Bảo mật mạng công nghiệp với ứng dụng VPN trên Router 3G/LTE SCALANCE M874-x

SIEMENS

Mục lục

1. MỤC TIÊU CHUNG

- Tài liệu này xây dựng tập trung vào hệ thống mạng trên nền tảng IP (internet)
- Giới thiệu tổng quan các giải pháp kết nối mạng từ xa dựa theo danh mục sản phẩm bộ điều khiển SIMATIC S7 và bộ định tuyến SCALANCE
- Các giải pháp kết nối SCALANCE M874-x trở thành VPN Client
- Hướng dẫn cấu hình SCALANCE M874-x kết nối 4G làm chức năng VPN Client

2. GIỚI THIỆU VỀ KẾT NỐI TỪ XA (REMOTE NETWORK)

2.1. Kết nối từ xa và bảo mật công nghiệp

Mạng kết nối từ xa là cơ sở hạ tầng truyền thông công cộng hoặc cá nhân để phủ sóng trên các khu vực rộng và khoảng cách xa, ví dụ mạng di động hoặc điện thoại cố định
Sự phân bố địa lý của các hệ thống tự động nhỏ hoặc các máy đơn lẻ làm tăng nhu cầu về điều khiển từ xa (telecontrol) và các dịch vụ bảo trì/chẩn đoán hoặc sửa chữa lỗi từ xa (teleservice)

Siemens cung cấp danh mục sản phẩm toàn diện cho giải pháp kết nối mạng từ xa bao gồm cả cơ sở hạ tầng truyền thống (điện thoại và đường dây chuyên dụng) và cơ sở hạ tầng dựa trên nền tảng IP (internet)

Các ứng dụng có thể truy cập từ xa trong mạng kết nối từ xa như:

- Telecontrol: các trạm kết nối RTU (thiết bị đầu cuối – remote terminal unit) được phân phối trên một khu vực địa lý rộng với một hoặc nhiều hệ thống điều khiển trung tâm nhằm mục đích vận hành, điều khiển và giám sát
- Teleservice: dữ liệu trao đổi giữa các hệ thống kỹ thuật từ xa như hệ thống máy, nhà máy và hệ thống máy tính cho mục đích phát hiện lỗi, chẩn đoán, bảo trì, sữa chữa hay nâng cấp…

Từ khi kết nối từ xa được thiết lập cho các nhà máy thực hiện thông qua mạng công cộng như internet (public network) thì yêu cầu quan trọng trong hệ thống đó là tăng cường bảo vệ, chống lại gián điệp (tin tặc) cũng như thao túng dữ liệu thì VPN (mạng ảo riêng – Virtual Private Network) được sử dụng.

2.2. Mạng ảo VPN

VPN là một mạng riêng ảo sử dụng mạng internet làm mạng chuyển tiếp để truyền dữ liệu đến mạng ảo đích đến (destination). Mạng ảo riêng và mạng chuyển tiếp không cần phải tương thích bởi một nhà cung cấp.

Mặc dù VPN sử dụng cơ chế định địa chỉ của mạng chuyển tiếp nhưng nó vẫn sử dụng các gói tin trong mạng ảo của riêng mình để tách biệt việc vận chuyển các gói dữ liệu riêng biệt này với các gói tin còn lại. Chính vì điều này, mạng ảo VPN được sử dụng như một mạng chia sẻ, hoặc lô-gic.

Các bộ định tuyến VPN có thể được cài đặt là một VPN qua nhiều giao thức khác nhau như: IPsec, OpenVPN, SSTP.

Để thiết lập kết nối mạng ảo VPN trên một giao tiếp dữ liệu bảo mật qua VPN phải có cả máy chủ VPN server và máy kết nối VPN Client.

2.3. Danh mục sản phẩm tích hợp chức năng bảo mật

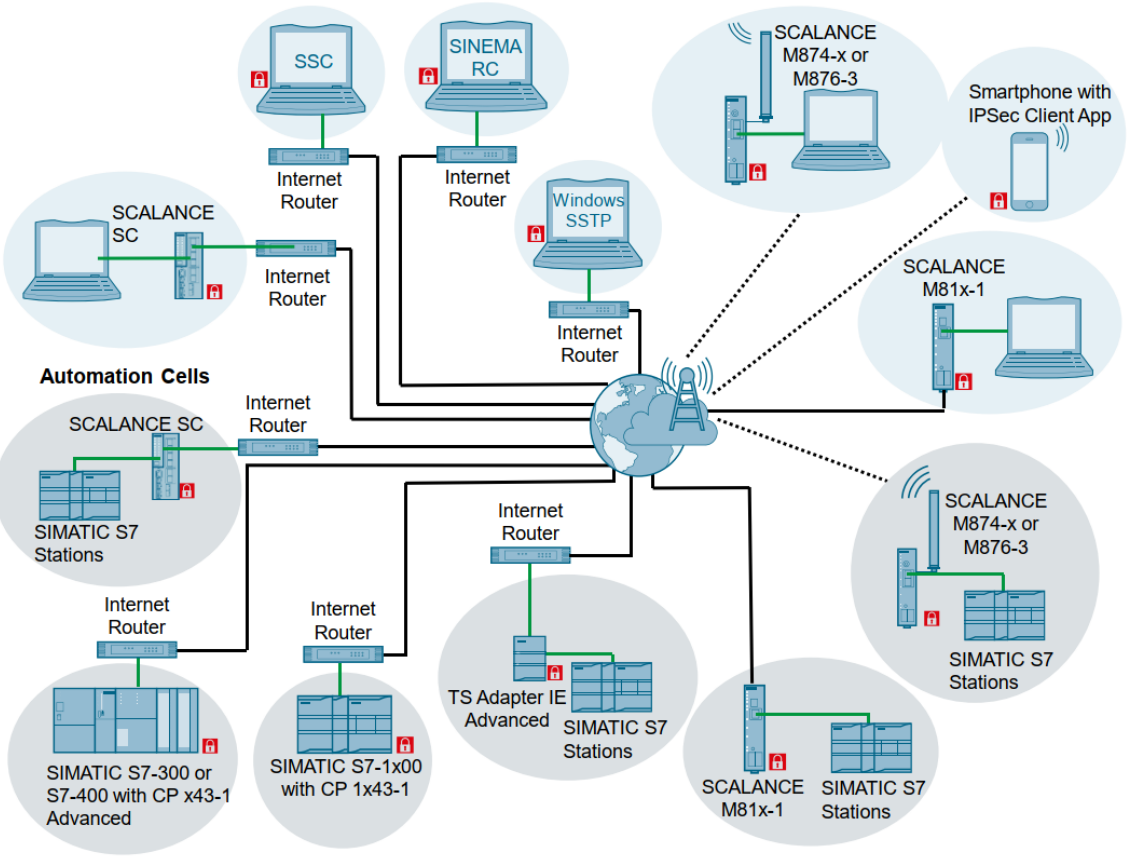
Thông qua sự kết hợp của các biện pháp bảo mật khác nhau như tường lửa (firewall) và VPN, các mô-đun bảo mật bảo vệ các thiết bị riêng lẻ hoặc toàn bộ hệ thống tự động hóa để chống lại:

- Gián điệp dữ liệu (Data espionage)
- Thao tác dữ liệu (Data manipulation)
- Truy cập không mong muốn (Unwanted access)

Bạn đọc có thể lựa chọn các sản phẩm và giải pháp bảo mật dựa theo sản phẩm các bộ điều khiển SIMATIC S7 và các mô-đun bảo mật như:

- SINEMA Remote Connect
- SOFTNET Security Client
- SCALANCE S615, SCALANCE SC63x-2C und SC64x-2C
- SCALANCE M-800
- Mô-đun CP x43-1 Advanced, CP 1x43-x và CP 1628
- TS Adapter IE Advanced
- LOGO! CMR

Để hiểu rõ hơn các bạn có thể xem hình sau đây:



***Hình 2.1**. Thiết lập kết nối VPN theo các bộ điều khiển SIMATIC S7*

2.4. SCALANCE M87x

Bộ định tuyến SCALANCE M87x phù hợp ứng dụng cho mạng di động:

- SCALANCE M874-3 / M876-3: UMTS (3G): 800, 850, 900, 1900 hoặc 2100 MHz
- SCALANCE M876-4: LTE (4G): 800, 900, 1800, 2100 hoặc 2600 MHz

Các mô-đun này có đặc điểm kỹ thuật như:

- Hỗ trợ VPN để xác thực bảo mật các nút mạng, mã hóa dữ liệu và xác minh tính toàn vẹn của dữ liệu
    - IPsec VPN
    - OpenVPN kết nối tới SINEMA RC
- Phạm vi ứng dụng rộng, có thể sử dụng ở bất cứ nơi nào có mạng di động
- Truyền và nhận tin nhắn SMS
- Hỗ trợ RSTP và VRRPv3
- Kết nối với các trạm tĩnh (stationary) hoặc các trạm di động
- Đơn giản hóa việc kết nối các mạng nội bộ bằng truyền thông IP qua mạng WAN

- Chỉ định tường lửa IP (IP firewall) để phân biệt và phân quyền truy cập vào các bộ phận cụ thể của nhà máy
- Kết nối đơn giản tới SINEMA RC thông qua giao diện tự cấu hình (kích hoạt KEY-PLUG SINEMA RC)

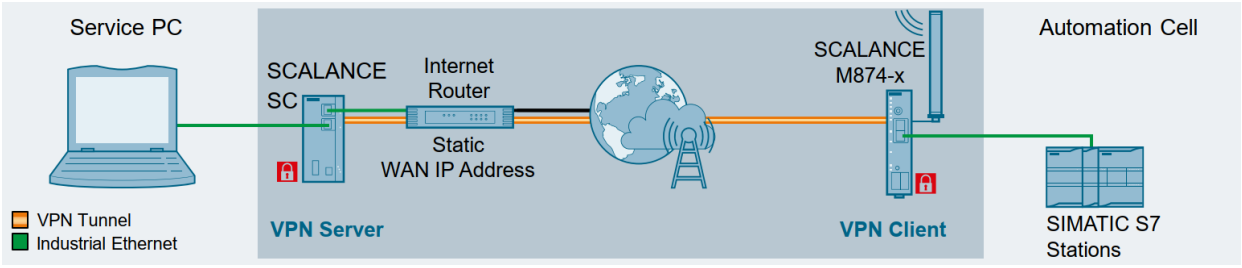
3. KẾT NỐI VPN CLIENT VỚI SCALANCE M874-X

Trong phần này, bạn đọc cùng tham khảo một số giải pháp kết nối VPN Client bằng SCALANCE M874-x với khai báo IPsec với các VPN Server được cấu hình trên các bộ SCALANCE SC hoặc CP x43-1 Advanced.

Yêu cầu chung khi cấu hình SCALANCE M874-x làm VPN Client:

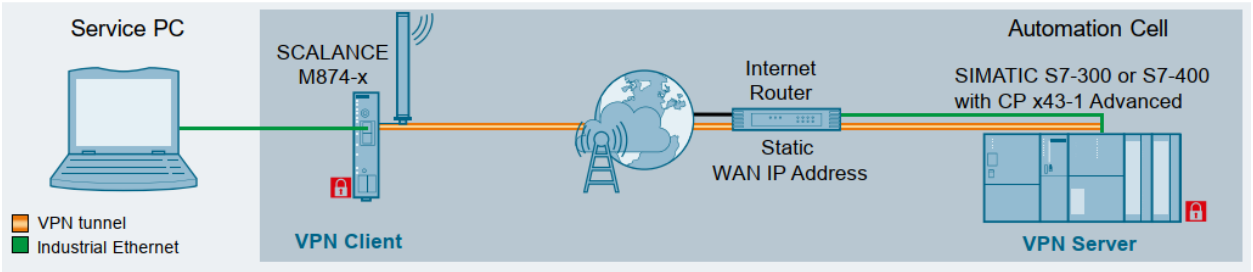
- Địa chỉ IP tĩnh (public) cho bộ định tuyến Internet của VPN server
- Bộ định tuyến Internet hỗ trợ chức năng forwarding bên VPN server
- Cấu hình thông tin APN cho VPN Client (phụ thuộc nhà cung cấp mạng di động)

3.1. Kết nối VPN Client với SCALANCE SC (VPN server)



***Hình 3.1**. Kết nối VPN giữa SCALANCE SC (VPN server) và SCALANCE M 874-x*

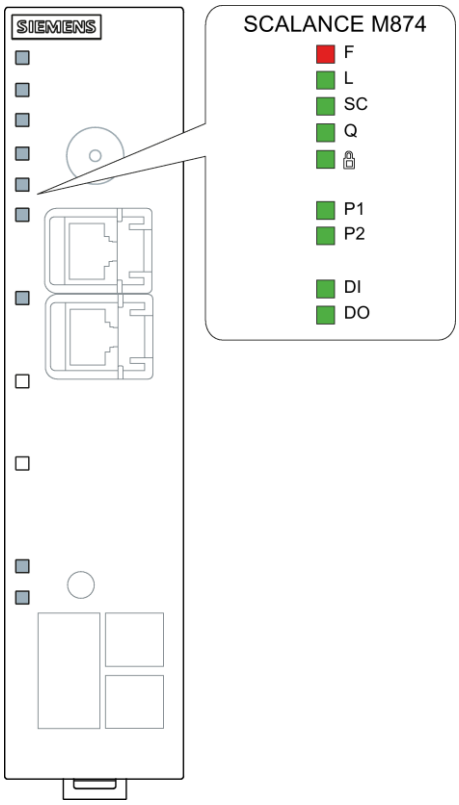
3.2. Kết nối VPN Client với CP x43-1 Advanced (VPN server)



***Hình 3.2**. Kết nối VPN giữa CP x43-1 Advanced (VPN server) và SCALANCE M 874-x*

4. CÀI ĐẶT SCALANCE M874-X VPN CLIENT

4.1. Mô tả trạng thái thiết bị



Hình 4.1. *Hình dạng của SCALANCE M874-x*

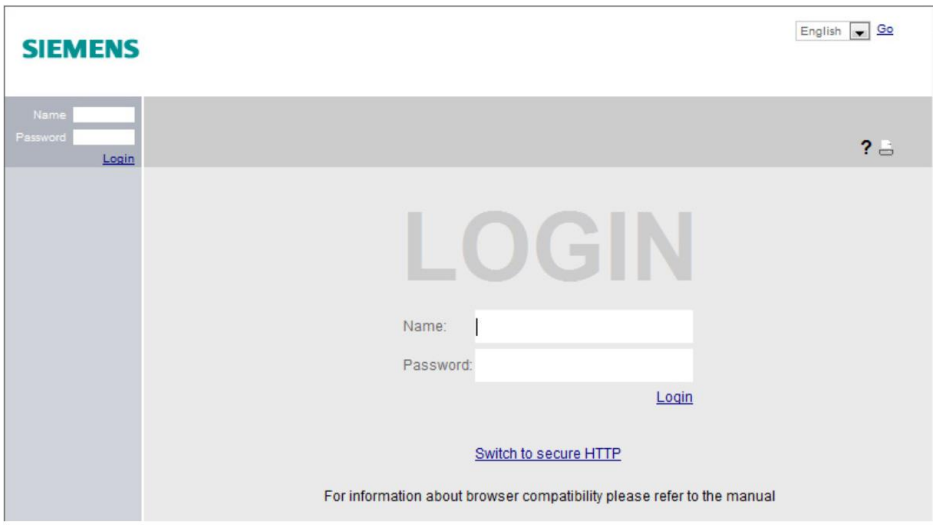
Bảng 4.1*. Mô tả trạng thái SCALANCE M 874-x*

Đèn LED	Trạng thái	Ý Nghĩa
F	Tắt: ☐	Không lỗi
	Sáng: ■	Báo lỗi
	Nháy: ✳	Hệ thống đang tải/cập nhật firmware
L	Tắt: ☐	Thiết bị tắt, không nguồn cấp
	Sáng: ■	Thiết bị đang bật, có nguồn cấp
SC	Tắt: ☐	Thẻ SIM OK, không có kết nối
	Sáng: ■	Lỗi thẻ SIM
	Sáng: ■	Có kết nối
Q	Tắt: ☐	Không phản hồi Độ rộng tín hiệu < -109 dBm

	Nháy:	Tín hiệu yếu: -89 dBm đến -109 dBm
	Sáng:	Tín hiệu trung bình: -73 dBm đến -89 dBm
	ON:	Tín hiệu mạnh: > -73 dBm
	OFF:	Không có kết nối VPN
	ON:	Có VPN kết nối
	Nháy :	Một vài VPN kết nối
P1/P2	Tắt:	Không có kết nối LAN
	Sáng:	Có kết nối LAN
	Sáng:	Đang truyền dữ liệu

4.2. Cài đặt ban đầu

Sử dụng phần mềm PRONETA hoặc SINEC PNI Basic cấu hình địa chỉ IP cho thiết bị khi lần đầu sử dụng. Sau đó thực hiện các thao tác sau đây:

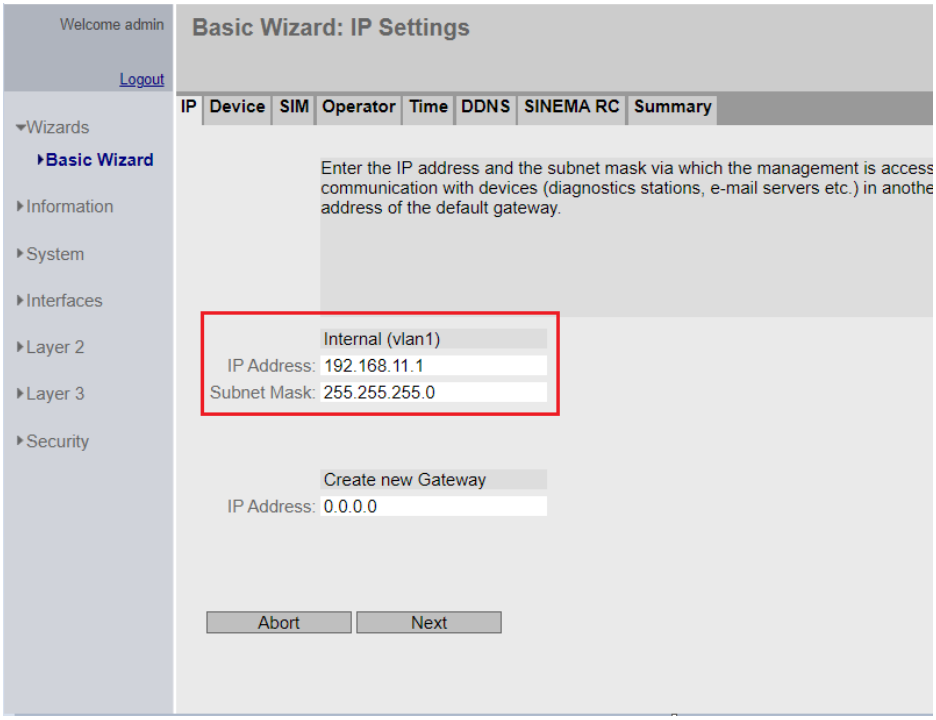
Bước.	Cách thức
1	Dùng trình duyệt web gõ địa chỉ IP vào thanh nhập địa chỉ. Màn hình đăng nhập sẽ xuất hiện. **Lưu ý:** máy tính phải cùng lớp mạng với thiết bị 

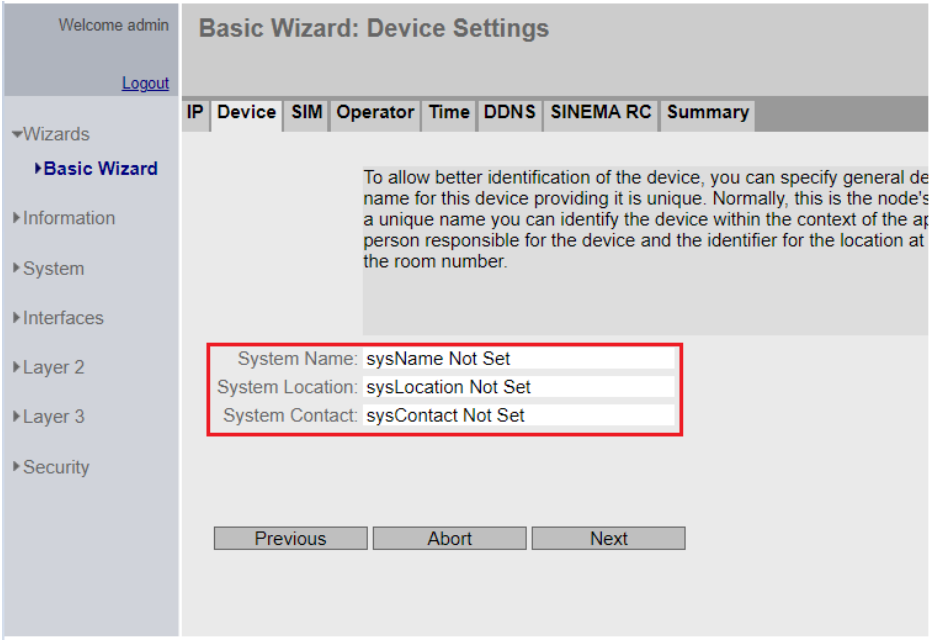
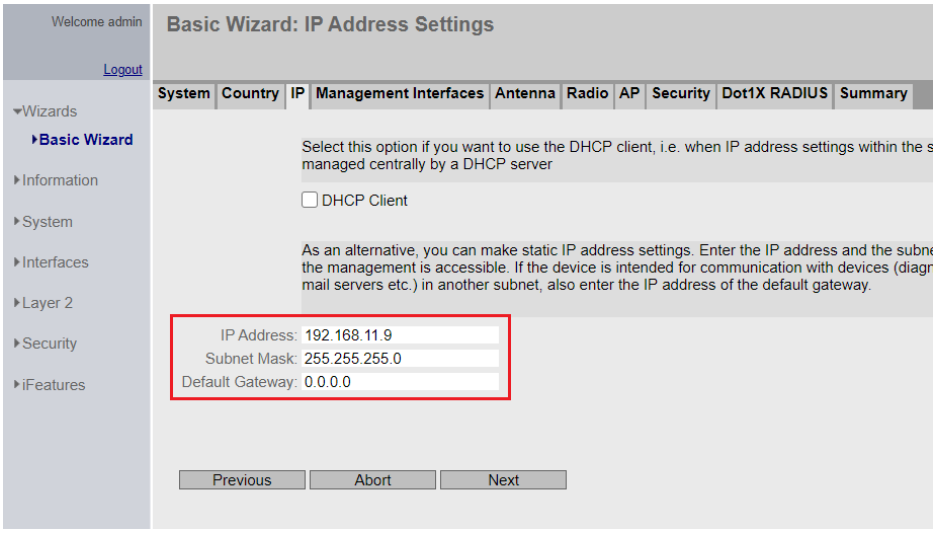
2	Tên đăng nhập và mật khẩu mặc định: ▪ User: admin ▪ Password: admin Sau khi đăng nhập thành công, hệ thống yêu cầu đổi mật khẩu cho lần đăng nhập tiếp theo
3	Vào tab Wizard → Basic Wizard cấu hình các thông số ban đầu

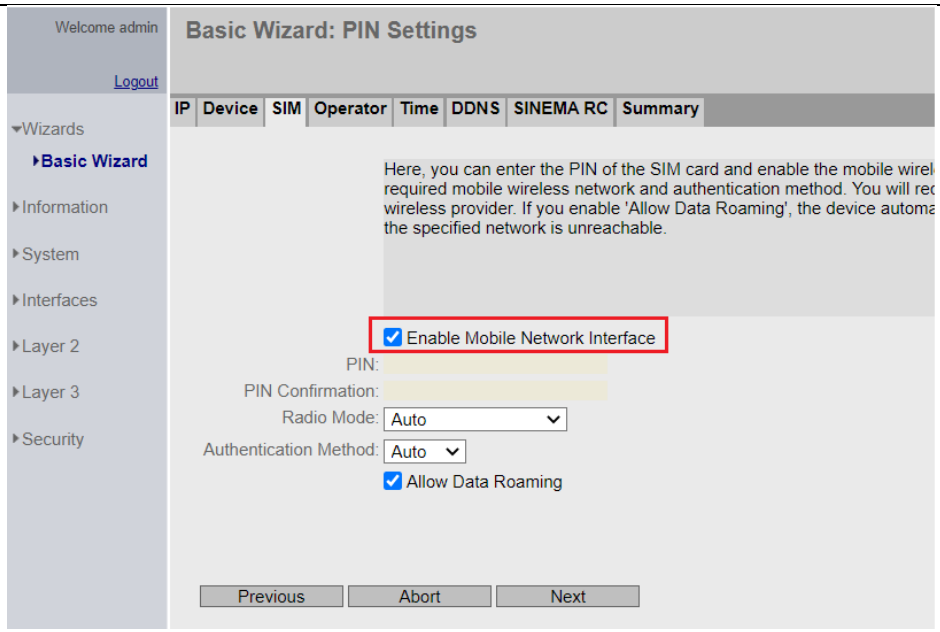
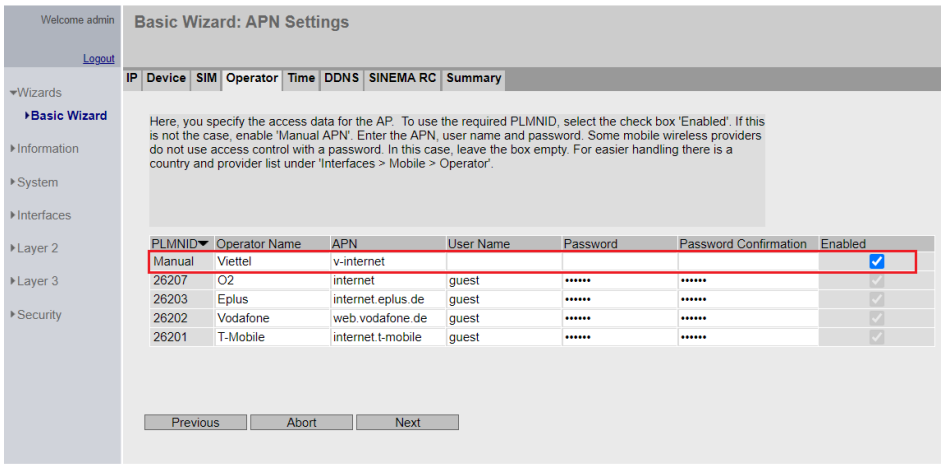
4.3. Cấu hình kết nối Internet qua SIM 4G

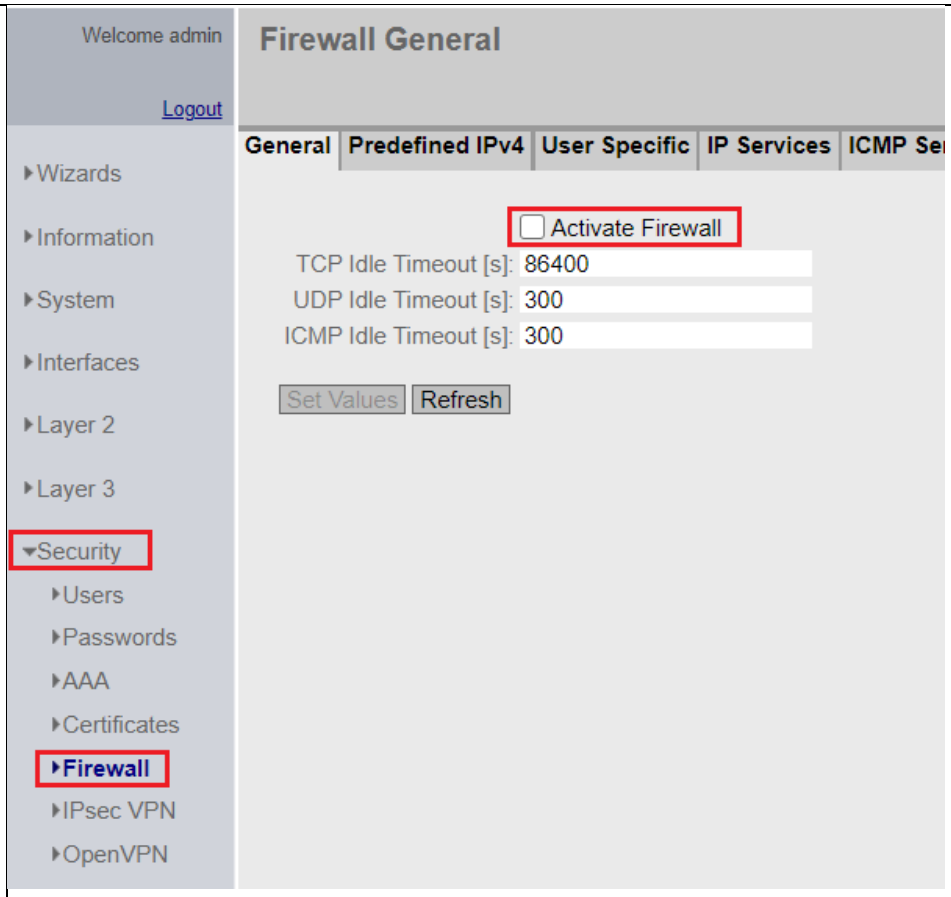
- **Yêu cầu :** SIM phải đăng kí 4G

Các bước kết nối Internet qua SIM 4G trên SCALANCE M 874-x thực hiện như sau:

Bước.	Cách thức
1	Đăng nhập vào thiết bị
2	Vào tab Wizard → Basic Wizard để cấu hình các thông số
3	Chọn tab IP, nhập địa chỉ IP và Subnet Mask 
4	Chọn tab Device, có thể điền thông tin hoặc có thể không

	▪ System Name: Tên hệ thống ▪ Sysytem Location: Vị trí hệ thống ▪ System Contact: Thông tin liên lạc hệ thống Sau đó chọn **Next** 
5	Đến tab IP, cấu hình địa chỉ IP cho thiết bị. Sau đó chọn **Next** 
6	Chọn tab SIM, kích hoạt tùy chọn **Enable Mobile Network Interface**

	
7	Tab Operator, nhập cấu hình APN của nhà mạng di động**.** Sau đó, kích hoạt tùy chọn Enabled như hình minh họa**.** Nhấn **Next** 
8	Chọn Security → Firewall → General. Bỏ tích chọn **Active Firewall** (trường hợp không sử dụng tường lửa)

	
9	Lưu thiết lập

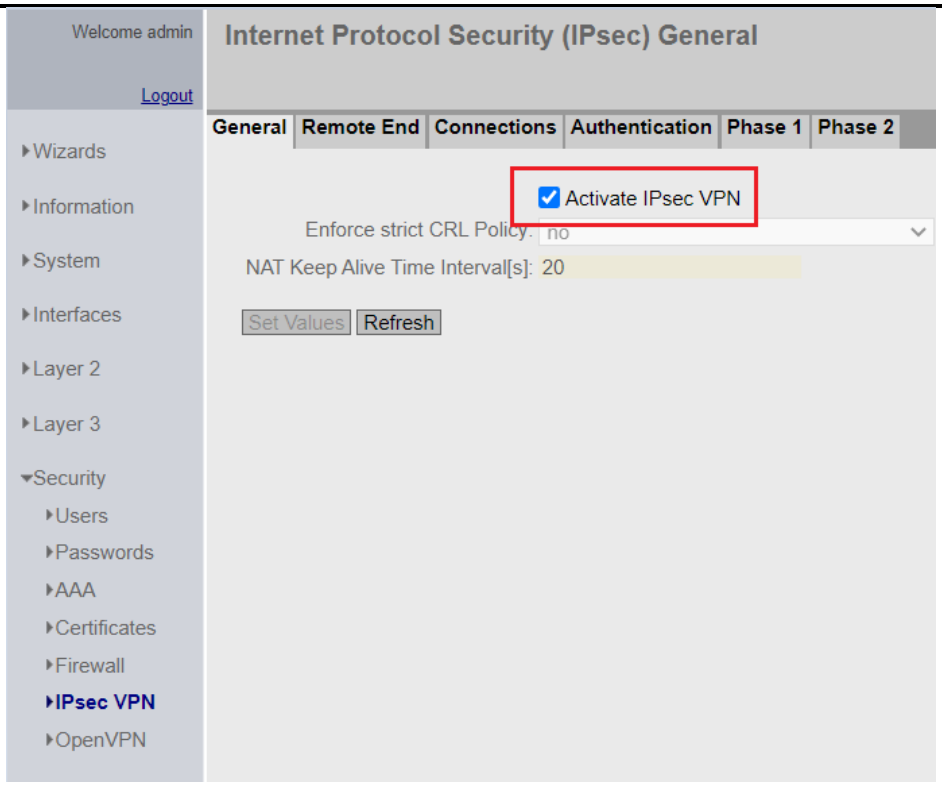
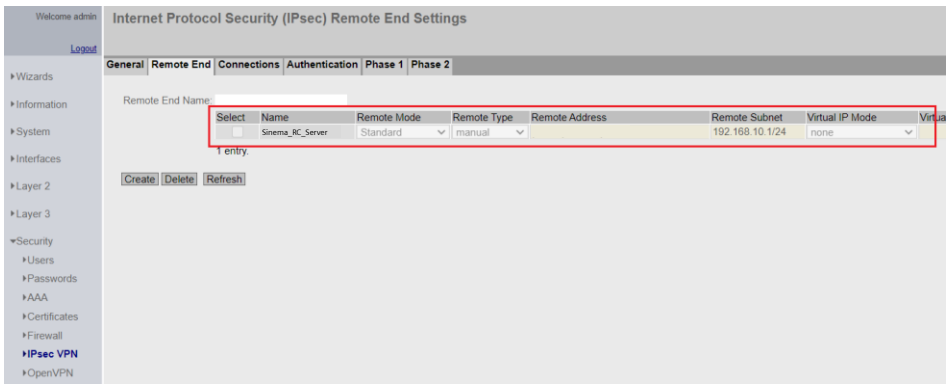
Sau khi thực hiện xong, SCALANCE M874-x có thể truy cập Internet.

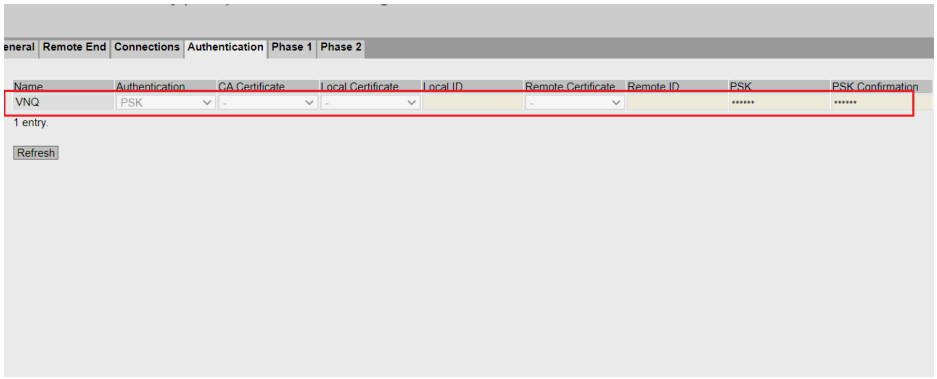
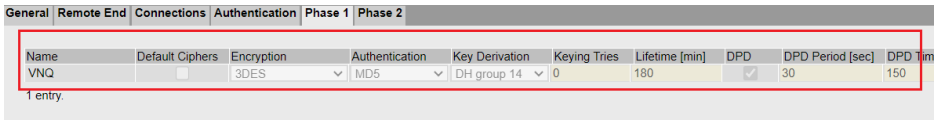
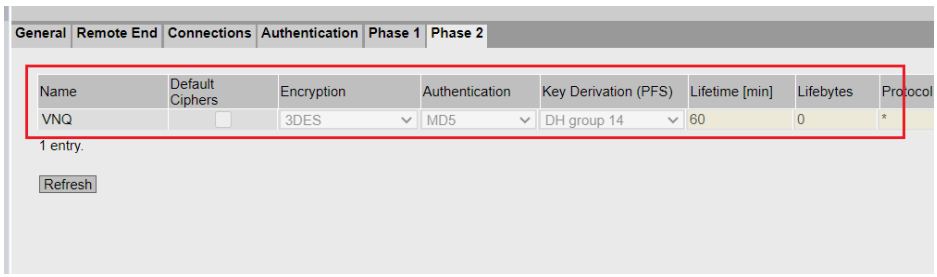
4.4. Cấu hình SCALANCE M874-x làm VPN Client

- **Yêu cầu**:
  - M874-x phải kết nối Internet bằng SIM 3G/4G
  - Có một VPN Server với tên miền riêng

Các bước cấu hình SCALANCE M 874-x làm chức năng VPN Client:

Bước	Cách thức
1	Chọn Security → Ipsec VPN và kích hoạt **Active Ipsec VPN**

	
2	Chọn tab Remote End, cấu hình kết nối tới VPN Server. Chọn Create để tạo cấu hình mới và cài các thông số sau: ▪ Name: Tên cho VPN Server ▪ Remote Mode: mặc định là Standard ▪ Remote type : mặc định là manual ▪ Remote Address: nhập tên miền hay địa chỉ IP tĩnh của Server ▪ Remote Subnet: dãy địa chỉ IP local LAN của VPN Server 
3	Chọn tab Authentication: ▪ Authentication: PSK (Pre Shared Key)

	▪ PSK: mã PSK VPN Server ▪ PSK Confirmation: Xác nhận mã PSK Sau đó chọn **Next** 
4	Chọn tab Phase 1 và chú ý các thông số sau: ▪ Encryption: 3DES (phụ thuộc VPN Server hỗ trợ chuẩn nào nhưng thường là tất cả các chuẩn) ▪ Authentication: MD5 (phụ thuộc VPN Server hỗ trợ) 
5	Chọn tab Phase 2 và cấu hình tương tự như Phase 1: 
6	Lưu cấu hình và trở lại tab **Connection** → chọn **Start** tại cột **Operation.** Lưu cấu hình lần nữa Kết nối thành công đèn LED hình móc khóa sẽ sáng màu xanh lá cây

5. THÔNG TIN LIÊN HỆ

Cảm ơn sự quan tâm của quý vị!

Để tìm hiểu thêm hoặc cần sự trợ giúp, xin vui lòng liên hệ:

Anh Trần Văn Hiếu

Quản lý Trung tâm Đào tạo Công nghiệp số Siemens Việt Nam

Email: mailto:tran-van.hieu@siemens.com

www.siemens.com.vn

www.facebook.com/Siemens.Vietnam

Thông tin pháp lý

Sử dụng các ứng dụng mẫu

Các ứng dụng mẫu minh họa giải pháp của các tác vụ tự động hóa thông qua sự tương tác của một số thành phần dưới dạng văn bản, đồ họa và / hoặc mô-đun phần mềm. Các ứng dụng mẫu là một dịch vụ miễn phí của Siemens AG và / hoặc một công ty con của Siemens AG ("Siemens"). Siemens không bị ràng buộc và không đưa ra tuyên bố về tính hoàn chỉnh hoặc chức năng liên quan đến cấu hình và thiết bị cho ứng dụng mẫu. Các ứng dụng mẫu chỉ nhằm trợ giúp các tác vụ điển hình; chúng không tạo thành các giải pháp dành riêng cho khách hàng. Người sử dụng tự chịu trách nhiệm vận hành sản phẩm đúng cách và an toàn theo các quy định hiện hành đồng thời phải kiểm tra chức năng của ứng dụng mẫu tương ứng và tùy chỉnh nó cho hệ thống của mình.
Siemens cấp cho người sử dụng, thông qua nhân viên được đào tạo kỹ thuật của mình, quyền sử dụng không độc quyền, không được cấp phép lại và không thể chuyển giao các ứng dụng mẫu. Người sử dụng chịu trách nhiệm với mọi thay đổi đối với các ứng dụng mẫu. Người sử dụng chỉ được phép chia sẻ các ứng dụng mẫu với các bên thứ ba hoặc sao chép các ứng dụng mẫu hoặc đoạn trích của chúng khi được kết hợp với các sản phẩm của riêng người sử dụng. Các ứng dụng mẫu không bắt buộc phải trải qua các thử nghiệm thông thường và kiểm tra chất lượng như một sản phẩm thương mại thông thường; chúng có thể có các khiếm khuyết về chức năng và hiệu suất cũng như các lỗi. Người sử dụng có trách nhiệm sử dụng ứng dụng mẫu nhằm đảm bảo bất kỳ trục trặc nào có thể xảy ra sẽ không gây thiệt hại về tài sản hoặc thương tích cho con người.

Miễn trừ trách nhiệm

Siemens sẽ không chịu bất kỳ trách nhiệm, vì bất kỳ lý do pháp lý nào, bao gồm, nhưng không giới hạn, trách nhiệm đối với khả năng sử dụng, tính khả dụng, tính toàn vẹn và không bị lỗi của các ứng dụng mẫu cũng như đối với thông tin liên quan, dữ liệu cấu hình và hiệu suất và bất kỳ thiệt hại nào phát sinh từ đó. Điều này sẽ không áp dụng trong các trường hợp trách nhiệm pháp lý bắt buộc, ví dụ như theo Đạo Luật Trách Nhiệm Sản Phẩm của CHLB Đức hoặc theo pháp luật của nước sở tại, hoặc trong các trường hợp cố ý, sơ suất nghiêm trọng hoặc thiệt hại nghiêm trọng về tính mạng, thương tật hoặc tổn hại sức khỏe, không tuân thủ bảo đảm, gian lận hoặc không tiết lộ về khiếm khuyết hoặc vi phạm nghiêm trọng các nghĩa vụ cơ bản của hợp đồng. Tuy nhiên, trách nhiệm của Siemens khi vi phạm cơ bản nghĩa vụ hợp đồng sẽ được giới hạn ở các thiệt hại có thể ước tính trước và điển hình của loại thỏa thuận liên quan, trừ khi thiệt hại phát sinh do cố ý hoặc sơ suất nghiêm trọng hoặc thiệt hại về tính mạng, thương tật hoặc tổn hại sức khỏe. Người sử dụng có trách nhiệm chứng minh các thiệt hại của mình. Người sử dụng sẽ đảm bảo Siemens không bị liên đới với các khiếu nại hiện có hoặc trong tương lai từ các bên thứ ba liên quan, ngoại trừ trường hợp Siemens phải chịu trách nhiệm bắt buộc.
Bằng cách sử dụng các ứng dụng mẫu, người sử dụng đồng ý rằng quy định nêu trên sẽ điều chỉnh toàn bộ trách nhiệm pháp lý của Siemens đối với các thiệt hại.

Thông tin khác

Siemens có quyền thực hiện các thay đổi đối với các ứng dụng mẫu bất kỳ lúc nào mà không cần thông báo. Trong trường hợp có sự khác biệt giữa các gợi ý trong ứng dụng mẫu và các ấn phẩm khác của Siemens như danh mục sản phẩm, nội dung của tài liệu khác sẽ được ưu tiên.
Các điều khoản sử dụng của Siemens (https://support.industry.siemens.com) cũng sẽ được áp dụng.

Thông tin an ninh

Siemens cung cấp các sản phẩm và giải pháp có chức năng An Ninh Công nghiệp hỗ trợ hoạt động an toàn của các nhà máy, hệ thống, máy móc và mạng.
Để bảo vệ các nhà máy, hệ thống, máy móc và mạng khỏi các nguy cơ an ninh mạng, khách hàng cần thực hiện - và liên tục duy trì một mô hình an ninh công nghiệp toàn diện, tiên tiến. Các sản phẩm và giải pháp của Siemens là một nhân tố của mô hình này.
Khách hàng có trách nhiệm ngăn chặn việc truy cập trái phép vào nhà máy, hệ thống, máy móc và mạng của mình. Các hệ thống, máy móc và thành phần liên quan chỉ nên được kết nối với mạng doanh nghiệp hoặc Internet nếu và trong phạm vi cần thiết và chỉ khi các biện pháp bảo mật thích hợp (ví dụ: tường lửa và/hoặc phân đoạn mạng) được áp dụng.
Để biết thêm thông tin về các biện pháp an ninh công nghiệp có thể được thực hiện, vui lòng truy cập https://www.siemens.com/industrialsecurity.
Các sản phẩm và giải pháp của Siemens trải qua quá trình phát triển liên tục để đảm bảo an toàn hơn. Siemens đặc biệt khuyến nghị khách hàng cập nhật sản phẩm ngay khi các bản cập nhật được phát hành và sử dụng các phiên bản sản phẩm mới nhất. Việc sử dụng các phiên bản sản phẩm không còn được hỗ trợ và việc không áp dụng các bản cập nhật mới nhất có thể làm tăng khả năng khách hàng gặp phải các nguy cơ an ninh mạng.
Để được cập nhật thông tin về các bản cập nhật sản phẩm, hãy đăng ký Nguồn Dữ Liệu An Ninh Công Nghiệp Của Siemens (Siemens Industrial Security RSS Feed) tại: https://www.siemens.com/industrialsecurity.

SIEMENS