuyến, và tạo cấu hình địa chỉ IP của thiết bị điều khiển VPN dùng cho thiết bị đầu cuối
Pha xác thực
2
Thiết bị đầu cuối khởi tạo quá trình thỏa thuận của phiên SSL thứ nhất tới thiết bị điều khiển VPN, đó là, gửi tin nhắn ClientHello
3
Cổng bộ định tuyến bổ sung mục nhập định tuyến trực tiếp tới tùy chọn mở rộng của tin nhắn ClientHello, và gửi, tới thiết bị điều khiển VPN, tin nhắn ClientHello mang mục nhập định tuyến trực tiếp
4
Thiết bị điều khiển VPN thu tin nhắn ClientHello được gửi bởi cổng bộ định tuyến, và thu được mục nhập định tuyến trực tiếp được mang trong tin nhắn ClientHello
5
Tạo khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa của phiên SSL thứ nhất, và thiết lập thành công phiên SSL thứ nhất
6
Thiết bị đầu cuối gửi yêu cầu xác thực tới thiết bị điều khiển VPN, và yêu cầu xác thực mang ký hiệu nhận dạng của thiết bị đầu cuối
Tới FIG. 7B
Tới FIG. 7B
Tới FIG. 7B

FIG. 7A

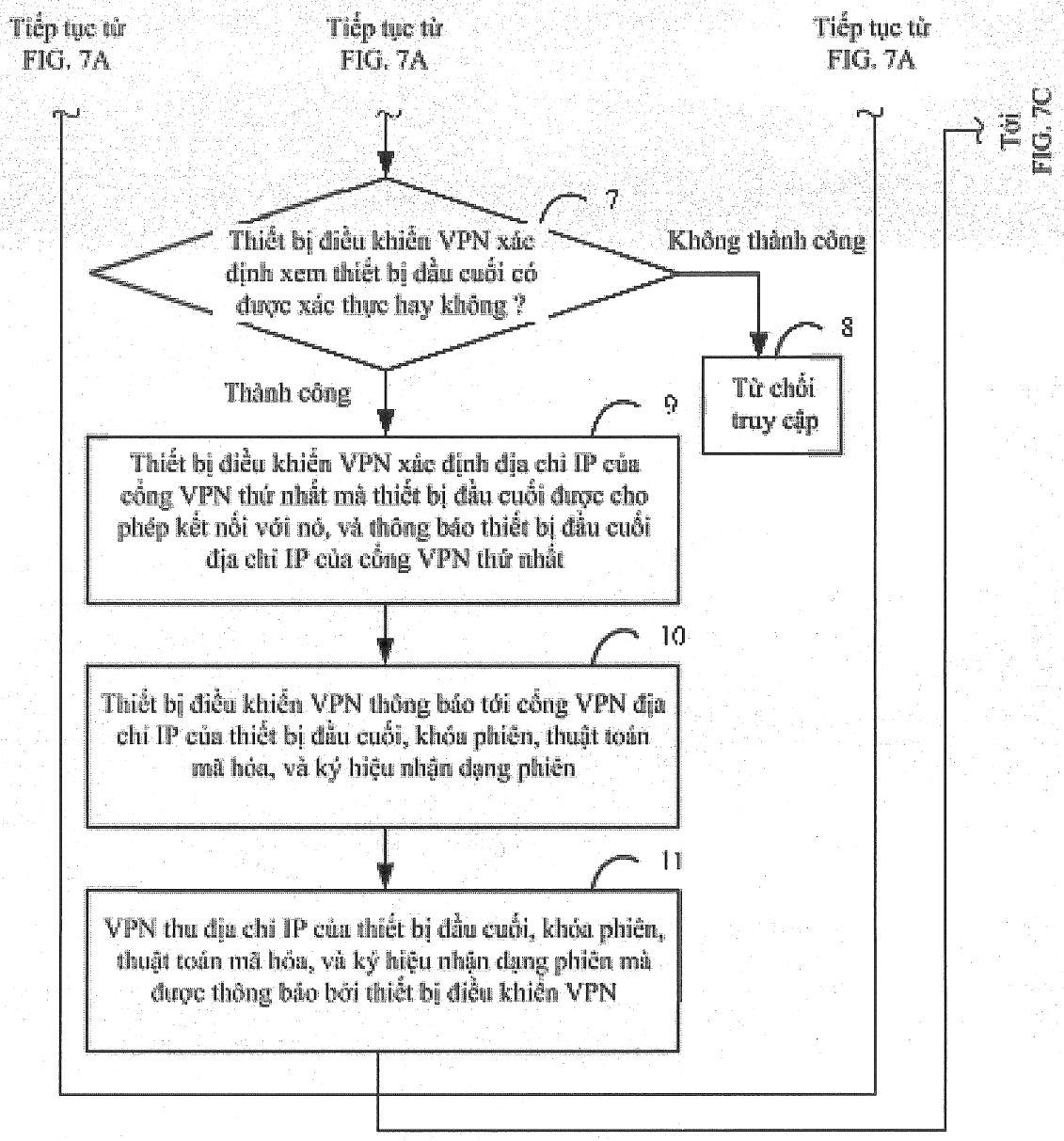

Tiếp tục từ FIG. 7A
Tiếp tục từ FIG. 7A
Tiếp tục từ FIG. 7A
Tới FIG. 7C
7
Thiết bị điều khiển VPN xác định xem thiết bị đầu cuối có được xác thực hay không ?
Không thành công
8
Từ chối truy cập
Thành công
9
Thiết bị điều khiển VPN xác định địa chỉ IP của cổng VPN thứ nhất mà thiết bị đầu cuối được cho phép kết nối với nó, và thông báo thiết bị đầu cuối địa chỉ IP của cổng VPN thứ nhất
10
Thiết bị điều khiển VPN thông báo tới cổng VPN địa chỉ IP của thiết bị đầu cuối, khóa phiên, thuật toán mã hóa, và ký hiệu nhận dạng phiên
11
VPN thu địa chỉ IP của thiết bị đầu cuối, khóa phiên, thuật toán mã hóa, và ký hiệu nhận dạng phiên mà được thông báo bởi thiết bị điều khiển VPN

FIG. 7B

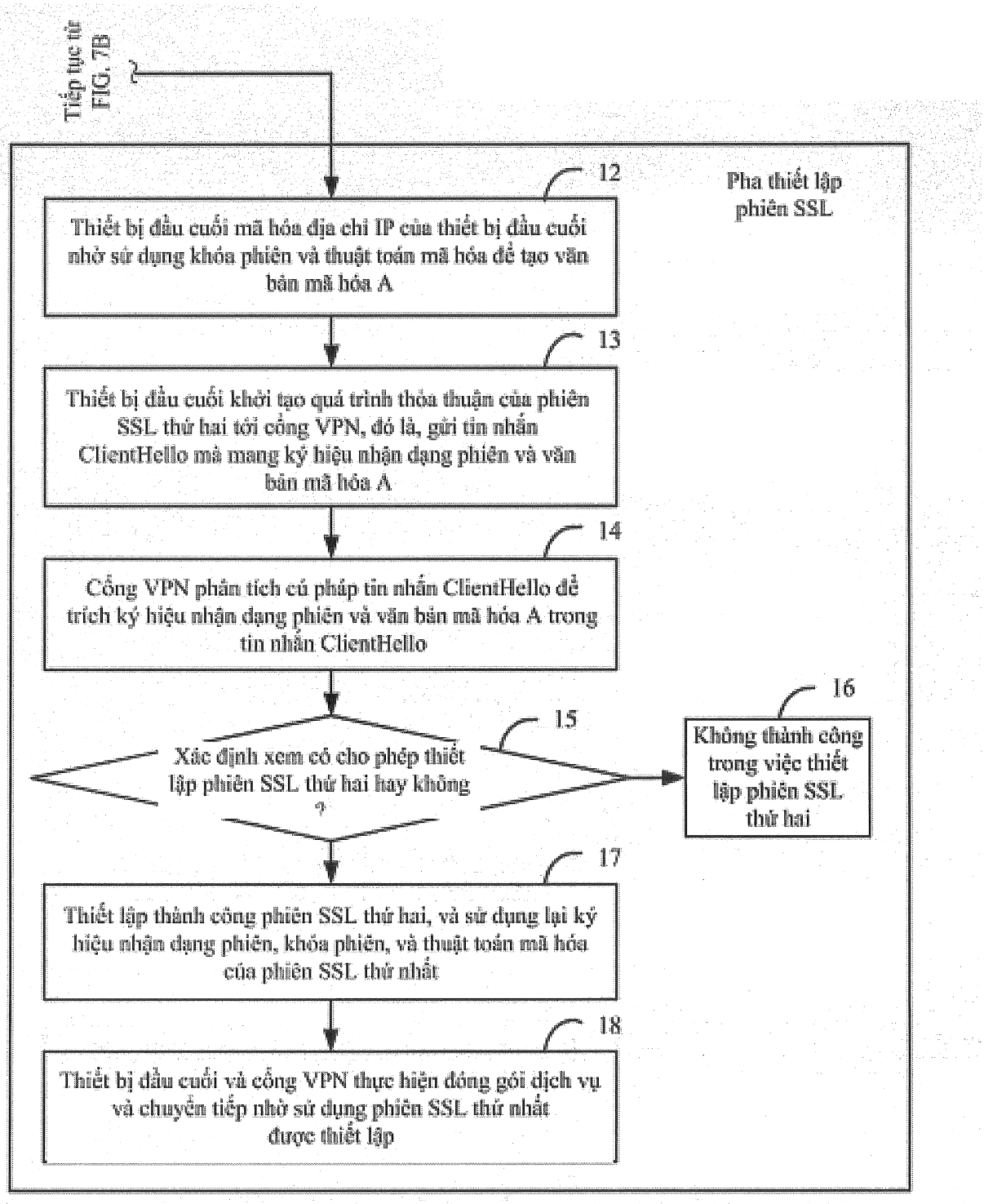

Tiếp tục từ FIG. 7B
Pha thiết lập phiên SSL
12
Thiết bị đầu cuối mã hóa địa chỉ IP của thiết bị đầu cuối nhờ sử dụng khóa phiên và thuật toán mã hóa để tạo văn bản mã hóa A
13
Thiết bị đầu cuối khởi tạo quá trình thỏa thuận của phiên SSL thứ hai tới cổng VPN, đó là, gửi tin nhắn ClientHello mà mang ký hiệu nhận dạng phiên và văn bản mã hóa A
14
Cổng VPN phân tích cú pháp tin nhắn ClientHello để trích ký hiệu nhận dạng phiên và văn bản mã hóa A trong tin nhắn ClientHello
15
Xác định xem có cho phép thiết lập phiên SSL thứ hai hay không ?
16
Không thành công trong việc thiết lập phiên SSL thứ hai
17
Thiết lập thành công phiên SSL thứ hai, và sử dụng lại ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa của phiên SSL thứ nhất
18
Thiết bị đầu cuối và cổng VPN thực hiện đóng gói dịch vụ và chuyển tiếp nhờ sử dụng phiên SSL thứ nhất được thiết lập

FIG. 7C

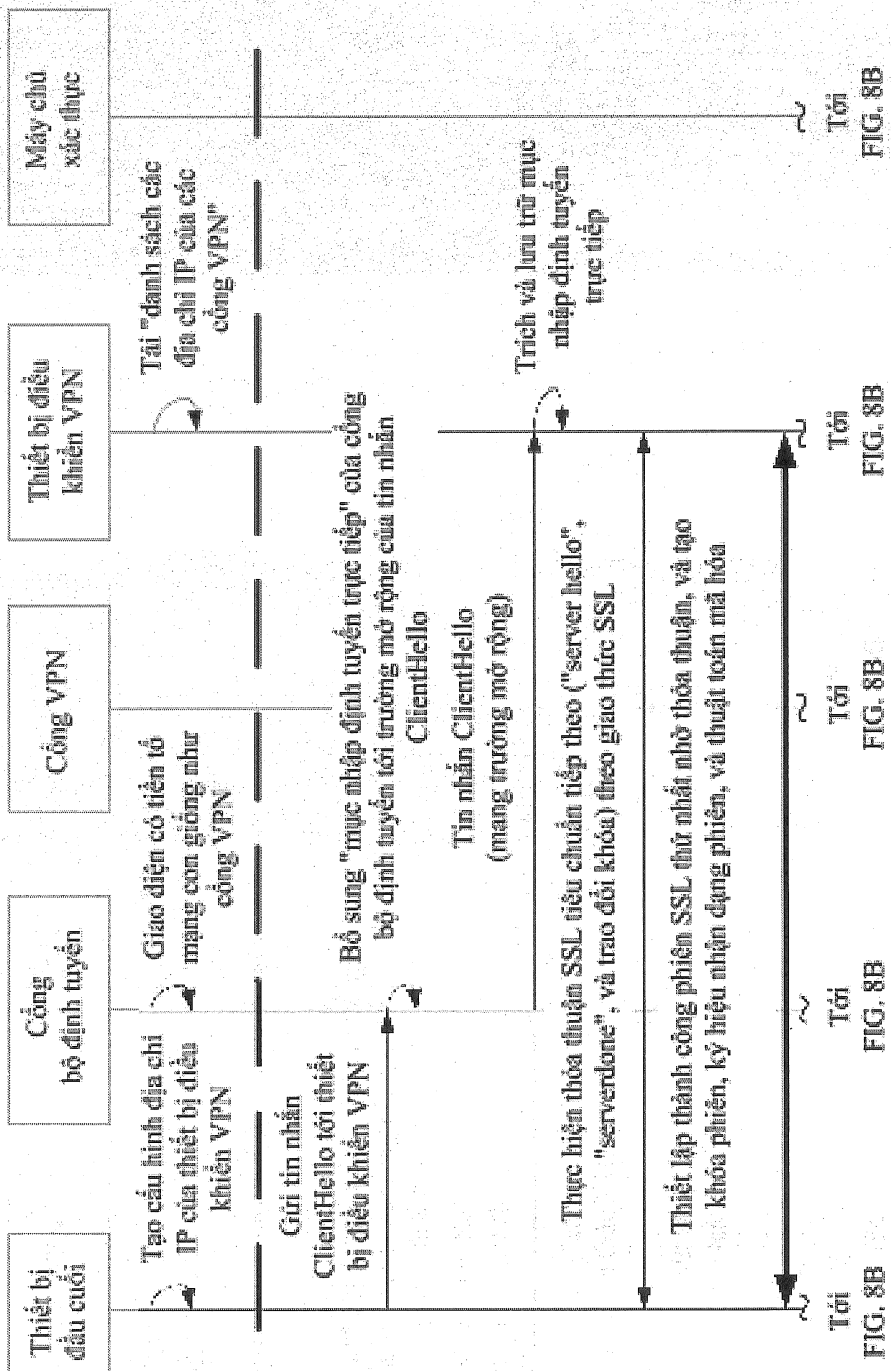

Thiết bị đầu cuối
Cổng bộ định tuyến
Cổng VPN
Thiết bị điều khiển VPN
Máy chủ xác thực
Pha chuẩn bị
Pha xác thực
Tạo cấu hình địa chỉ IP của thiết bị điều khiển VPN
Giao diện có tiền tố mạng con giống như cổng VPN
Tải "danh sách các địa chỉ IP của các cổng VPN"
Gửi tin nhắn ClientHello tới thiết bị điều khiển VPN
Bổ sung "mục nhập định tuyến trực tiếp" của cổng bộ định tuyến tới trường mở rộng của tin nhắn ClientHello
Tin nhắn ClientHello (mang trường mở rộng)
Trích và lưu trữ mục nhập định tuyến trực tiếp
Thực hiện thỏa thuận SSL tiêu chuẩn tiếp theo ("server hello", "serverdone", và trao đổi khóa) theo giao thức SSL
Thiết lập thành công phiên SSL thứ nhất nhờ thỏa thuận, và tạo khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa
Tới FIG. 8B
Tới FIG. 8B
Tới FIG. 8B
Tới FIG. 8B
Tới FIG. 8B

FIG. 8A

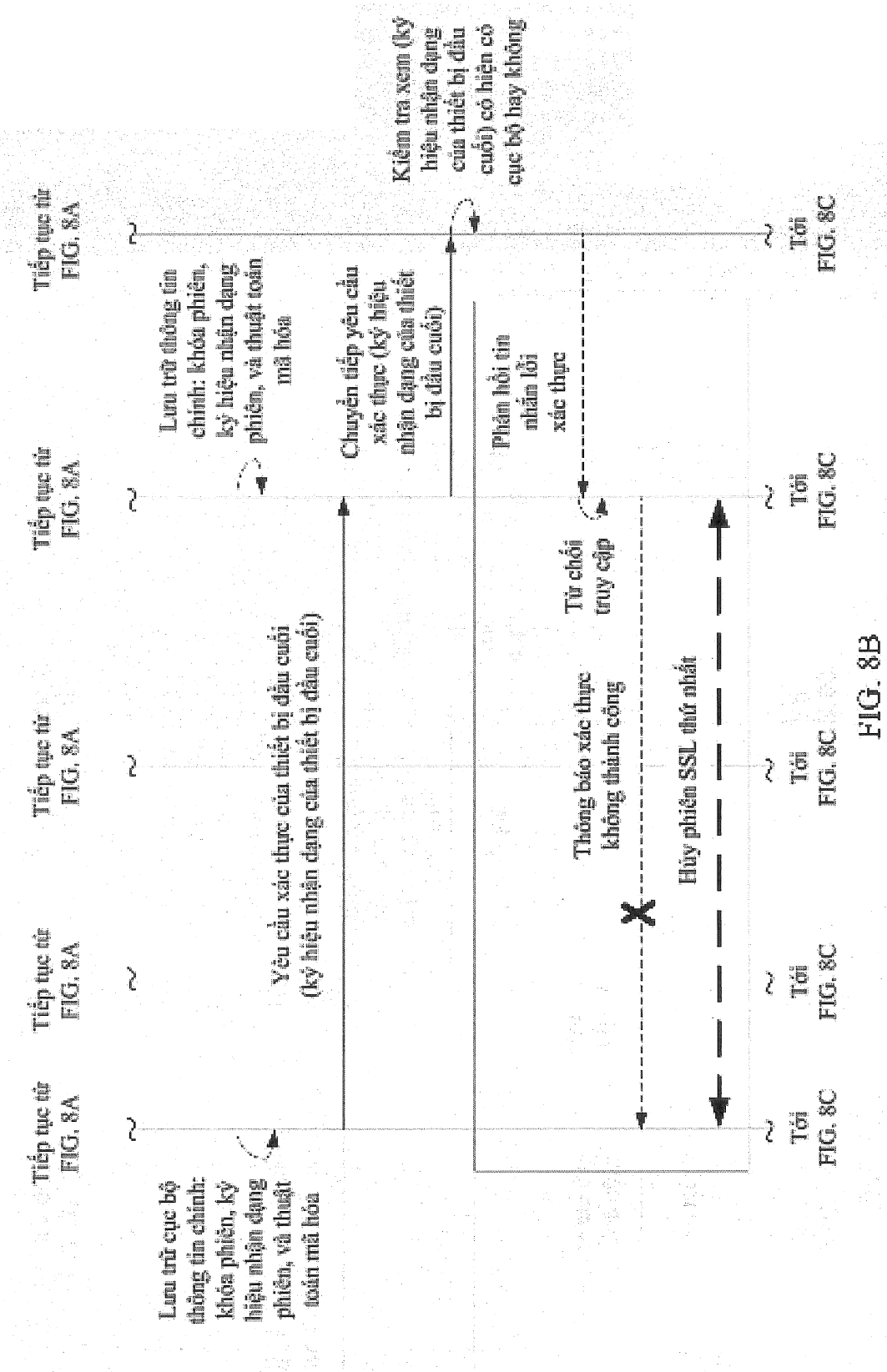

Tiếp tục từ FIG. 8A
Tiếp tục từ FIG. 8A
Tiếp tục từ FIG. 8A
Tiếp tục từ FIG. 8A
Tiếp tục từ FIG. 8A
Lưu trữ cục bộ thông tin chính: khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa
Yêu cầu xác thực của thiết bị đầu cuối (ký hiệu nhận dạng của thiết bị đầu cuối)
Lưu trữ thông tin chính: khóa phiên, ký hiệu nhận dạng phiên, và thuật toán mã hóa
Chuyển tiếp yêu cầu xác thực (ký hiệu nhận dạng của thiết bị đầu cuối)
Kiểm tra xem (ký hiệu nhận dạng của thiết bị đầu cuối) có hiện có cục bộ hay không
Phản hồi tin nhắn lỗi xác thực
Từ chối truy cập
Thông báo xác thực không thành công
Hủy phiên SSL thứ nhất
Tới FIG. 8C
Tới FIG. 8C
Tới FIG. 8C
Tới FIG. 8C
Tới FIG. 8C

FIG. 8B

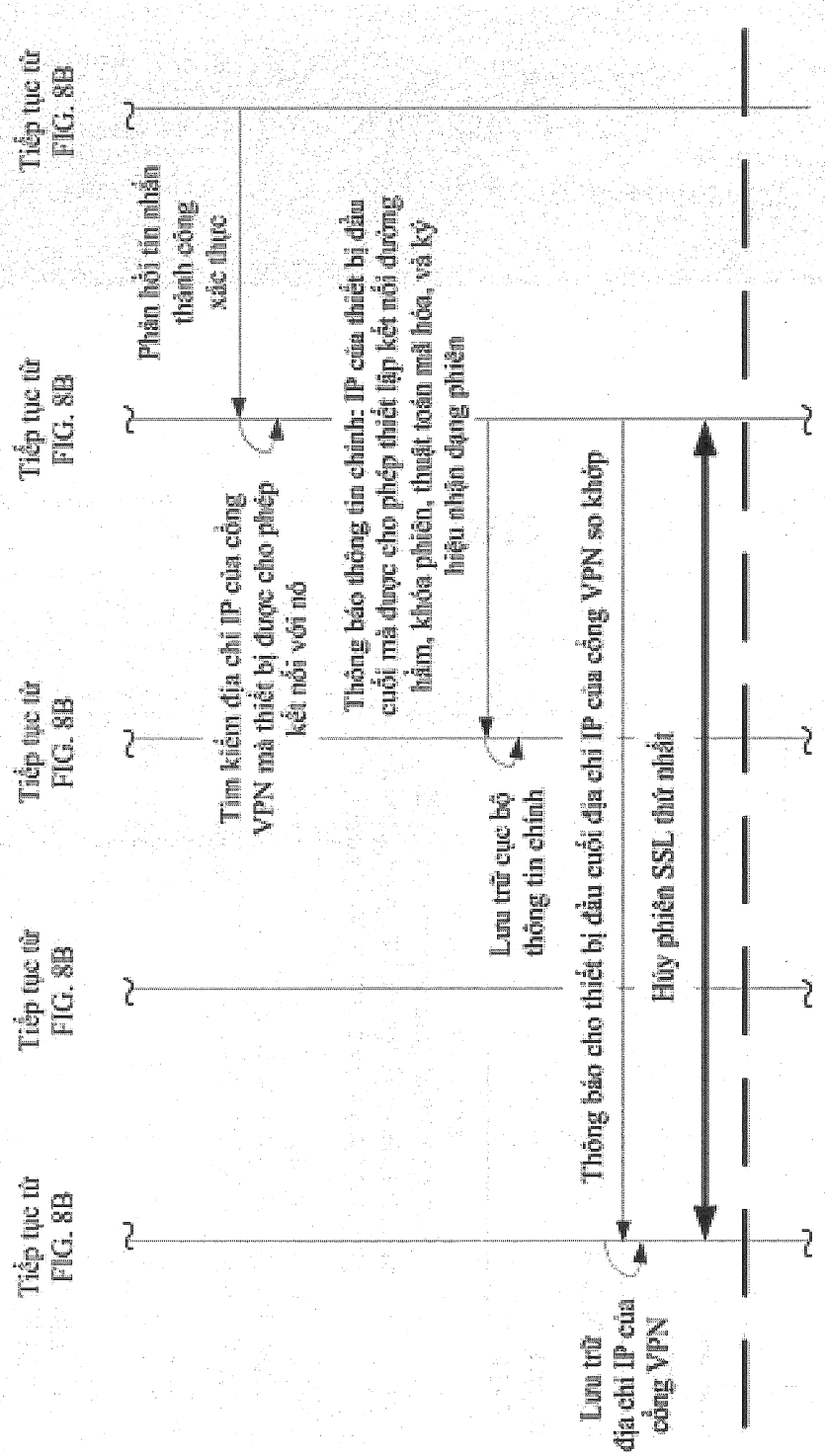

Tiếp tục từ FIG. 8B
Phản hồi tin nhắn thành công xác thực
Tiếp tục từ FIG. 8B
Tiếp tục từ FIG. 8B
Tìm kiếm địa chỉ IP của cổng VPN mà thiết bị được cho phép kết nối với nó
Thông báo thông tin chính: IP của thiết bị đầu cuối mà được cho phép thiết lập kết nối đường hầm, khóa phiên, thuật toán mã hóa, và ký hiệu nhận dạng phiên
Tới FIG. 8D
Tiếp tục từ FIG. 8B
Lưu trữ cục bộ thông tin chính
Tới FIG. 8D
Tiếp tục từ FIG. 8B
Thông báo cho thiết bị đầu cuối địa chỉ IP của cổng VPN so khớp
Hủy phiên SSL thứ nhất
Tới FIG. 8D
Lưu trữ địa chỉ IP của cổng VPN

FIG. 8C

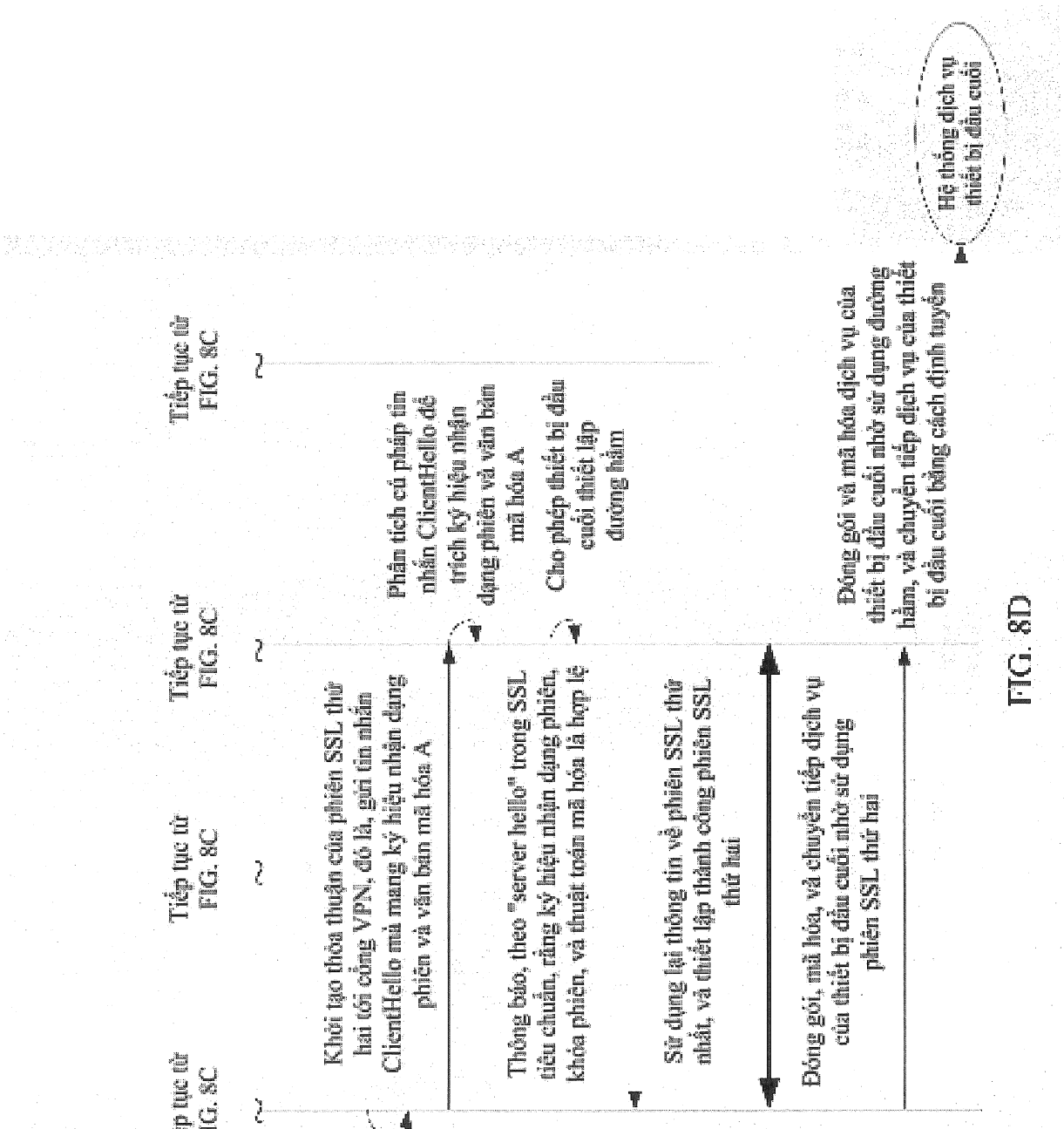

Tiếp tục từ FIG. 8C
Tiếp tục từ FIG. 8C
Tiếp tục từ FIG. 8C
Tiếp tục từ FIG. 8C
(1) Gọi ký hiệu nhận dạng phiên được lưu trữ
(2) Mã hóa IP của thiết bị đầu cuối nhờ sử dụng khóa phiên, và thu được, bằng cách tính toán, A=Encrypt (khóa phiên và IP của thiết bị đầu cuối)
Khởi tạo thỏa thuận của phiên SSL thứ hai tới cổng VPN, đó là, gửi tin nhắn ClientHello mà mang ký hiệu nhận dạng phiên và văn bản mã hóa A
Phân tích cú pháp tin nhắn ClientHello để trích ký hiệu nhận dạng phiên và văn bản mã hóa A
Thông báo, theo "server hello" trong SSL tiêu chuẩn, rằng ký hiệu nhận dạng phiên, khóa phiên, và thuật toán mã hóa là hợp lệ
Cho phép thiết bị đầu cuối thiết lập đường hầm
Pha thiết lập đường hầm dịch vụ
Sử dụng lại thông tin về phiên SSL thứ nhất, và thiết lập thành công phiên SSL thứ hai
Đóng gói, mã hóa, và chuyển tiếp dịch vụ của thiết bị đầu cuối nhờ sử dụng phiên SSL thứ hai
Đóng gói và mã hóa dịch vụ của thiết bị đầu cuối nhờ sử dụng đường hầm, và chuyển tiếp dịch vụ của thiết bị đầu cuối bằng cách định tuyến
Hệ thống dịch vụ thiết bị đầu cuối

FIG. 8D

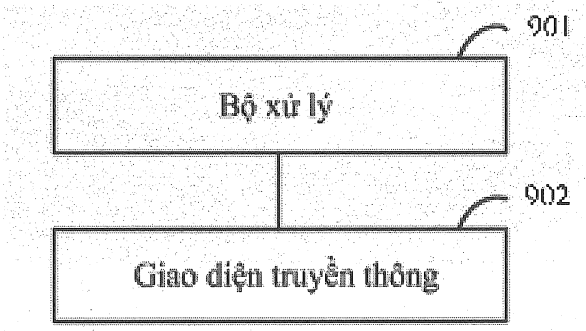


FIG. 9

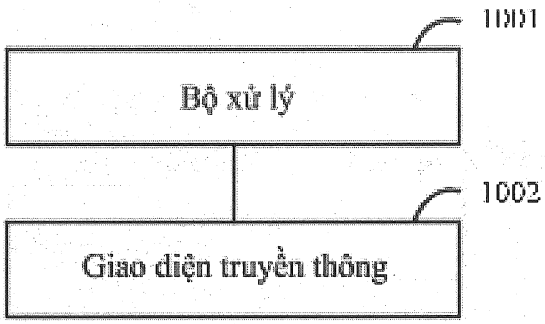


FIG. 10

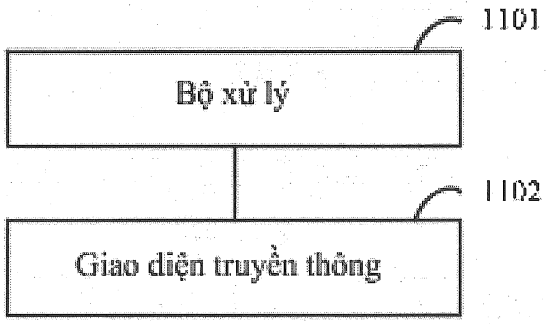


FIG. 11

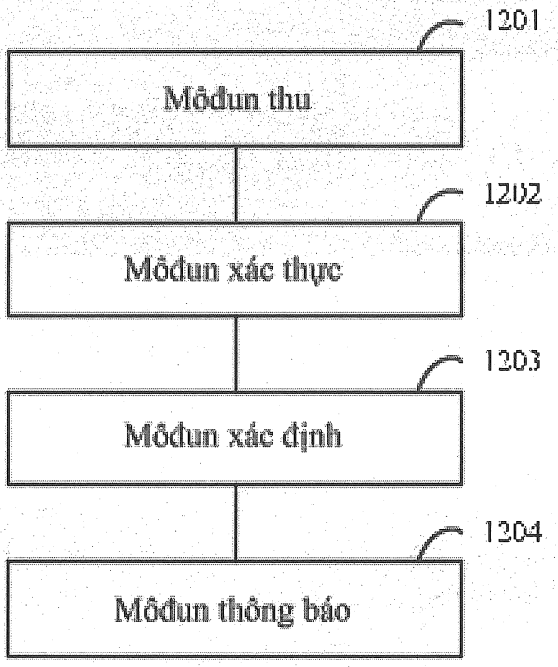

1201
Môđun thu
1202
Môđun xác thực
1203
Môđun xác định
1204
Môđun thông báo

FIG. 12

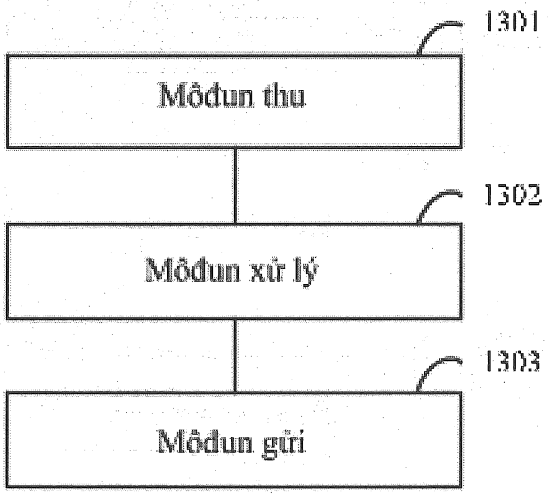

1301
Môđun thu
1302
Môđun xử lý
1303
Môđun gửi

FIG. 13

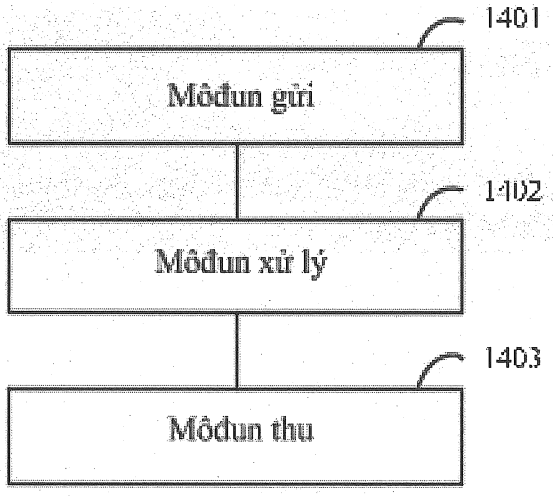


FIG. 14