Tài liệu hướng dẫn
Cấu hình FortiOS v6.0

Chuẩn bị cho:

Lập bởi:
Tech Horizon

Phần kiểm soát Các thay đổi

Ngày	Người thực hiện	Version	Nội dung
		6.0	Tạo tài liệu

Xem xét

Ngày	Tên và chức vụ

Nhận tài liệu

Ngày	Tên và chức vụ

MỤC LỤC

1. Mô tả tài liệu

Tài liệu kỹ thuật được lập ra với cấu hình từ căn bản đến nâng cao nhằm mục đích giúp cho người quản trị hiểu các tính năng cũng như có thể cấu hình và quản trị thiết bị firewall FortiGate và thiết bị Forti-AP. Với tài liệu này người quản trị sẽ có cái nhìn về thiết bị firewall FortiGate một cách tổng quan và dễ dàng cho việc quản trị thiết bị.

2. Cấu hình căn bản

2.1: Login và system

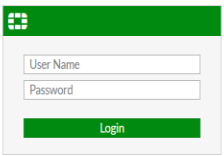
Để login vào thiết bị ta có 2 cách như sau:

- Login Console:
    - Bit per second: 9600
    - Data bit: 8
    - Parity: none
    - Stop bit: 1
    - Flow control: none
- Login Web Interface:
    - https://192.168.1.99
    - Username: admin
    - Password:
- System: Xem trạng thái thông tin thiết bị như ngày, giờ, license...
- Login vào màn hình cấu hình Fortinet firewall theo thông số bên dưới:

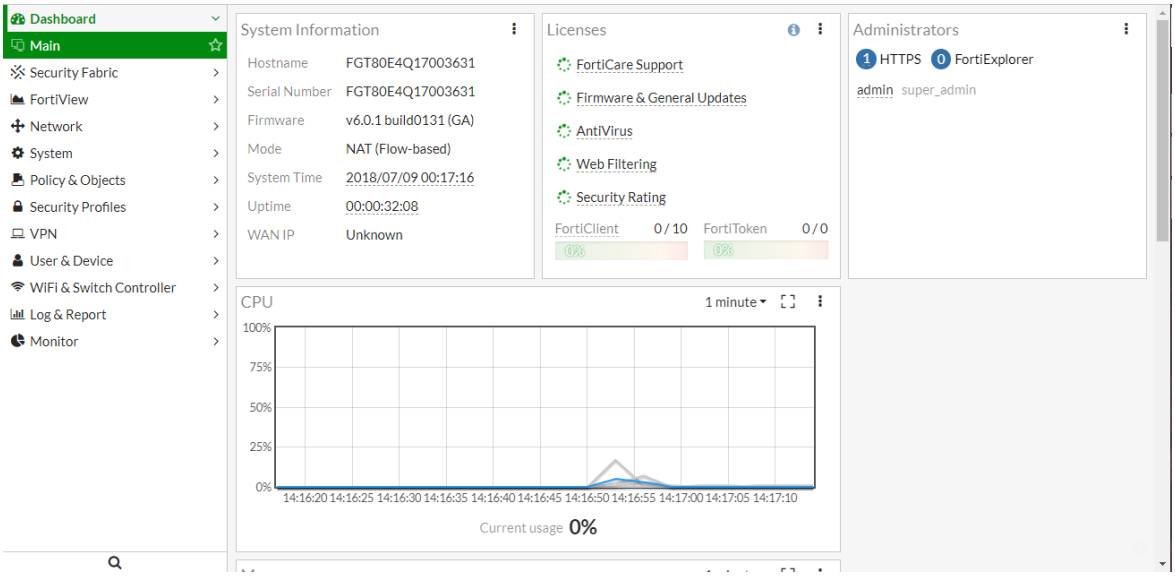
https://192.168.1.99

Name: admin

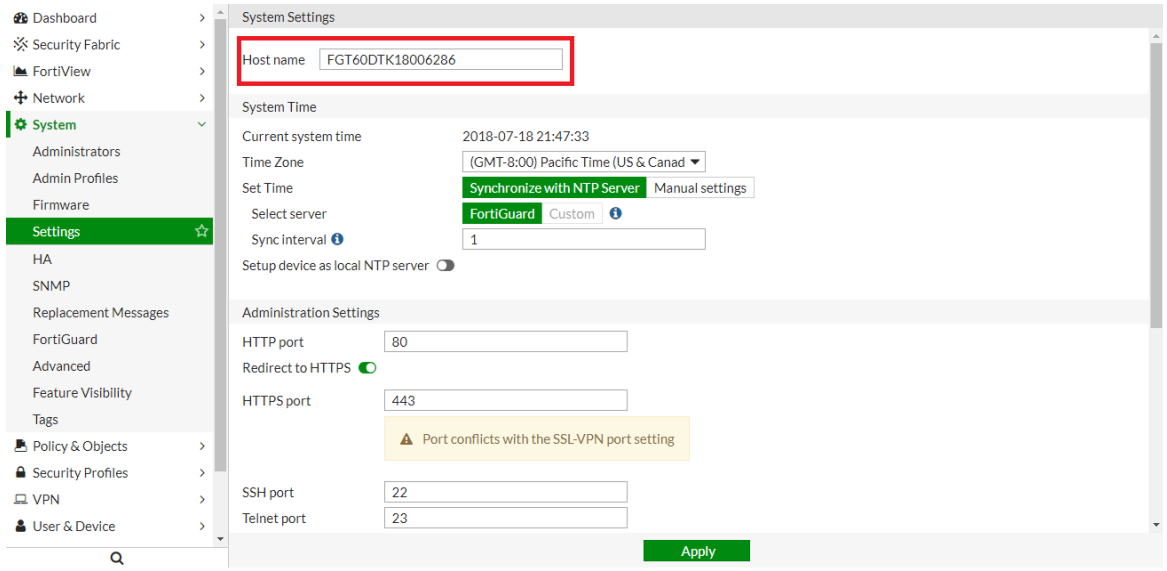
Password: để trống



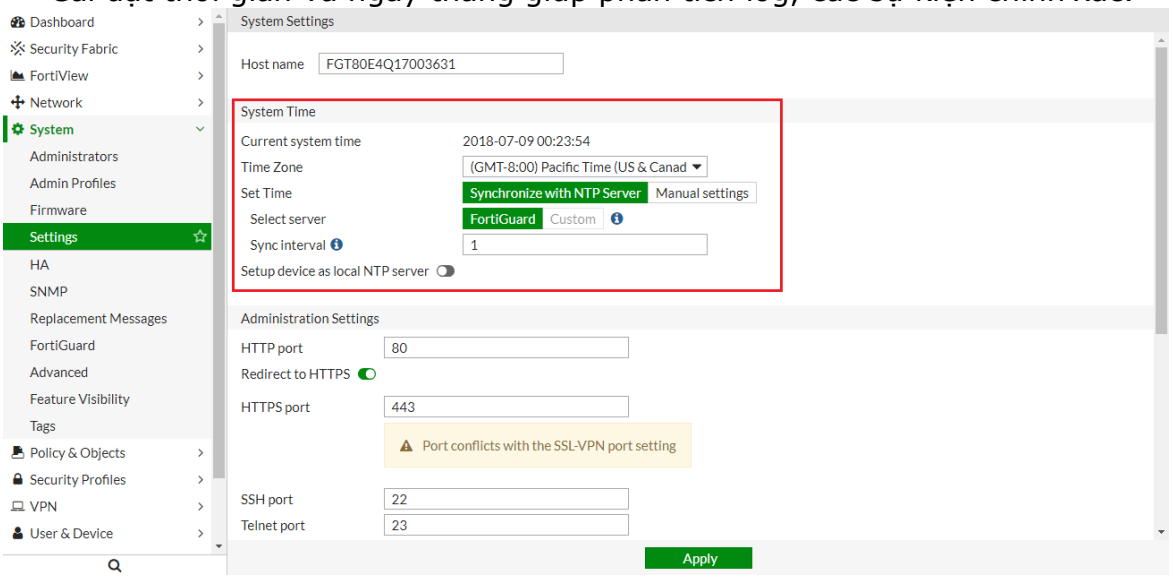
- Màn hình chính của Fortinet firewall:



- Để thay đổi tên của thiết bị cho phù hợp ta vào **System -> Setting** thực hiện đổi tên theo ý muốn.



- Cài đặt thời gian và ngày tháng giúp phân tích log, các sự kiện chính xác.

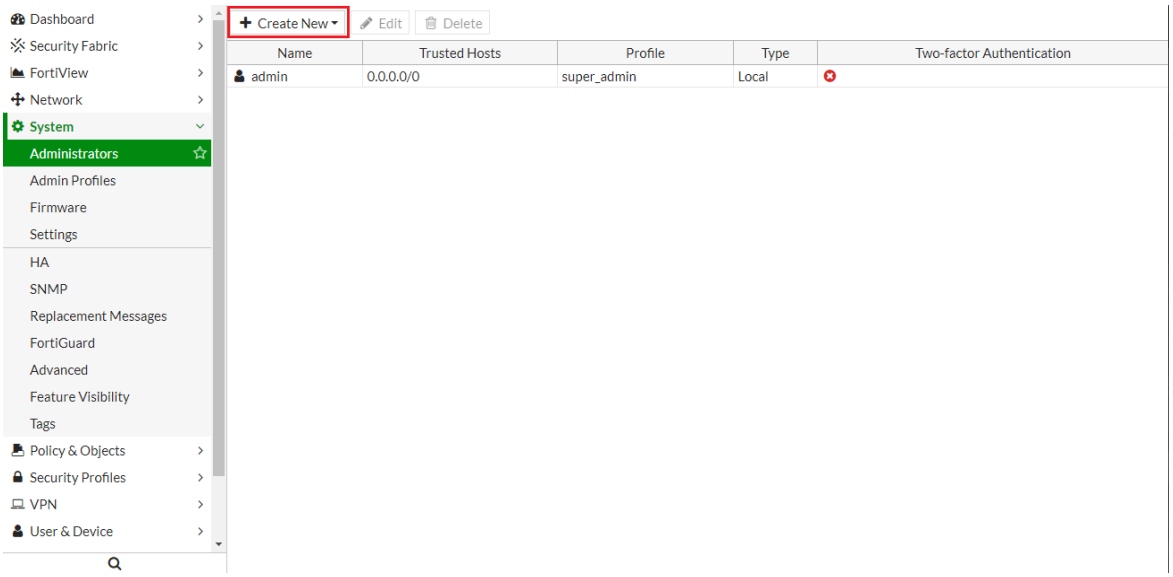


2.2: Tạo tài khoản quản trị thiết bị

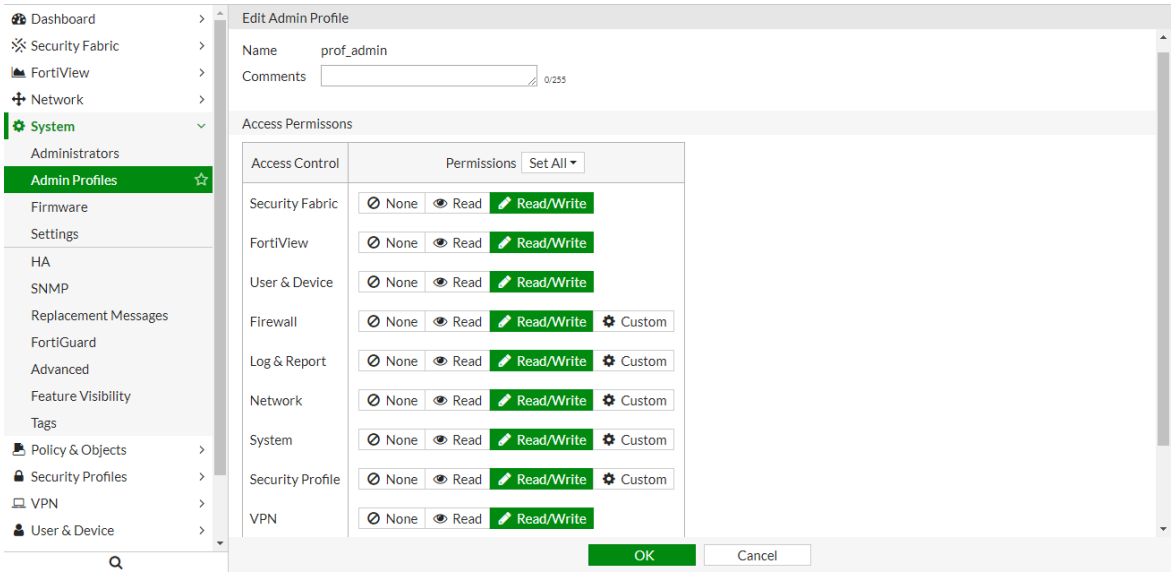
- Fortinet firewall chia thành nhiều cấp administrator

- Administrator:
  - Toàn quyền trên hệ thống
  - Tạo, xóa và quản lý tất cả các loại administrator khác
  - Read/Write administrator
- Tương tự như administrator nhưng không thể tạo, sửa và xóa các admin users:
  - Read-only user

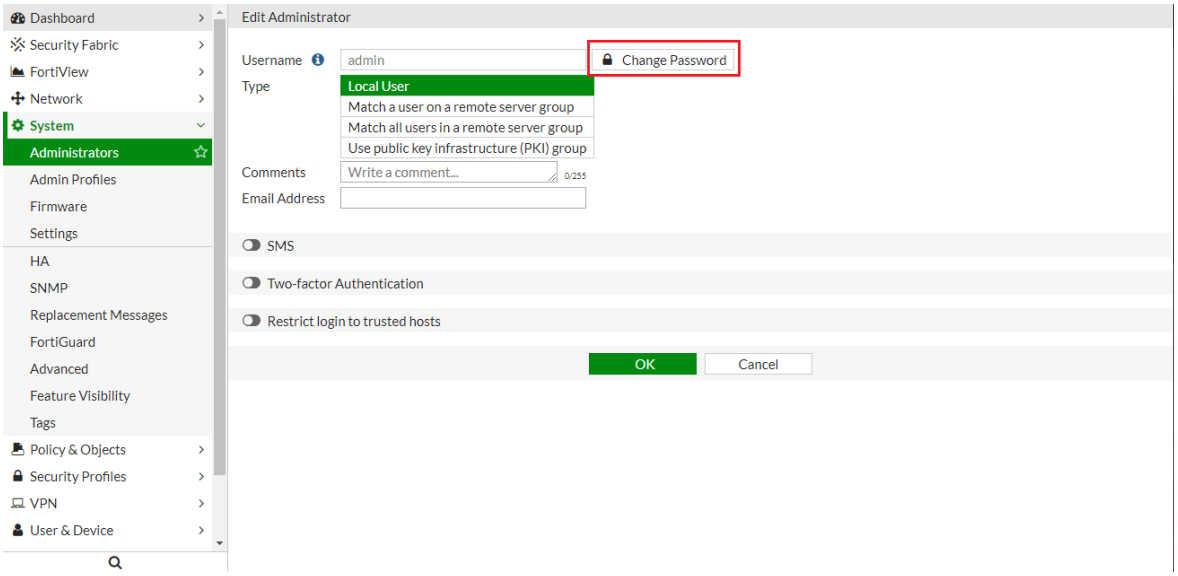
- Ta cấu hình như hình bên dưới để tạo một tài khoản mới cho việc quản trị thiết bị firewall: **System ->Administrators -> Create New**



- Điền thông tin User, Password và chọn Profile cho user.
- Sau khi tạo tài khoản xong ta cấp quyền truy cập vào thiết bị cho tài khoản vừa tạo theo như hình bên dưới:

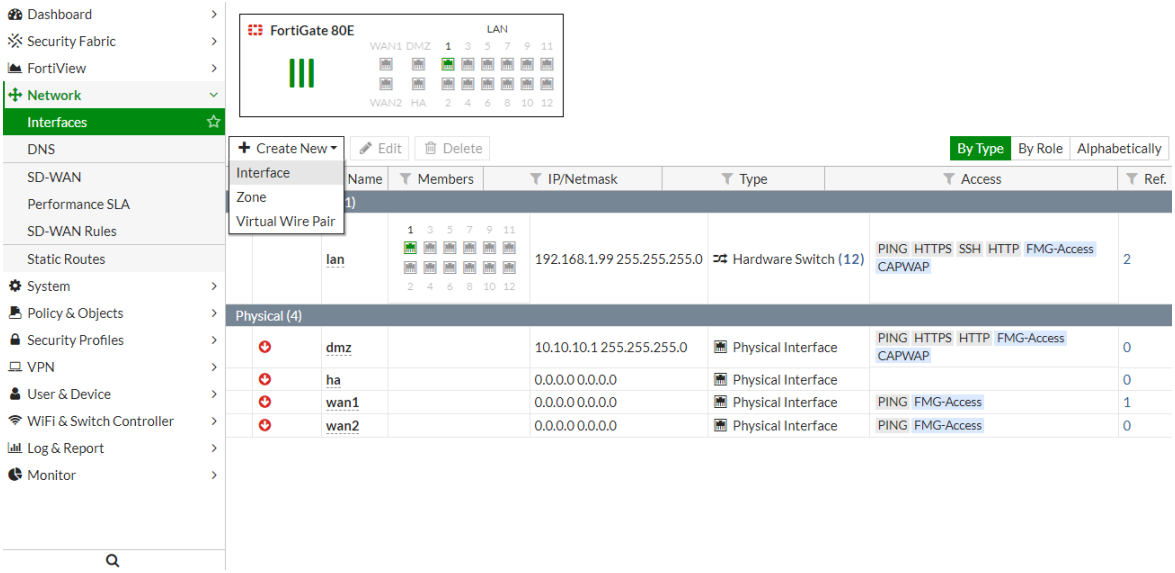


- Ta có thể đổi Password của tài khoản Administrator theo như hình bên dưới:

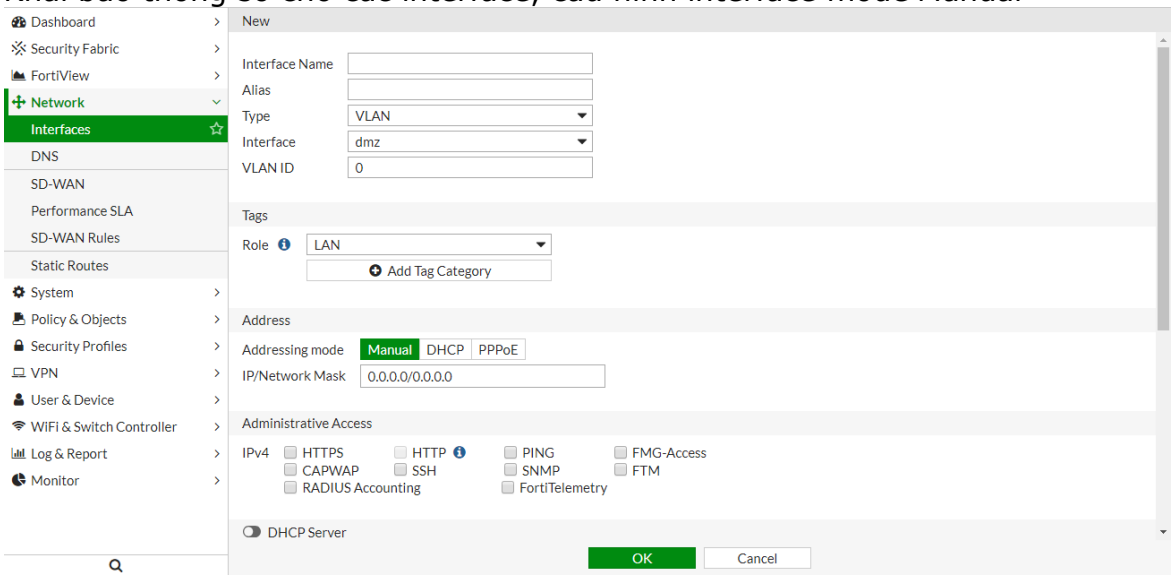


2.3: Cấu hình Network Interface

- Network interface hỗ trợ khai báo IP tĩnh, IP động, PPPoE, ta có thể cấu hình các interface theo như hình bên dưới:



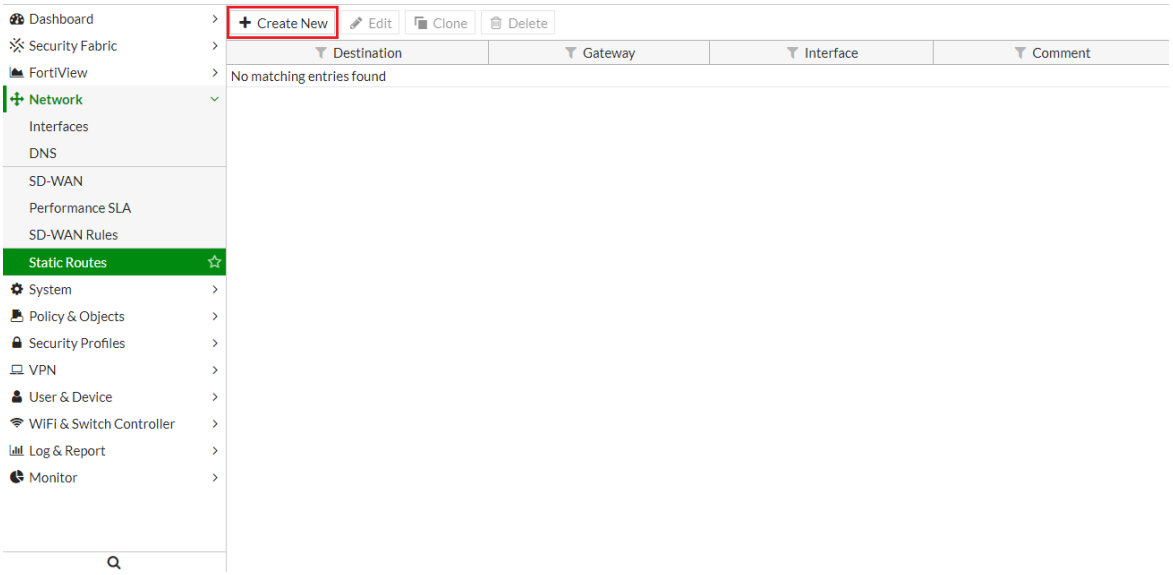
- Khai báo thông số cho các interface, cấu hình interface mode Manual



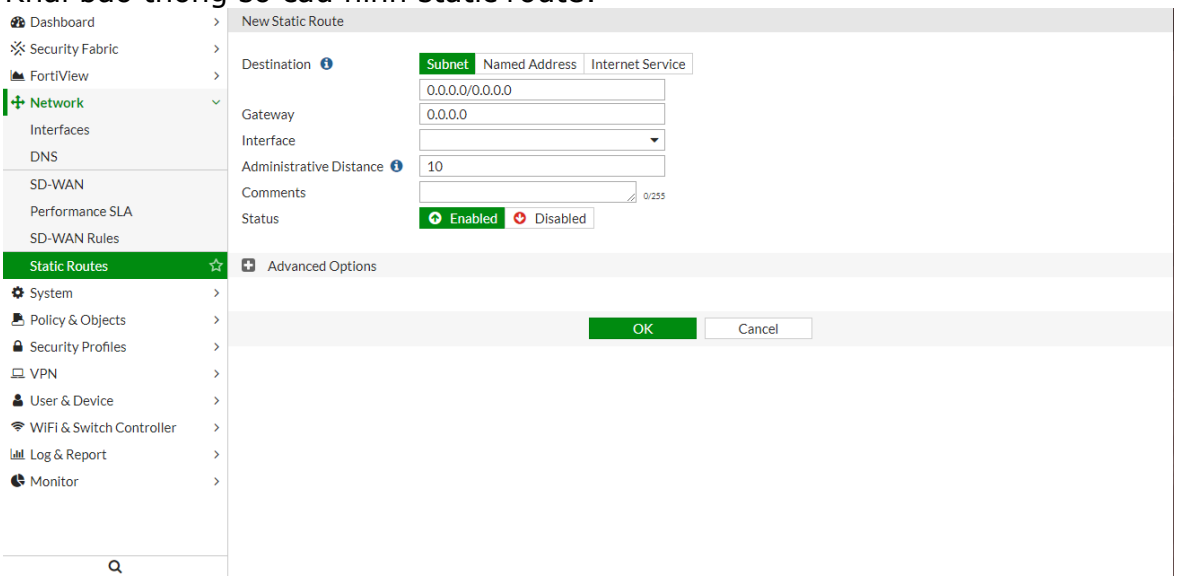
2.4: Cấu hình Routing

- Để truy cập đến các mạng không liền kề, cần tạo thêm các route tương ứng:
  - Destination
    - Routes được dựa trên IP đích
  - Source
    - Routes được dựa trên IP nguồn
- Để truy cập đến mạng bên ngoài, cần khai báo thêm default route.

- Để cấu hình static route ta thực hiện như hình bên dưới:



- Khai báo thông số cấu hình static route:

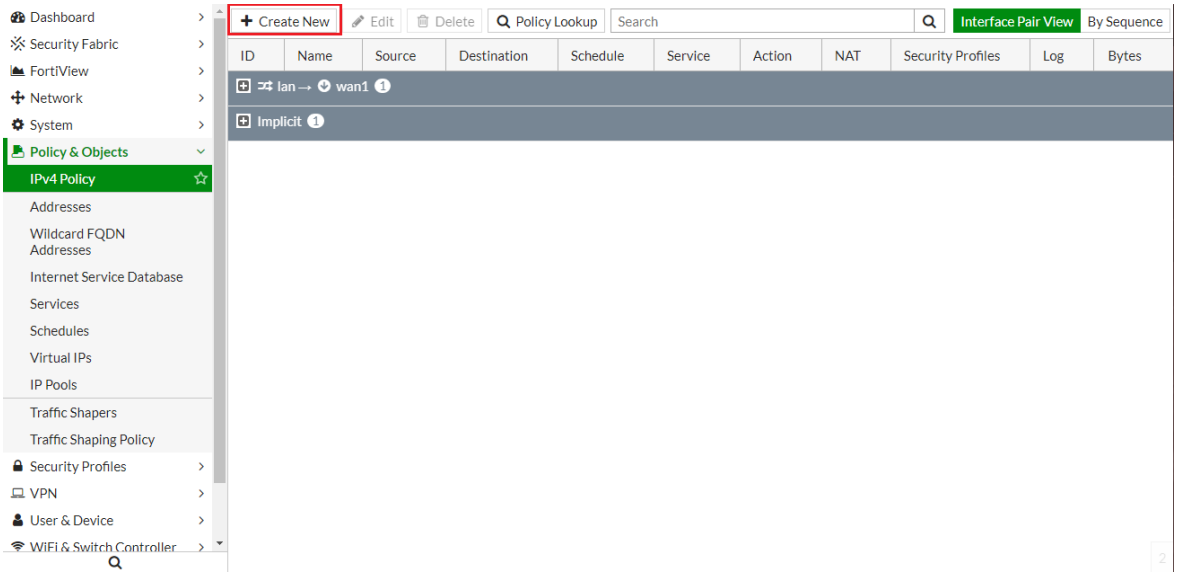


2.5: Cấu hình Firewall Policy

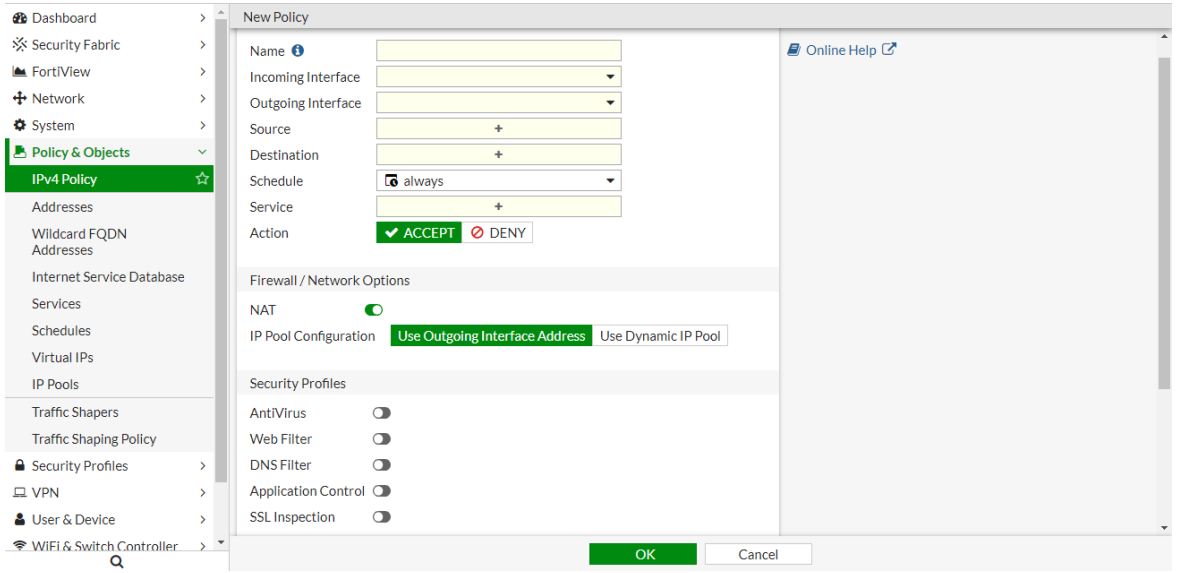
- Policy dùng để Kiểm soát traffic vào ra giữa các zone với nhau và áp các chính sách cho các Zone
- Khi route được quyết định thì policy sẽ được thực thi.
- Tất cả các model đều có policy mặc định.

- **Để tạo một chính sách (policy) ta thực hiện như bên dưới:**

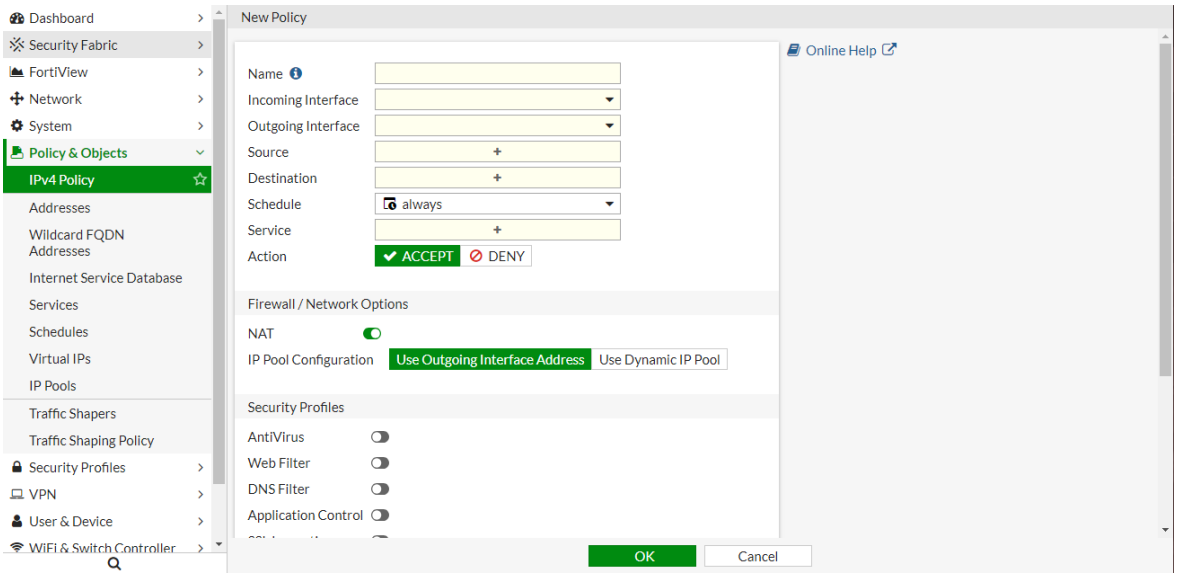
  Policy & Objects -> IPv4 Policy -> Create New.



Các nội dung cần khai báo trong **Policy** gồm: Name, Incoming Interface, Outgoing Interface, Source, Destination, Schedule, Service, Action.



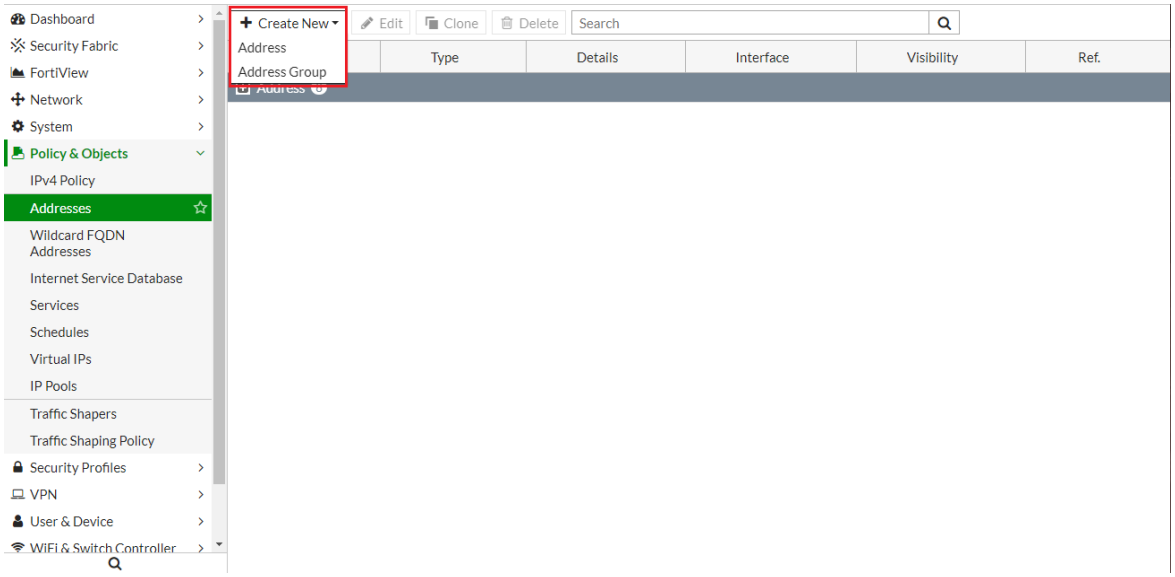
- *Action*: áp dụng các hành động trong policy
    - Các lựa chọn trong Action:
        - Accept (cho phép)
        - Deny (cấm)



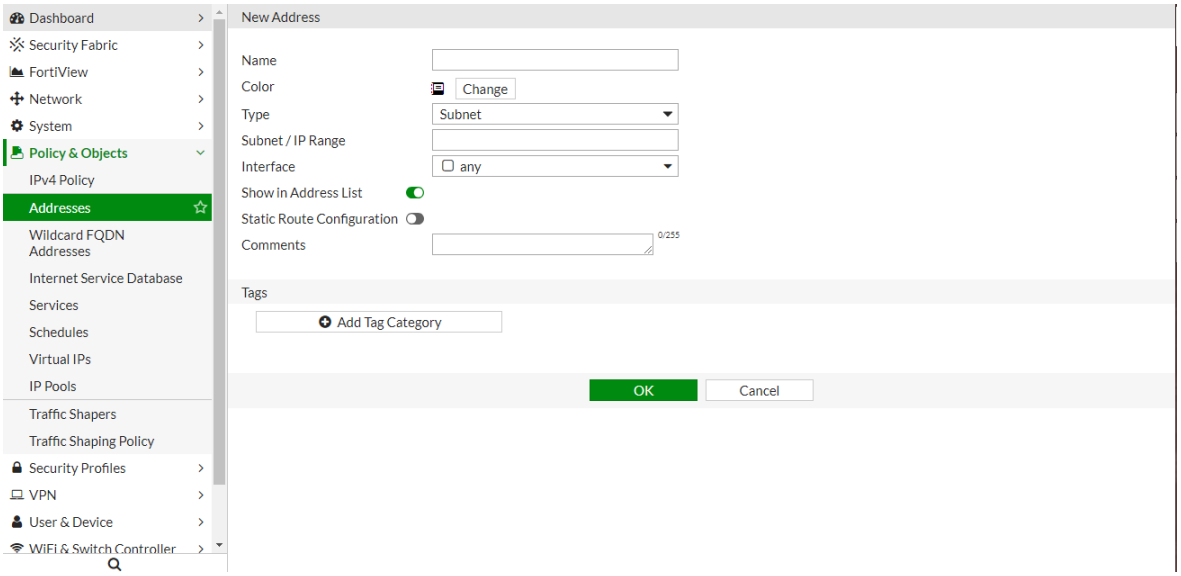
- Dưới đây là cách khai báo một số thông số trong policy:

  + *Source Address và Destination Address:* Có thể chọn 1 địa chỉ hoặc là một nhóm địa chỉ IP được định nghĩa bằng "Address" nhằm đơn giản hóa các policy. Để tạo một địa chỉ mạng ta thực hiện:

  Policy & Objects -> IPv4 Policy -> Create New -> Address.

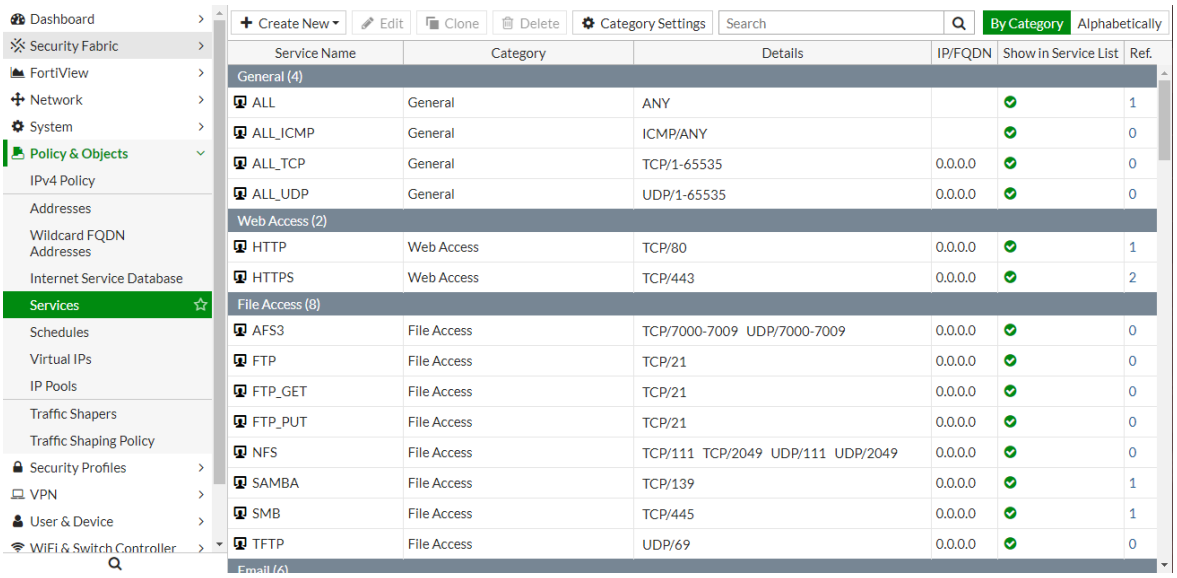


- Khai báo các thông số cho một Address.
    - Cho phép tạo subnet, dãy IP, hoặc 1 địa chỉ.
    - Chú ý: khi tạo 1 địa chỉ thì subnet là 32.

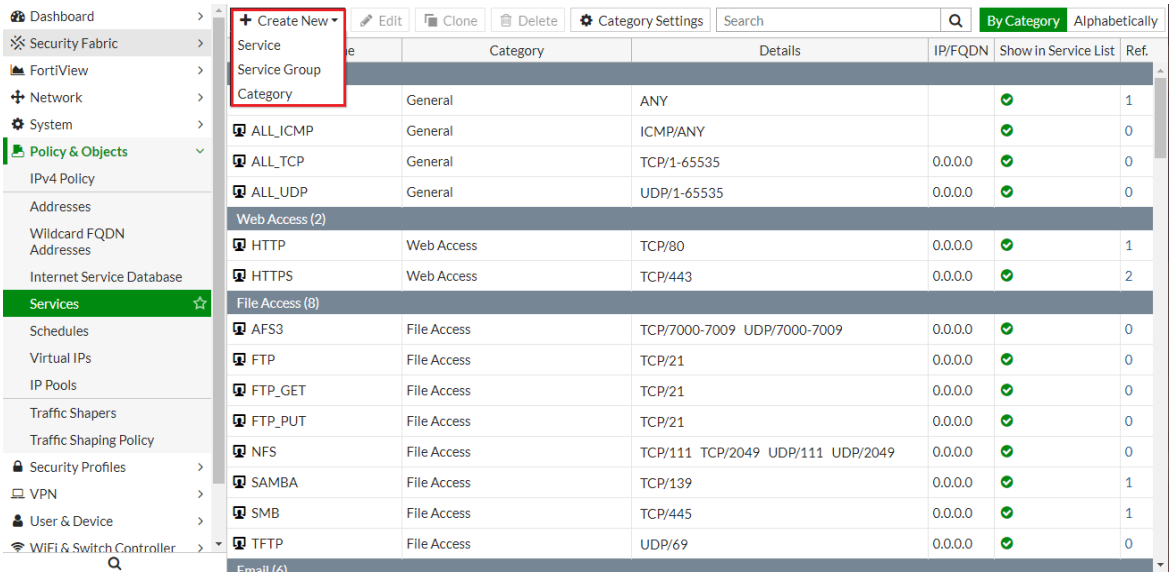


- *Services*: Fortinet firewall đã định nghĩa sẵn rất nhiều dịch vụ (predefined) và nhóm dịch vụ được sử dụng phổ biến.
    - Service Any đại diện cho tất cả các services (ports).
    - Group service và services phục vụ cho việc lập chính sách truy cập.
    - Group service và services giúp lập chính sách rõ ràng, chính xác.

Những Service đã định nghĩa trước được liệt kê chi tiết.



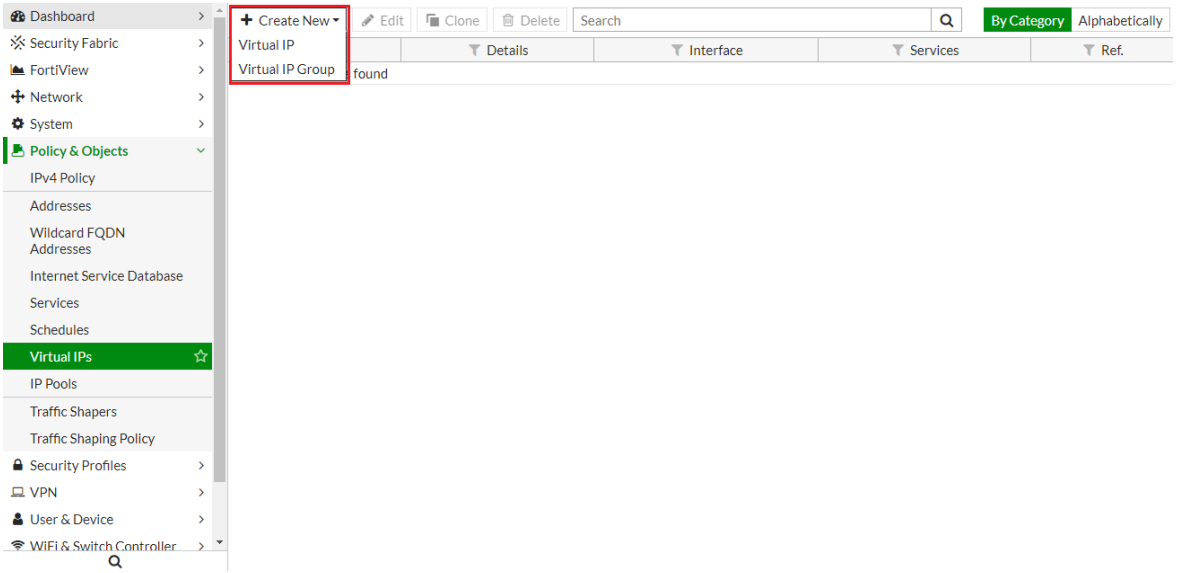
Ngoài những services được định nghĩa sẵn ta có thể tạo thêm bằng "**Create new**":



2.6: NAT (Virtual IP)

- NAT tĩnh
  - Một IP nguồn được chuyển thành địa chỉ một IP đích trong bất kỳ thời gian nào.
- NAT động
  - IP này thay đổi trong các thời gian và trong các kết nối khác nhau.
- VIP (Virtual IP): Một dạng của Destination NAT. Cho phép người dùng bên ngoài truy cập những dịch vụ vào mạng bên trong. Mở port để đi vào giao tiếp với địa chỉ IP bên trong và port của nó.

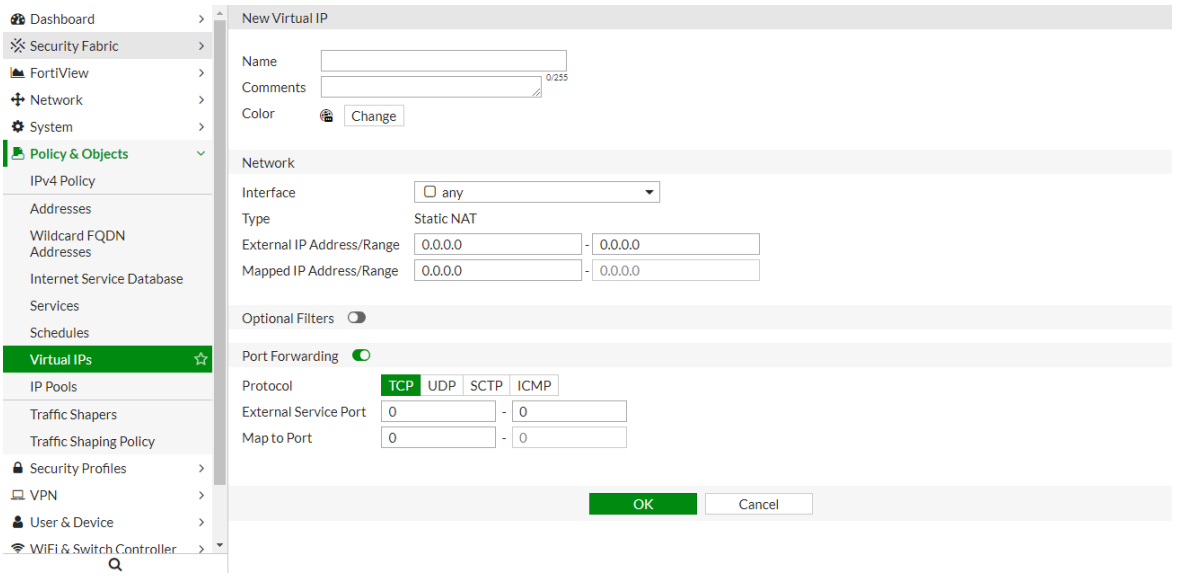
Tạo policy từ WAN -> Internal với source address từ any -> VIP address.



External IP Address/Range: IP Wan

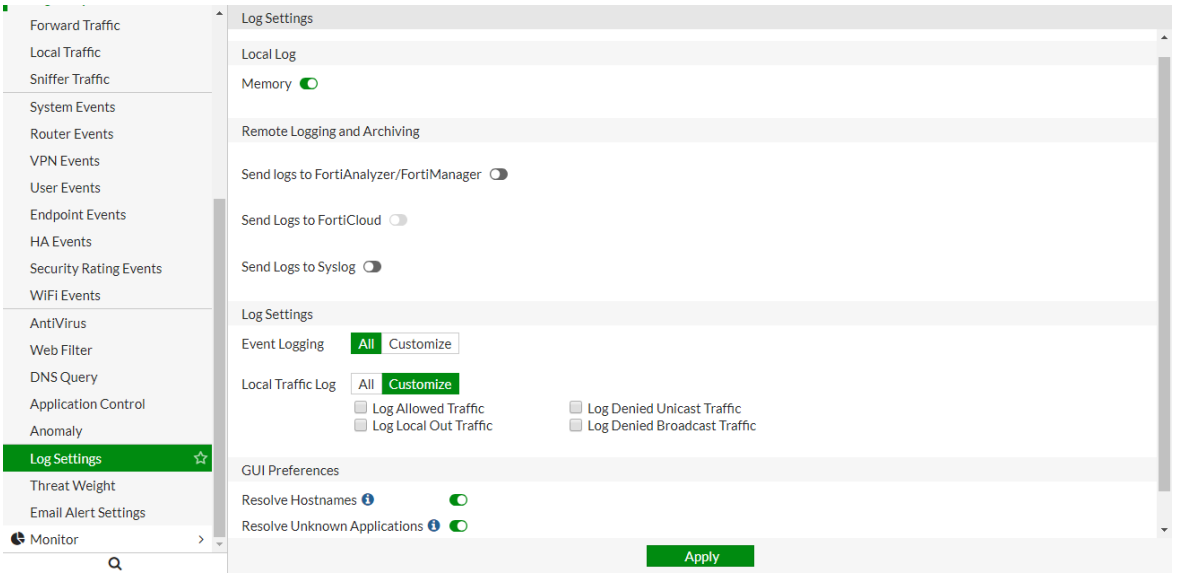
Mapped IP Address/Range: IP Local

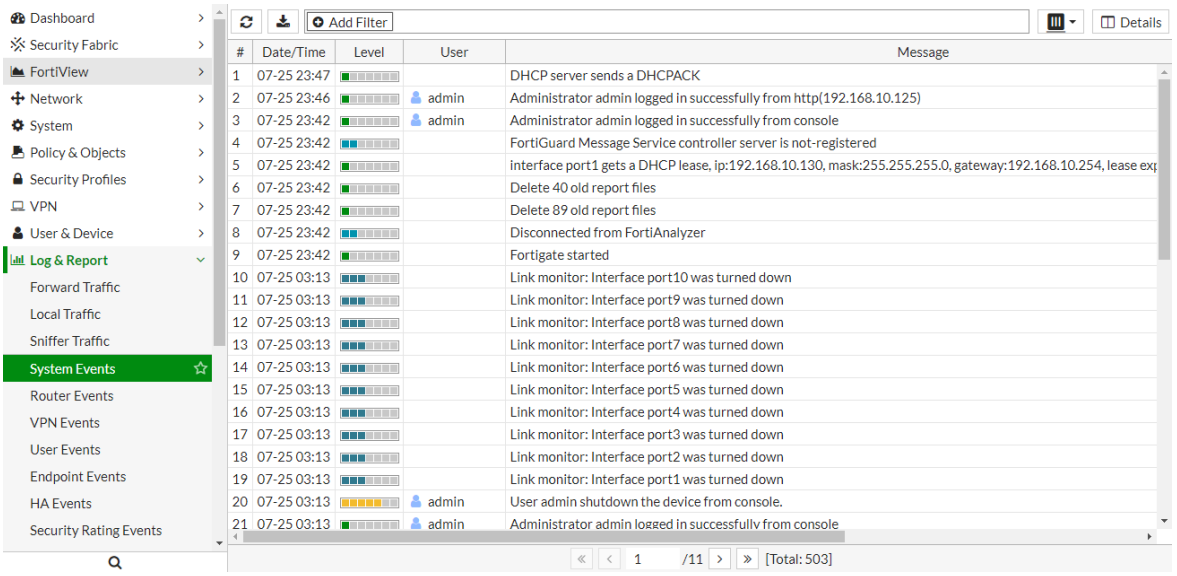
Mặc định là dạng Nat 1 – 1, nếu chỉ muốn cho sử dụng 1 port hoặc 1 range port thì tick vào "Port Forwarding" và điền thông tin port vào.



2.7: Log và Report

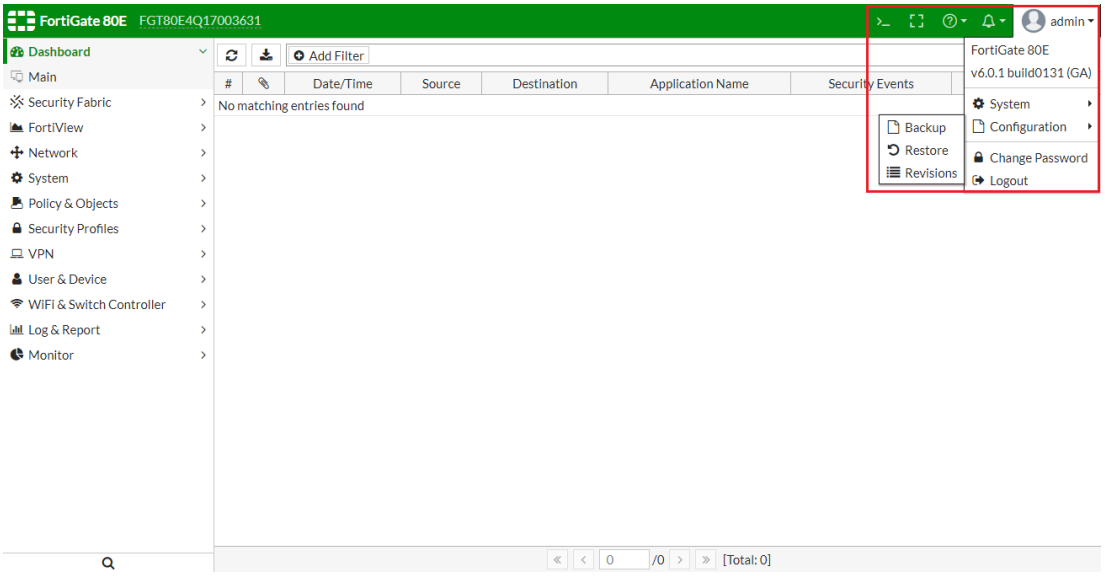
- Log để ghi lại những thao tác vào ra của traffic.
- Report cho phép người quản trị xuất báo cáo và tình trạng traffic.
- Cấu hình trong Log & Report -> Log Setting.
- Cho phép ghi log một cách chi tiết với nhiều lựa chọn.
- Log được ghi trên RAM hay Disk hoặc với thiết bị Forti-Analyzer của hãng Fortinet.





2.8: Backup và Restore

- Sử dụng để lưu trữ dự phòng và phục hồi cấu hình tốt nhất khi cần thiết.
- Để backup và restore ta làm như hình:

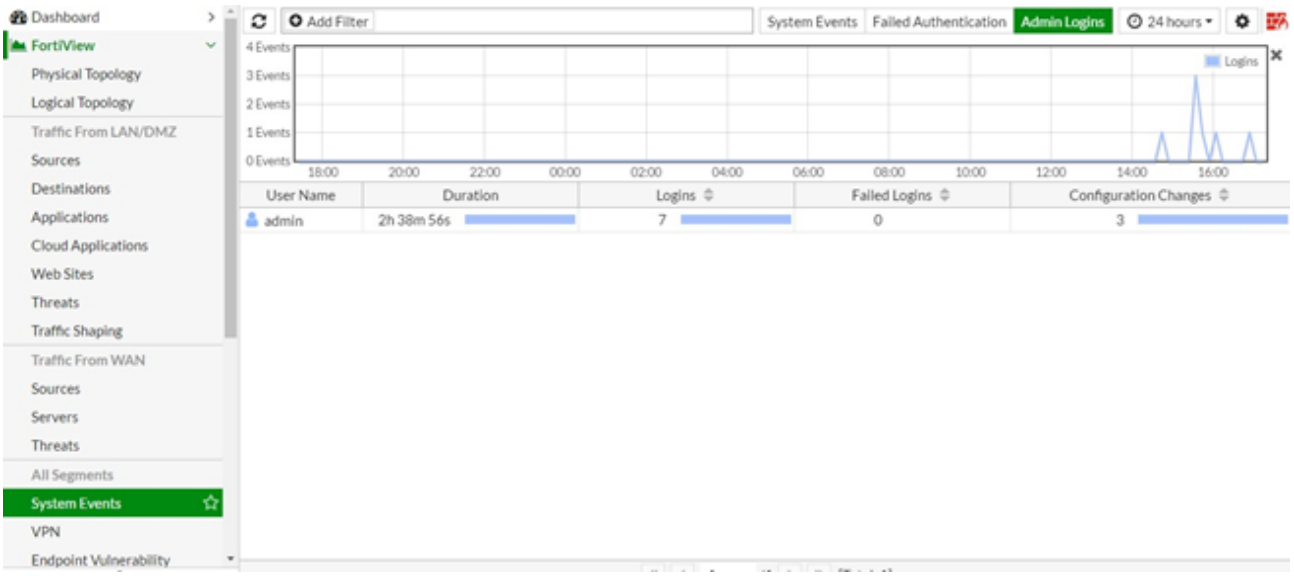


3. FortiView

FortiGate firmware 5.2 trở lên hỗ trợ tính năng FortiView giúp người quản trị có thể monitor hệ thống chi tiết hơn, cụ thể bao gồm thông tin chi tiết về Source, Destination, Application, dung lượng data mà người dùng sử dụng, từ đó admin sẽ đưa ra các chính sách phù hợp cho từng user.

- FortiView cung cấp cho người quản trị các bộ lọc bao gồm:
  - Sources
  - Applications
  - Cloud
  - Applications
  - Destinations
  - Web
  - Sites
  - Threats
  - All
  - Sessions
  - System
  - Events
  - Admin
  - Logins
  - VPN

- Khoảng thời gian mà người dùng có thể xem được trong FortiView tối đa là 24 giờ cho các thiết bị model 100D trở lên.

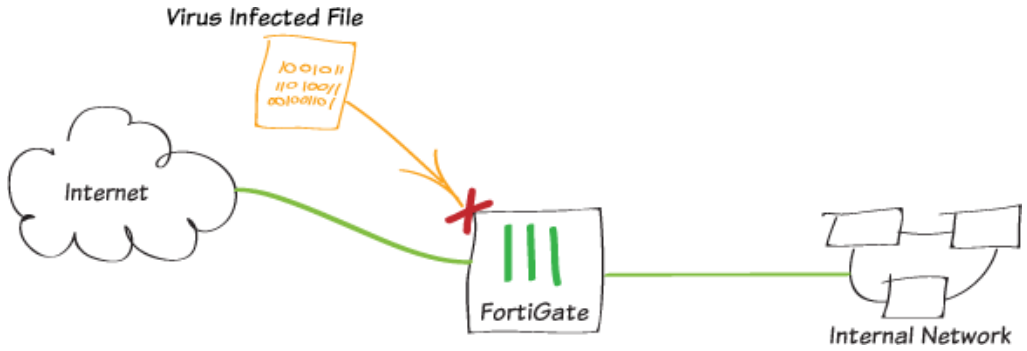


4. Anti-Virus

4.1: Môtả

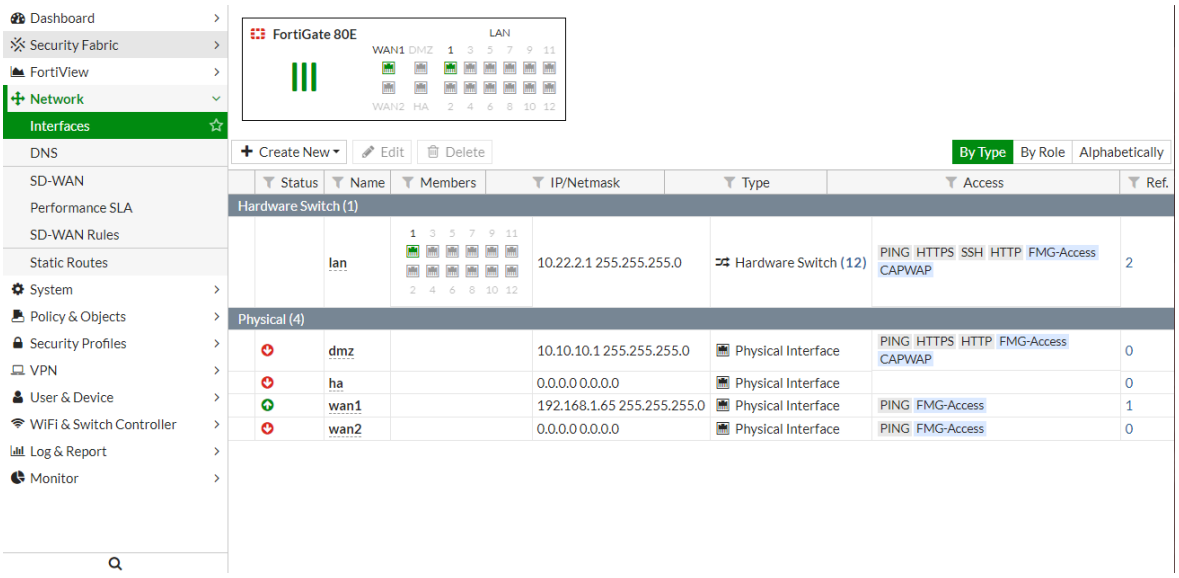
Bài lab nhằm mục đích dò tìm và ngăn chặn các nội dung bị nhiễm virus.

4.2: Mô hình

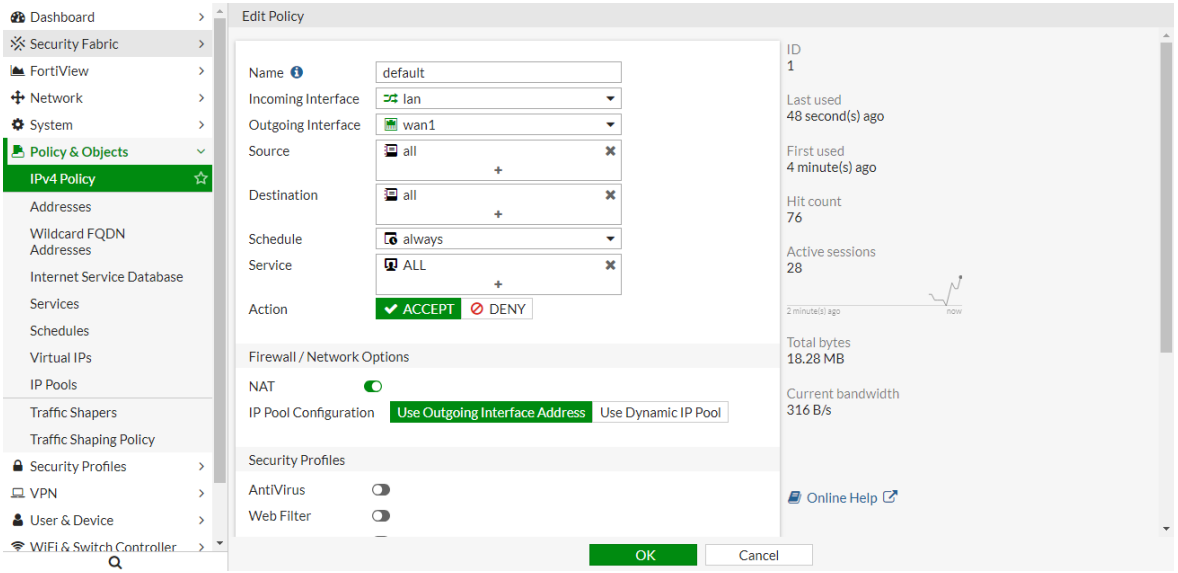


4.3: Cấu hình

B1: Cấu hình Interface



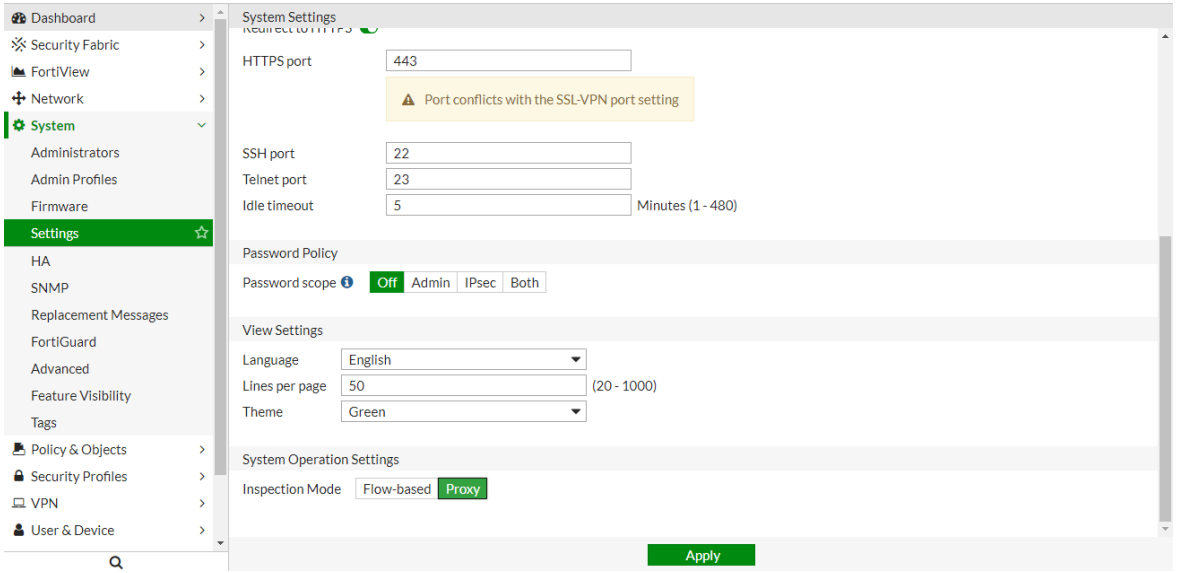
B2: Tạo Policy để đi internet



B3: Scan Virus: tạo Profile Scan ta có thể chọn quét mặc định bằng cách check hết vào virus scan hay theo yêu cầu của người quản trị.

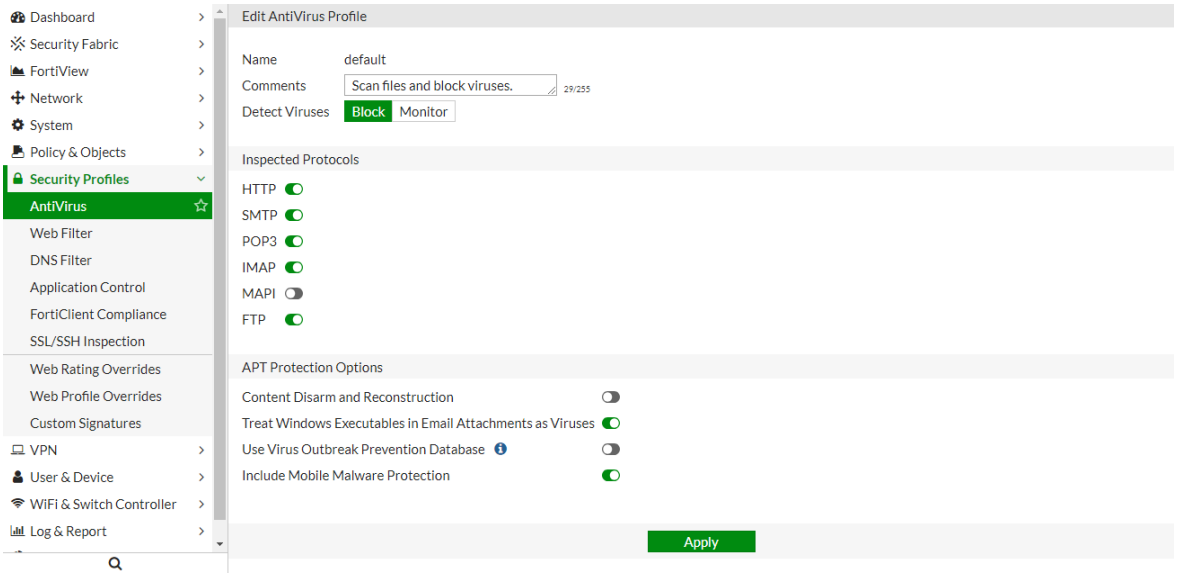
Ta có thể chọn quét theo 2 chế độ: **Proxy-base** hoặc **Flow-base.**

System -> Settings -> System Operation Settings -> Proxy.



Tạo **Profile Scan.**

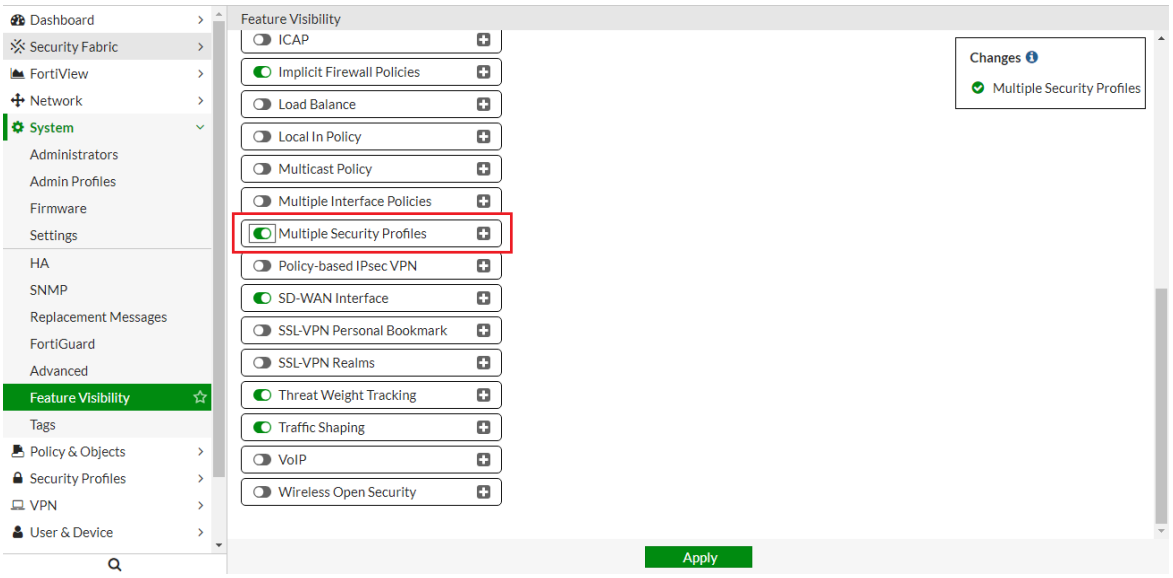
Security Profiles -> AntiVirus.



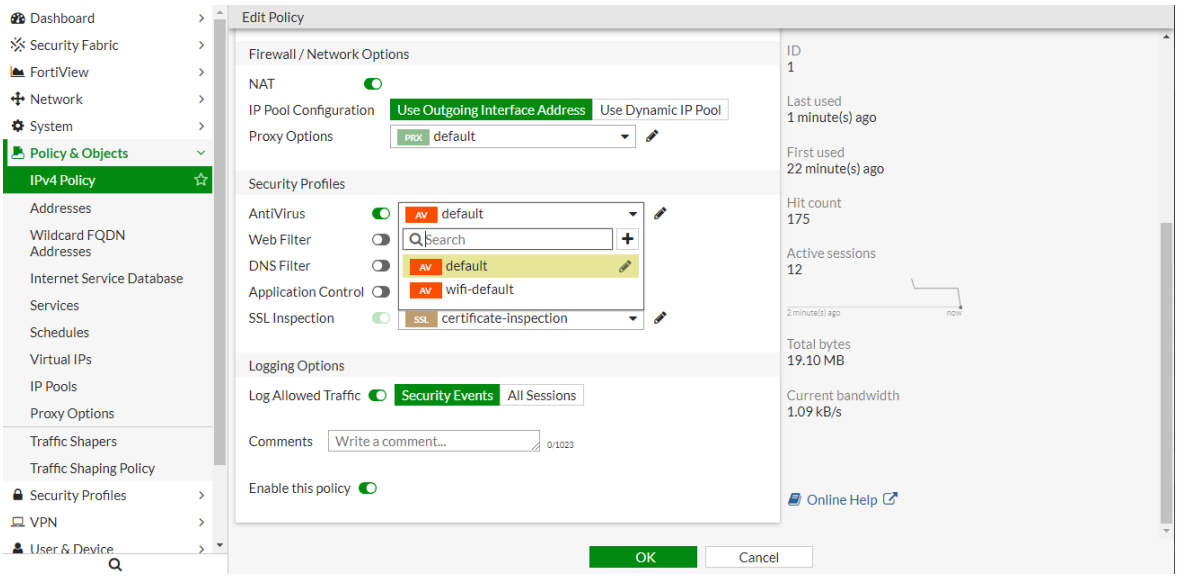
B4: Áp dụng Profile Scan vào Policy:

Trước hết, enable **Multiple Security Profile.**

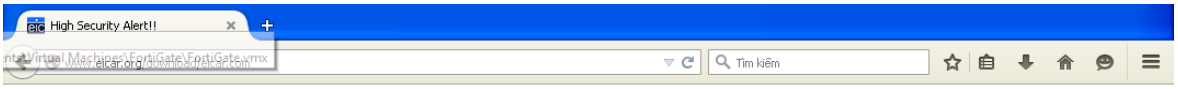
System -> Feature Visbility -> enable Multiple Security Profiles.

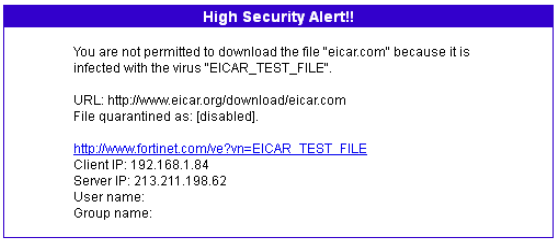


Áp dụng vào **Policy: *Policy & Objects -> IPv4 Policy -> enable Antivrus.***

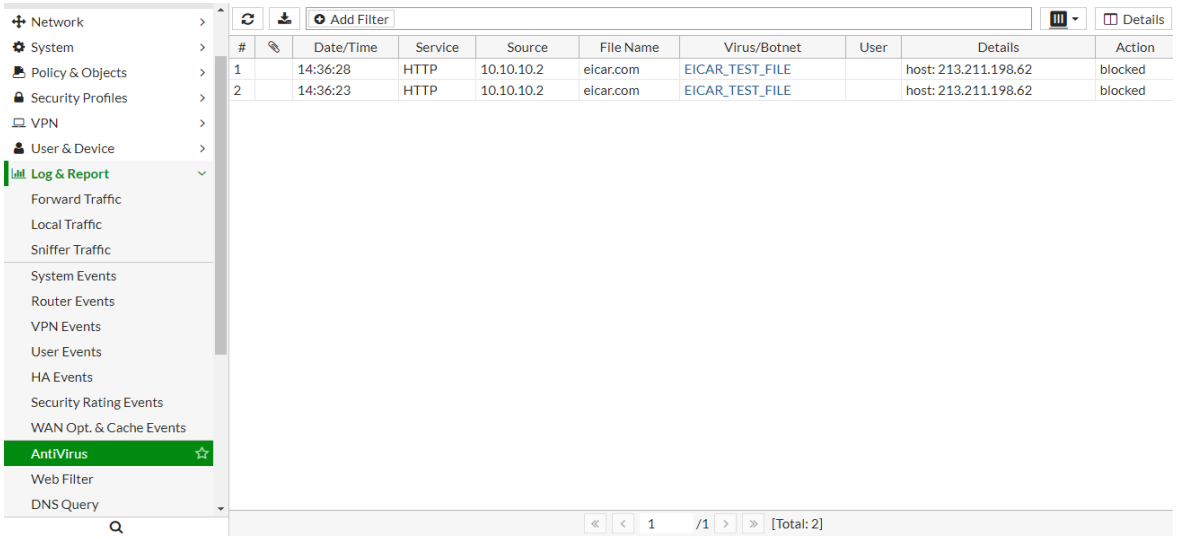


Kiểm tra: bằng cách download file chưa Virus tại **[Đây.](#)**





Xem log: ***Log & Report -> AntiVirus.***



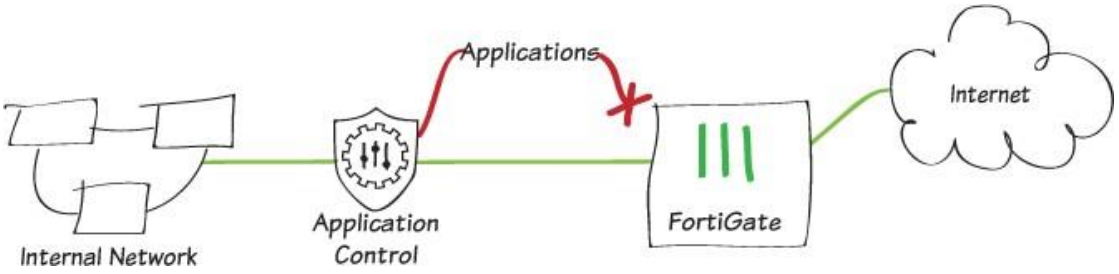
5. Application Control

5.1: Mô tả

- Application Control được sử dụng để dò và kiểm tra các hành động của các ứng dụng phát sinh trên mạng. Dựa trên giao thức IPS decoders, application control có thể log và quản lý các hành động của các ứng dụng: phân tích hệ thống mạng để xác định các ứng dụng chạy có đúng port và chuẩn giao thức không.

- FortiGate xác định các ứng dụng phát sinh trên hê thống mạng bằng cách sử dụng Application Control (AP) sensor. Thông qua AP sensor để tùy chỉnh và quản lý các hành động của các ứng dụng khi đã áp dụng vào firewall policy.
- Ta có thể điều khiển được truyền tải mạng thông thường bằng địa chỉ nguồn và đích, hay port, số lượng và các thuộc tính truyền tải được gắn bởi firewall policy. Nếu muốn kiểm tra lưu lượng của của 1 ứng dụng chỉ định thì phương pháp này không thể đảm bảo được yêu cầu.
- Đặc điểm của Application control là kiểm tra các ứng dụng phát sinh trên mạng thông qua signature, không cần đến địa chỉ server hay port. Application Control có các signature bao gồm hơn 1000 ứng dụng, dịch vụ và giao thức.

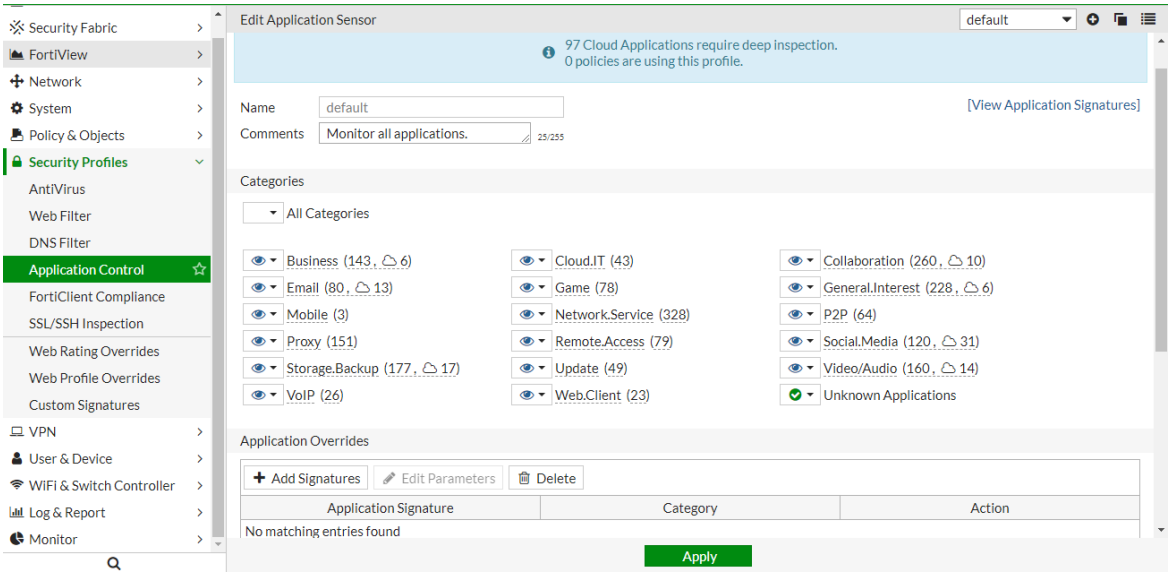
5.2: Mô hình



5.3: Cấu hình

Cấm User sử dụng **Firefox** trong hệ thống.

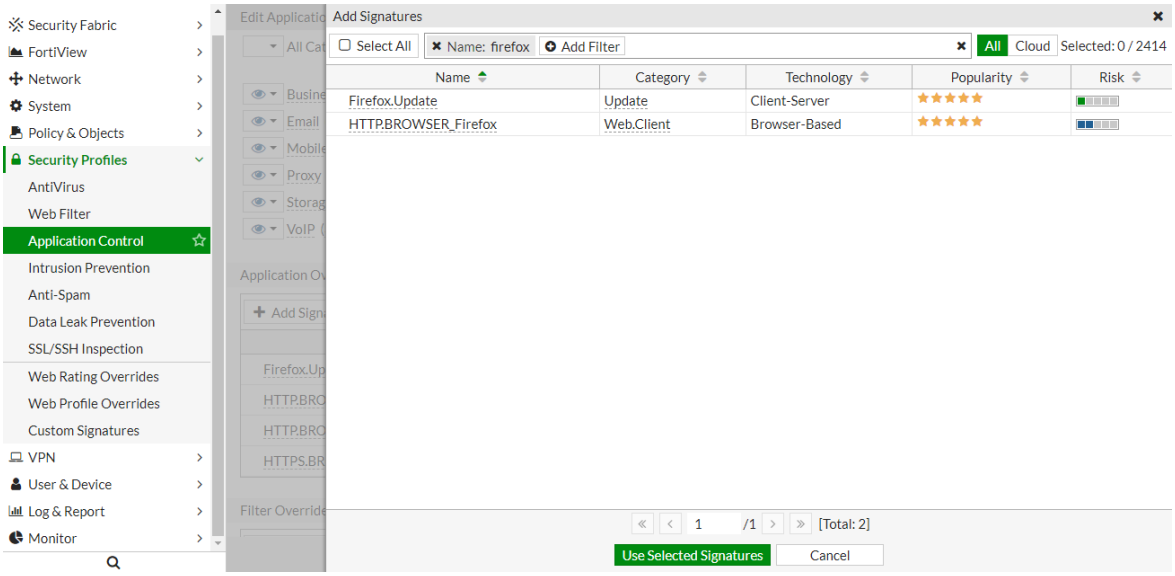
Security Profiles -> Application Control.



- *Categories:* có thể Allow, Block hoặc Monitor theo các categories mà Fortinet đã định nghĩa sẵn.
- *Application Overrides:* Trong trường hợp muốn áp dụng cho 1 ứng dụng cụ thể ta vào *Application Overrides -> Add Signatures.* Trong ví dụ chúng ta sẽ Block ứng dụng **Firefox**.

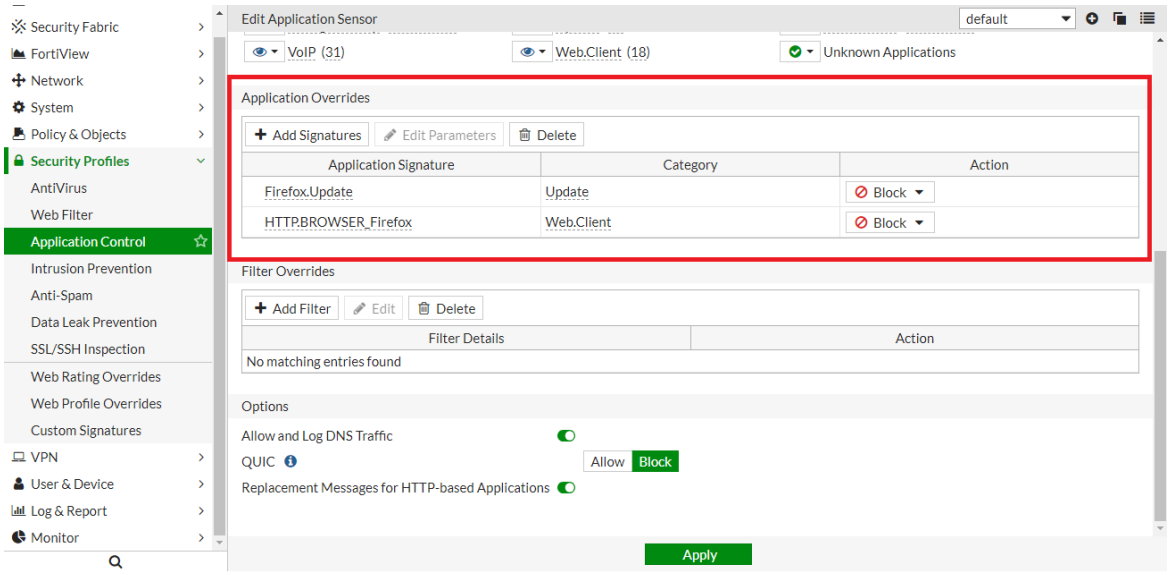
Block Firefox:

Security Profiles -> Application Control -> Application Overrides -> Add Signatures.



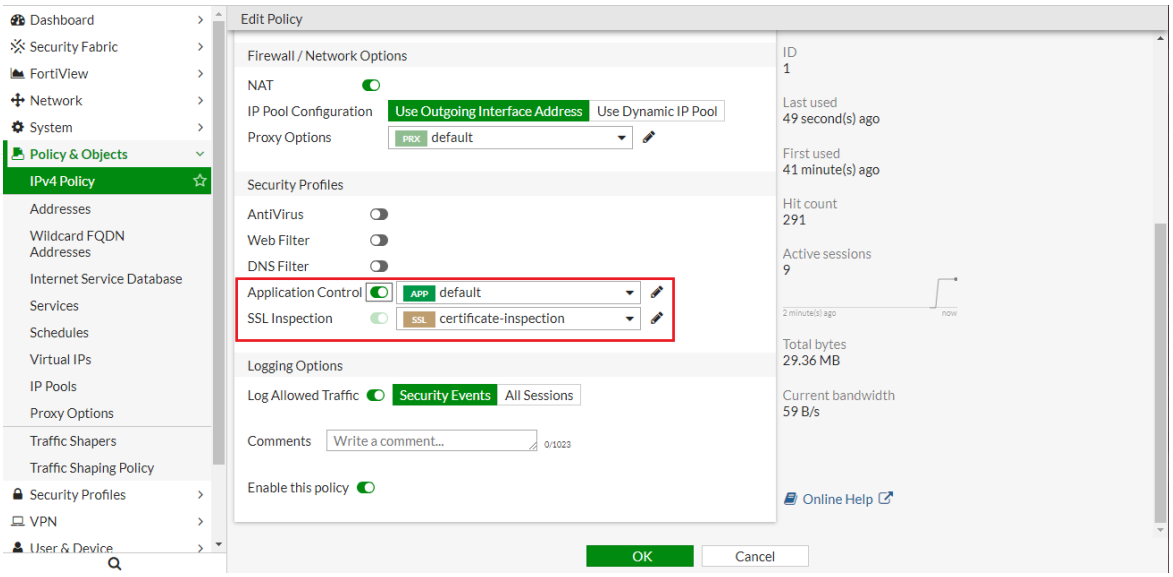
Chọn các dịch vụ **Firefox** cần Block.

Action -> Block.



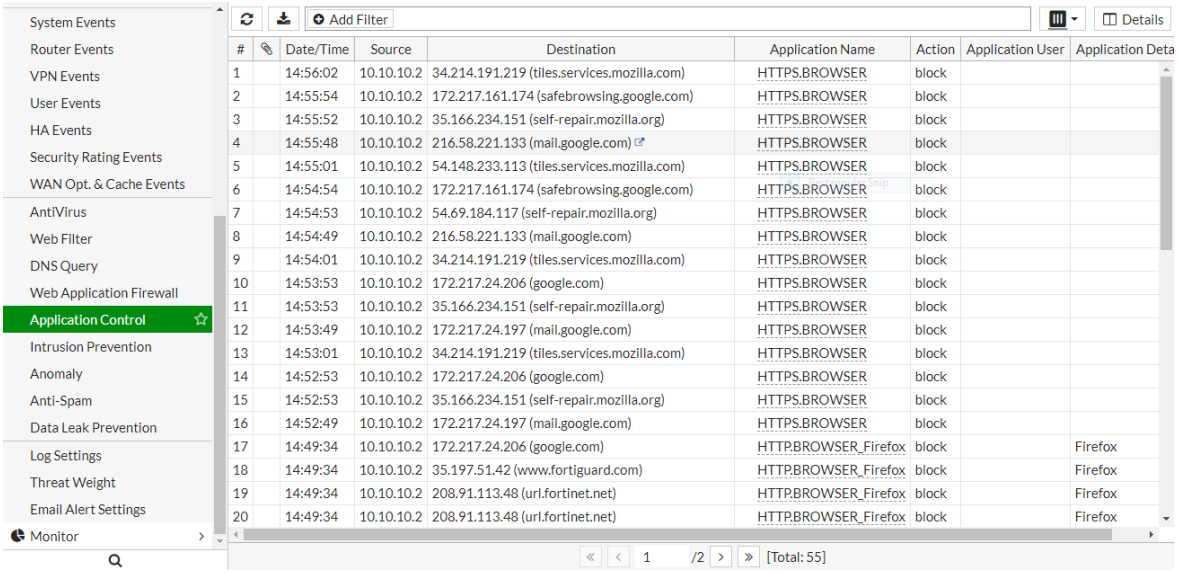
Áp dụng **Application Control** đã định nghĩa vào **Policy**.

Policy & Objects -> IPv4 Policy -> enable Application Control.



Xem log:

Log & Report -> Application Control.



6. Data Leak Prevention

6.1: Mô tả

- Một tổ chức dữ liệu cần được bảo vệ không những từ những truy xuất bất hợp lệ bên ngoài mà còn kiểm tra những cái bên trong. Người dùng không thể nhận thức được các giá trị khi mà dữ liệu bị lộ ra ngoài hay bị sử dụng bởi người khác.
- The FortiGate Date Leak Prevention(DLP) system bảo vệ các dữ liệu quan trọng khỏi bị đánh cắp. Người quản trị xác định các phần tử dữ liệu khi đi qua FortiGate sẽ được kiểm tra coi có phù hợp không. Hệ thống DLP được cấu hình

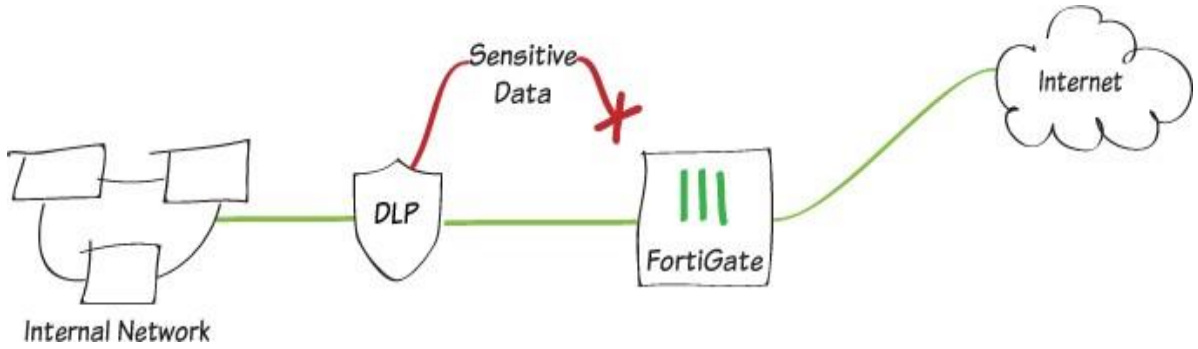
  bằng các quy luật riêng biệt, kết hợp quy luật của DLP sensor và sau đó áp đặt các sensor này vào profile.
- Các bước để kiểm tra mà tổ chức chống dữ liệu thất thoát khuyến cáo:
  - Quan sát và theo dõi các nơi mà dữ liệu bị lỗ hổng.
  - Hạn chế các đường truyền tải có thể xảy ra lỗ hổng.
  - Dò xét và loại bỏ dự liệu bị lỗi.
- Các loại dữ liệu:
  - Text, bao gồm các HTML và nội dung email

- Plaintext, nội dung PDF
- Các loại file MS Word
- Các loại file MS Office

- *DLP sensor*: sử dụng lọc dữ liệu.Thông qua áp đặt DLP sensor vào Policy thì dữ liệu sẽ được cho qua hay cấm tùy vào cấu hình.
- *DLP Filter***:** Mỗi DLP sensor có 1 hay nhiều bộ lọc tùy vào cấu hình. Bộ lọc kiểm tra truyền tải dữ liệu sử dụng DLP fingerprint như đối với file là kiểm tra tên hay kiểu, đối với file lớn thì kiểm tra dung lượng... Các hành động trong bộ lọc là: Log Only, Block, Exempt và Quarantine User, IP address, hay Interface.
- *Fingerprint*: cho phép bạn tạo một thư viện file cho FortiGate kiểm tra. Điều này nghĩa là nó sẽ tạo 1 checksum fingerprint để xác định loại file và khi file chạy trên đường truyền thì nó sẽ được so sánh với fingerprint database.
- *File Filter*: sử dụng danh sách lọc để kiểm tra hệ thống truyền tải mạng đối với các file có phù hợp không.
- *File Size***:** kiểm tra kiểu và dung lượng file.
- *Regular expression*: FortiGate sẽ kiểm tra truyền tải mạng về các chỉ định giao thức thông thường.

6.2: Mô hình

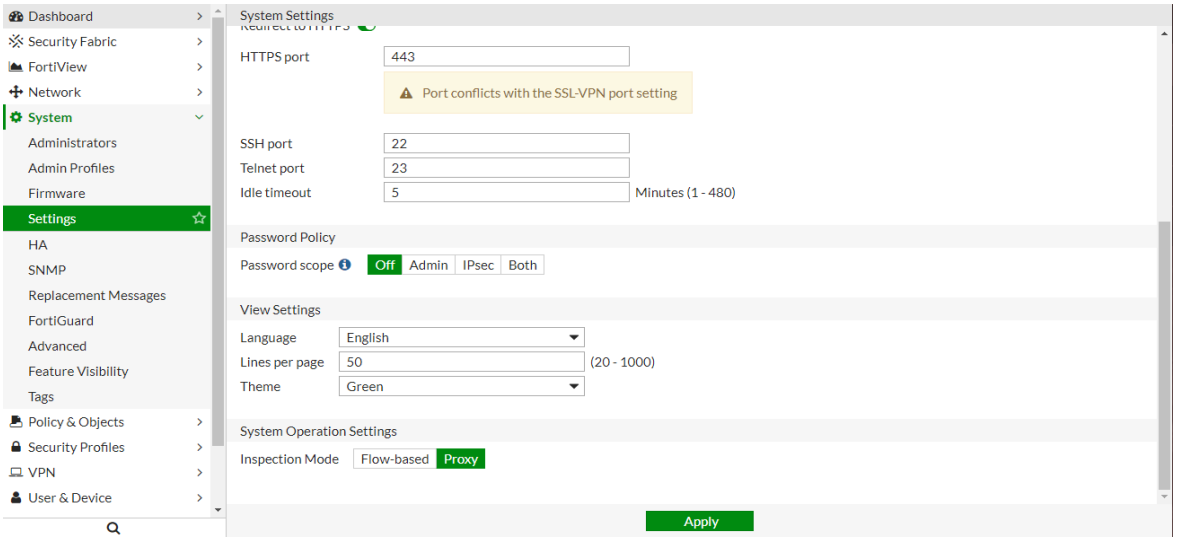
Để bảo vệ dữ liệu không bị truyền ra ngoài nên phải xác định user nào sẽ gửi email dung lượng trên 5Mb.



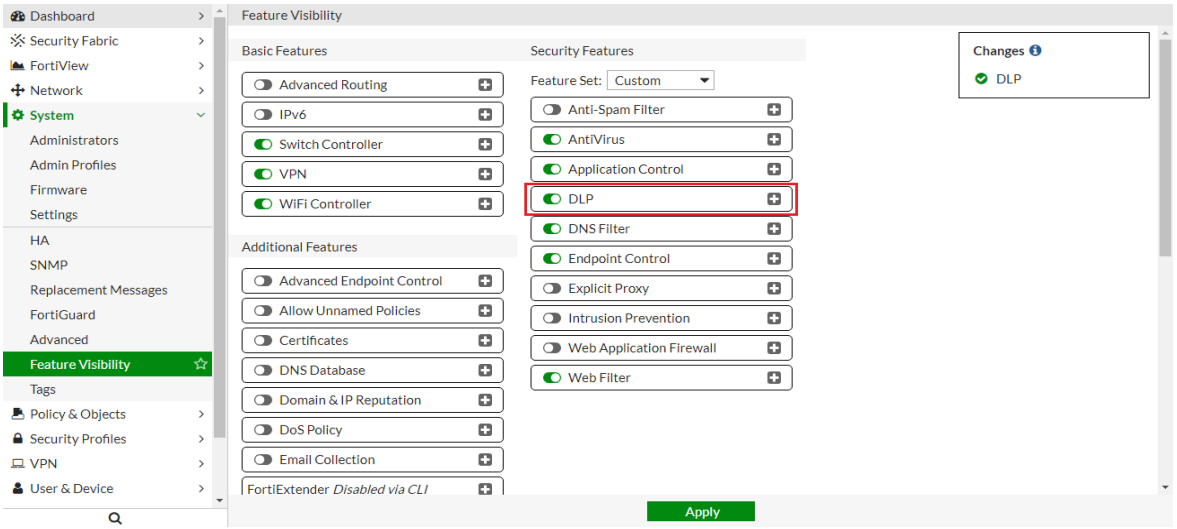
6.3: Cấu hình

Để cấu hình DLP, FortiGate Firewall phải chạy ở chế độ **Proxy-base**.

System -> Setting -> System Operations Settings -> Proxy.

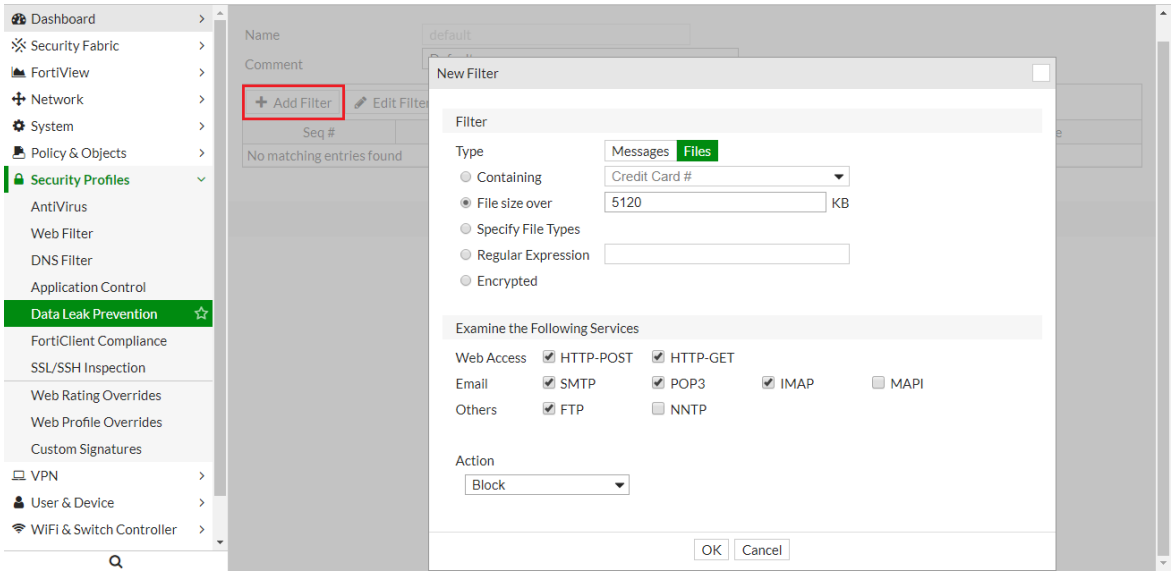


System -> Feature Visibility -> enable DLP

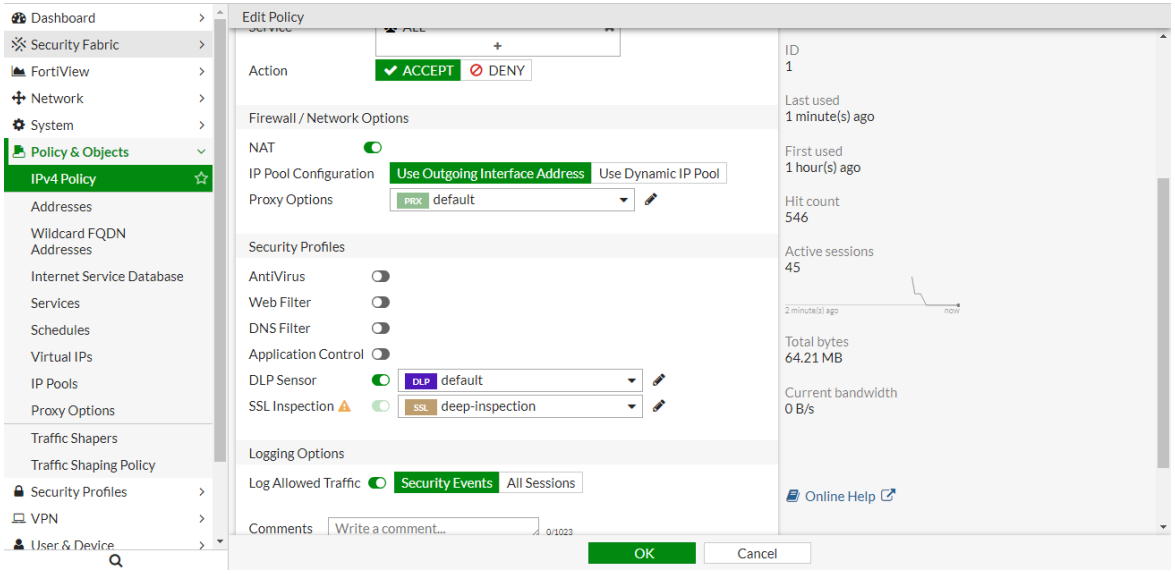


B1: Cấu hình Sensor:

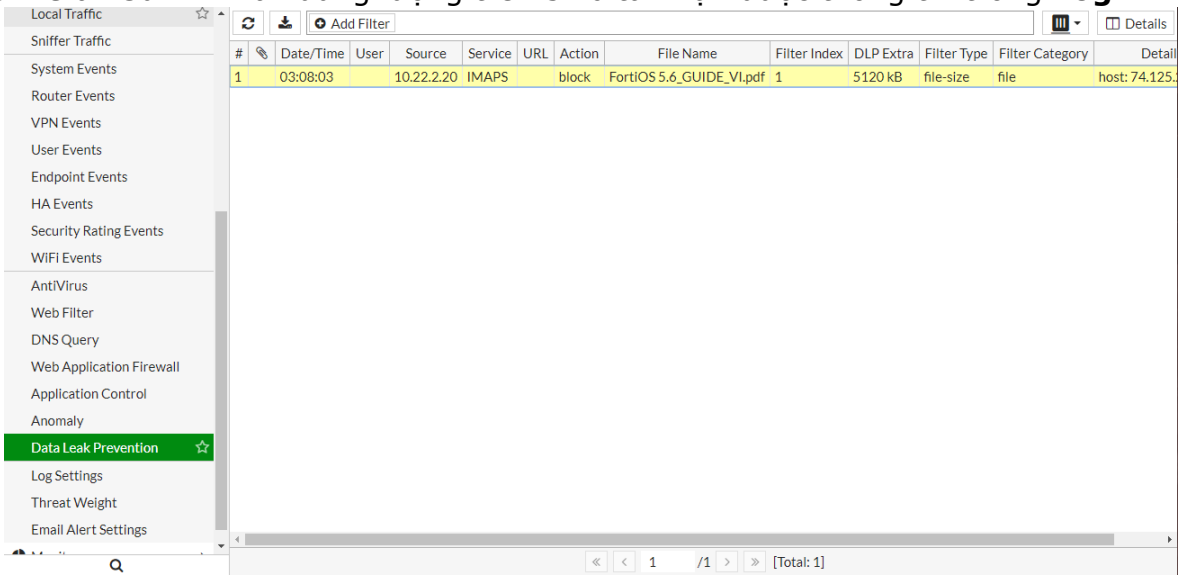
Security Profiles -> Date Leak Prevention -> Add Filter.



B2: Áp dụng vào Policy.



Kiểm tra: Gửi 1 Email dung lượng trên 5Mb ta nhận được thông tin trong **Log.**



7. Anti-Spam

7.1: Mô tả

Tính năng anti-spam nhằm hạn chế và ngăn chặn các email có nội dụng không tốt và những email không tồn tại. Với tính năng này sẽ giúp cho hệ thống email được bảo vệ tốt hơn và hoạt động ổn định hơn.

- *Fortiguard Ip address check*:
    - Fortigate sẽ gửi các truy vấn tới Fortiguard Antispam Service để xác định Ip address của client có nằm trong blacklisk không. Nếu có, Fortigate sẽ coi mail từ IP đó là spam.
- *Fortiguard URL check*:

- Fortigate truy vấn tới FortiGuard Antispam service để xác định URL có trong nội dung mail có liên quan tới spam hay không. Nếu có, Fortigate xác định email này là spam.

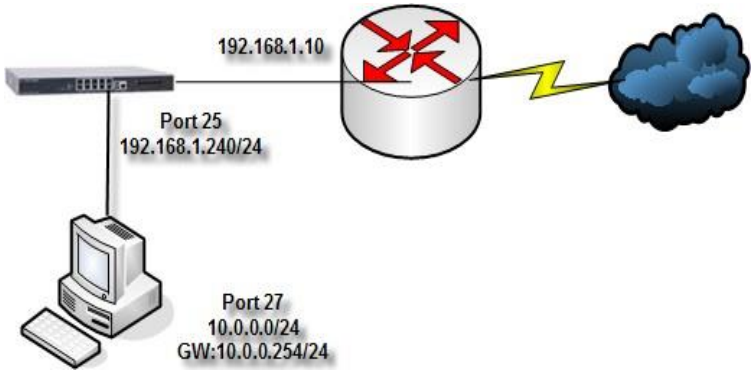
- *Detect phishing URLs in email:*
    - Fortigate gửi các URL links trong email tới Fortiguard để xác định nếu links có liên quan tới một trang phishing nào đó đã được xác định. Nếu có, link sẽ bị xóa khỏi mail. Phần còn lại của URL không còn là một hyperlink khả dụng.
- *FortiGuard email checksum check:*
    - Fortigate gửi một đoạn dữ liệu hash của email tới FortiGuard Antispam Server, ở đó nó sẽ được so sánh với hash của các tin nhắn spam được lưu trữ trong cơ sở dữ liệu của Fortiguard. Nếu trùng, email bị gắn cờ spam.
- *FortiGuard spam submission:*
    - Spam submission là một cách bạn có thể thông báo cho Fortiguard về một email không phải là spam nhưng bị gắn cờ spam. Khi bạn kích hoạt tính năng này, Fortigate thêm một link ở cuối mỗi email được cho là spam. Bạn có thể chọn link này để thông báo tới Fortiguard rằng email này không phải là spam.
- *IP address black/white list check:*
    - Fortigate so sánh IP address của client gửi email với các Ip address black/white có trong email filter profile. Nếu trùng, Fortigate sẽ thực hiện các Action đã được cấu hình.
- *HELO DNS lookup*:
    - Fortigate lấy các domain name xác định bởi client trong lời chào HELLO được gửi khi bắt đầu khởi động các phiên SMTP và thực hiện DNS lookup để xác định nếu như domain tồn tại. Nếu lookup thất bại, Fortigate xác định rằng bất kì tin nhắn nào được truyền đi trong phiên SMTP này đều là spam.
- *Email address black/white list check: L*à mục blacklist tự tạo của người quản trị.
    - Fortigate so sánh địa chỉ người gửi email ở trong phần MAIL FROM, với các địa chỉ email black/white list được xác định trong email filter profile.

Nếu tìm thấy, fortigate sẽ thực hiện các Action tương ứng đã được cấu hình.

- *Banned word check:*
  - Fortigate chặn các email dựa vào việc so sánh nội dung của tin nhắn với các từ hoặc các dạng được lựa chọn trong spam filter banned word list. Tính năng này chỉ được cấu hình trên command line.

7.2: Mô hình

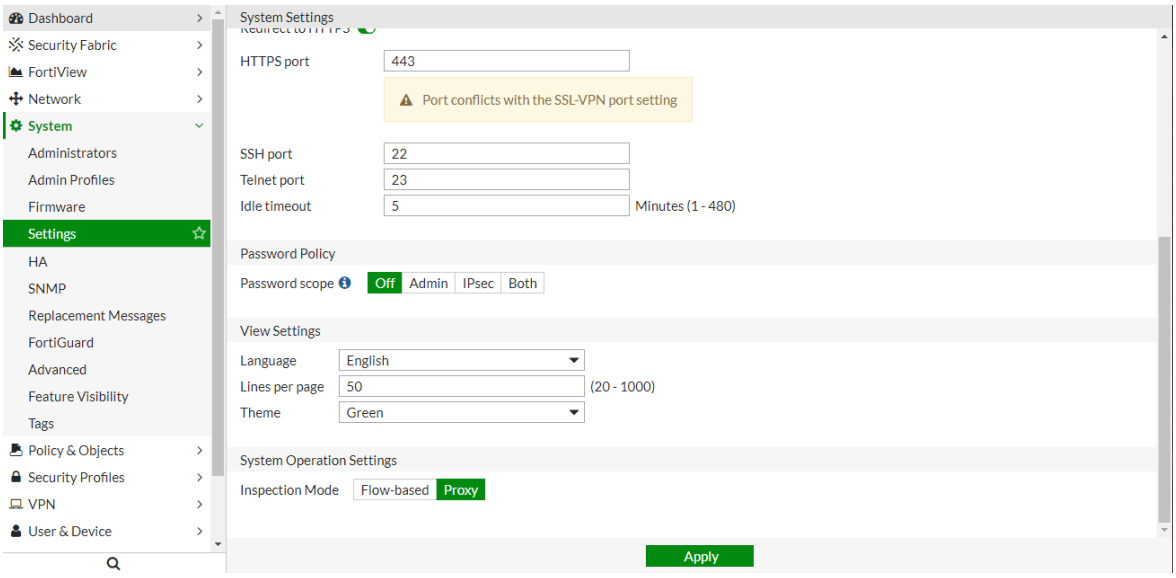
Ngăn chặn mail chỉ định và mail có nội dung chỉ định thành spam mail để user biết và check mail ko cần thiết.



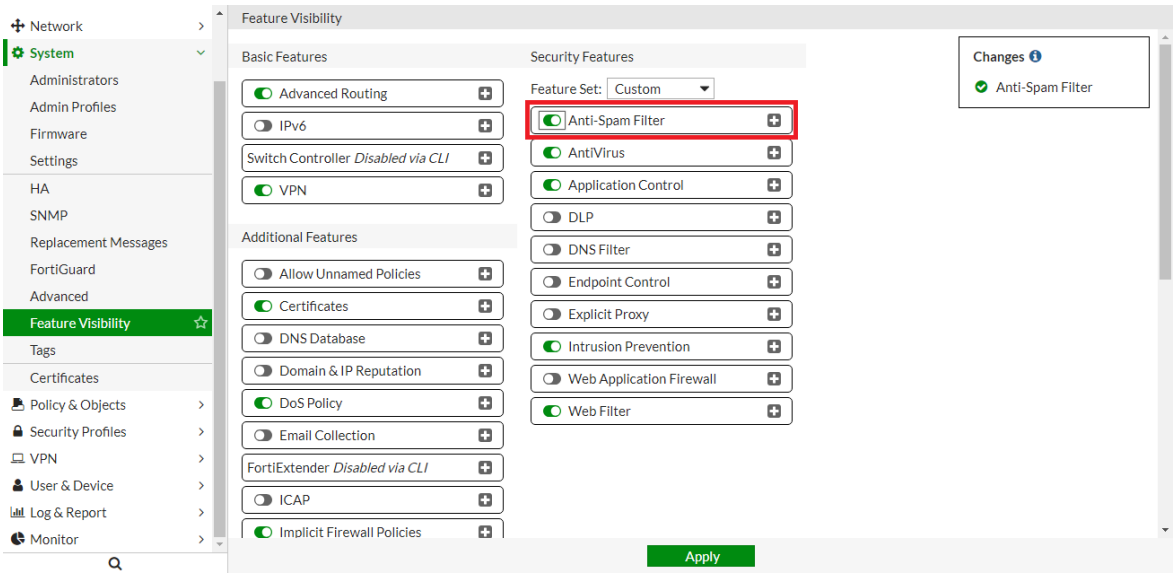
7.3: Cấu hình

Để cấu hình Anti-Spam, Firewall phải chạy ở chế độ Proxy-base.

System -> Setting ->Operations Settings -> Proxy -> Apply.

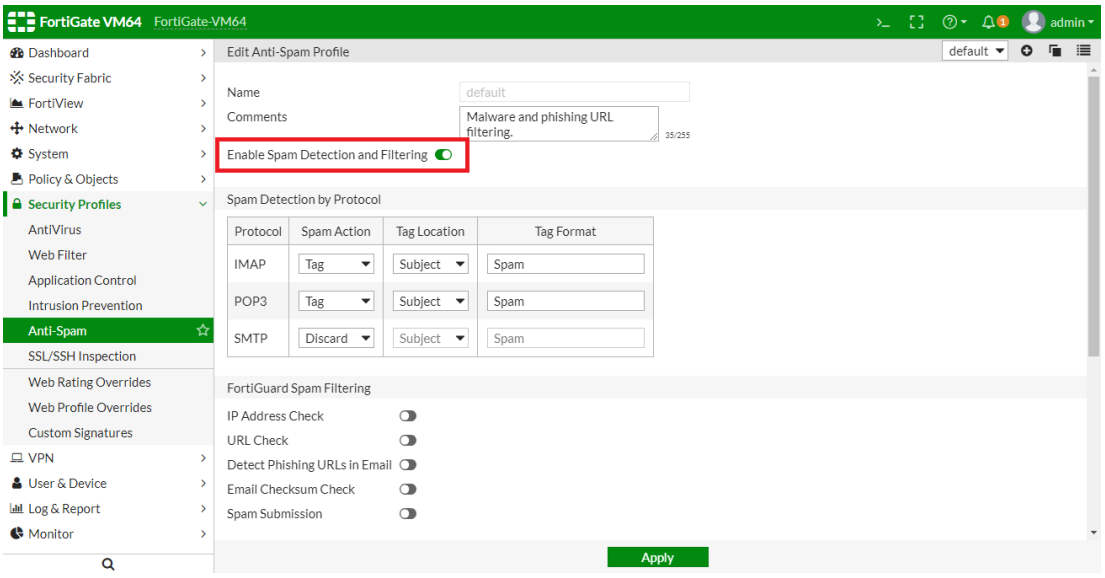


System -> Feature Visibility -> Enable Anti-Spam Filter -> Apply.



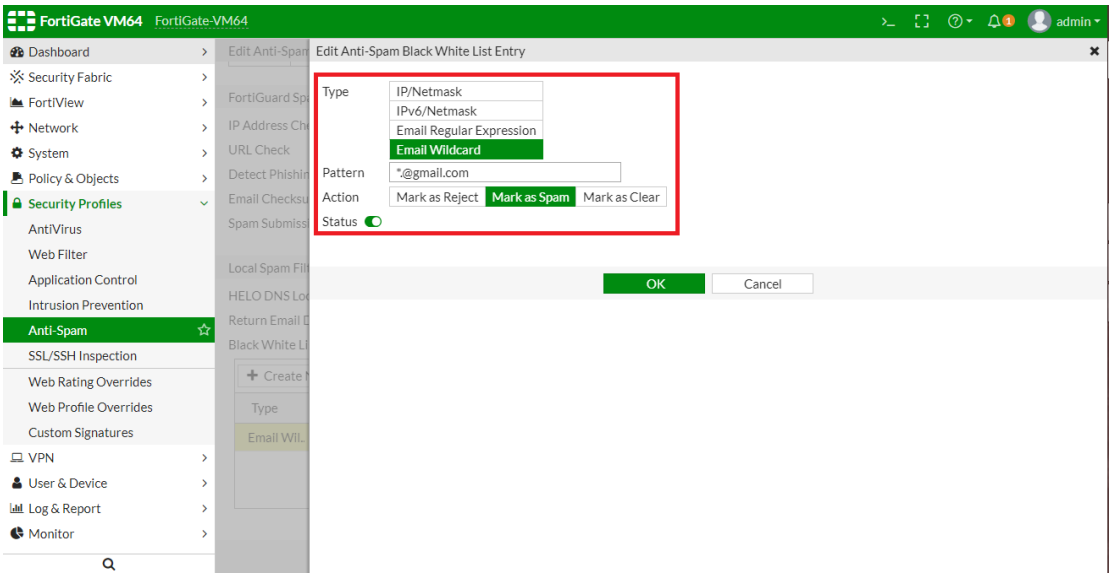
Ví dụ: Cấu hình đánh dấu Spam các email *@gmail.com

B1: *Security Profile -> Anti-spam -> Enable Spam Detection and Filtering.*



B2: Tạo Email list tên là Black-List: cho các mail có đuôi *@gmai.com và đặt hành động là Spam.

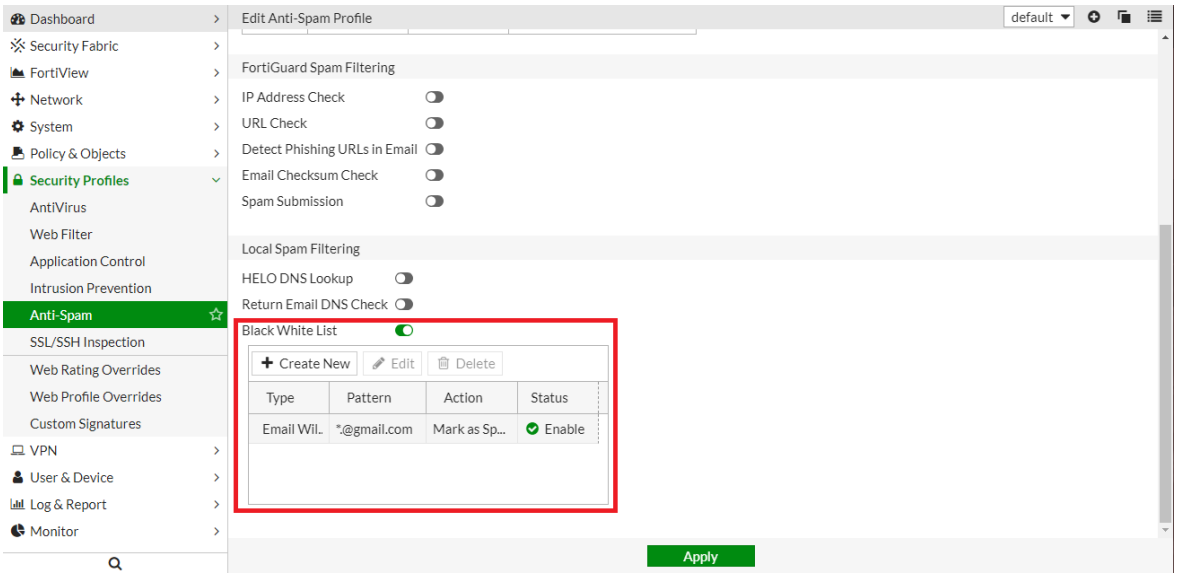
Security Profiles -> Anti-Spam -> enable Spam Detection & Filtering.



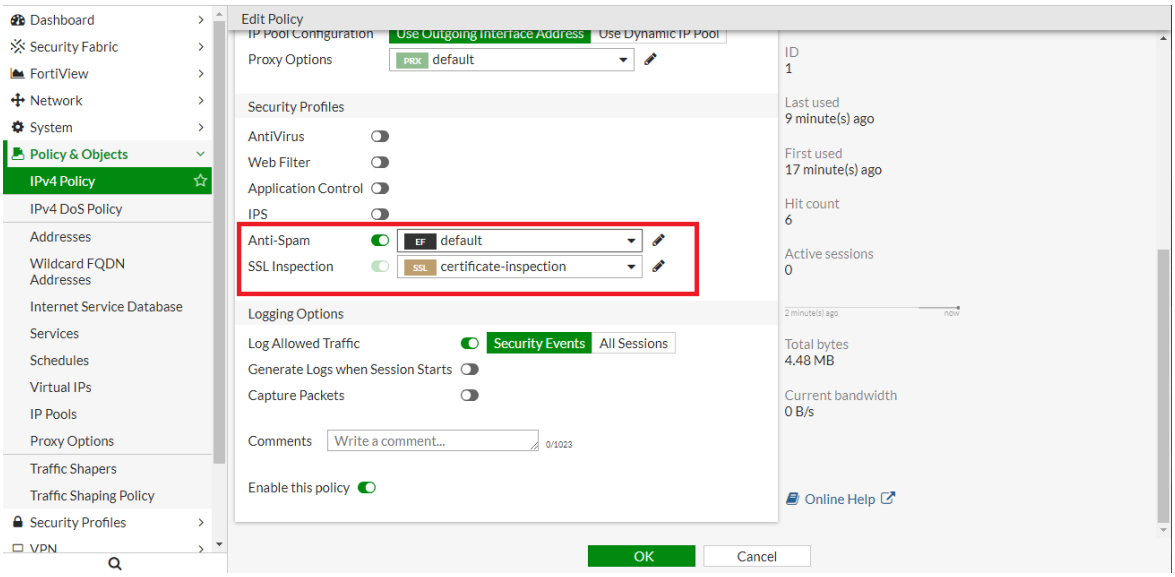
Enable Black White List.

Spam Action:

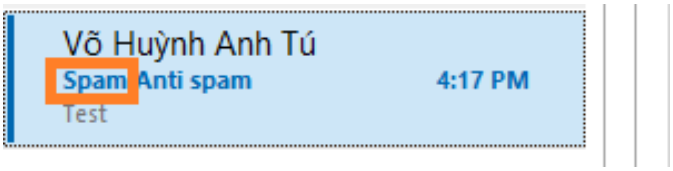
- **Discard:** là loại bỏ mail mà không có thông báo.
- **Tagged:** với các email bị xác định là spam sẽ bị gắn nhãn và truyền đi như thường, khi nhận được email này người dùng sẽ thấy chứ spam trên mục header của mail.



B3: Áp dụng Anti-Spam vào Policy:



Kiểm tra:



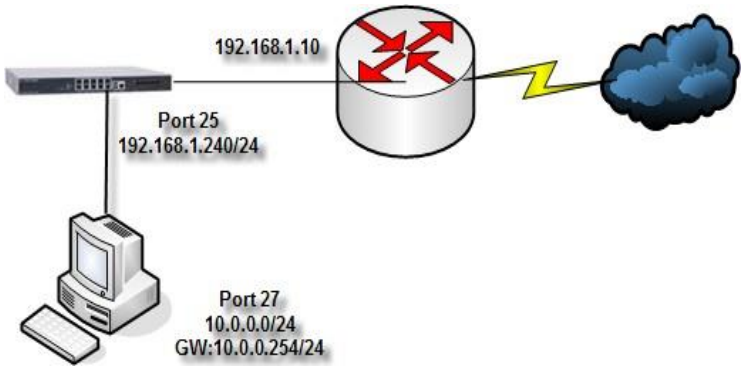
8. Web Filter & OverRide

8.1: Mô tả

Tính năng này giúp Fortigate lọc các luồng traffic HTTP. Ba phần chính của chức năng lọc web là Web Content Filter, URL Filter và FortiGuard Web Filtering Services, chúng sẽ tương tác với nhau để cung cấp sự điều khiển lớn nhất với bất kì người sử dụng internet nào, từ đó bảo vệ mạng của bạn trước bất kì nội dung nguy hiểm nào của internet. Web Content Filter chặn các trang web chứa các từ hoặc khuôn dạng mà bạn đã xác định trước đó. URL filtering sử dụng URLs và dạng URL để ngăn chặn các trang web từ những nguồn cụ thể đã được xác định trước. FortiGuard Web Filtering cung cấp nhiều categories để bạn có thể lựa chọn sử dụng để lọc các luồng traffic web.

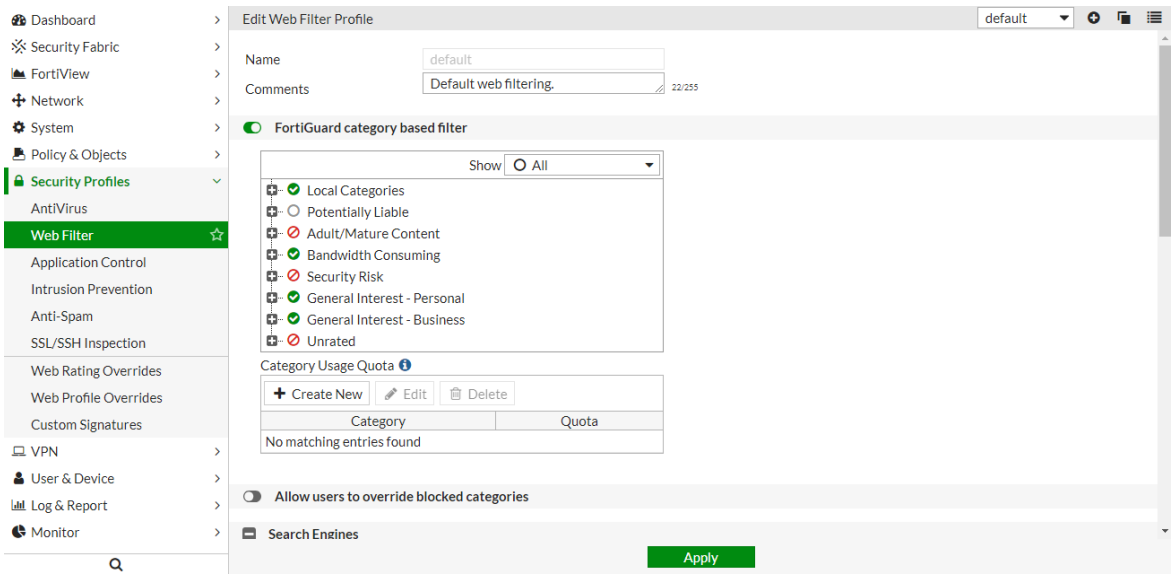
8.2: Mô hình

Cấm user không truy cập vào web chỉ định (VD: ngoisao.net) Cấm user ko thể truy cập được web có nội dung game hay web có từ "game".



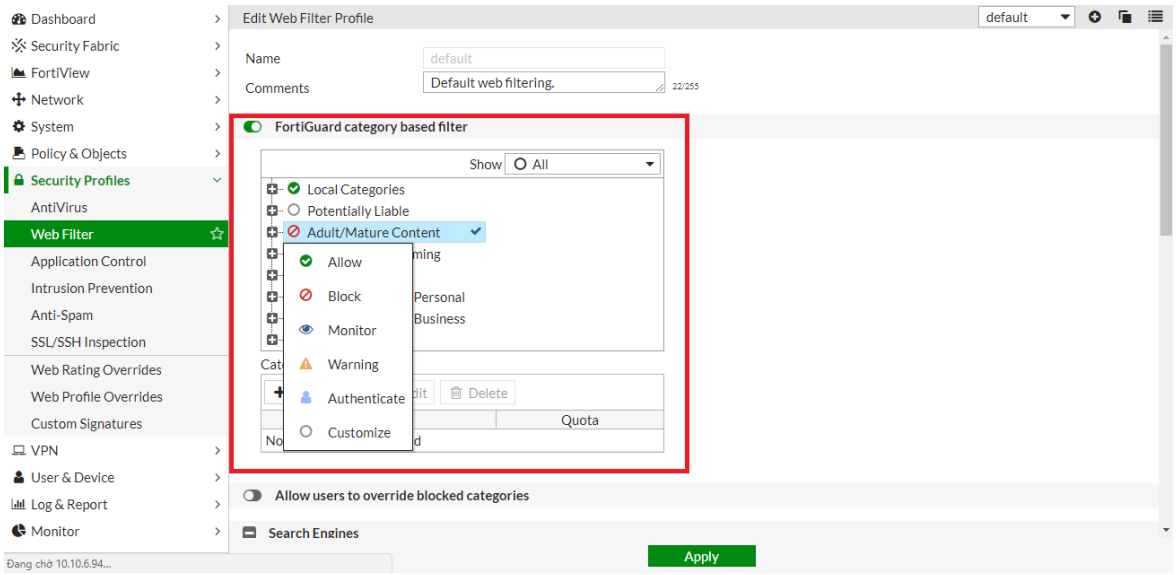
8.3: Cấu hình

Tạo Profiles Web Filter:



- Cấu hình cấm các trang web có nội dung người lớn bằng **FortiGuard Categories.**

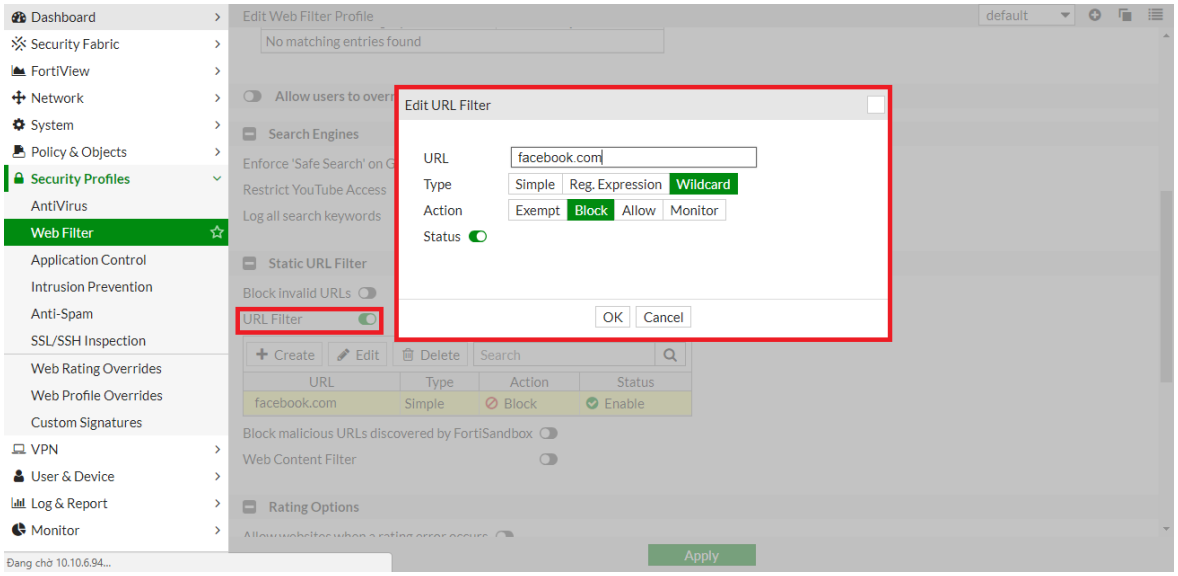
Security Profiles -> Web Filter -> enable FortiGuard Category.



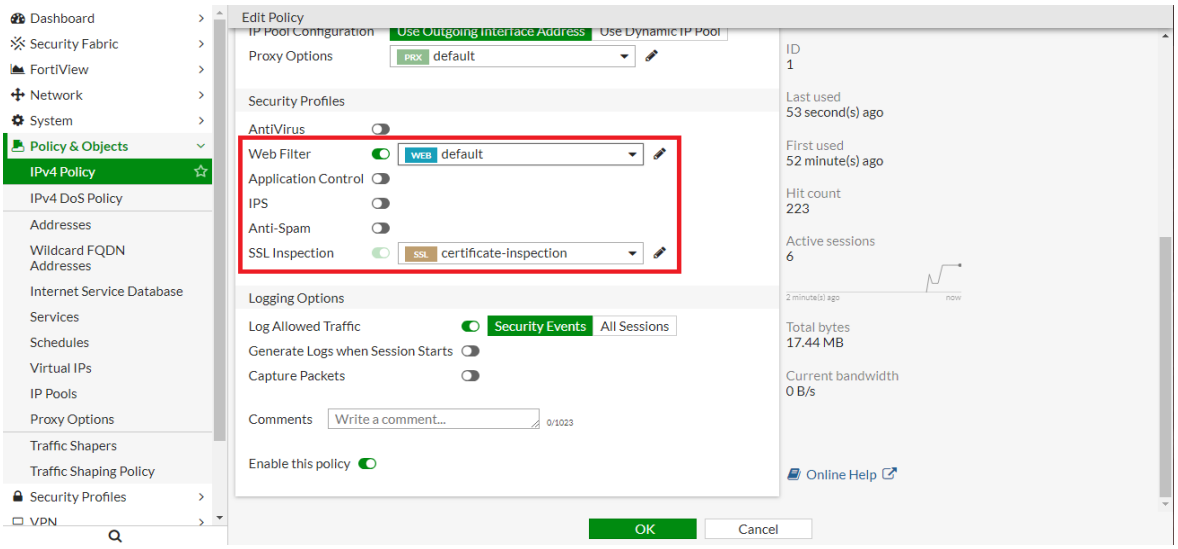
Ở đây người quản trị sẽ có nhiều lựa chọn như: Allow, Block, Monitor, Warning, Authenticate (bắt phải xác thực mới có thể dùng)… để áp dụng cho từng trường hợp cụ thể, ở đây chúng ta chọn Warning cho Games.

- **Cấu hình Block Web: *facebook.com***

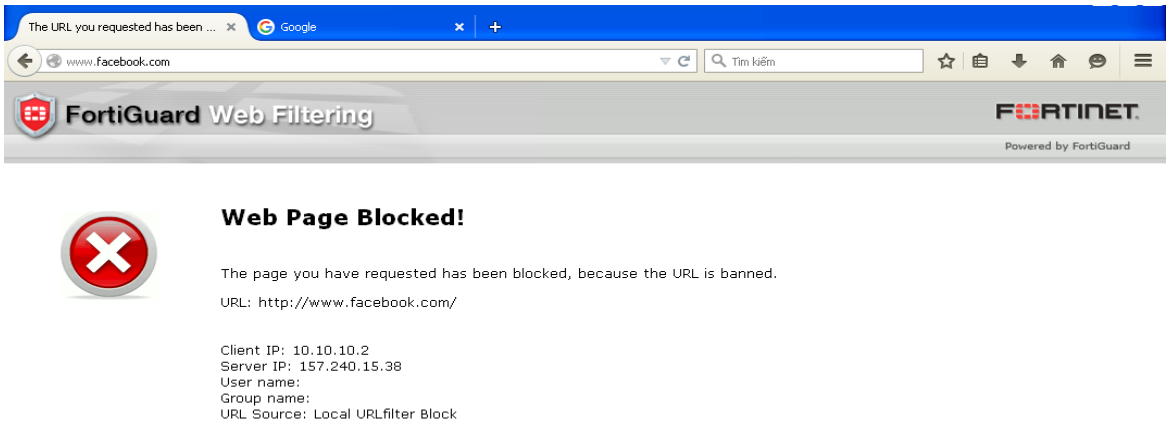
Security Profiles -> Web Filter -> Static URL Filter -> Create New.



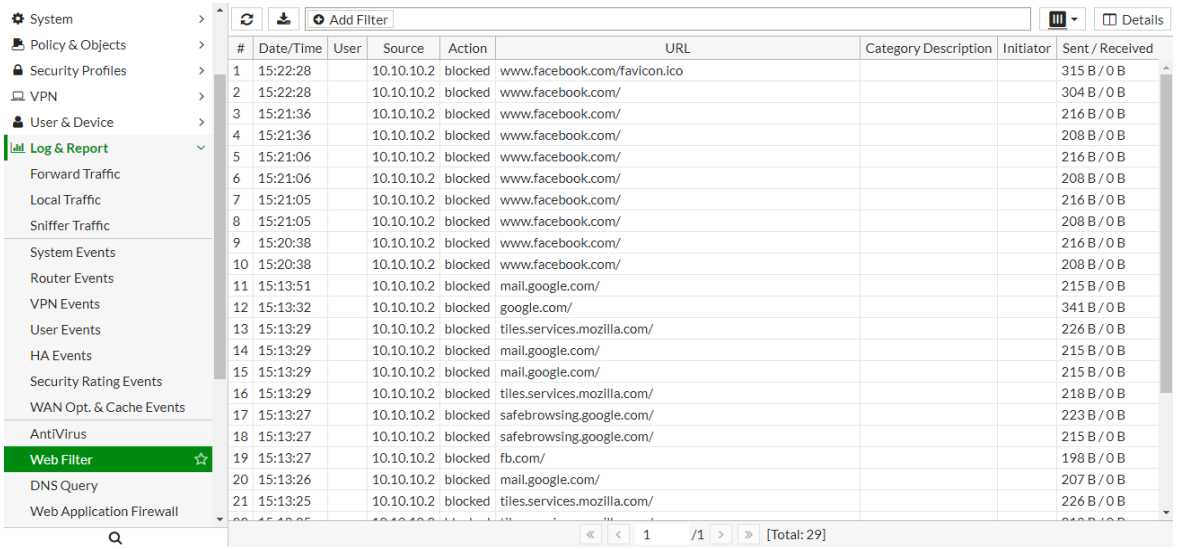
Áp dụng Profile vào Policy.



Kiểm tra:



Xem log:



9. Cấu hình wireless controller để quản lý thiết bị phát sóng Forti-AP

9.1: Tổng quan

Cấu hình Fortigate wirless Controller bao gồm 3 thành phần chính (một tùy chọn):

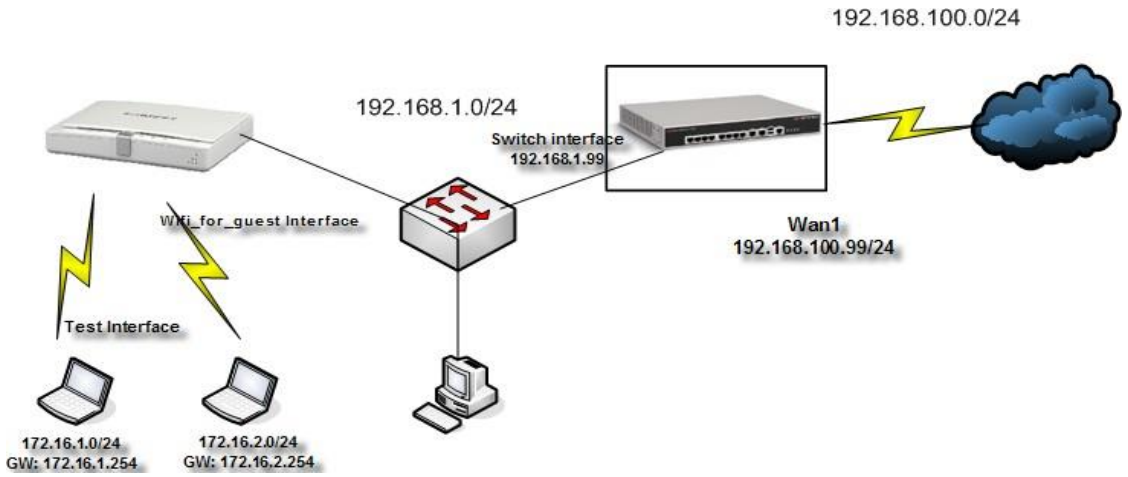
- **SSID** (*Service Set Identifier ~ Network name*): Xác định một virtual wireless network interface, bao gồm cả các tùy chỉnh bảo mật. Một SSID có thể coi là một mạng wireless riêng, bất kể có bao nhiêu Aps đã được cung cấp. Tuy nhiên, nếu cần có thể tạo ra nhiều SSID để cung cấp nhiều dịch vụ hoặc đặc quyền cho các nhóm người dùng khác nhau. Mỗi SSID có một policy và sự xác thực riêng biệt. Mỗi radio trong một AP có thể hỗ trợ lên tới 8 SSID. SSID cần được định danh để clients có thể dễ lựa chọn và sử dụng. Mỗi SSID (wireless interface) được cấu hình sẽ có một field để định danh. Trong mục cấu hình quản lý AP bạn chọn mạng wireless bằng các giá trị của SSID. Trong phần Policy bạn chọn wireless interfaces bằng tên của SSID.
- **Rogue AP** (*option*): Khi trong vùng mạng của bạn xuất hiện vài APs có thể của hàng xóm, nó có thể gây ra lỗ hổng bảo mật với mạng của bạn nếu như các máy tính nối mạng có dây trong mạng nội bộ truy cập vào các mạng của các AP này. Với lựa chọn On – Wire Rogue AP Detection Technique, nó sẽ so sánh địa chỉ Mac của traffic đáng ngờ với các địa chỉ Mac trong mạng. Nếu các wireless traffic tới từ các AP không phải của Fortinet được thấy trong mạng wired thì AP đó bị coi là rogue (đáng ngờ). Quyết định về Aps nào bị cho là rogue được tạo ra trong Rogue AP monitor. Khi đã xác định một AP là một rogue ta có thể chặn nó lại. Để chặn các AP này, Fortigate Wifi Controller gửi các gói tin reset tới các AP này. Tiếp đến, địa chỉ Mac của rogue AP bị blocked trong các firewall policy. Ta lựa chọn hành động chặn trong Rogue AP monitor
- **AP Profile**: Định nghĩa các tùy chỉnh trong radio, như dải băng (vd 802.11g) và lựa chọn kênh. Tên trong AP Profile để SSID áp dụng vào nó. Quản lí APs có thể sử dụng các profile có sẵn hoặc hoặc có thể tạo các custom AP profile
- **Managed Access Point**: Đại diện cho local wireless Aps trong FortiWiFi và FortiAP, những thiết bị mà được Fortigate nhận ra. Có một Managed AP xác

định cho mỗi một thiết bị AP. Một AP xác định có thể tự động tùy chỉnh các AP Profile hoặc chọn một custom AP Profile. Khi các tùy chọn trong các profile mặc định được sử dụng, Managed AP xác định chọn các SSID được mang trong AP.

9.2: Sơ đồ

Fortinet AP có thể chạy được cùng lúc 2 dải băng tầng.

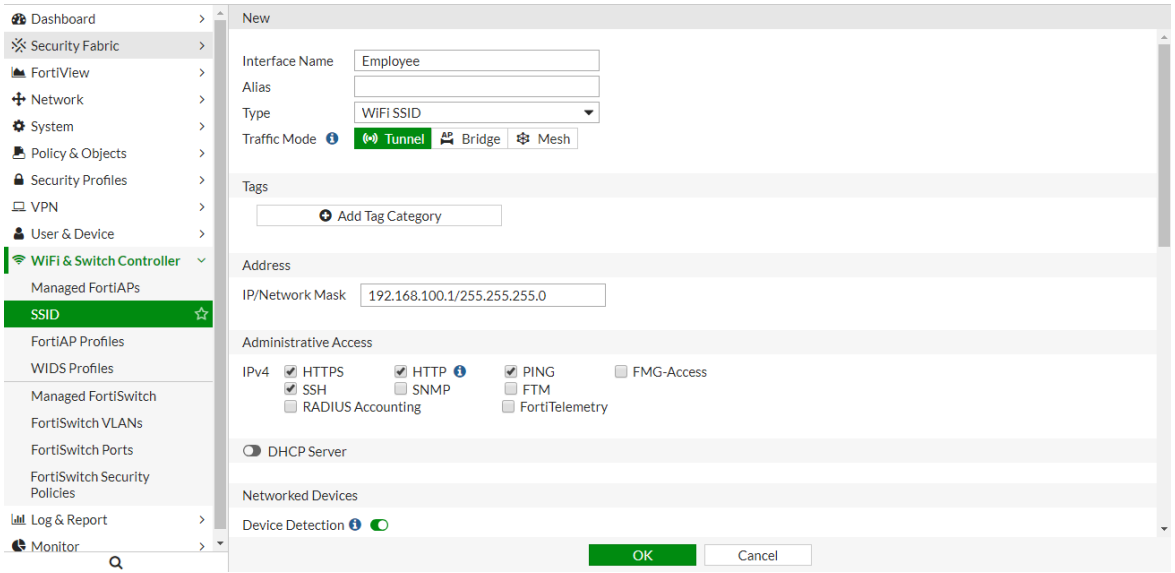
Có Thể Cấu hình với nhiều virtual AP với SSID tương ứng với virtual AP đó:



9.3: Cấu hình

B1: Tạo SSID

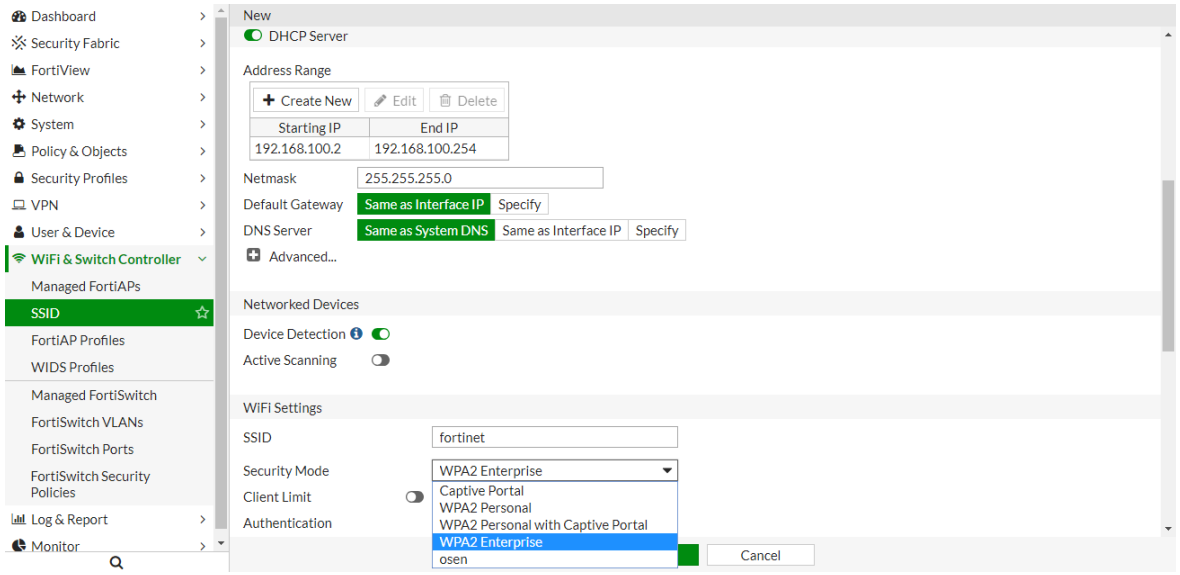
WiFi Controller > WiFi Network > SSID Create New.



Phần chọn Administrator Access để bảo mật chỉ nên chọn Ping để kiểm tra trạng thái, còn không cho truy cập vào.

+ Tạo *DHCP Server*: Tick chọn *enable*.

Trong phần này ta cũng có thể sử dụng tính năng *Mac Filter*, cho phép permit hay block user dựa vào Mac.



Trong phần lựa chọn Security Mode có 3 lựa chọn:

+ WPA/WPA2 – Personal:

- Chỉ yêu cầu preshared key đối với clients. Có thể tốt đối với một người hoặc một nhóm người được tin tưởng. Nhưng nếu số user tăng, sẽ là khó khăn khi phân phối key mới và mức độ nguy hiểm cho mạng cũng tăng lên.

+ WPA/WPA2 – Enterprise:

- User cần xác thực thông tin, được xác định thông qua một authentication server, thường là Radius. Hoặc FortiOS có thể chứng thực WPA – Enterprise user thông qua xây dựng các user group. User group này có thể bao gồm Radius server và có thể chọn user bằng Radius user group. Cái này có thể tạo ra Role – Based Access Control (RBAC).

+ Captive Portal:

- Bảo mật kết nối user tới một giao diện web portal định nghĩa trong Replacement Message. Để có thể vượt qua được web portal, user phải xách thực với Fortigate.

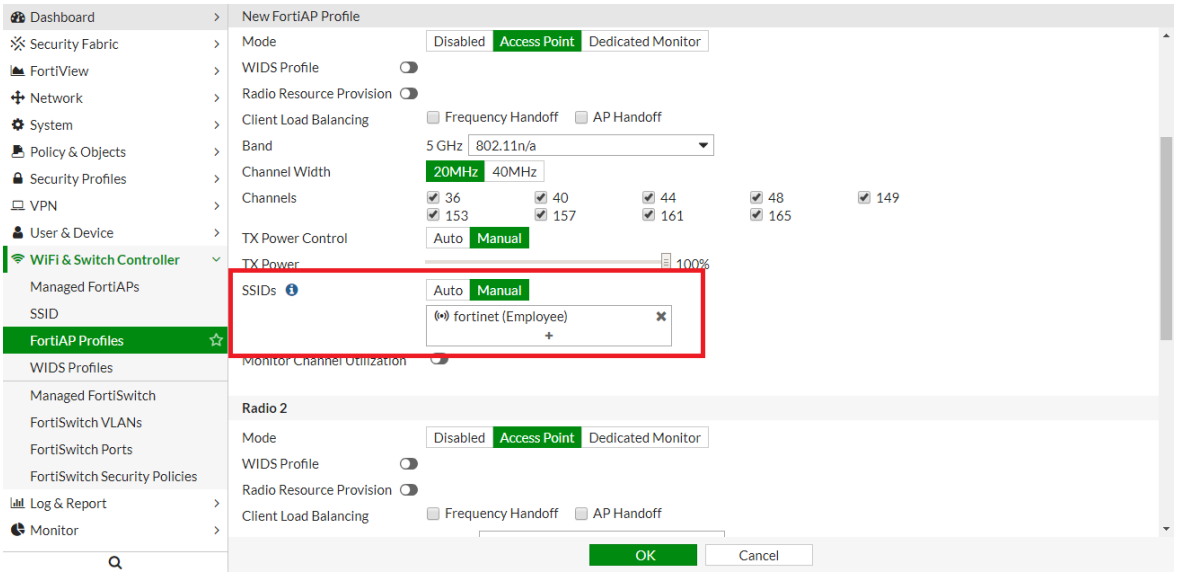
+ Block Intra – SSID Traffic:

- Enable nếu muốn ngăn cản các giao tiếp trực tiếp giữa các client trong mạng.

B2: Tạo AP profile hoặc sử dụng profile có sẵn:

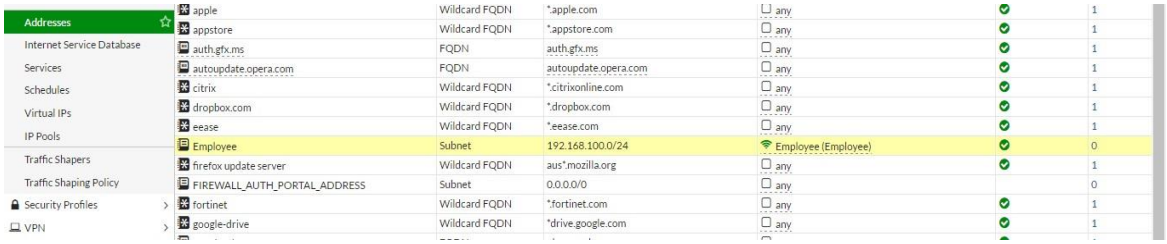
Wifi & Switch Controller -> FortiAP Profiles -> Create New.

- Add các SSID vào các AP profile phù hợp.

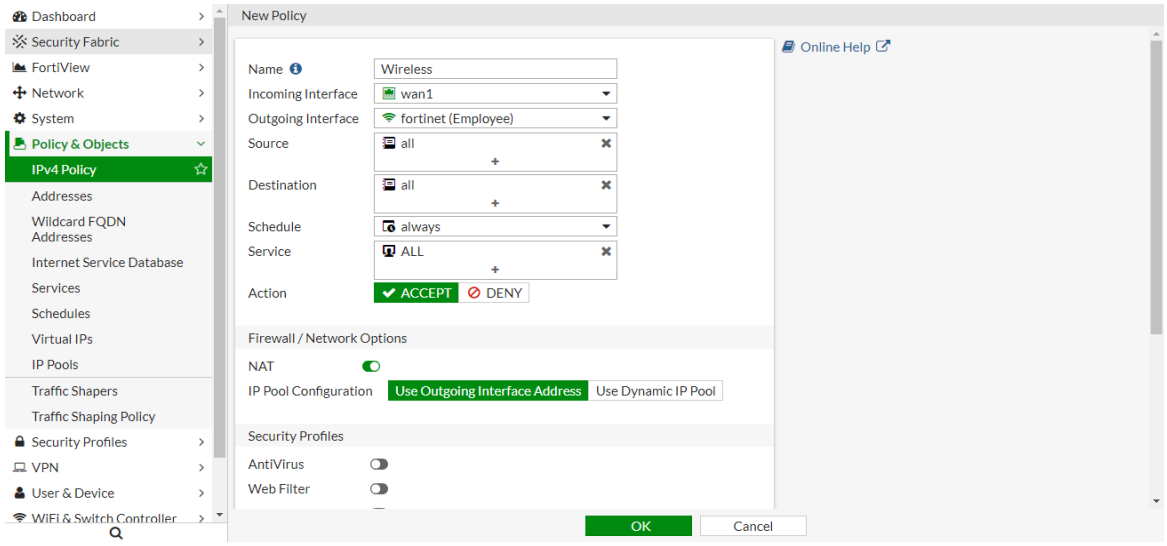


B3: Tạo các policy cho các SSID

Đầu tiên nên tạo các address*: Firewall Objects> Address*



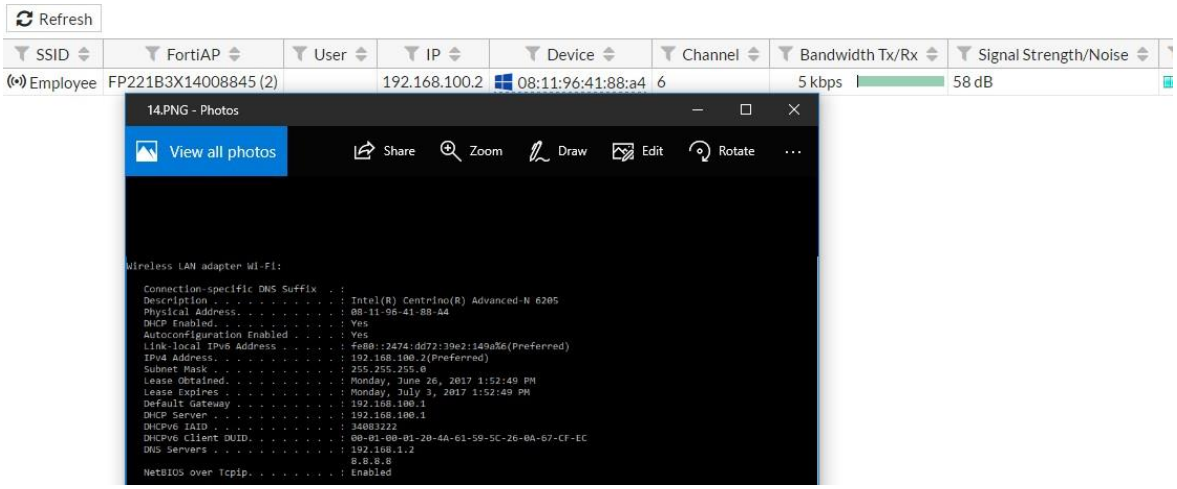
Add vào **Policy:**



Kiểm tra với Employee: ***Monitor -> Wifi Client Monitor.***

```
Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Intel(R) Centrino(R) Advanced-N 6205
   Physical Address. . . . . . . . . : 08-11-96-41-88-A4
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::2474:dd72:39e2:149a%6(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.100.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, June 26, 2017 1:52:49 PM
   Lease Expires . . . . . . . . . . : Monday, July 3, 2017 1:52:49 PM
   Default Gateway . . . . . . . . . : 192.168.100.1
   DHCP Server . . . . . . . . . . . : 192.168.100.1
   DHCPv6 IAID . . . . . . . . . . . : 34083222
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-20-4A-61-59-5C-26-0A-67-CF-EC
   DNS Servers . . . . . . . . . . . : 192.168.1.2
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```



10. BYOD: Bring Your Own Device

10.1: Giới thiệu

Ngày nay số lượng các thiết bị di động và thiết bị cá nhân thông minh gia tăng ngày càng nhanh, đồng nghĩa với việc quản lí, áp dụng chính sách an ninh bảo mật thông tin trong mạng nội bộ ngày càng khó. Nhưng với FortiOS 5.2 được tích hợp tính năng BYOD giúp việc này trở lên dễ dàng hơn rất nhiều: tự động xác định thiết bị có trong mạng, tự động đưa vào các group phù hợp cùng với đó là smart policy giúp việc áp dụng các chính sách hết sức dễ dàng, linh hoạt.

10.2: Cấu hình

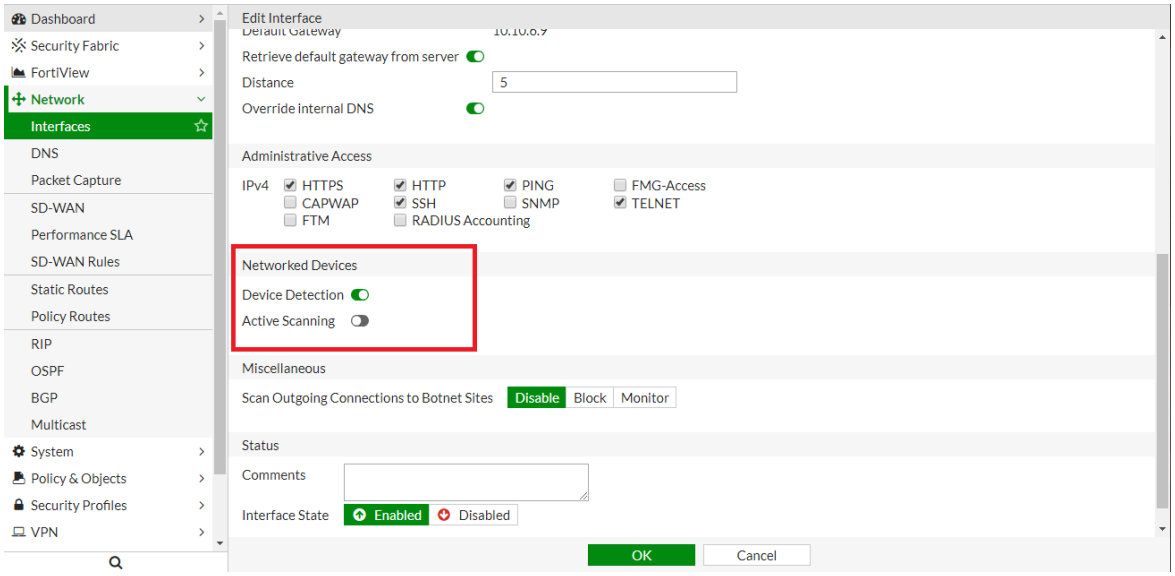
Việc cấu hình hết sức đơn giản, gồm 3 bước chính: Device Identification,

Access Control, Security Application.

Trong đó access control thực hiện bằng cách thiết lập các policy, security application thực hiện dựa vào các UTM Profile và được add vào trong Policy.

B1: Device Identity

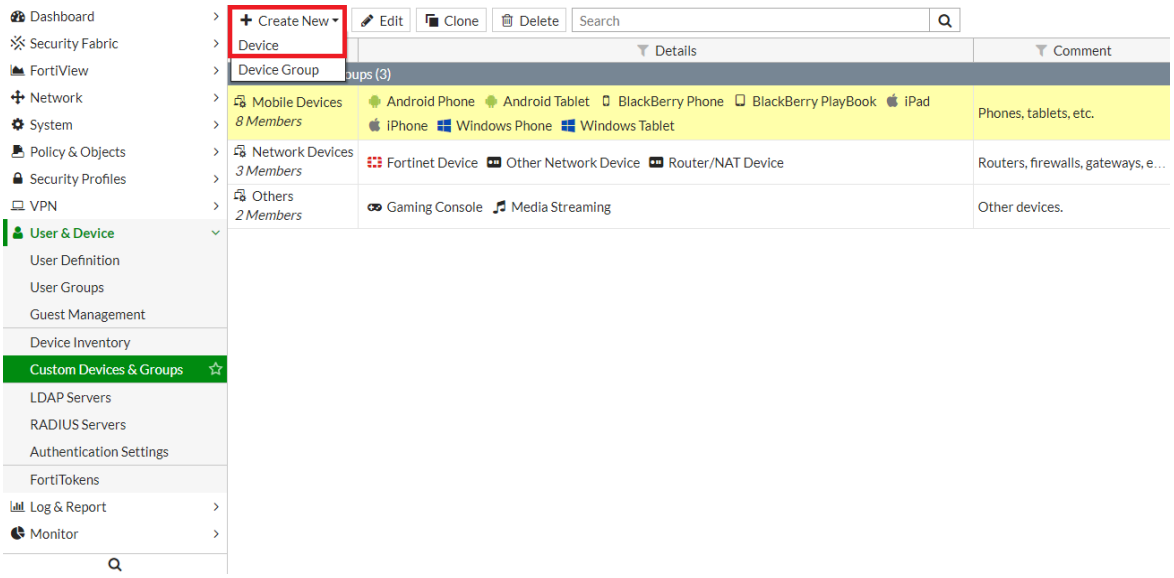
Để FG tự động tìm kiếm các thiết bị đang được sử dụng trong mạng, cần enable *Detect and Identify Devices* trong các interface.



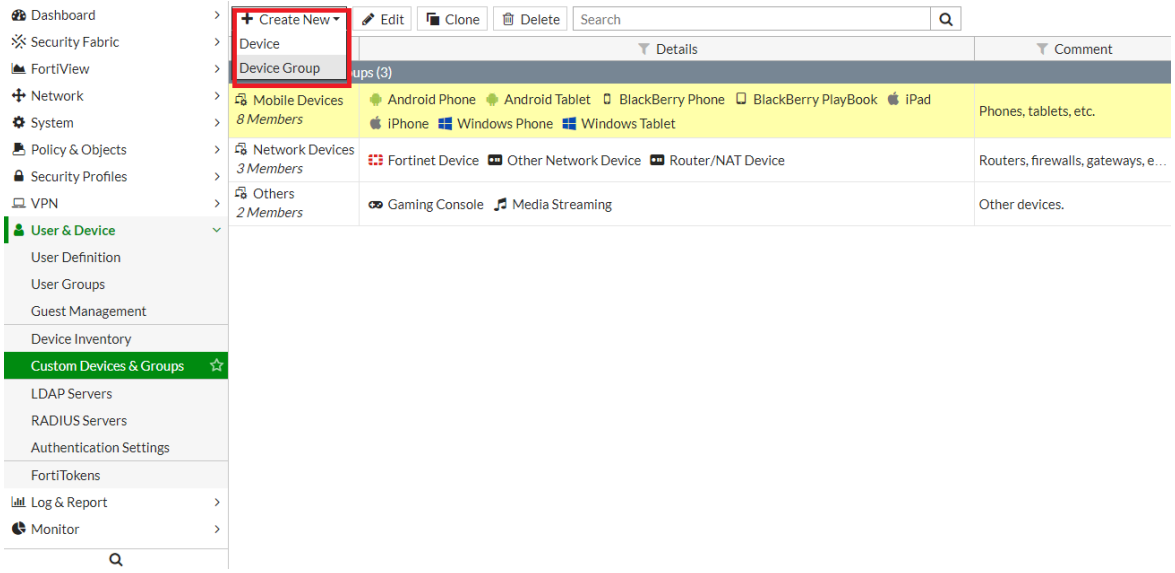
Để xem kết quả các thiết bị được FG tự động xác định: ***User & Device -> Custom Devices and Groups.***

Hoặc có thể tự add thiết bị vào bằng cách: ***User & Device -> Custom Devices and Groups*** chọn ***Create New -> Device.***

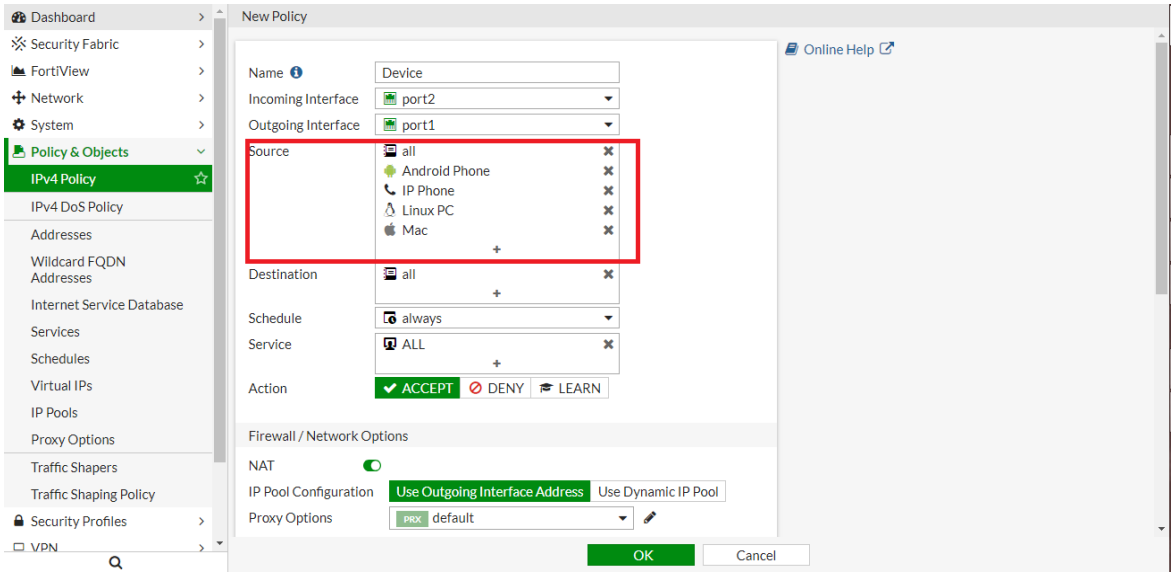
Cũng có thể thay đổi các thông số của các thiết bị đã được xác định như thêm Mac address, miêu tả, type, group…bằng cách: ***User & Device -> Custom Devices and Groups***.



Sau đó, có thể tạo group và đưa các thiết bị vào hoặc sử dụng các group mặc định của FG: ***User & Device> Custom Devices and Groups -> Create new -> Group Device.***



Tạo Policy cho từng Device



11. Two Factor Authentication

11.1: Giới thiệu

Với cách đăng nhập tiêu chuẩn yêu cầu username và password. Đây được gọi là **one factor authentication** – password của bạn là một phần thông tin mà bạn cần để truy cập vào hệ thống.

Với two factor authentication sẽ yêu cầu thêm một số thông tin nữa của bạn để đăng

nhập thành công. Tổng quát lại có thể nói two factor là một số thứ mà bạn biết (password) và một số thứ bạn có (certificate, token…). Điều này gây trở ngại rất lớn đối với hacker khi muốn lấy cắp thông tin đăng nhập của bạn. Ví dụ nếu bạn có một thiết bị FortiToken, hacker sẽ phải cần sử dụng cả nó và biết password của bạn để có thể sử dụng account của bạn.

Two – factor authentication có thể dùng cho tất cả user lẫn admin account. Nhưng trước khi bạn sử dụng tính năng này cho administrator account, bạn cần đảm bảm rằng bạn có administrator account thứ 2 để có thể đăng nhập được vào Fortigate khi mà không thể xác thực với administrator account kia do một vài lí do nào đó.

Có 4 phương pháp mà **two – factor authentication** sử dụng:

Certificate:

Yêu cầu certificate và password khi xác thực cho các PKI users. Certificate đã được cài đặt trên các máy tính của user. Việc yêu cầu một password cũng bảo vệ việc sử dụng trái phép máy tính đó. Lựa chọn nữa cho user là có thể điền vào code từ FortiToken của họ thay vì certificate.

Email:

Two – factor authentication gửi một dãy số có 6 chữ số được tạo ra ngẫu nhiên cho một địa chỉ email cụ thể. Users sẽ điền code đó vào khi đăng nhập. Cái token code này là hợp lệ trong 60s. Nếu bạn điền code này sau khoảng thời gian 60s, nó sẽ không được chấp nhận. Lợi ích là nó không yêu cầu dịch vụ di động khi xác thực. Tuy nhiên, một vấn đề tiềm tàng là nếu server email của bạn không chuyển được mail tới bạn trước 60s thì token đó sẽ bị hết hạn. Code được tạo ra và gửi email tại thời điểm đăng nhập, vì vậy bạn phải đăng nhập vào email trước thời điểm có thể nhận được code.

***SMS*:**

Two – factor authentication gửi một token code trong một đoạn tin nhắn sms text tới thiết bị di động được chỉ định để dùng khi đăng nhập. Token code này được coi là hợp lệ trong vòng 60s. Nếu tại thời điểm bạn điền code mà quá thời gian này, code sẽ không được chấp nhận. Lợi ích của cách này là nó không yêu sử dụng dịch vự email trước khi đăng nhập.

FortiToken:

Sinh ra các one – time password. Nó là một thiết bị rất nhỏ với 1 nút bấm để hiển thị ra một code gồm 6 chữ số dùng để xác thực. Code này được điền vào cùng với

usernam và password khi sử dụng **two – factor authentication**. Code này được hiển

thị sau mỗi 60s, và khi không sử dụng thì trên màn hình của nó sẽ hiển thị dung lượng pin. Nó cũng là một ứng dụng di động với FortiToken Mobile, thực hiện chức năng tương tự. Tại bất kì thời gian nào thông tin được truyền đi bởi FortiToken đều được mã hóa. Khi Fortigate nhận được code nó sẽ so sánh với số SN của FortiToken, truyền và lưu giữ nó dưới dạng mã hóa. Điều này giữ cho sự giao tiếp luôn được đảm bảo an toàn ở mức cao. FortiToken có thể được thêm vào các user account trong mạng local, IPSec, SSL VPN và cả Administrator. Một FortiToken có thể được liên kết với duy nhất một account trong một thiết bị ForitGate.

Nếu một user mất thiết bị FortiToken của họ, nó có thể bị khóa bởi FortiGate vì vậy nó không thể truy cập vào mạng của FortiGate. Sau khi nó được tìm thấy, FortiToken đó sẽ được unlock trong FG để cho phép truy cập lại.

Chú ý *User* trong FortiGate có 6 loại:

+ *Local user:* (password lưu trong FortiGate) username và password phải phù hợp với user account lưu trong FortiGate. Xác thực bằng các chính sách bảo mật của FG.

+ *Remote user:* (password được lưu trên các remote server) username phải phù hợp với các user account lưu trên FortiGate và username, password phải phù hợp với một user account lưu trên một remote authentication server ví dụ như *LDAP, RADIUS, TACACS+* server

+ *FSSO user:* users trong MS Windows hoặc Novell có thể sử dụng mạng xác thực của họ để đăng nhập vào tài nguyên mà FortiGate bảo vệ. Truy cập được điều khiển thông qua FSSO user group cái mà chứa windows hoặc Novell user group cùng các thành viên.

+ *Peer user:* Peer user là những người giữ các digital certificate để xác thực client. Không cần mật khẩu trừ khi two – factor authen được bật.

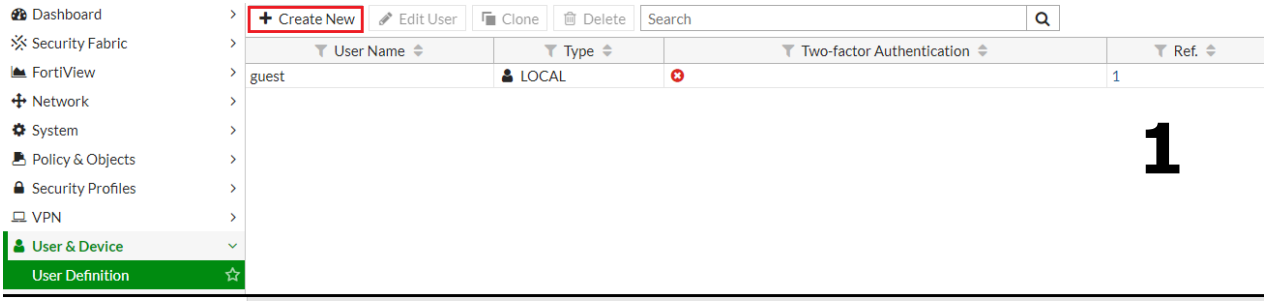
+ *IM user:* là kiểu user không cần xác thực. FortiGate có thể allow hoặc block mỗi IM user name thông qua truy cập vào giao thức IM. Một chính sách global cho mỗi giao thức IM sẽ quản trị việc truy cập của những giao thức này.

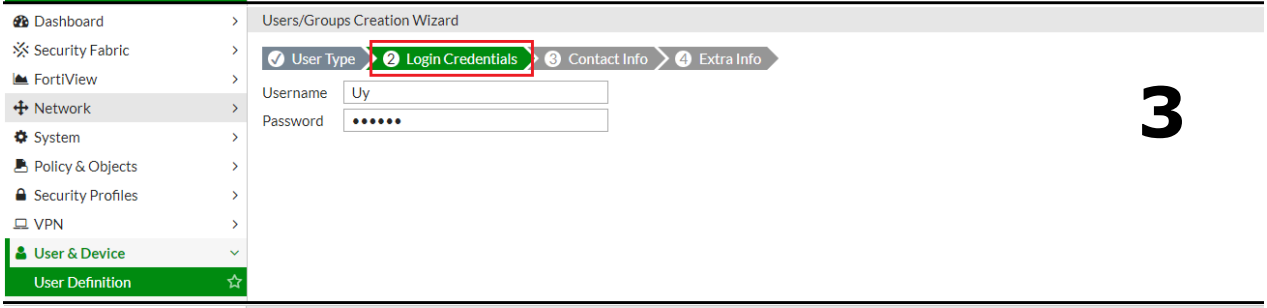
+ *Guest user:* Những user này áp dụng cho người dùng không thuộc mạng local, bị hạn chế về quyền hạn truy cập.

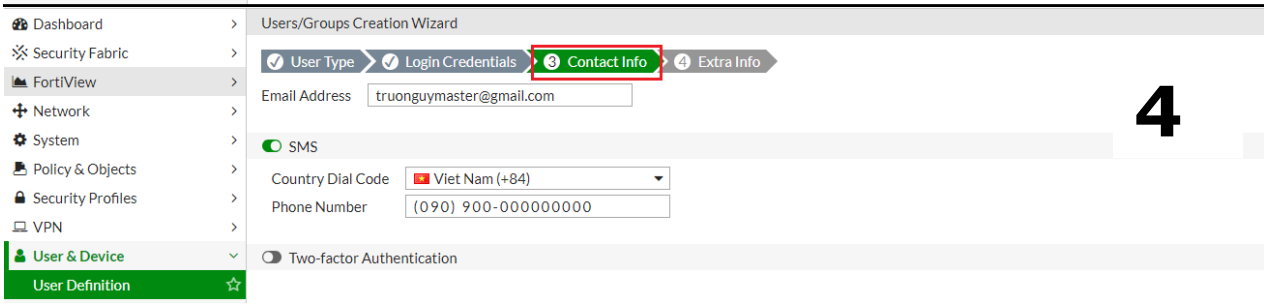
11.2: Cấu hình

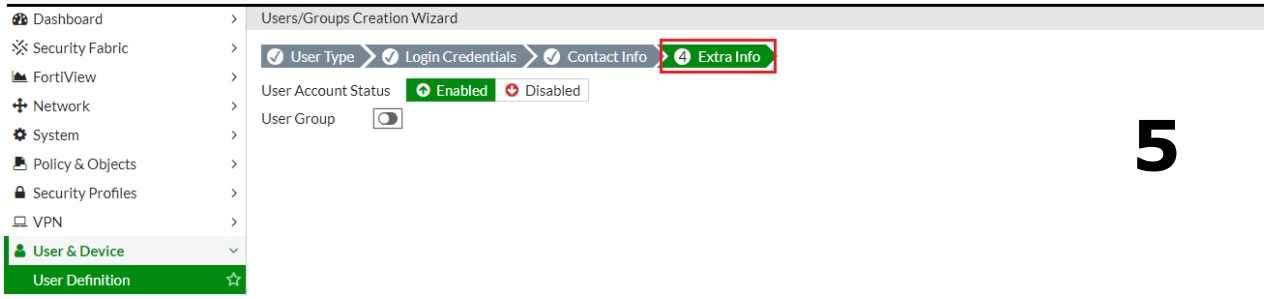
Cấu hình xác thực Local user, remote Radius user:

User & Device -> User Definition.

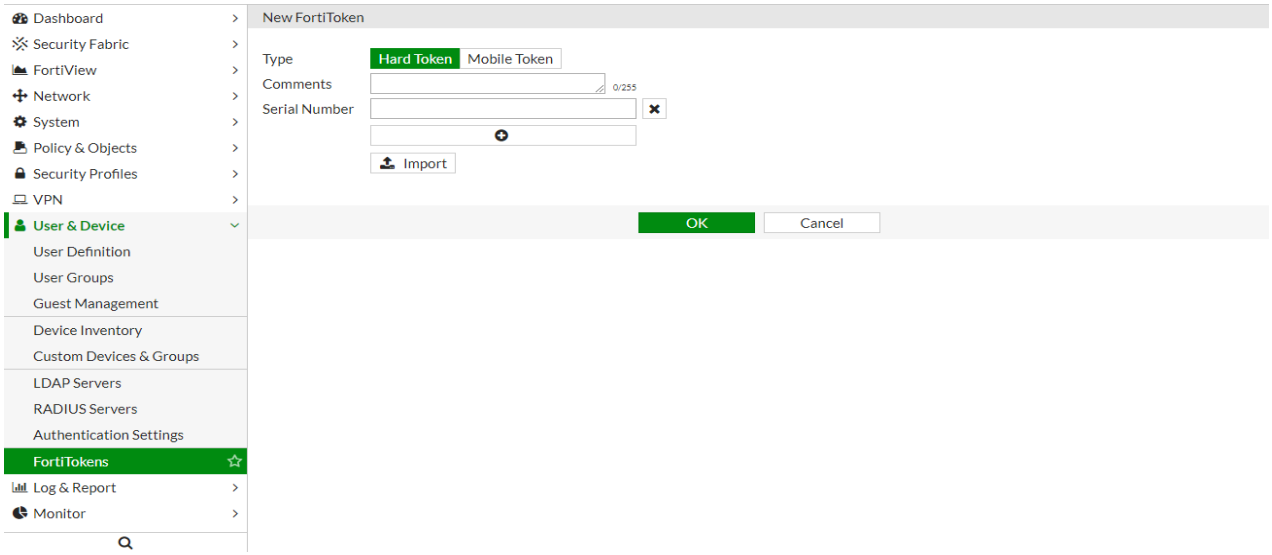








Tạo liên kết FortiToken vs FG*: User & Device -> FortiTokens -> Create new.*



Cần chú ý, trên giao diện web thì chỉ chọn được token, nếu muốn chọn sms hay email cần cấu hình qua CLI (được trình bày ở dưới).

Cấu hình user xác thực two – factor authentication bằng CLI:

User authenticated using email

```
config user local
  edit user6
    set type password


    set passwd ljt_pj4h7epfdw
    set two_factor email
    set email-to user6@sample.com
  end
```

User authenticated with a FortiToken

```
config user local
  edit user5
    set type password

    set passwd ljt_pj2gpepfdw
    set two_factor fortitoken
    set fortitoken 182937197
    end
```

User authenticated using SMS text message

```
config system sms-server
  edit "Sample Mobile Inc"
     set mail-server mail.sample.com
  end
config user local
  edit user7
    set type password
    set passwd 3ww_pjt68dw
   set two_factor sms
   set sms-server custom
   set sms-custom-server "Sample Mobile Inc"
   set sms-phone 2025551234
 end
```

Tạo các PKI user xác thực bằng Certificate

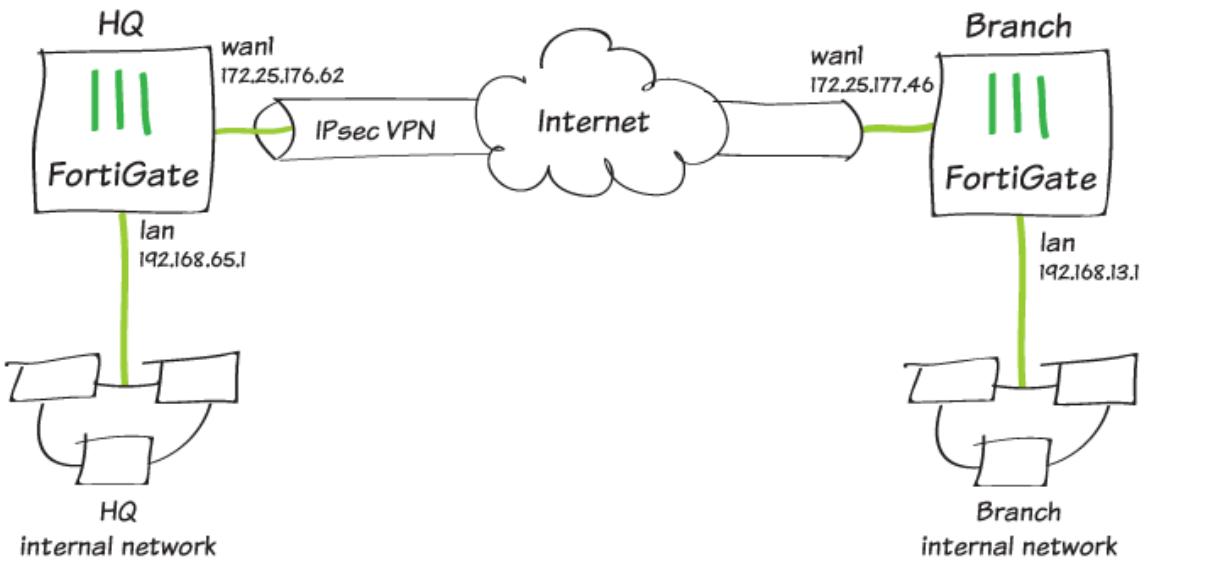
```
config user peer
edit peer1
set subject E=peer1@mail.example.com
set ca CA_Cert_1
set two-factor enable
set passwd fdktguefheygfe
end
```

12. VPN - Routed-Based IPsec VPN

12.1: Giới thiệu

Khi cấu hình Ipsec VPN theo kiểu Route Base, một interface Ipsec ảo sẽ được tạo ra trên Interface vật lý kết nối đến Remote Gateway. Đối với Route-based VPN, đòi hỏi phải tạo hai Policy giữa interface Ipsec ảo và interface nối với mạng internal: Một policy với Source Interface là interface Ipsec ảo và Destination Interface là interface local và một policy khác theo chiều ngược lại. Tùy chọn Action cho cả hai policy này là *Accept.* Việc tạo policy hai chiều nhằm đảm bảo traffic sẽ được thông suốt giữa hai đầu VPN.

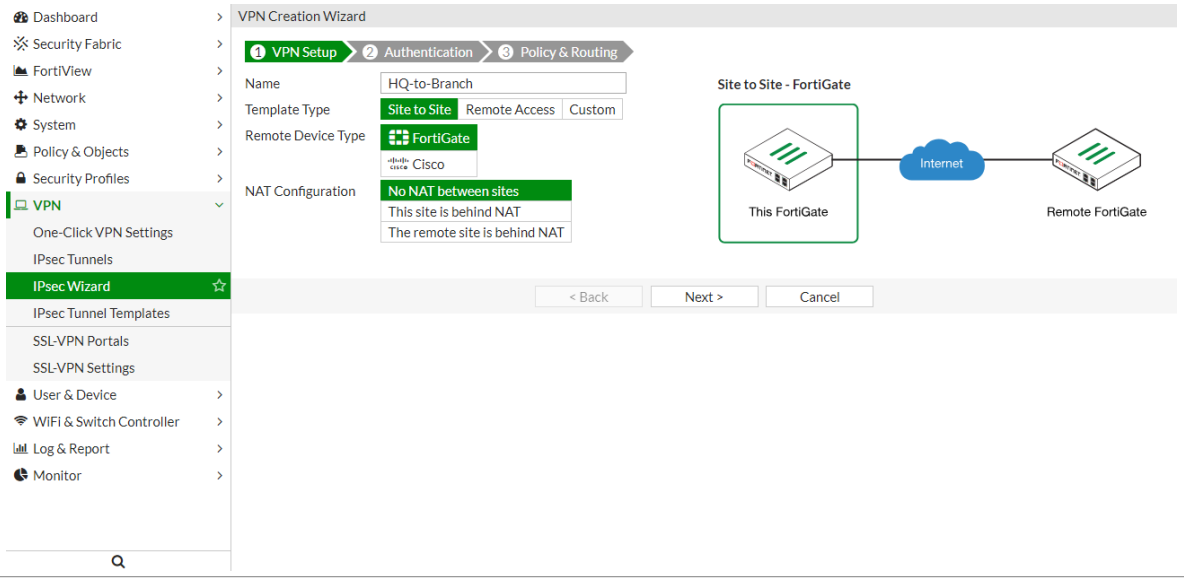
12.2: Cấu hình



B1: Cấu hình IPsec VPN trên HQ

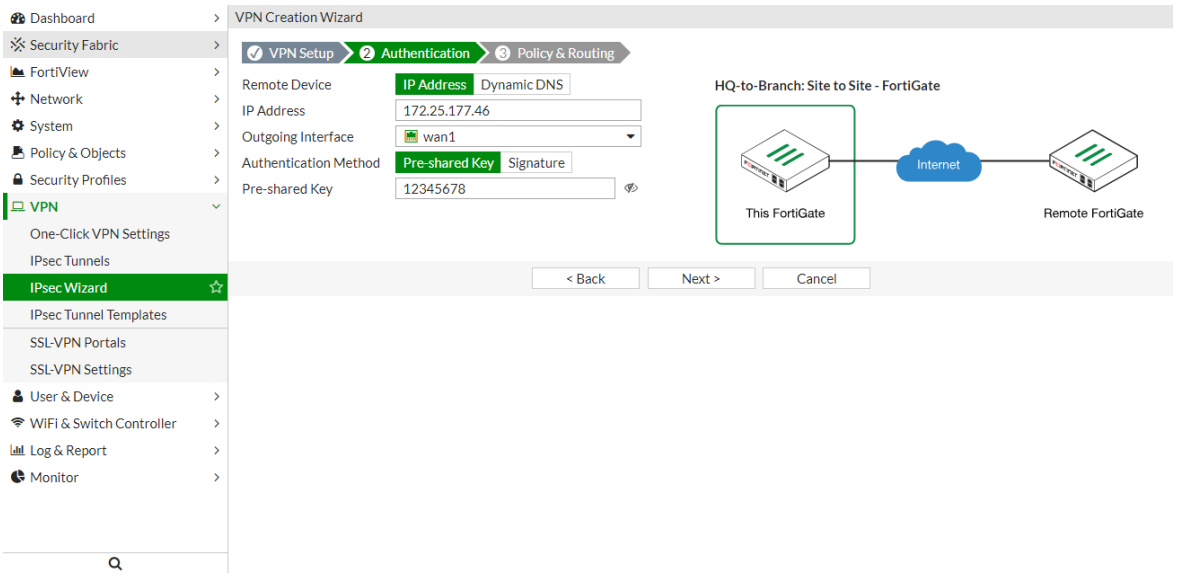
Trên FortiGate site HQ: ***VPN -> IPsec -> Wizard VPN Setup***

- Name: *HQ-to-Branch*
- Template: *Site to Site – FortiGate.*
- Chọn *Next.*



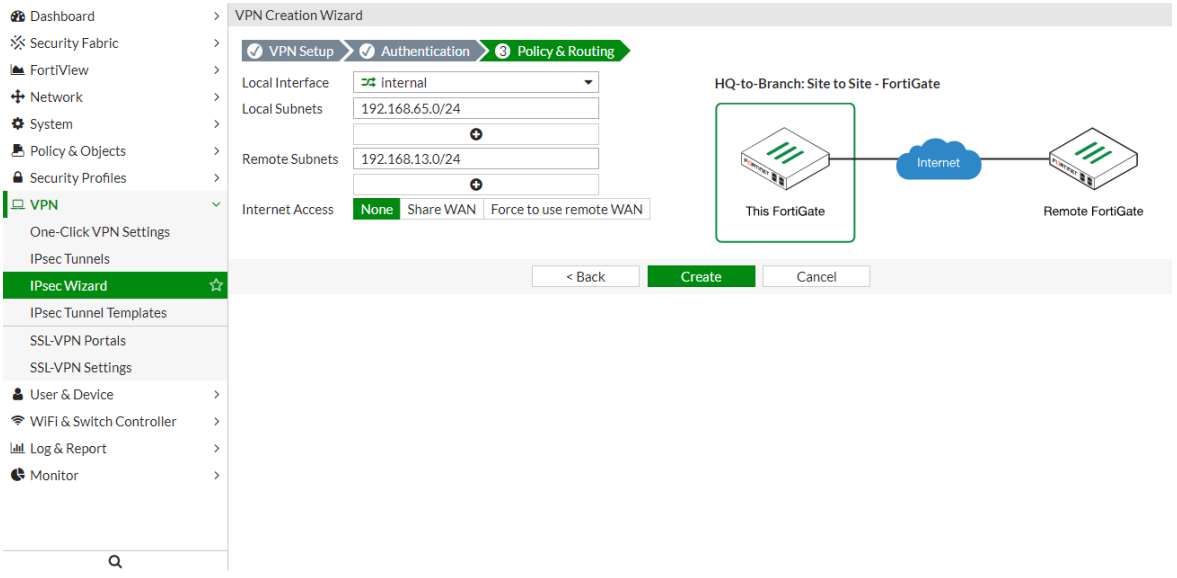
Authentication:

- Remote Gateway nhập thông tin IP Branch FortiGate, trong ví dụ này là: IP: 172.25.177.46
- Outgoing Interface: là Interface kết nối Internet của site HQ.
- Pre-shared Key : 12345678
- Chọn Next.

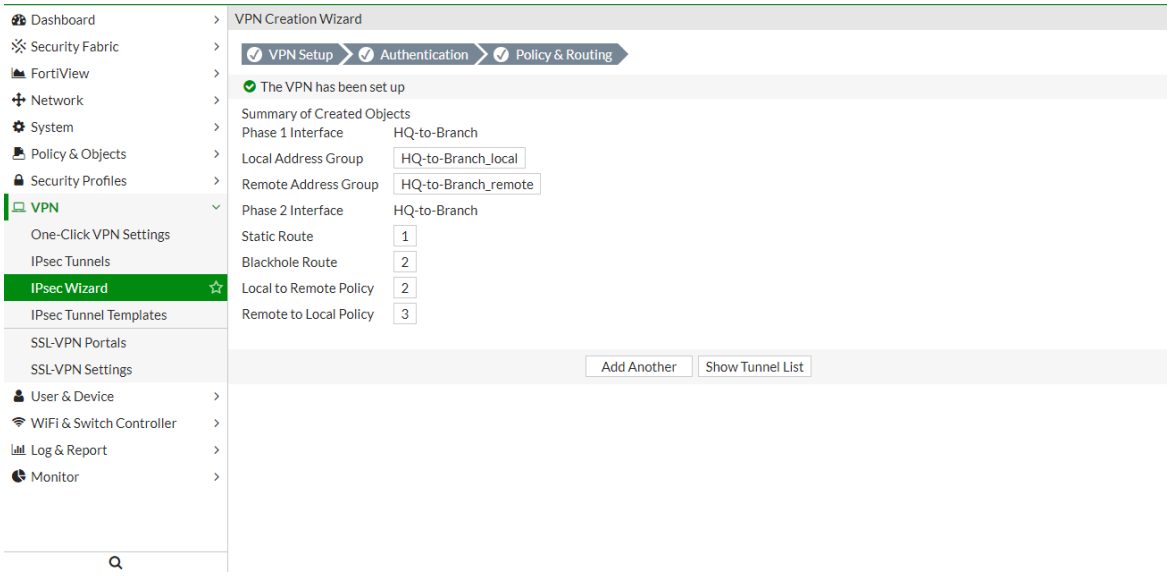


Policy & Routing:

- Local Interface: Interface LAN của site HQ
- Local Subnets: Lớp mạng LAN của site HQ
- Remote Subnets: Lớp mạng LAN của site Branch
- Chọn Create để hoàn thành tạo mới VPN



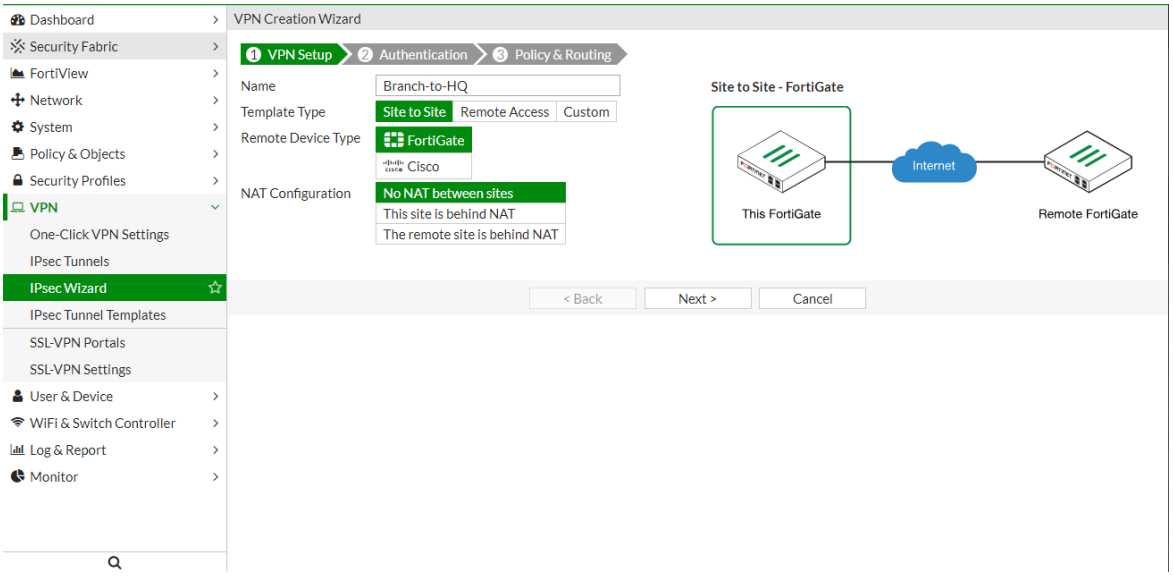
Kết quả: Tạo thành công *HQ-to-Branch* trên FortiGate site HQ.



B2: Cấu hình IPsec VPN trên Branch

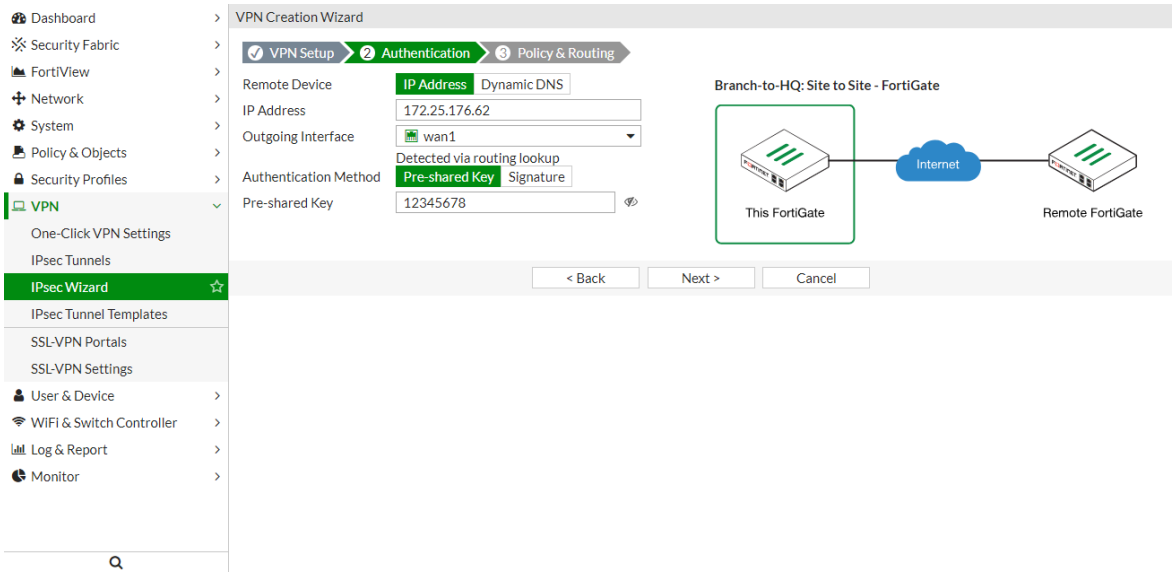
Trên FortiGate site Branch: ***VPN -> IPsec -> Wizard VPN Setup***

- Name: *Branch-to-HQ*
- Template: *Site to Site – FortiGate.*
- Chọn *Next.*



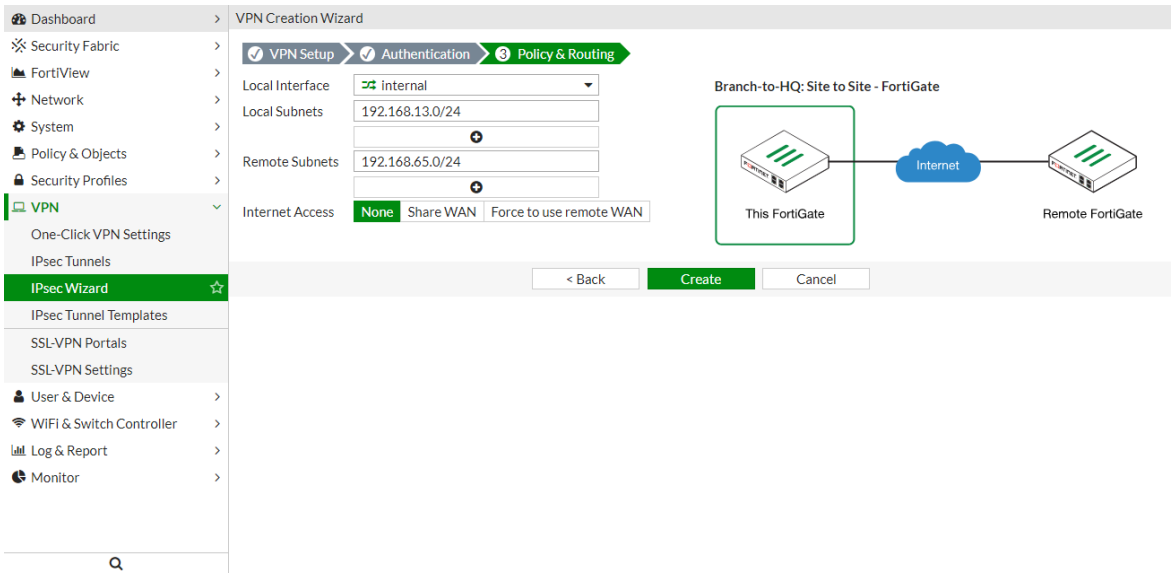
Authentication:

- Remote Gateway: nhập thông tin IP HQ FortiGate, trong ví dụ này là: IP: 172.25.176.62
- Outgoing Interface: là Interface kết nối Internet của site Branch
- Pre-shared Key : 12345678
- Chọn Next.

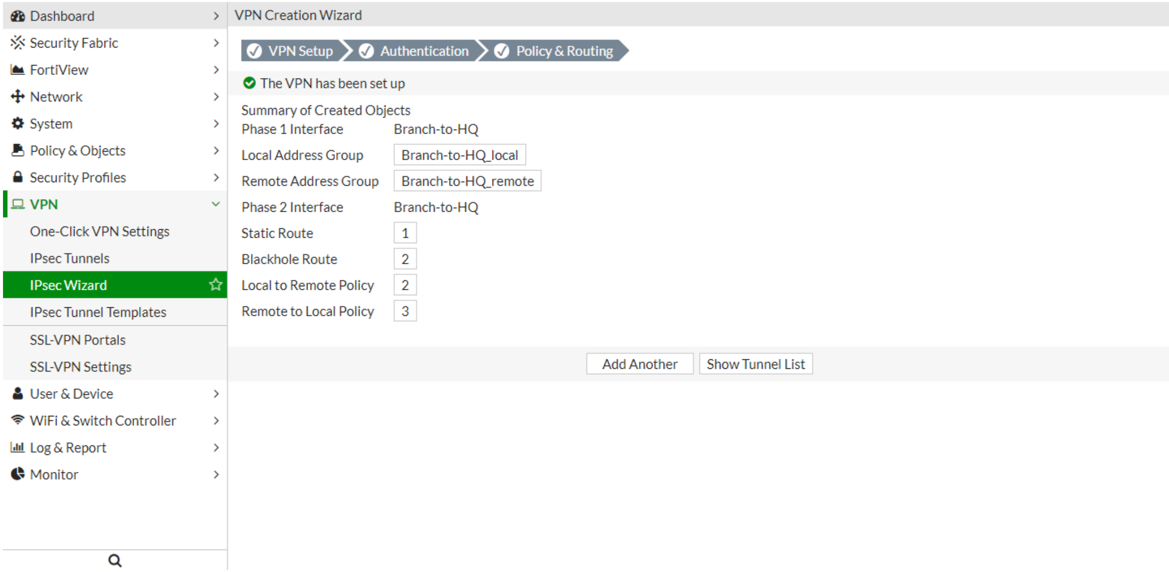


Policy & Routing:

- Local Interface: Interface LAN của site Branch
- Local Subnets: Lớp mạng LAN của site Branch
- Remote Subnets: Lớp mạng LAN của site HQ
- Chọn Create để hoàn thành tạo mới VPN

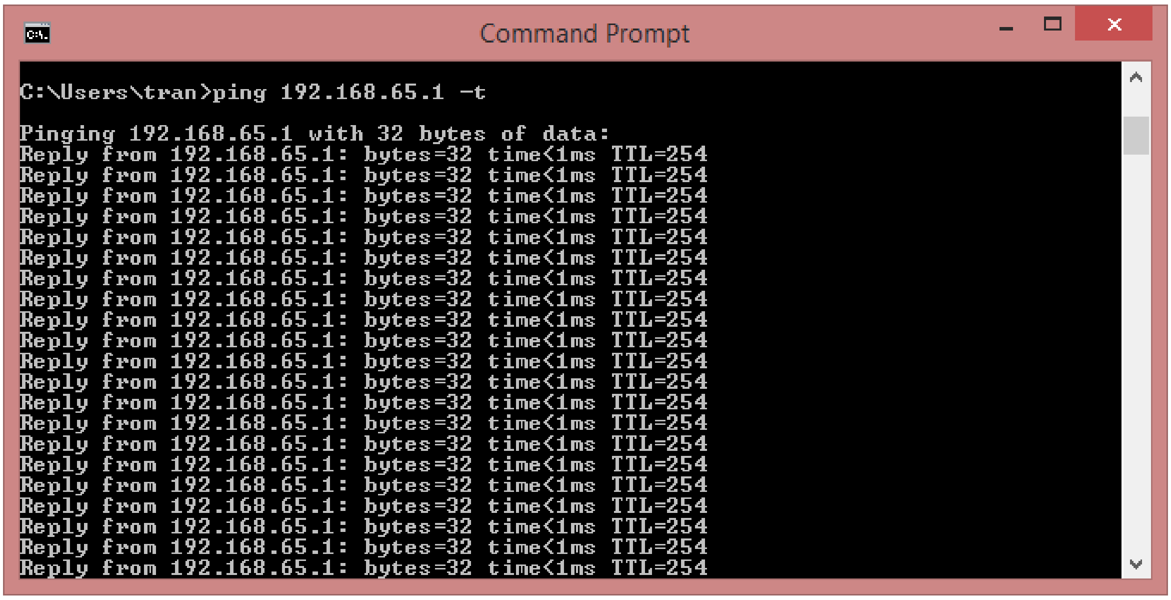


Kết quả: Tạo thành công *Branch-to-HQ* trên FortiGate site Branch:

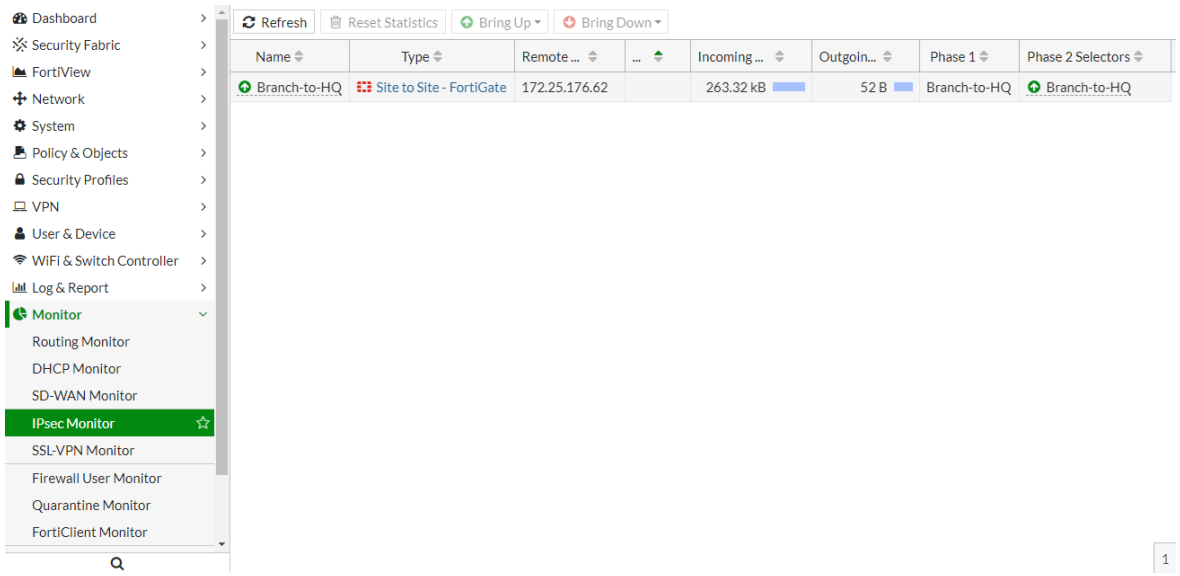


B3: Kết quả sau khi cấu hình thành công trên 2 site:

Ping thành công lớp mạng giữa hai site.



Vào ***Monitor*** -> ***IPsec Monitor*** kiểm tra trạng thái kết nối VPN đã Up.

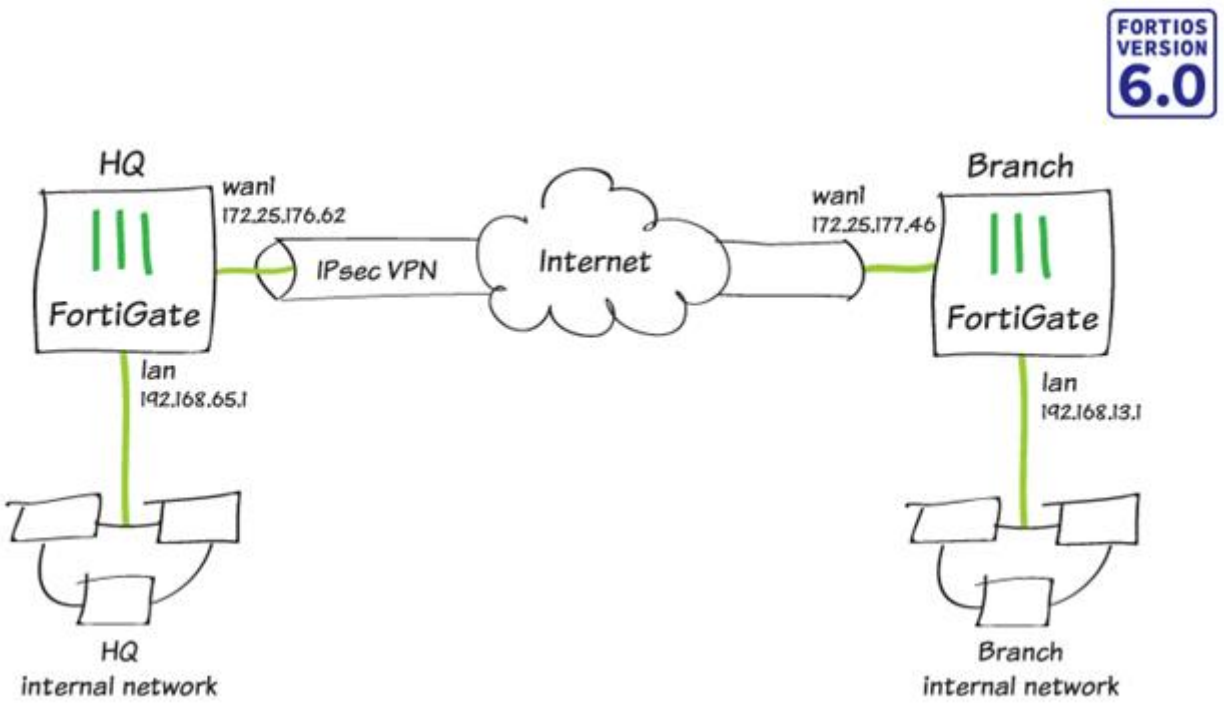


13. VPN - Policy-Based IPsec VPN

13.1: Giới thiệu

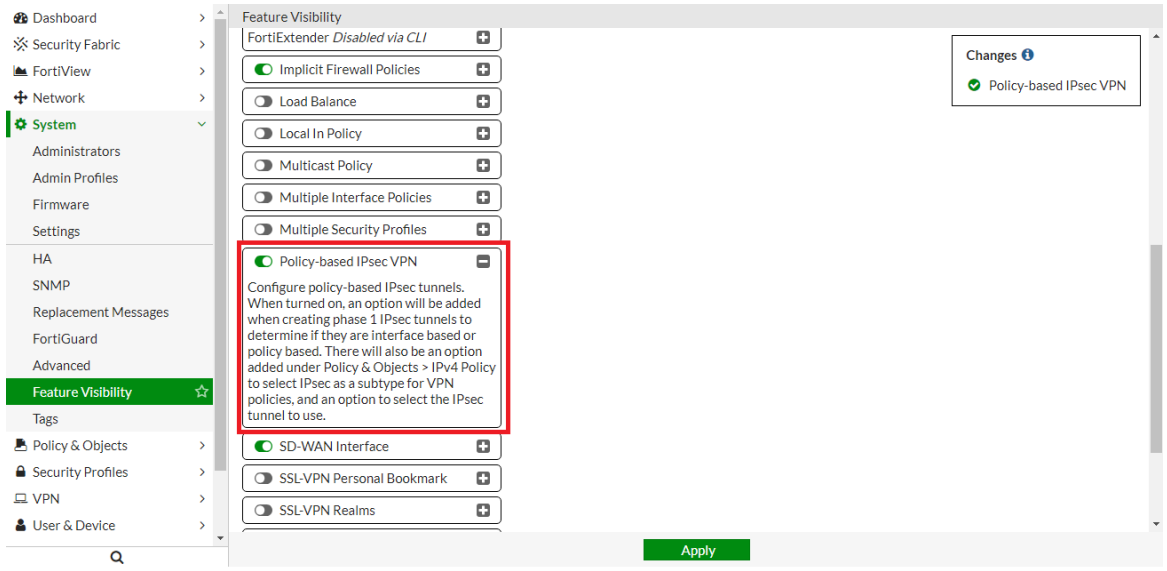
Đối với Ipsec VPN Policy-based, ta chỉ cần tạo duy nhất một policy cho cả hai chiều kết nối. Ở phần định nghĩa Policy Type, ta chọn VPN và phần Policy Subtype chọn Ipsec, sau đó chọn VPN Tunnel đã tạo trong Phase1.

13.2: Cấu hình



B1: Bật tính năng Policy-Based VPN trên HQ Forigate.

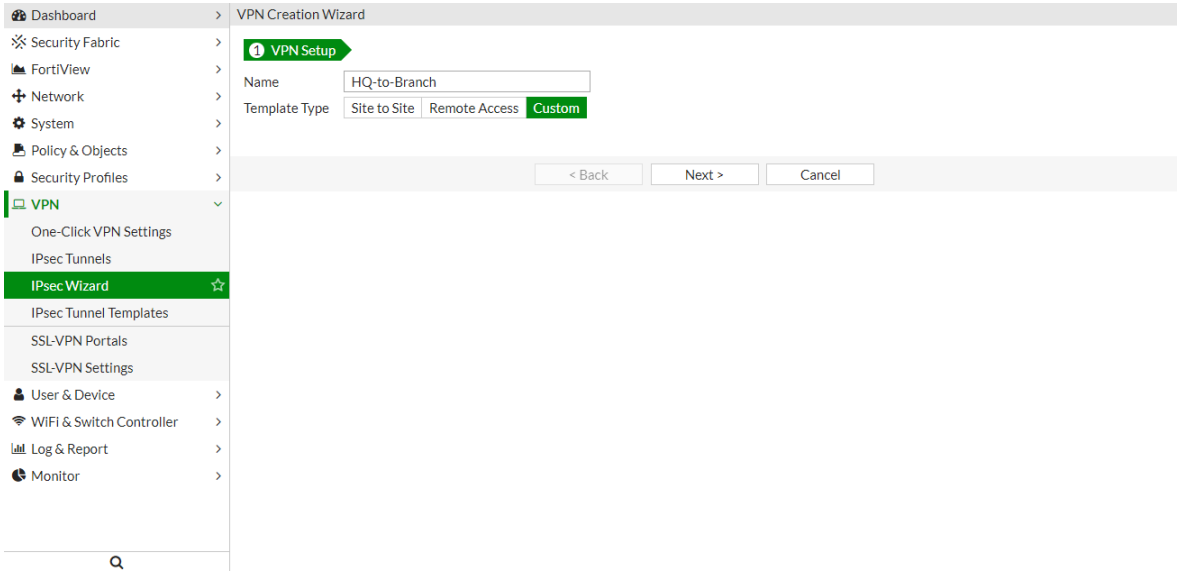
Trên HQ Fortigate, vào ***System*** -> ***Feature Visbility*** -> ***enable Policy-based IPsec VPN.***



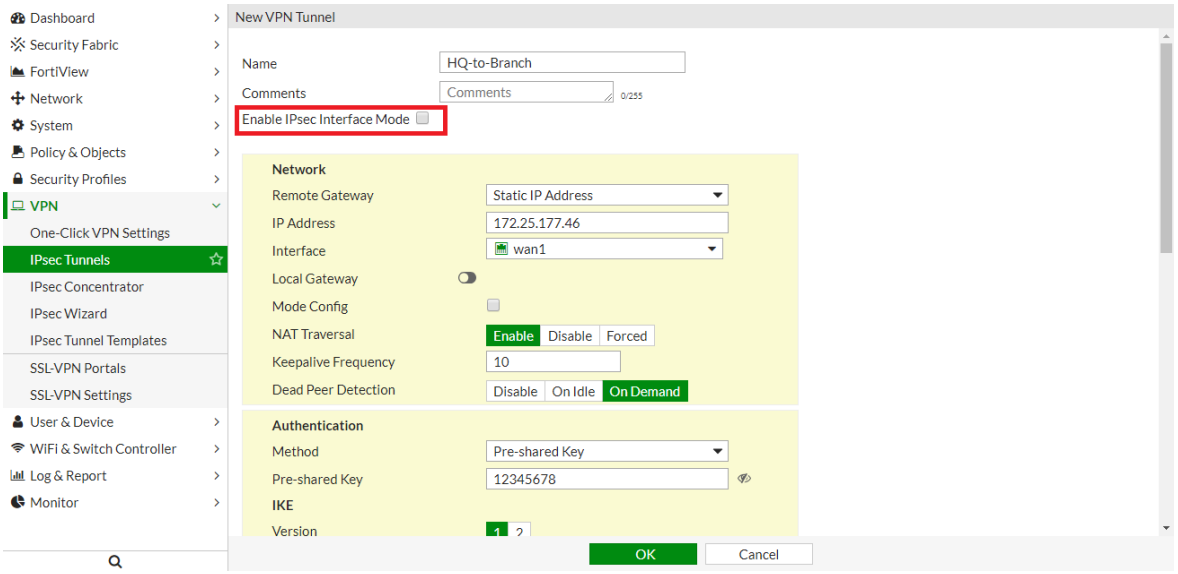
B2: Cấu hình IPsec VPN Phase1 và Phase 2 trên HQ

VPN -> IPsec Wizard.

Chọn **Custom** VPN Tunnel (No Template) -> Next.

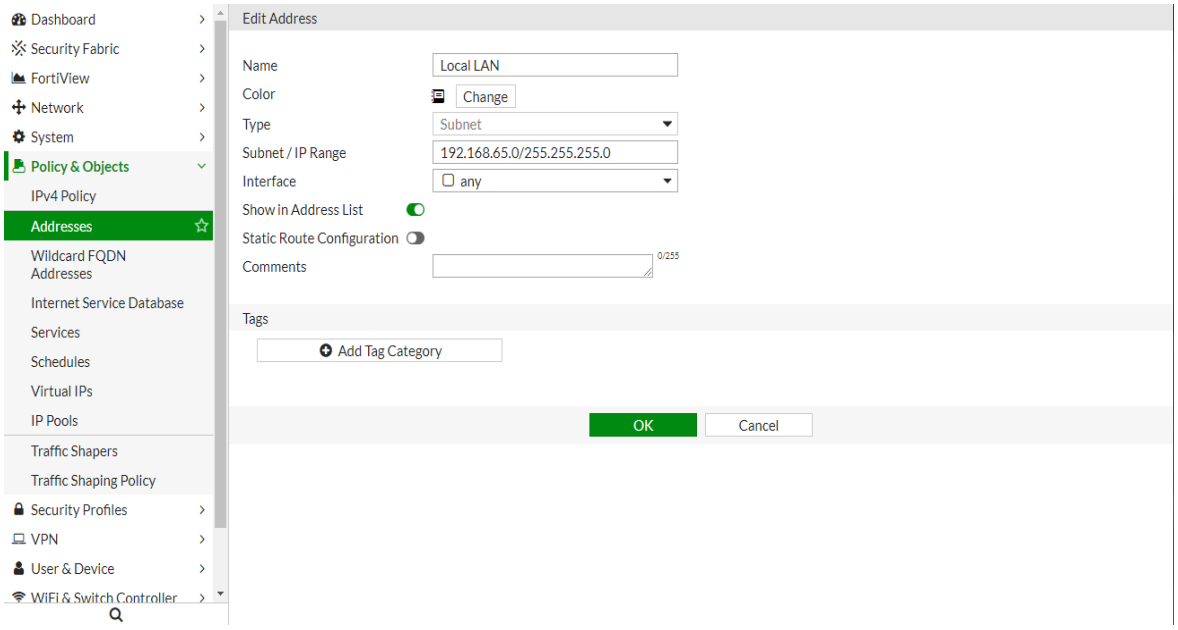


- Disable IPsec Interface Mode.
- Interace: chọn Interface kết nối Internet của site HQ.
- IP Address: điền địa chỉ IP của FortiGate site Branch.
- Pre-shared Key: nhập mã key để xác thực giữa 2 thiết bị FortiGate.

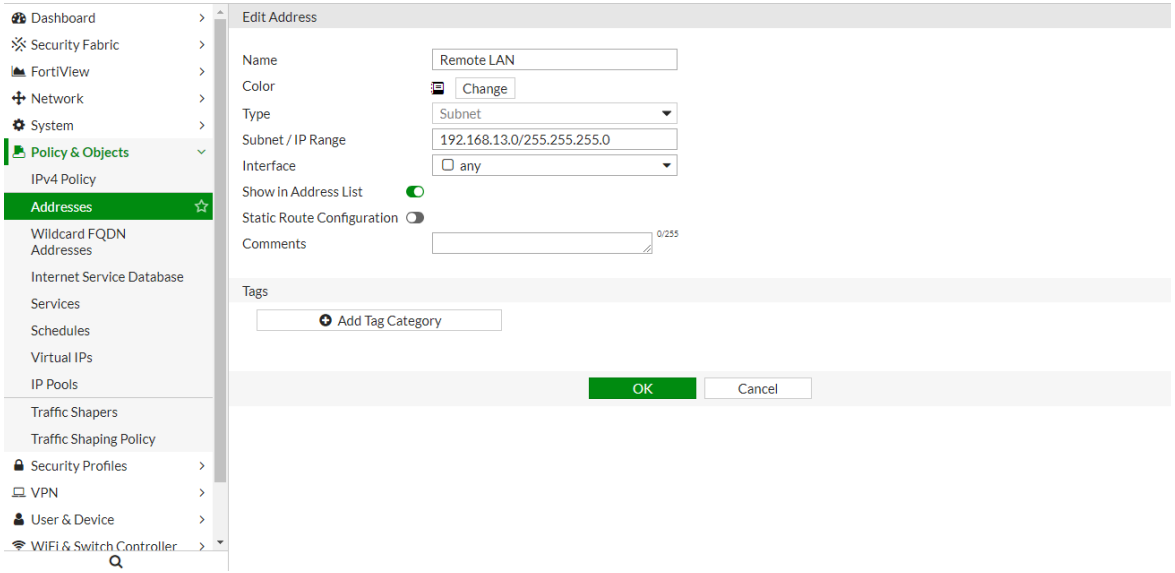


B3: Định danh địa chỉ mạng LAN nội bộ và LAN truy cập từ xa của Branch trên HQ.

- Trên HQ Fortigate, vào ***Policy & Objects*** -> ***Address*** -> ***Create New -> Address.***
- Chúng ta phải định danh được địa chỉ local của HQ và địa chỉ local của Branch.
- Định danh địa chỉ cho LAN nội bộ của HQ với mạng : 192.168.65.0/24

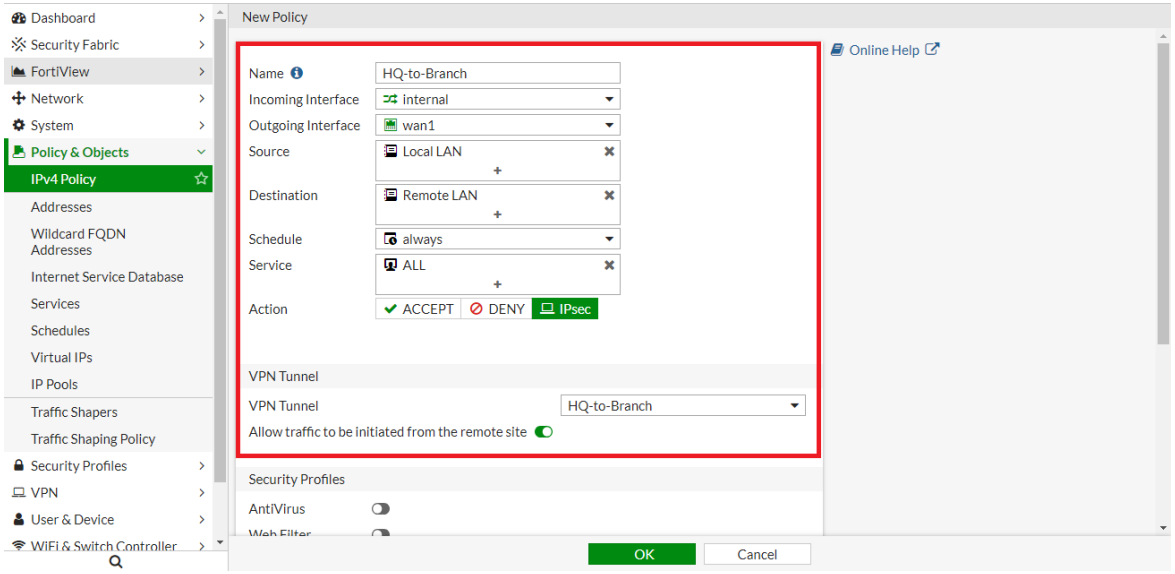


- Định danh địa chỉ cho LAN nội bộ của Branch với mạng: 192.168.13.0/24



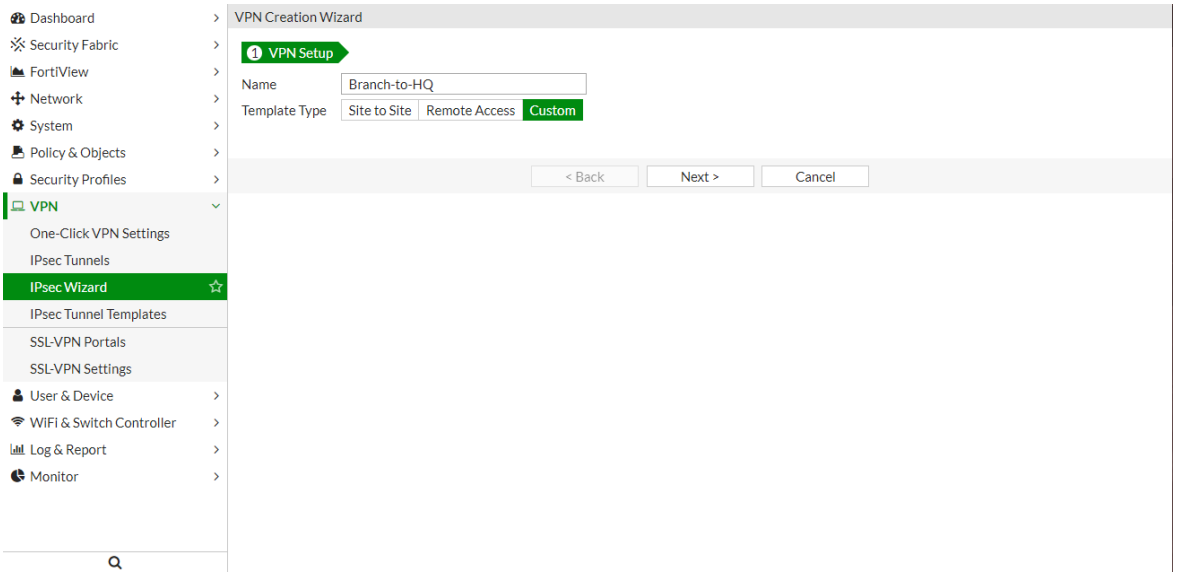
B4: Tạo một Policy cho HQ

- Trên HQ Fortigate, vào ***Policy & Objects*** -> ***Ipv4 Policy -> Create New.***



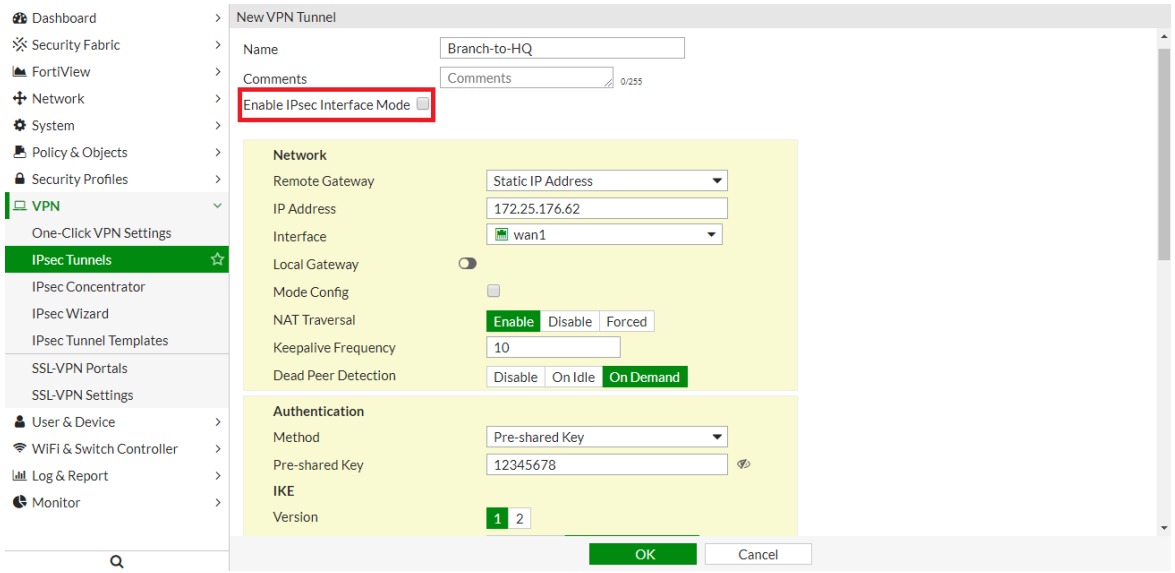
B5. Cấu hình IPsec VPN Phase1 và Phase2 trên Branch.

- Đầu tiên, bật tính năng Policy-Based VPN trên Branch Forigate.
- Đi tới ***VPN -> IPsec Wizard.***
- Chọn **Custom** VPN Tunnel (No Template) -> Next.



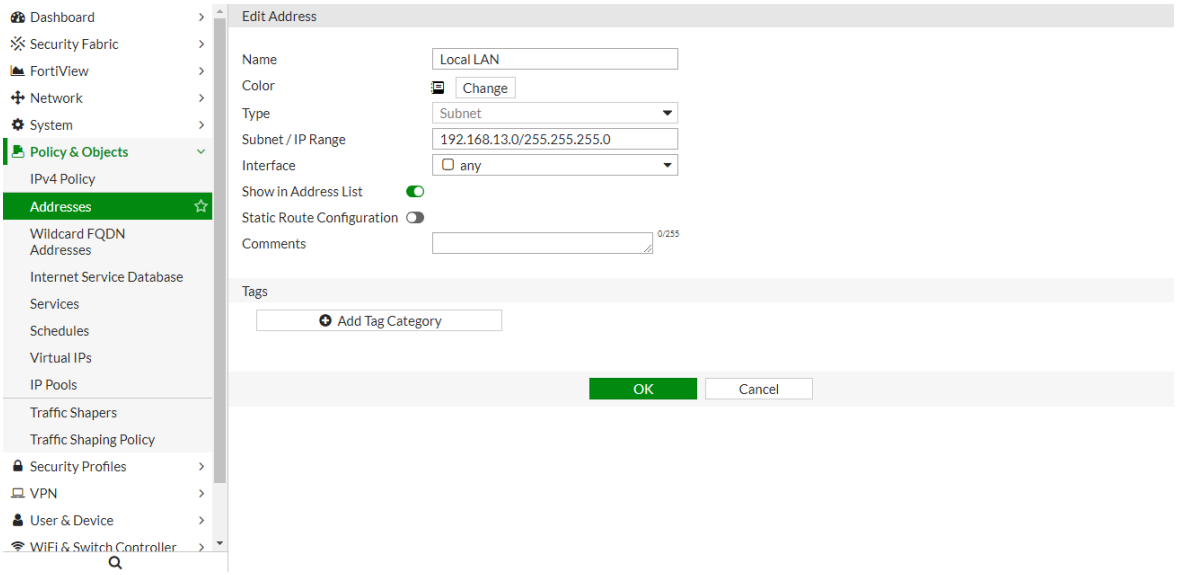
Disable IPsec Interface Mode.

- IP Address: điền địa chỉ IP của FortiGate site Branch.
- Interace: chọn Interface kết nối Internet của site HQ.
- Pre-shared Key: nhập mã key để xác thực giữa 2 thiết bị FortiGate.

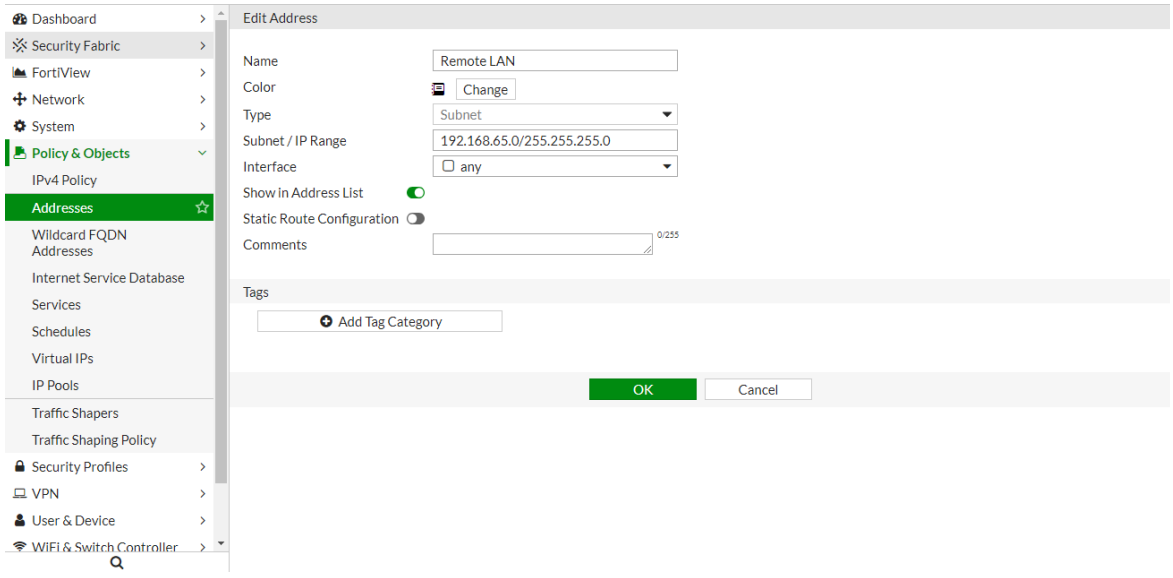


B6. Định danh địa chỉ mạng LAN nội bộ và LAN truy cập từ xa của HQ trên Branch

- Trên HQ Fortigate, vào ***Policy & Objects*** -> ***Address -> Create New -> Address.***
- Chúng ta phải định danh được địa chỉ local của HQ và địa chỉ local của Branch.
- Định danh địa chỉ cho LAN nội bộ của HQ với mạng : 192.168.13.0/24

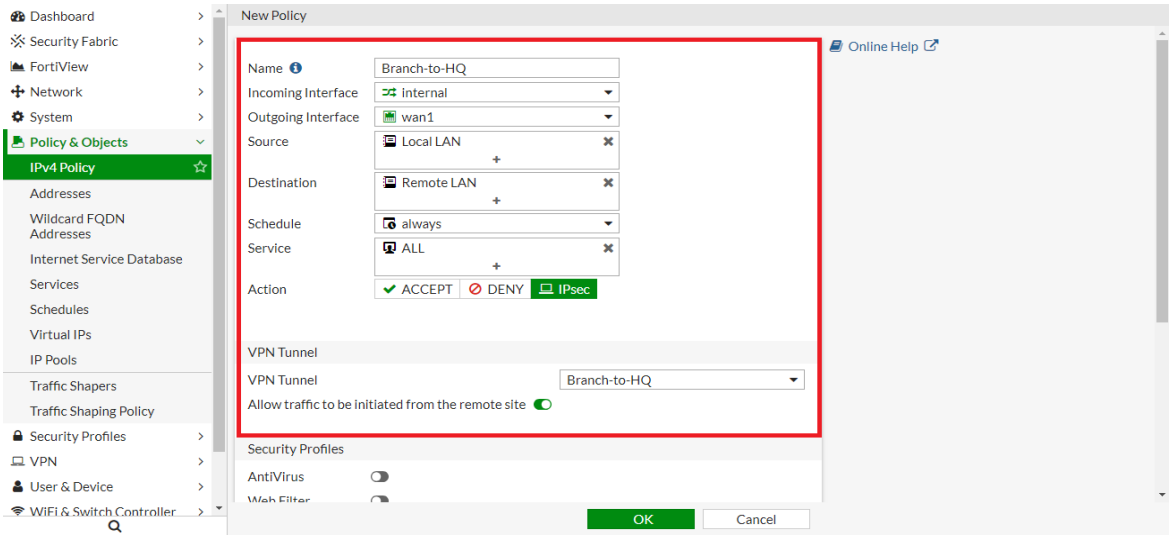


- Định danh địa chỉ cho LAN nội bộ của Branch với mạng: 192.168.65.0/24



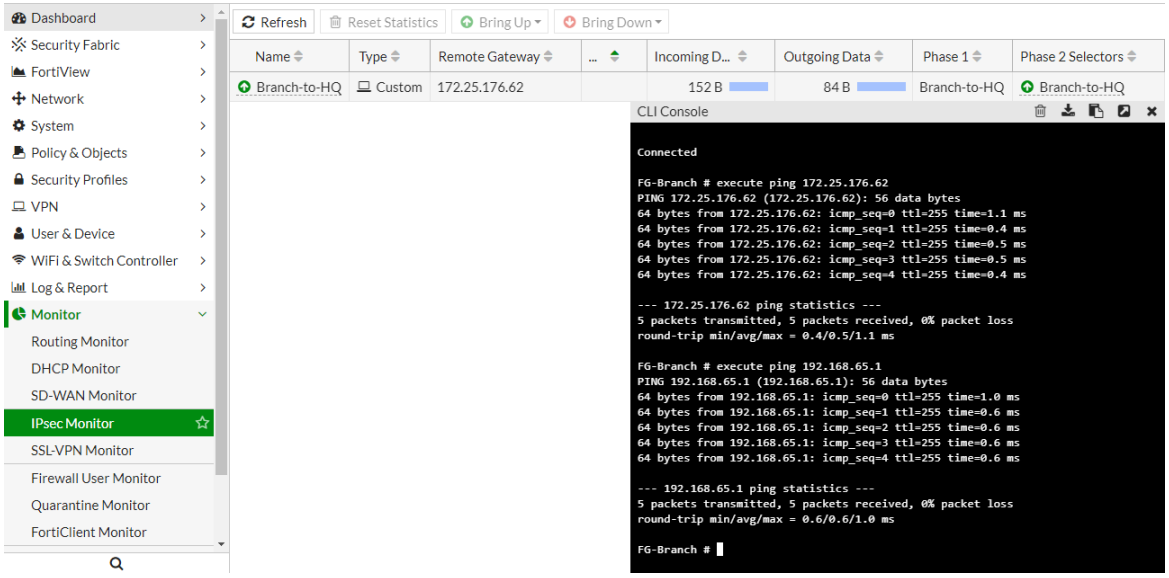
B7. Tạo một Policy cho Branch.

- Trên Branch Fortigate, vào ***Policy & Objects*** -> ***Ipv4 Policy -> Create New.***



B8. Kết quả.

Vào ***Monitor*** -> ***IPsec Monitor.***

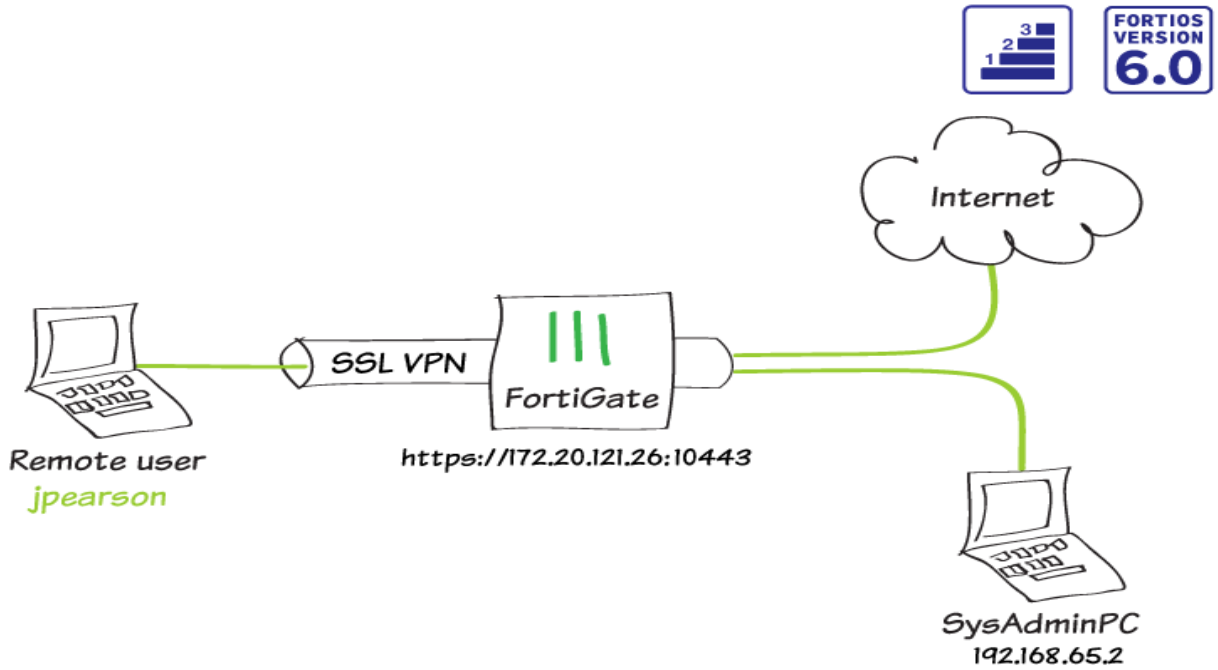


14. SSL VPN

14.1: Giới thiệu

SSL VPN là một công nghệ VPN được phát triển dựa trên nền giao thức SSL, hoạt động ở tầng 7 của mô hình OSI. SSL VPN được sử dụng để kết nối những người dùng di động, từ xa vào tài nguyên mạng công ty thông qua giao thức HTTPS.

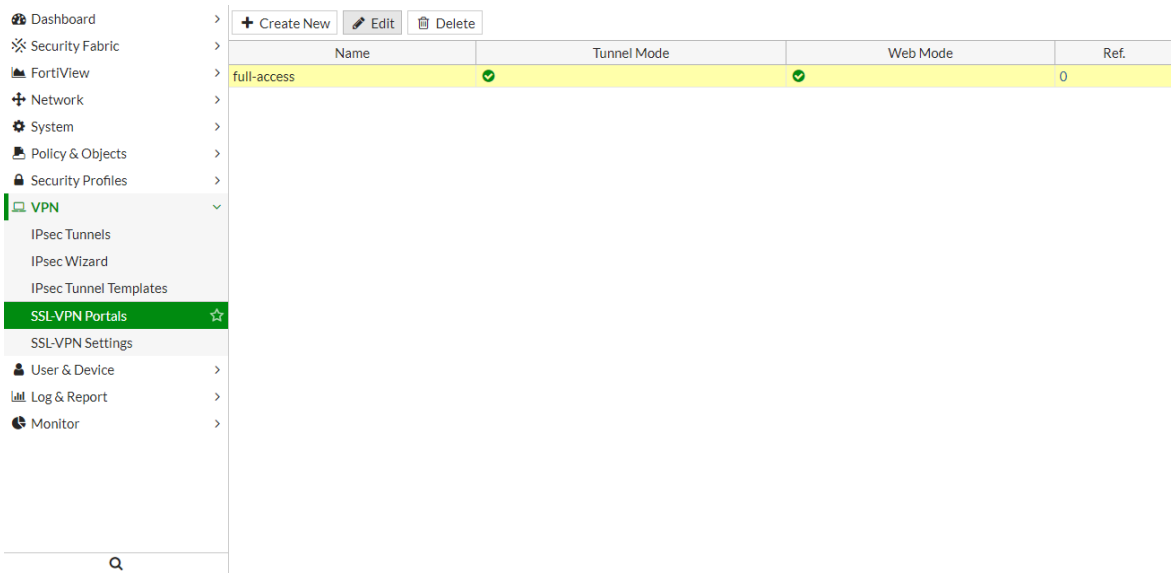
14.2: Cấu hình



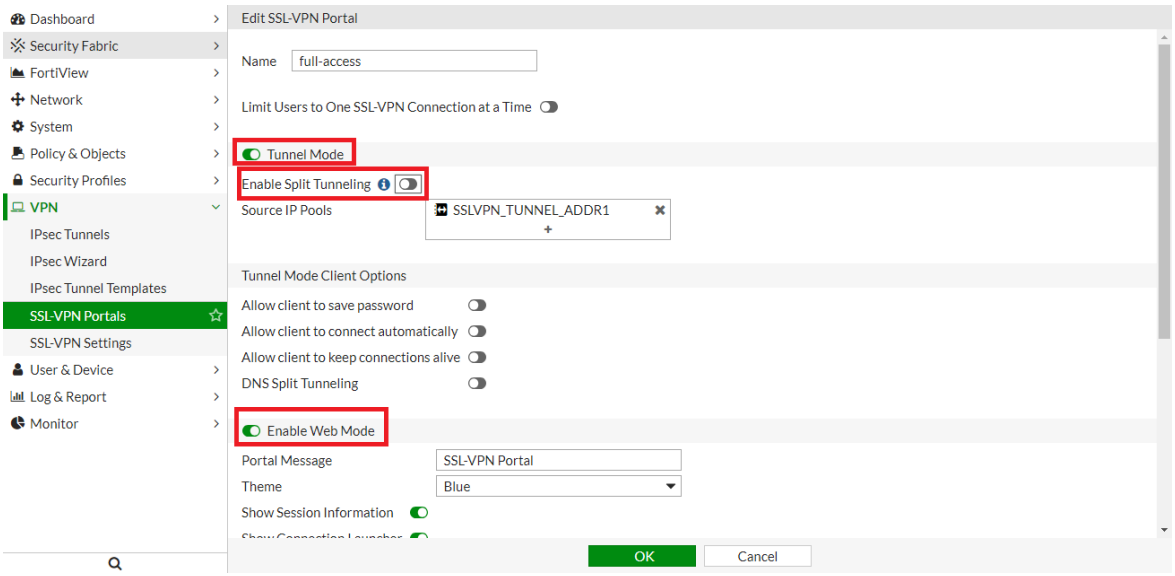
Các bước cấu hình SSL VPN:

B1. Tạo SSL-VPN portal.

- Tạo Groups SSL VPN: ***VPN -> SSL-VPN Portals -> Create New (hoặc Edit để chỉnh sửa).***

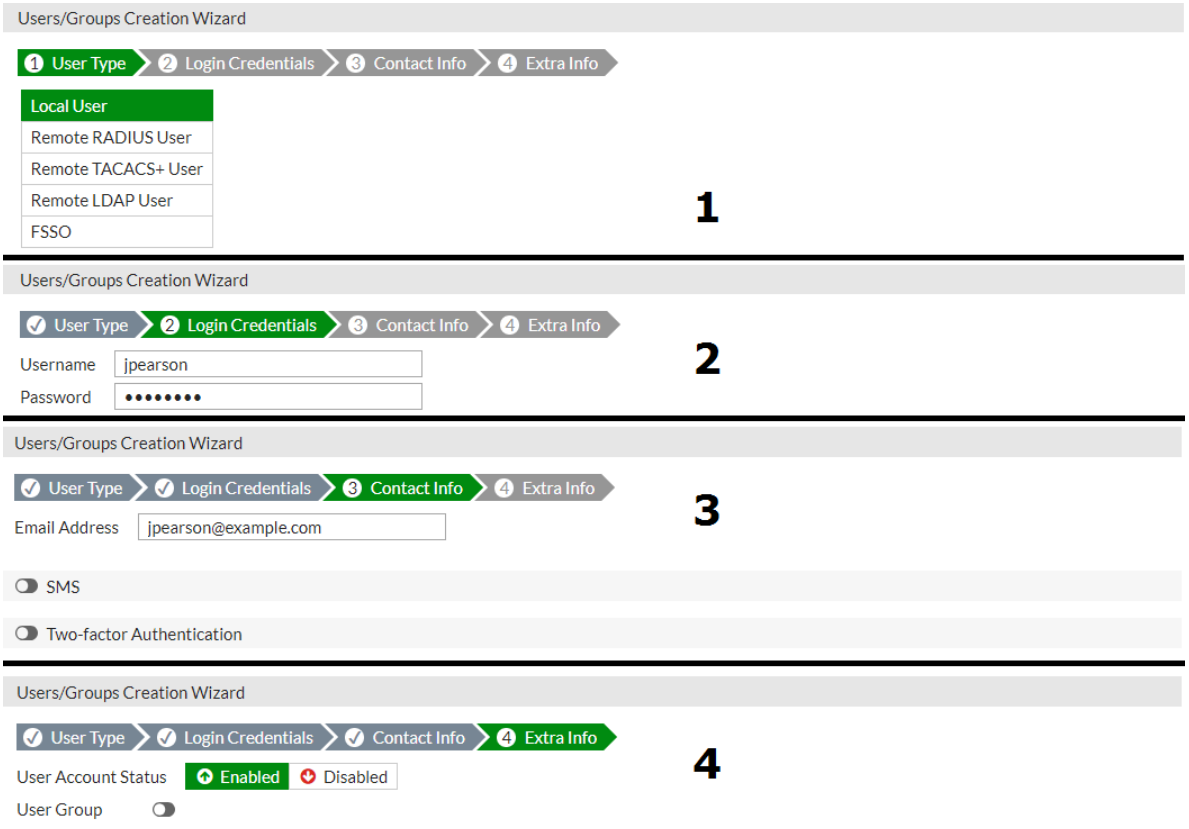


Enable ***Tunnel Mode*** và ***Web Mode***.
Disable ***Split Tunneling.***



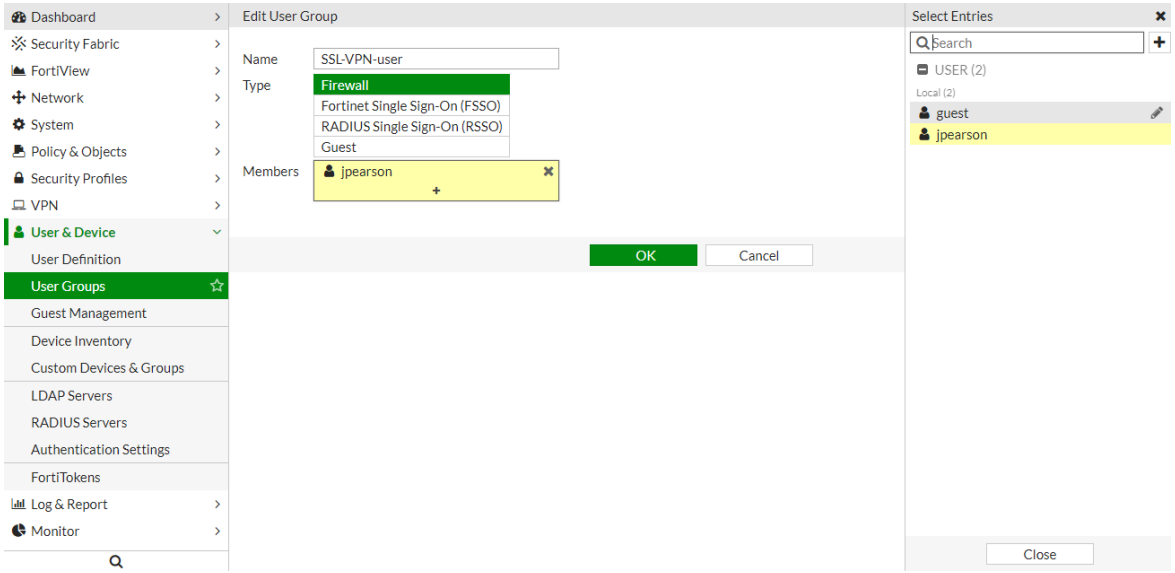
B2: Tạo User & User Group: ***User & Device -> User Definition -> Create new.***

Tạo user ***Jpearson.***



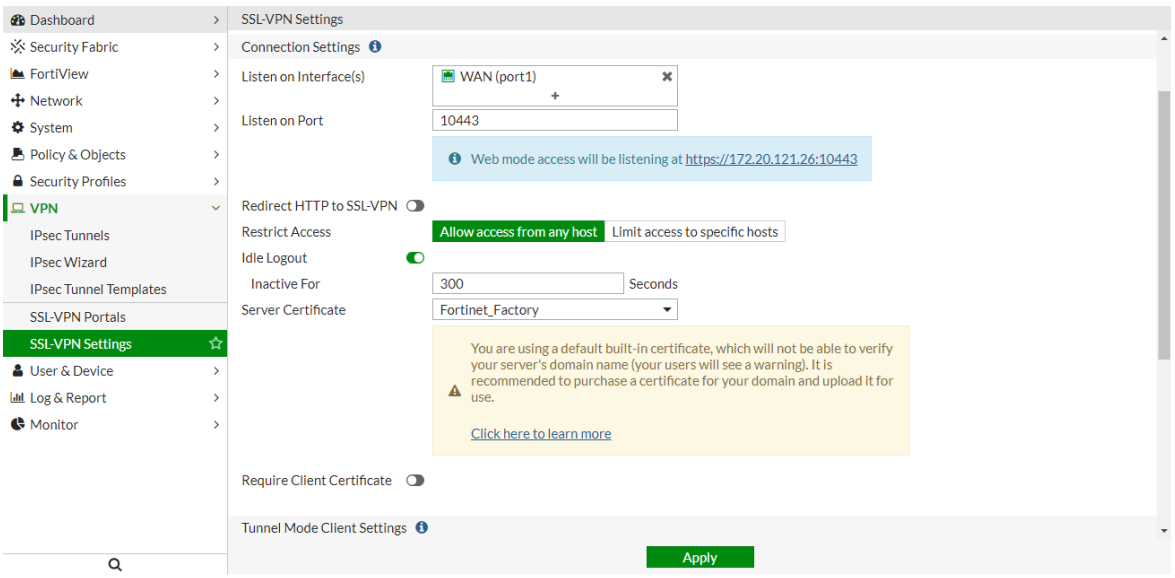
User & Device -> User Groups -> Create New.

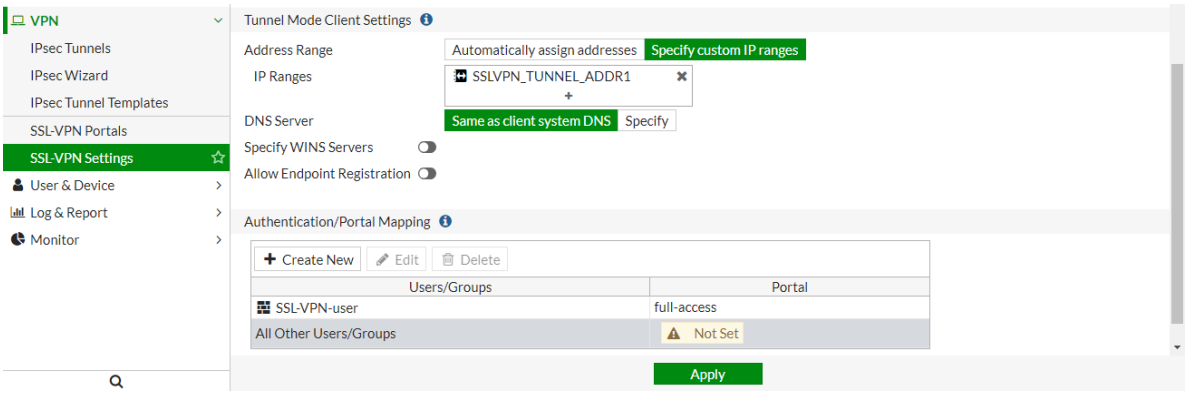
Tạo Group **SSL-VPN-user.**



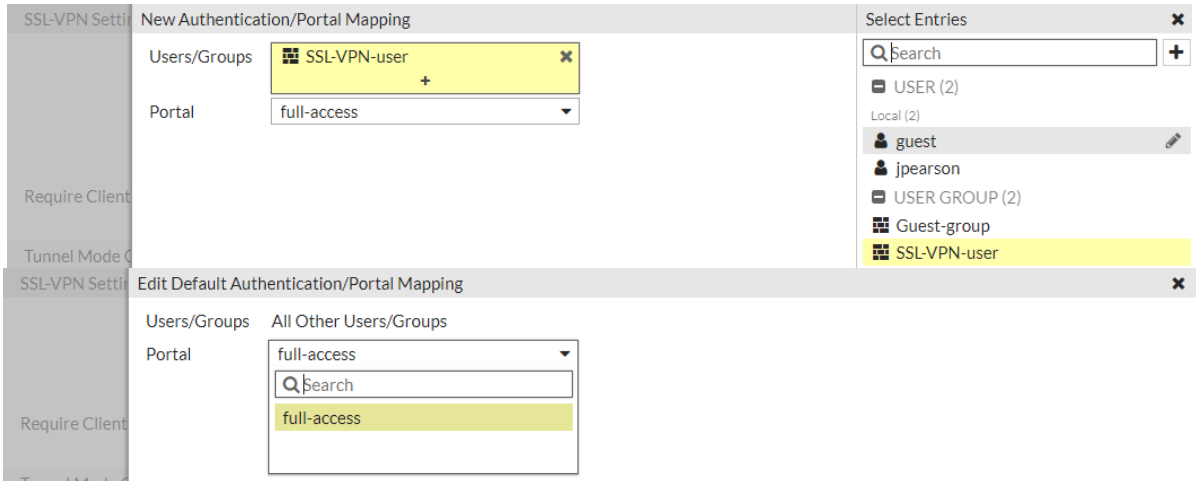
B3: Cấu hình SSL VPN:

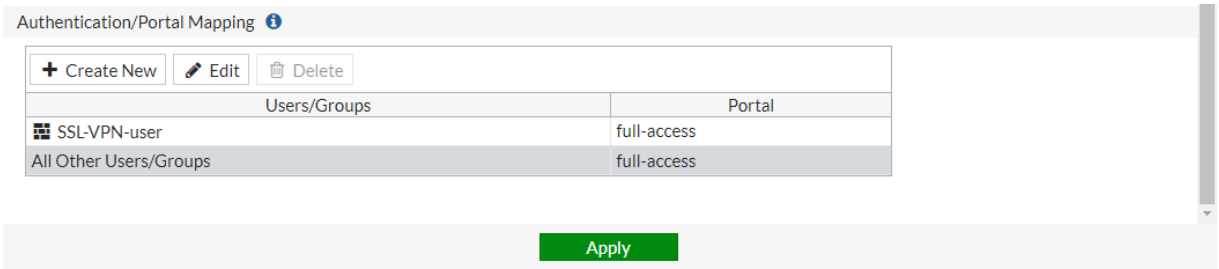
- Vào ***VPN ->SSL-VPN Settings.***
    - Listen on Interface(s): Interface kết nối Internet.
    - Listen on Port: Port sử dụng cho kết nối SSL VPN, mặc định **443** có thể bị trùng ta nên đổi thành **10443**.
    - Restrict Access: **Allow access from any host**.
    - Server Certificate: **Fortinet_Factory**.





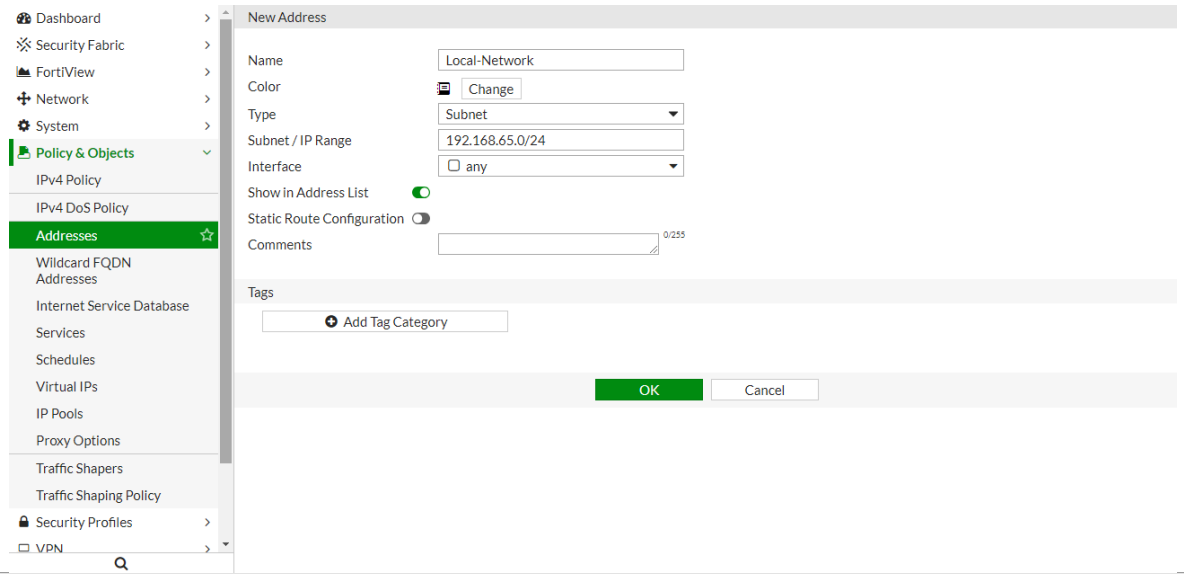
Authentication/Portal Mapping: thêm các user hoặc group để xác thực khi kết nối VPN.





B4: Thêm Address cho Policy.

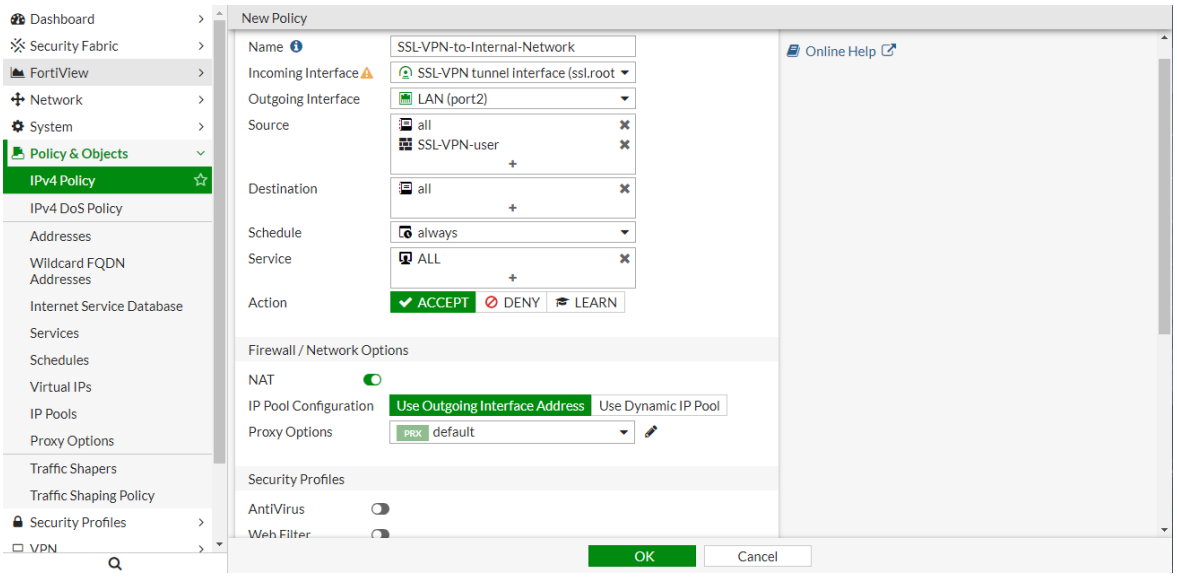
Policy & Objects -> Address -> Create New.



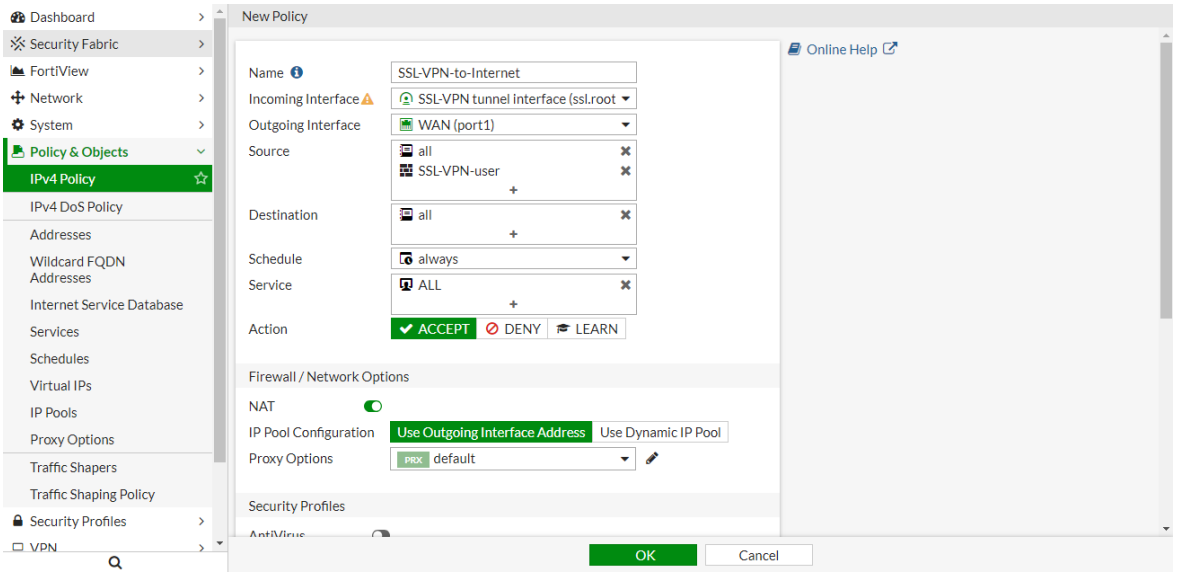
B5: Tạo Policy để sử dụng SSL.

Policy & Objects -> IPv4 Policy -> Create New.

Tạo **Policy** đi **Internal.**

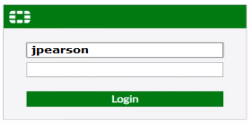


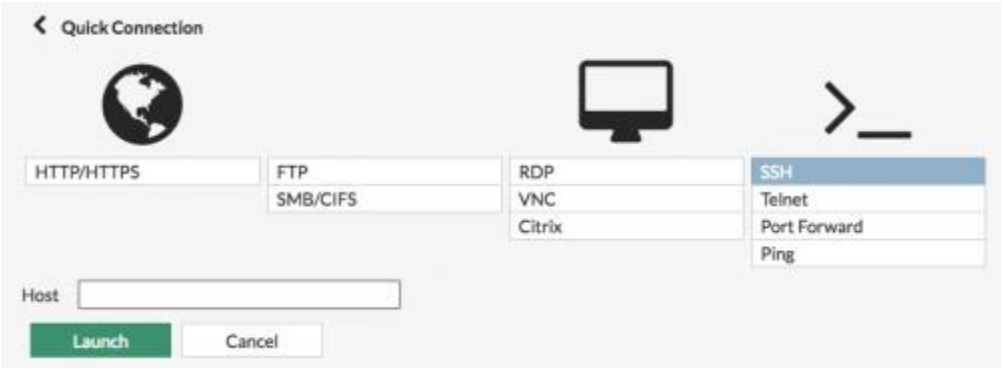
Tạo **Policy** đi **Internet.**



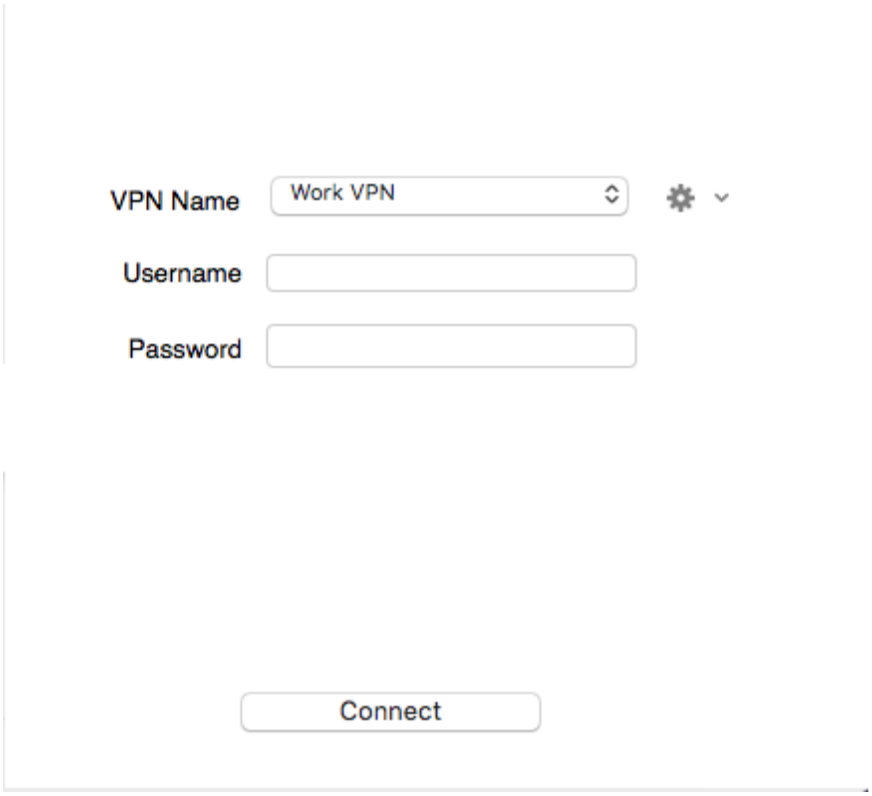
B6: Kết quả.

- Login bằng giao diện Web:





Login bằng FortiClient:

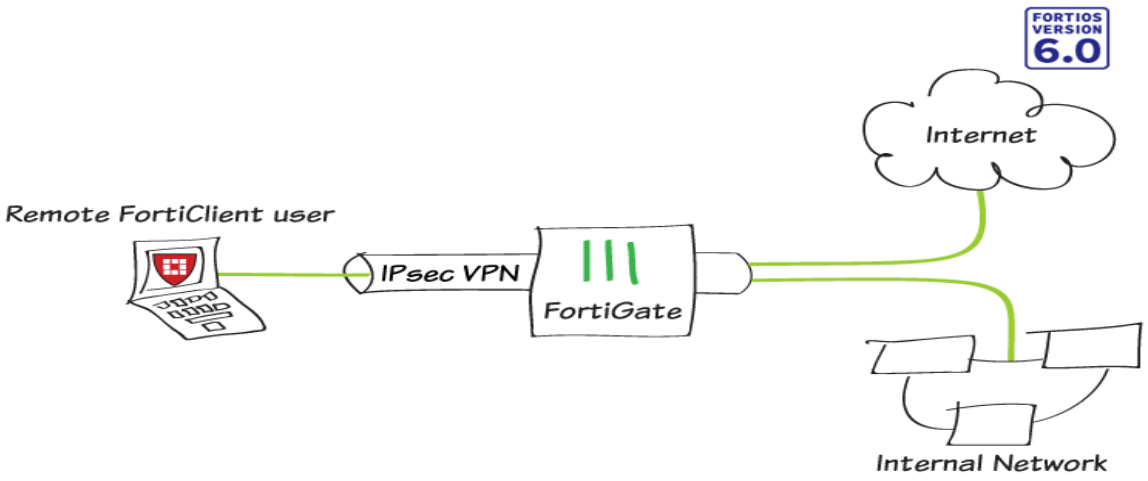


15. VPN IPSec CLIENT-TO-GATEWAY

15.1: Giới thiệu

Cũng giống như SSL VPN, IPSEC VPN Client sẽ tạo một tunnel giữa client và mạng riêng của công ty, tất cả traffic sẽ được mã hóa trên kênh kết nối này. Điểm khác nhau giữa SSL VPN và IPSec VPN là giao thức kết nối và tầng hoạt động trong mô hình OSI.(IPSec hoạt động ở lớp Network còn SSL VPN hoạt động ở lớp Application).

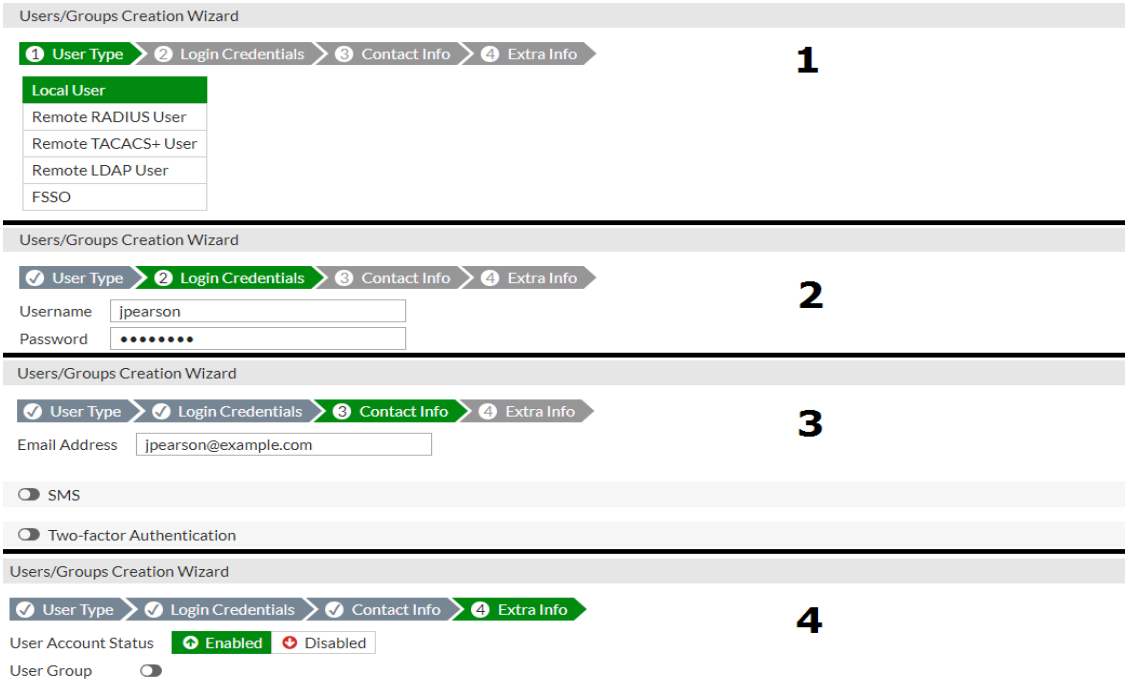
15.2: Cấu hình



B1: Tạo User Definition và User Groups.

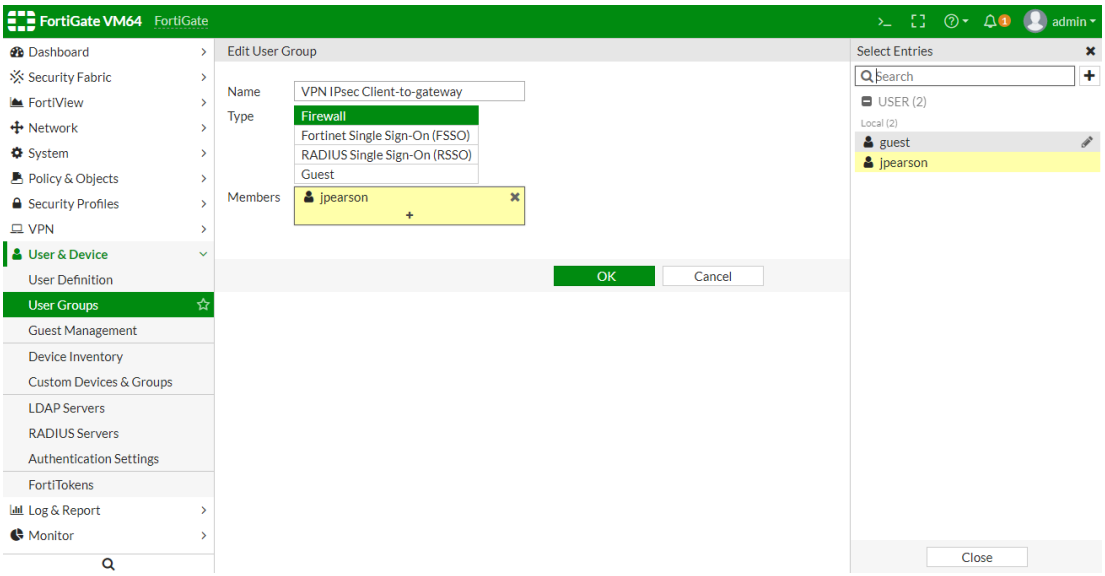
- Định nghĩa User & Group: ***User & Device -> User Definition -> Create new.***

  Tạo user ***jpearson***



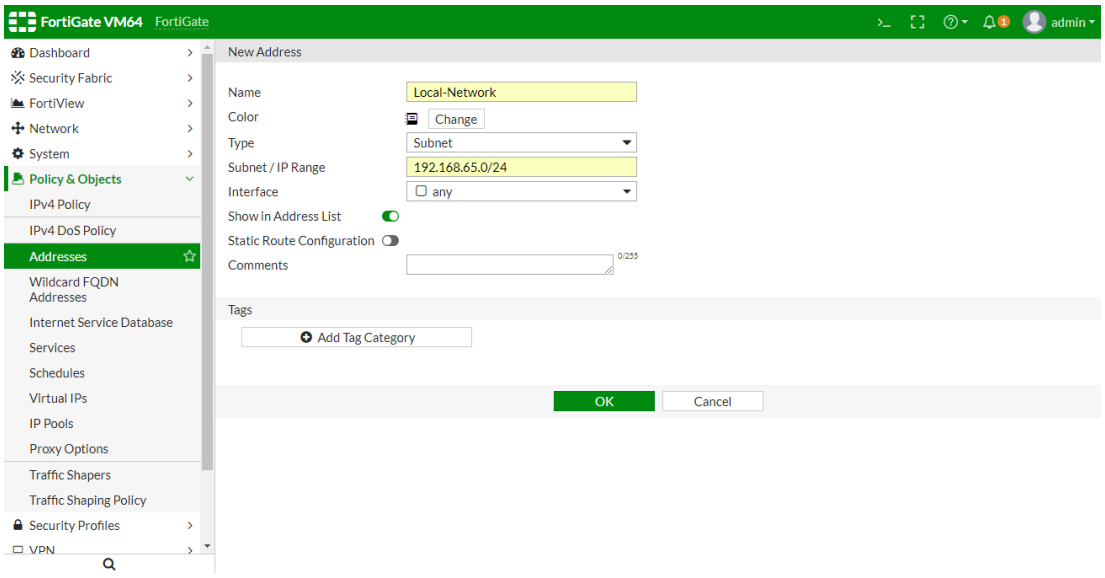
- Tạo Groups IPsec client-to-gateway:

  User & Device -> User Groups -> Create new.



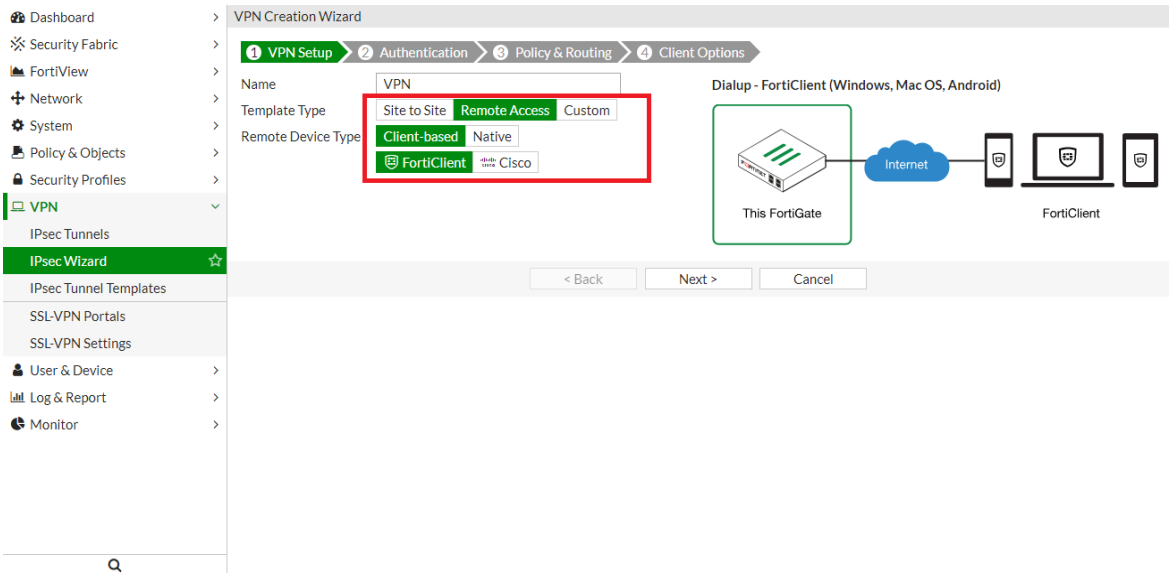
B2: Tạo Address.

Policy & Objects -> Addresses -> Create New.

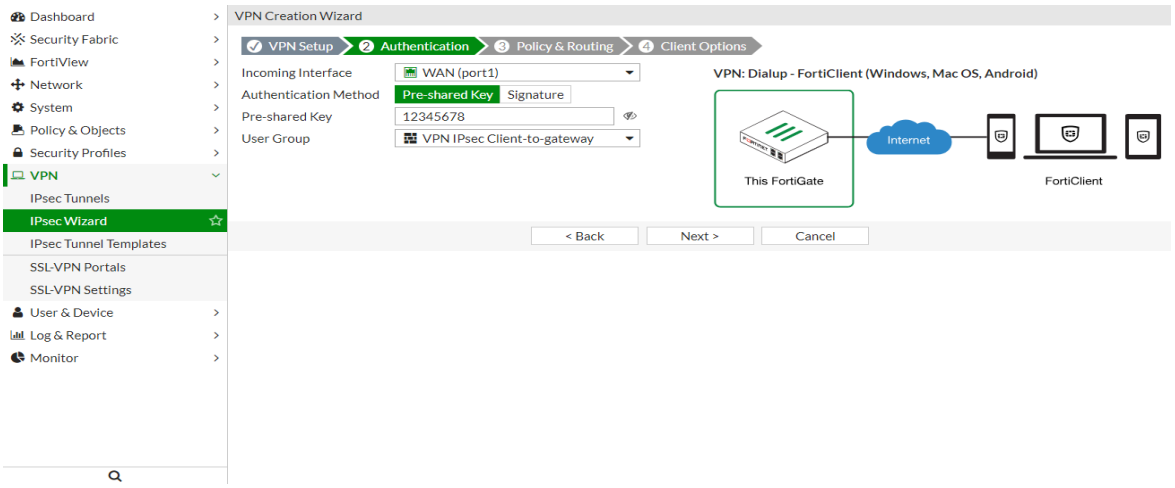


B3: Cấu hình VPN Ipsec FortiGate bằng Ipsec VPN Wizard.

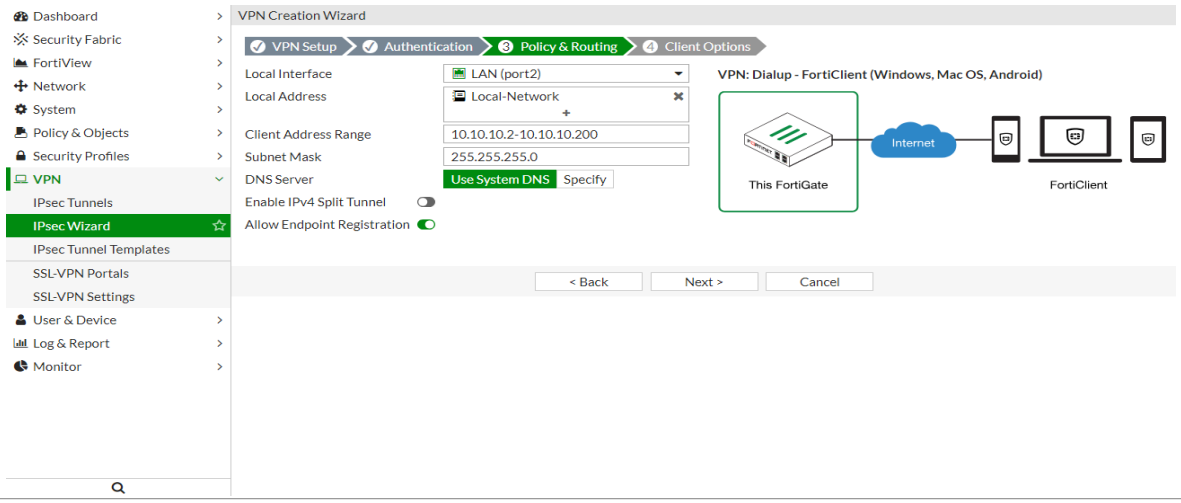
- Đi tới **VPN -> IPsec Wizard.**
- **Name:** Đặt tên cho kết nối VPN.
- **Template:** Reamote Access.
- **Next.**



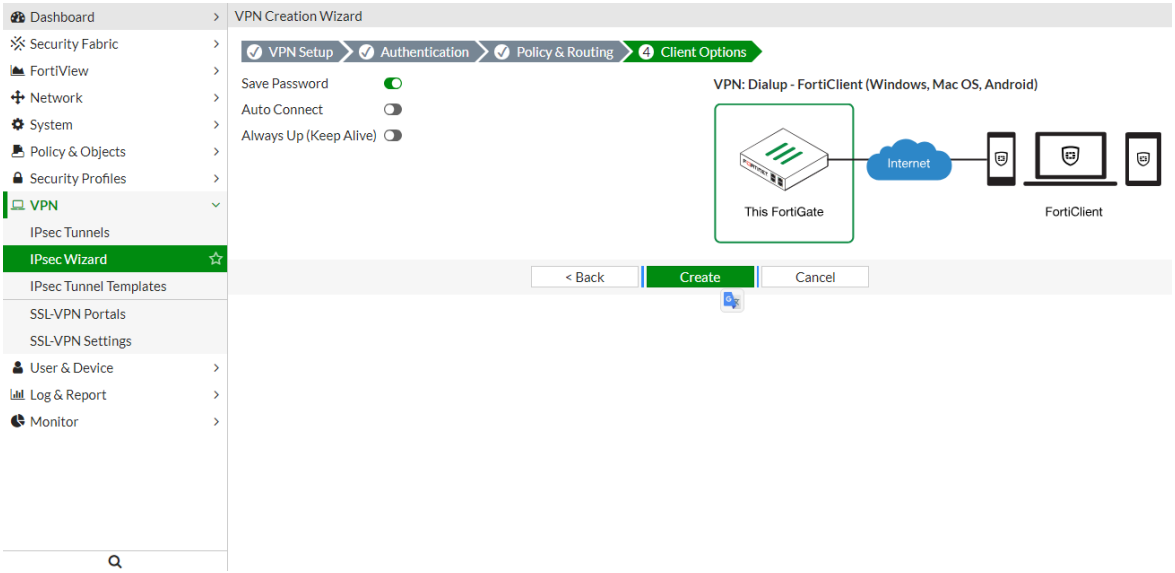
- **Incoming Interface:** Interface để User quay VPN vào.
- **Preshared Key:** Nhập mã khóa xác thực để xác thực kết nối VPN giữa FortiClient vs FortiGate.
- **User Group:** Chọn group hoặc user đã tạo bước 1.
- **Next.**



- **Local Interface:** Interface kết nối mạng LAN của FortiGate.
- **Local Address:** Lớp mạng cho phép Client VPN truy cập tới.
- **Client Address Range:** địa chỉ IP cấp cho client khi kết nối VPN thành công.
- **Subnet Mask:** Subnet của địa chỉ IP cấp cho Client.
- **DNS Server:** Có thể dùng DNS của hệ thống hoặc DNS do người dùng cấu hình bằng tay.
- **Enable Ipv4 Split Tunnel:** Enable tùy chọn này sẽ cho phép các traffic thông thường của client (vd: Internet) sẽ đi theo đường route thông thường, không đi qua Gateway của VPN. Điều này giúp giảm băng thông cho đường truyền.
- **Next.**

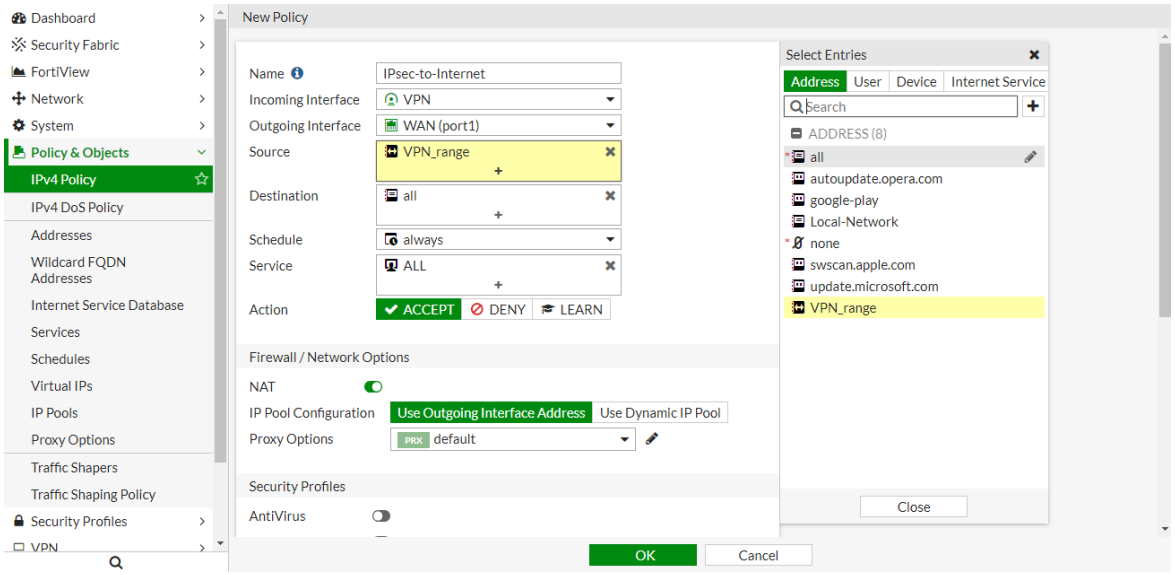


- Các tùy chọn thêm cho Client khi quay VPN.
- **Create.**



B4: Cấu hình Policy cho phép kết nối VPN.

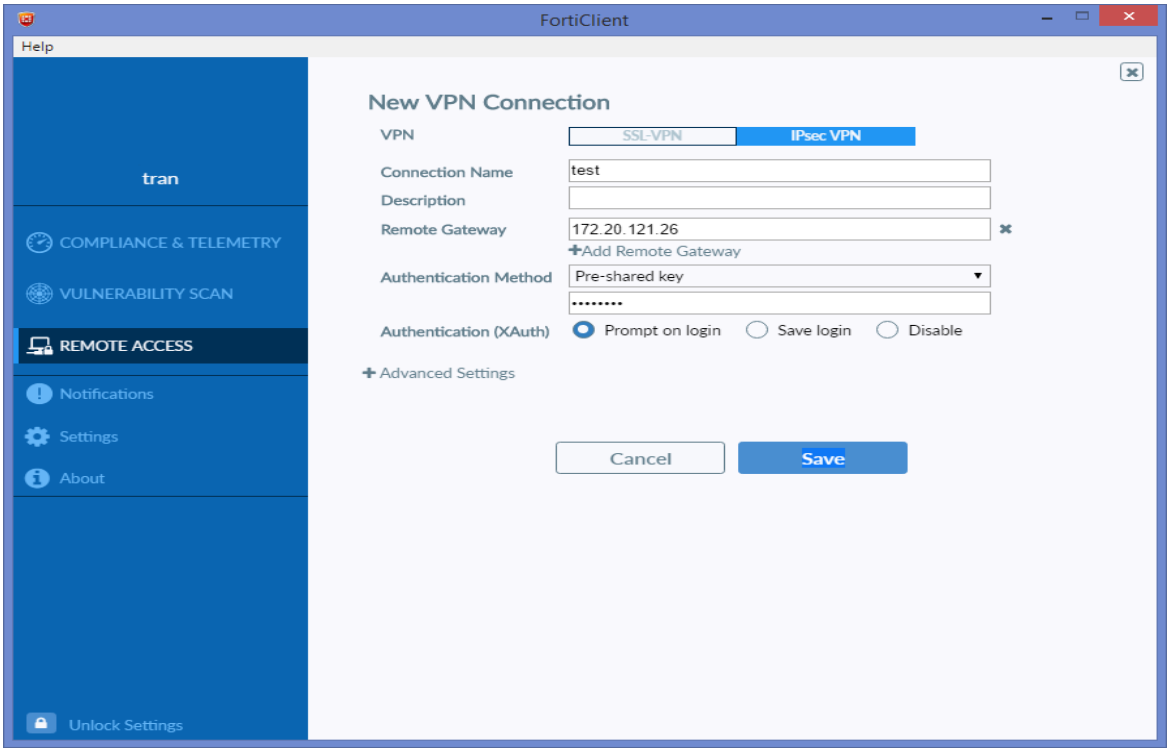
- Đi tới **Policy & Objects -> IPv4 Policy -> Create New.**



B5: Cấu hình trên phần mềm FortiClient để quay VPN.

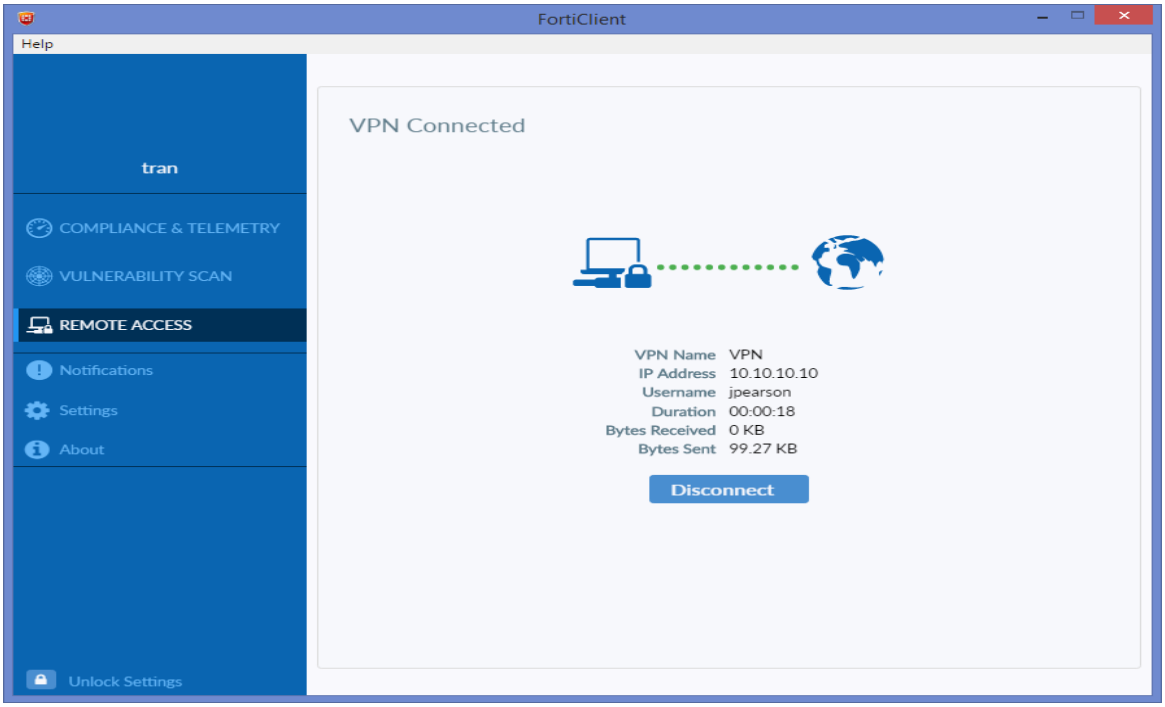
Mở phần mềm FortiClient: ***Remote Access -> Configure VPN -> IPsec VPN.***

- **Connection Name:** Tên kết nối VPN
- **Type:** loại kết nối VPN là SSL hoặc IPsec.
- **Remote Gateway:** IP của cổng kết nối Internet trên FortiGate
- **Pre-Shared Key:** Nhập mã xác thực đã cấu hình trên FortiGate



B6: Kết quả.

- Remote access với **Username**: jpearson
  Password(pre-share key): 12345678



- Kiểm tra **Log & Report.**