CÔNG TY CỔ PHẦN CÔNG NGHỆ MẠNG LANCS VIỆT NAM

Hotline: +84 868275959 | Email: info@lancsnet.com | Website: https://lancsnet.com/
Văn phòng: BT35 – TT3, đường số 23, KĐT thành phố Giao Lưu, Cổ Nhuế 1, Bắc Từ Liêm, Hà Nội, Việt Nam.

HƯỚNG DẪN SỬ DỤNG
THIẾT BỊ TƯỜNG LỬA LINKSAFE SMR 2506-E
- GIAO DIỆN WEB

Tài liệu phiên bản 1.0

WEBSITE HÃNG

https://lancsnet.com/

FEEDBACK

Email: info@lancsnet.com

TÀI LIỆU KHÁC

1. Giải pháp NGFW
2. Giải pháp SD-WAN
3. Giải pháp ZTNA + IAM
4. Giải pháp NOC

MỤC LỤC

CHƯƠNG I. GIỚI THIỆU CHUNG VỀ THIẾT BỊ NGFW

TƯỜNG LỬA THẾ HỆ MỚI (NGFW) là lá chắn bảo vệ giữa mạng nội bộ và môi trường bên ngoài, đảm bảo rằng chỉ những lưu lượng được phép mới có thể tiếp cận hệ thống, ngăn chặn các mối đe dọa từ bên ngoài và bảo vệ dữ liệu quan trọng. Điển hình là các tính năng: Firewall Zone, Firewall Policy, DoS protection…

Lợi ích giải pháp mang lại:

- Hệ thống phát hiện và ngăn chặn xâm nhập: Hỗ trợ Intrusion Detection System (IDS) và Intrusion Prevention System (IPS), Antivirus, Web Filter, DNS filter... giúp phát hiện và ngăn chặn các cuộc tấn công mạng, bảo vệ hệ thống trước các mối đe dọa từ bên ngoài.
- Thiết bị NGFW cũng thực hiện các chức năng như: Định tuyến, chuyển mạch và cung cấp các dịch vụ mạng cơ bản như DHCP, DNS, NAT.
- Hỗ trợ đa giao thức VPN như OpenVPN, PPTP, VTI, VXLAN, GRE và IPSec, giúp tạo các kết nối bảo mật giữa các văn phòng chi nhánh hoặc với người dùng từ xa.
- Tính năng đa phương tiện: Thiết bị hỗ trợ các dịch vụ đa phương tiện như cấu hình số thuê bao (SIP Device), thiết lập đường Trunk (SIP Peer), cung cấp dịch vụ gọi nhóm (Conference Call), dịch vụ tổng đài ảo (IVR), và dịch vụ đăng ký SIP.
- Quản lý và cấu hình dễ dàng: Thiết bị NGFW cung cấp giao diện quản lý web HTTP nhúng, tương thích với các trình duyệt web phổ biến như Internet Explorer, Mozilla Firefox, Google Chrome, Cốc Cốc, và Microsoft Edge. Người dùng có thể dễ dàng cấu hình và theo dõi hoạt động mạng từ bất kỳ thiết bị máy tính nào, đảm bảo việc quản lý mạng được thực hiện an toàn và thuận tiện.

Thành phần giải pháp:

- **Phần cứng:** Thiết bị NGFW

Hình 1: Hình ảnh thực tế của thiết bị NGFW

  - 4 cổng Ethernet 1Gb
  - 2 cổng SFP+
  - 1 cổng Console
  - 1 nút Reset
  - 2 cổng USB debug
- **Phần mềm:**
  - Phiên bản: 2.0

Đối tượng sử dụng tài liệu:

Sách hướng dẫn dành cho các quản trị mạng, người chịu trách nhiệm cho việc vận hành và quản lý các thiết bị mạng trên hệ thống. Sách hướng dẫn yêu cầu người dùng có hiểu biết cơ bản về mạng.

Cấu trúc của tài liệu:

Sách hướng dẫn cung cấp các thông tin chi tiết về các tính năng chính của thiết bị NGFW. Ngoài ra sách cũng mô tả giao diện cấu hình trên WEB của thiết bị.

Sách hướng dẫn bao gồm những phần chính như sau:

- **Chương I:** Giới thiệu về thiết bị NGFW
- **Chương II:** Hướng dẫn cấu hình các tính năng trên giao diện WEB người dùng

Các tài liệu liên quan khác:

Để biết thêm thông tin về quản lý thiết bị bằng giao diện CLI vui lòng tham khảo tài liệu *"Hướng dẫn sử dụng Thiết bị Tường lửa LinkSafe SMR 2506-E (giao diện CLI)"*.

CHƯƠNG II. CẤU HÌNH CÁC TÍNH NĂNG TRÊN DÒNG THIẾT BỊ NGFW

1 Các bước thiết lập ban đầu để cấu hình thiết bị

Bước 1: Kết nối máy tính vào một cổng MGMT bất kỳ của thiết bị NGFW.

Bước 2: Địa chỉ mặc định của cổng MGMT thiết bị NGFW

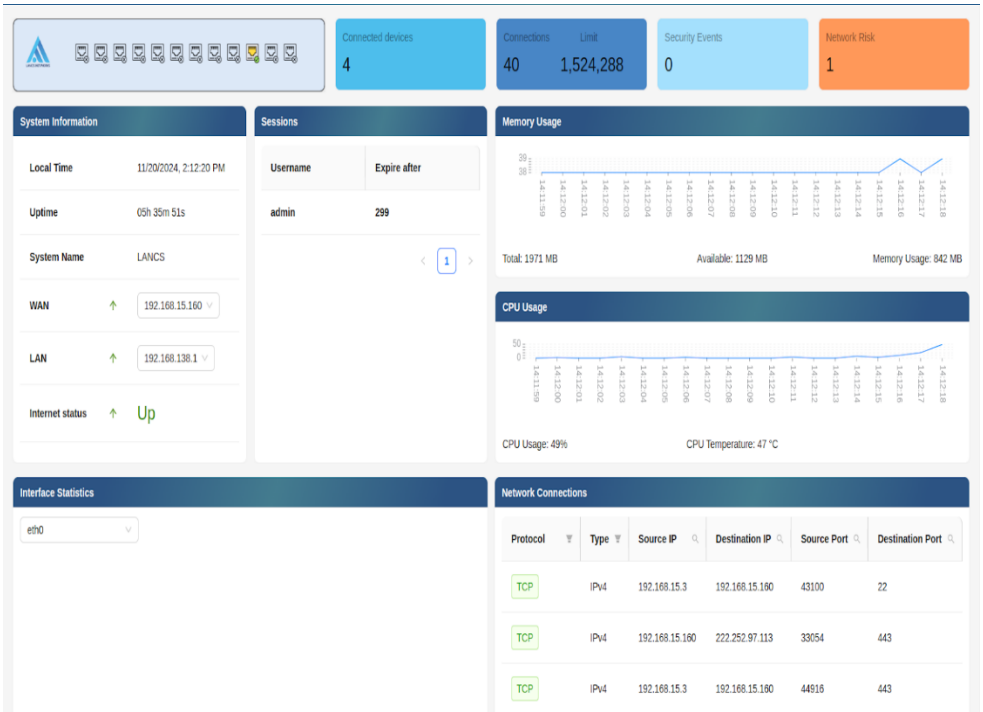
Bước 3: Mở trình duyệt web, truy cập vào địa chỉ "https://192.168.138.1". Giao diện đăng nhập thiết bị như sau:

Hình 2: Giao diện đăng nhập vào NGFW

Bước 4: Đăng nhập với tài khoản mặc định:

- Username: admin
- Password: 123456789abc

Bước 5: Vào giao diện quản lý và thực hiện các tác vụ. Giao diện hiển thị trình quản lý (Dashboard) trên NGFW:



Hình 3: Giao diện hiển thị trình quản lý (Dashboard) trên NGFW

- Giao diện hiển thị trình quản lý (Dashboard) gồm các thông tin chính như sau:
  - Hiển thị thông tin hệ thống (System Information): mô tả các thông tin liên quan đến hệ thống thiết bị NGFW như: Tên, người dùng, phiên bản OS, bộ nhớ…
  - Hiển thị trạng thái của cổng WAN, LAN: Trạng thái up/down và địa chỉ IPv4 được gán trên các cổng.
  - Hiển thị bản đồ lưu lượng: Thể hiện bằng hình ảnh của lưu lượng upload/download của cổng các cổng WAN/LAN.

2 Cấu hình cổng mạng (Interface) trên NGFW

Trong mục này người dùng thực hiện cấu hình giao diện các cổng WAN, LAN.

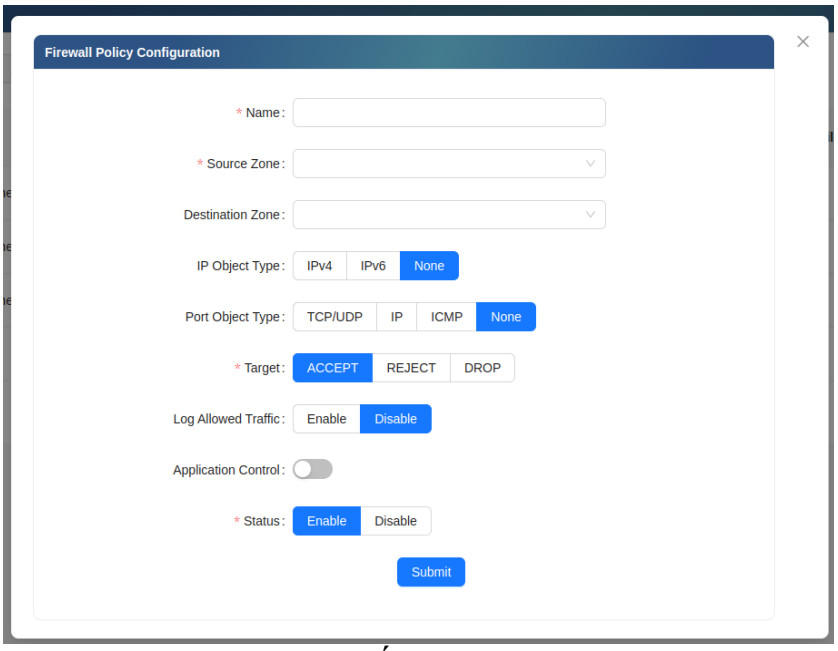
Hỗ trợ cấu hình một số tính năng mạng layer 2: Hỗ trợ các giao diện kiểm tra và cấu hình cho người dùng các tính năng: VLAN Interface, DMZ, Port Mirroring, và LACP.

2.1 Cấu hình cho phép miền mạng LAN sử dụng dịch vụ HTTP/HTTPS

Để cấu hình cho phép miền mạng LAN sử dụng dịch vụ HTTP/HTTPS thông qua miền mạng WAN trong lần đầu khởi động, ta thực hiện các bước như sau:

Bước 1: Chọn Policy & Object → Firewall Zone: Chọn List Network: WAN cho Zone WAN

Bước 2: Chọn Policy & Object → Firewall Policy, thêm policy truy cập WAN từ LAN như sau:



Hình 4: Giao diện cấu hình policy cho firewall

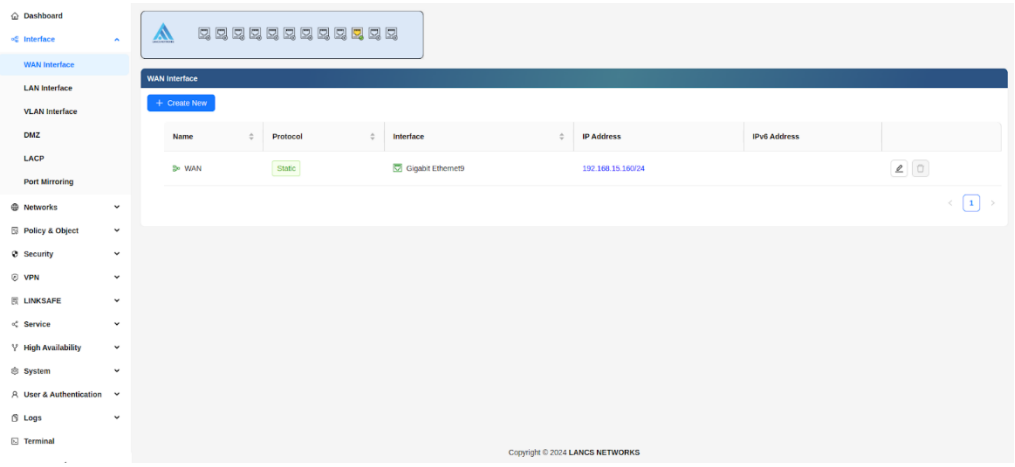
❖ Chọn 

- **Name**: Điền tên gợi nhớ. Ví dụ: Allow-LAN
- **Source zone:** chọn LAN
- **Destination zone:** chọn WAN
- **Port Object:** Cho phép dịch vụ (Port và Protocol) cụ thể. Nếu muốn chỉ cho phép HTTP, HTTPS, SSH thì có thể lựa chọn từ list sổ ra.
- **Target:** Chọn ACCEPT (ACCEPT: cho phép, DROP: loại bỏ, REJECT: loại bỏ và có thông báo phản hồi).
- **Status:** Chọn Enable (Có hay không cho policy được thực thi. (Enable: được thực thi, Disable: chỉ được lưu lại, nhưng không được thực thi).
- Các trường còn lại có thể bỏ qua.

Lưu ý: Hạn chế việc cấp quyền toàn bộ các dịch vụ (ALL_TCP, ALL_UDP).

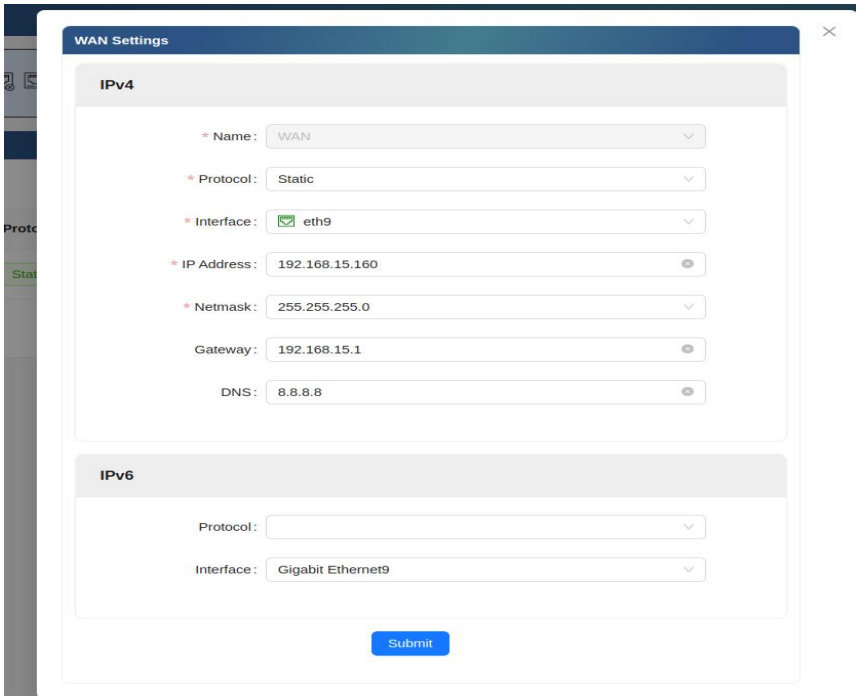
2.2 Cấu hình giao diện WAN trên NGFW

Trước khi đi vào cấu hình các thông tin cho giao diện WAN, người dùng cần kiểm tra trạng thái của cổng WAN tại trình quản lý (Dashboard):



Hình 5: Giao diện hiển thị thông tin và trạng thái WAN trên NGFW

❖ Từ giao diện trình quản lý người dùng truy cập đến → Interface → WAN Interface:



Hình 6: Giao diện hiển thị cấu hình cổng WAN

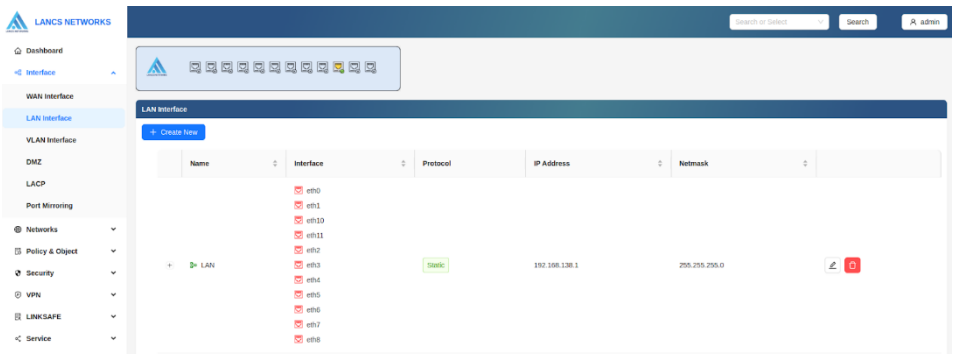
❖ Trong đó:

- **Name**: Nhập tên
- **Protocol**: Chế độ Static hoặc DHCP hoặc PPP
- **Interface Name**: Chọn cổng mạng có sẵn
- **IP Address**: Nhập IP Address

- **Netmask**: Nhập địa chỉ IP Netmask
- **Gateway**: Nhập đia chỉ Gateway
- **DNS**: Điền DNS
- Khi chọn các protocol là Static hoặc PPPoE cần điền thêm 1 số trường: địa chỉ IP, Subnet Mask, Gateway và Username/Password đối với protocol PPP
- **Submit**: *Lưu cấu hình.*

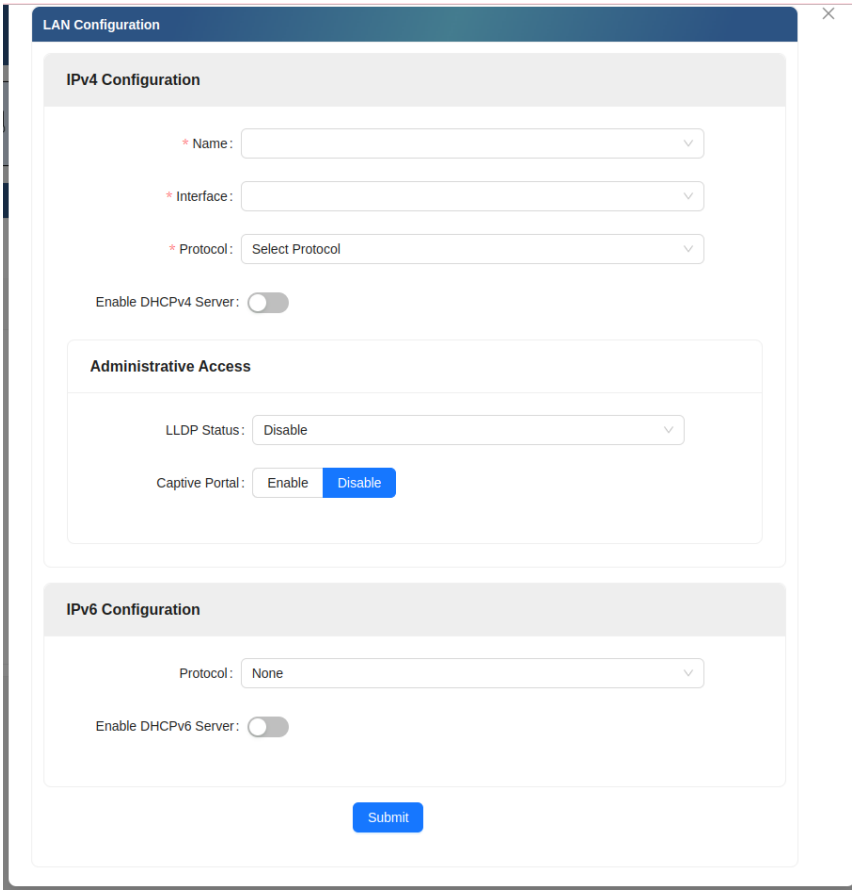
2.3 Giao diện cấu hình LAN Interface trên NGFW

Trước khi đi vào cấu hình các thông tin cho giao diện LAN, người dùng cần kiểm tra trạng thái của cổng LAN tại trình quản lý (Dashboard):



Hình 7: Giao diện hiển thị thông tin và trạng thái LAN trên NGFW

❖ Từ giao diện trình quản lý người dùng truy cập đến → Interface → LAN Interface → Create New:



Hình 8: Giao diện hiển thị cấu hình cổng LAN

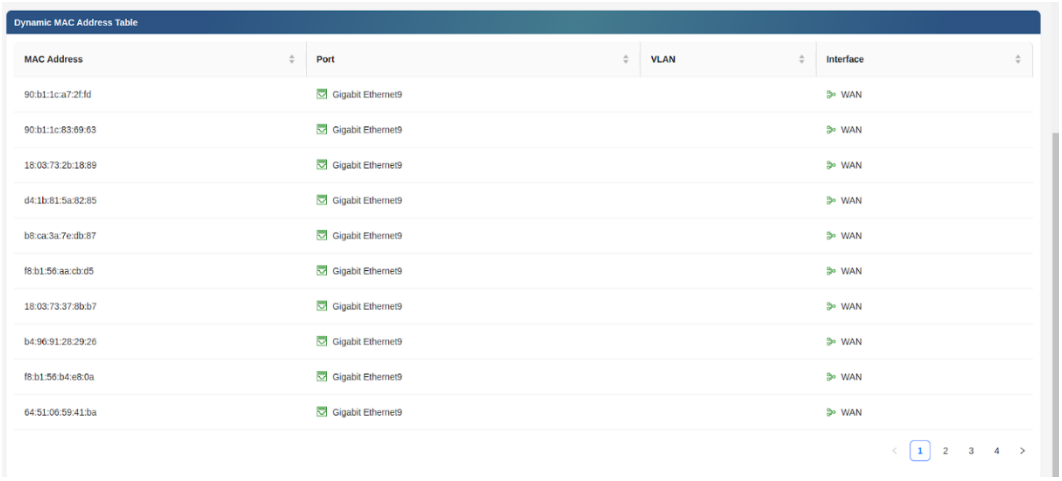
❖ Trong đó:

- **Name**: Chọn gán tên cổng
- **Interface Name**: Chọn cổng mạng
- **Protocol**: Chọn static
- **IP/Netmask**: Điền IP/Netmask
- **Enable DHCPv4 Server/Relay**: Chọn giao thức mạng để cấp phát IP
- Khi cấu hình Enable DHCPv4 Server cấu hình các tham số: DHCP Range, leasetime, Default gateway, DNS server
- **LLDP**: Enable/Disable
- **Captive Portal**: Enable/Disable
- **Submit**: Lưu cấu hình.

2.4 Kiểm tra thông tin chuyển mạch (Forwarding) trên NGFW

Giao diện hiển thị thông tin chuyển mạch (Forwarding):

❖ Từ giao diện quản lý → Network → FDB: Hiển thị thông tin các thiết bị cuối.

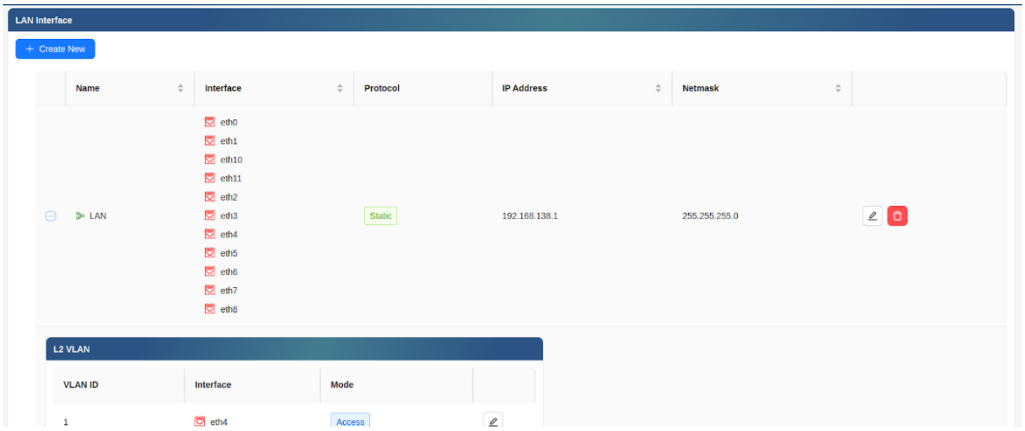


Hình 9: Giao diện hiển thị thông tin chuyển mạch trên NGFW

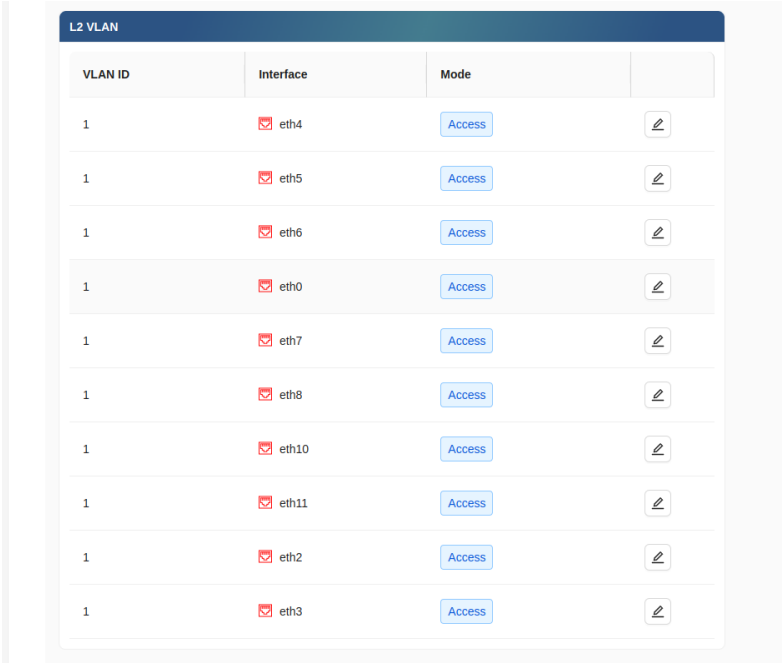
2.5 Giao diện cấu hình VLAN trên NGFW

Bước 1: Từ giao diện trình quản lý người dùng truy cập đến → Interface → LAN Interface → Chọn button "+" tại các LAN Interface.

Bước 2: Trong mục này người dùng có thể tạo các vùng mạng ảo trên các cổng LAN, chia LAN từ một miền mạng vùng VLAN 1 thành các vùng VLAN khác nhau:

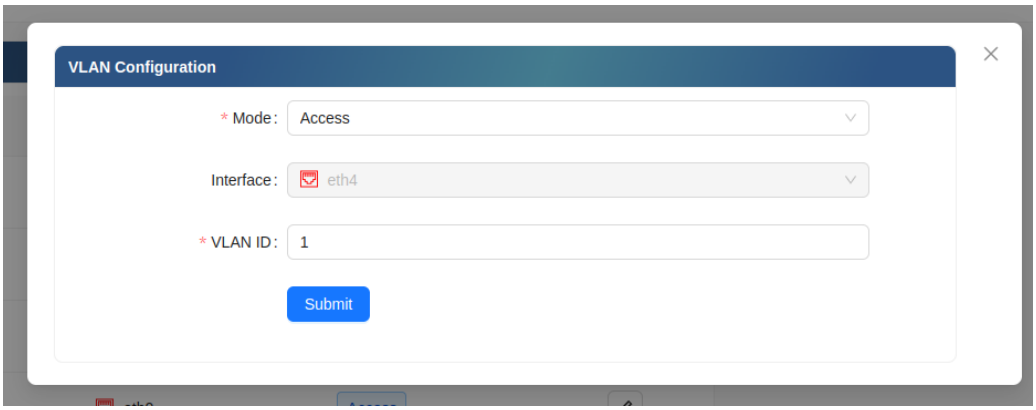


Hình 10: Giao diện quản lý LAN interface



Hình 11: Giao diện hiển thị thông tin VLAN

Bước 3: Nhấn button để chỉnh sửa VLAN ID.



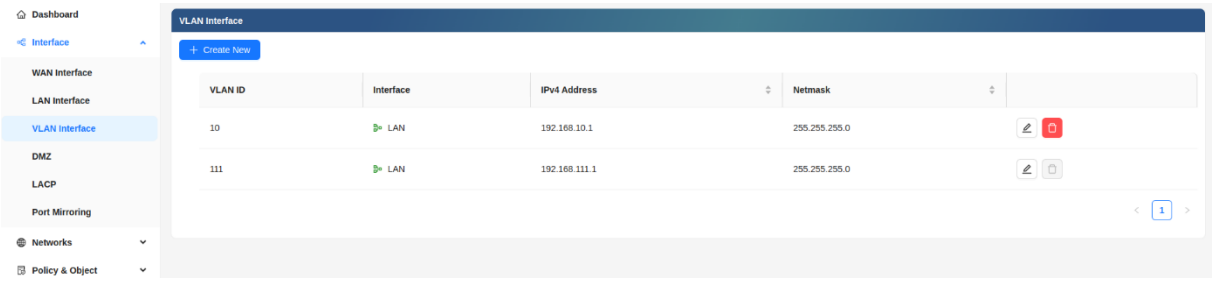
Hình 12: Giao diện cấu hình mạng VLAN

❖ Trong đó:

- **Mode**: Access/Trunk
- **VLAN ID**: Nhập giá trị VLAN

2.6 Giao diện cấu hình VLAN Interface trên NGFW

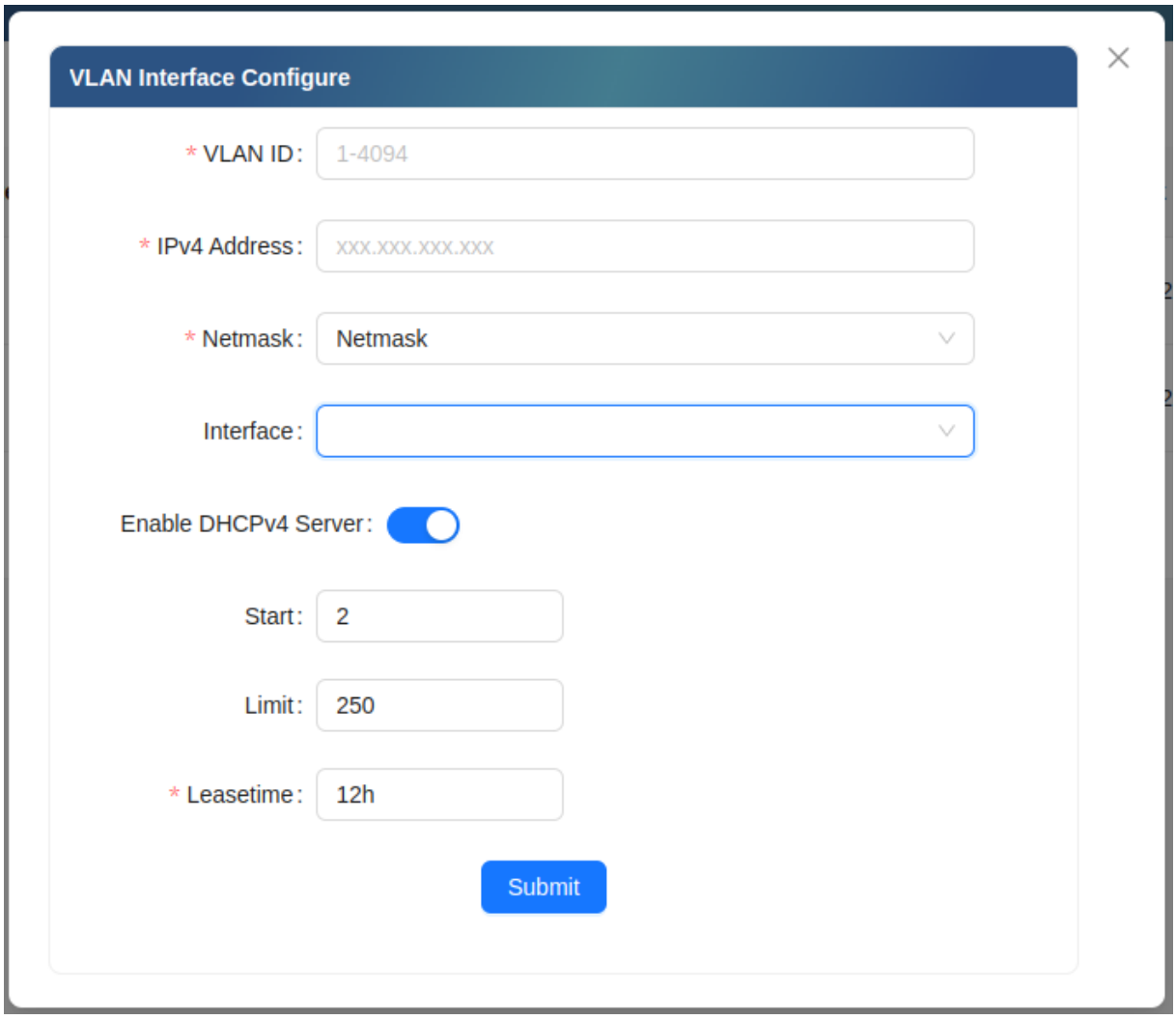
Từ giao diện trình quản lý người dùng truy cập đến → Interface → VLAN Interface:



Hình 13: Giao diện hiển thị thông tin VLAN Interface

2.6.1 Thêm VLAN Interface

Bước 1: Click chuột vào "Create New" trong VLAN Interface.



Hình 14: Giao diện cấu hình Vlan Interface

❖ Trong đó:

- **VLAN ID:** Hỗ trợ 1 – 4094 Vlan ID. Giá trị VLAN được gán cho từng cổng theo từng mode Access.
- **IP Address:** Địa chỉ IPv4.
- **Netmask:** Subnet Mask.
- **Interface:** Chọn cổng LAN.
- **Submit:** Lưu cấu hình.

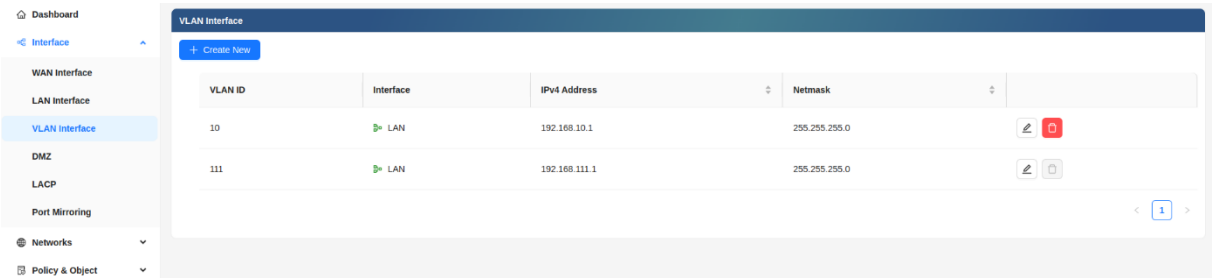
Bước 2: Thực hiện các thao tác khác:

❖ Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình VLAN Interface.

❖ Kích chuột vào  thực hiện tác vụ xóa thông tin VLAN Interface.

2.6.2 Cấu hình phạm vi cấp địa chỉ IP của Vlan Interface

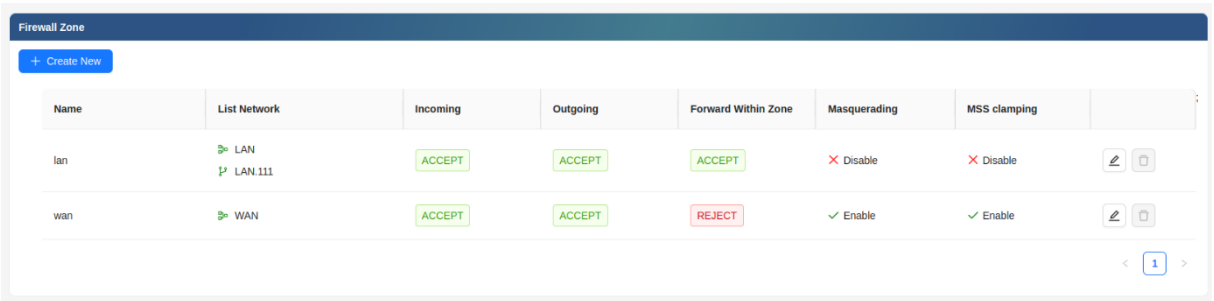
Bước 1: Chọn “Create New" trong phần VLAN Interface.



Hình 15: Giao diện cấu hình VLAN Interface

2.6.3 Thiết lập chính sách VLAN Interface

Bước 2: Add Firewall zone và config các chính sách policy ở Firewall Policy.



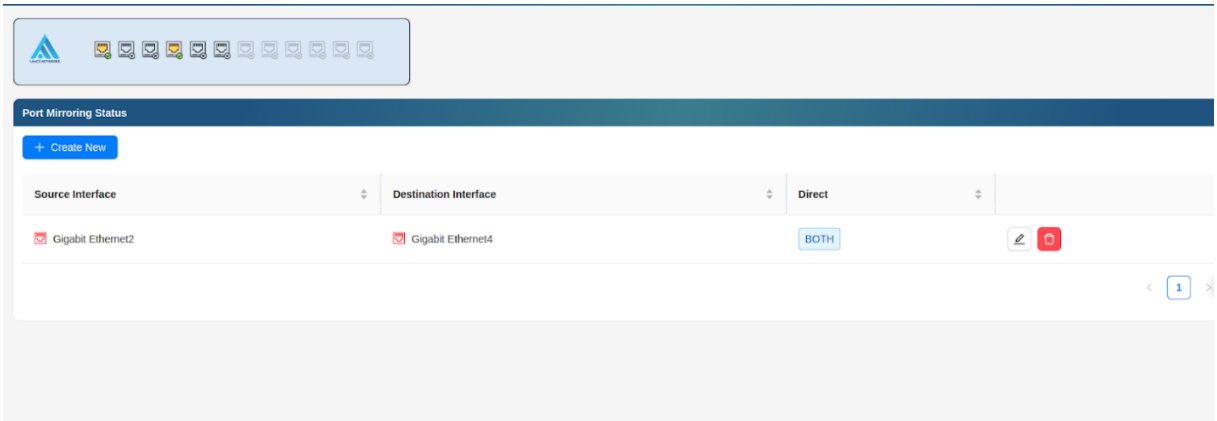
Hình 16: Giao diện cấu hình Vlan Policy

2.7 Cấu hình tính năng Port Mirroring trên NGFW

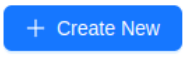
Giao diện hiển thị và cấu hình Port Mirroring:

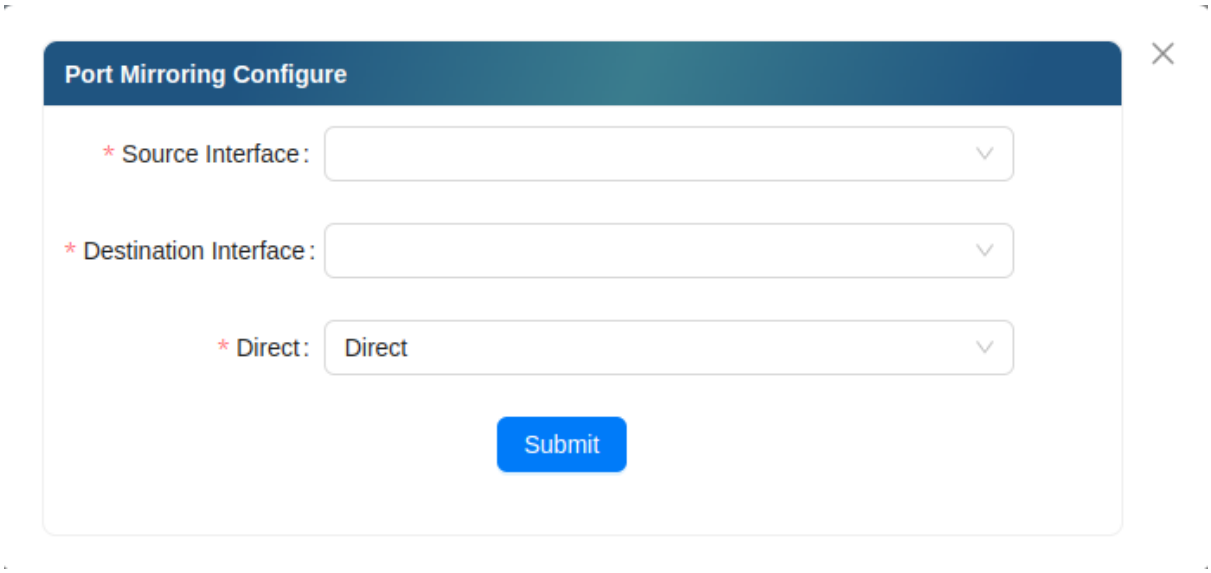
Bước 1: Từ giao diện quản lý → Interface → Port Mirroring.

❖ Trong mục này người dùng thực hiện cấu hình trên từng cổng, hỗ trợ 3 mode: TX (Chỉ truyền), RX (Chỉ nhận) và Both (Cả nhận và truyền):



Hình 17: Giao diện hiển thị thông tin cấu hình Port Mirroring

Bước 2: Click chuột vào  để thực hiện cấu hình Port Mirroring.



Hình 18: Giao diện cấu hình Port Mirroring

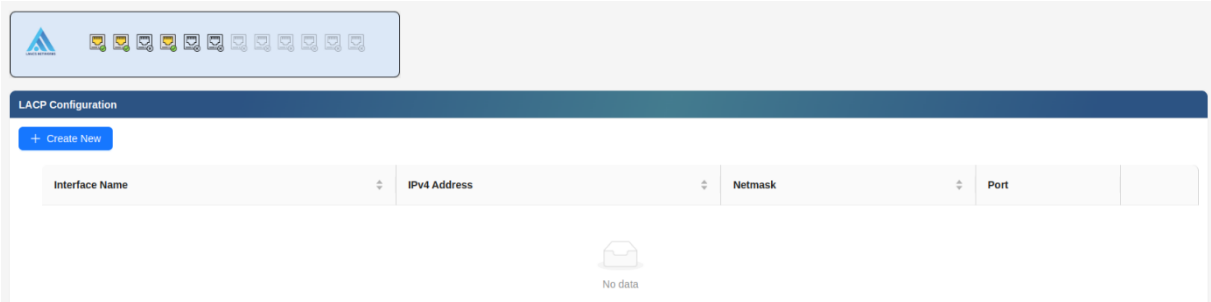
❖ Trong đó:

- **Source Interface:** Cổng nguồn để quản lý các cổng còn lại.
- **Destination Interface:** Lựa chọn cổng được quản lý bởi Source.
- **Direct:** Lựa chọn chế độ quản lý lưu lượng theo Tx, Rx hoặc cả 2 Both

Bước 3: Thực hiện các thao tác khác:

- ❖ Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình Port Mirroring.
- ❖ Kích chuột vào  thực hiện xóa cấu hình Port Mirroring.

2.8 Cấu hình tính năng liên kết link LACP trên NGFW

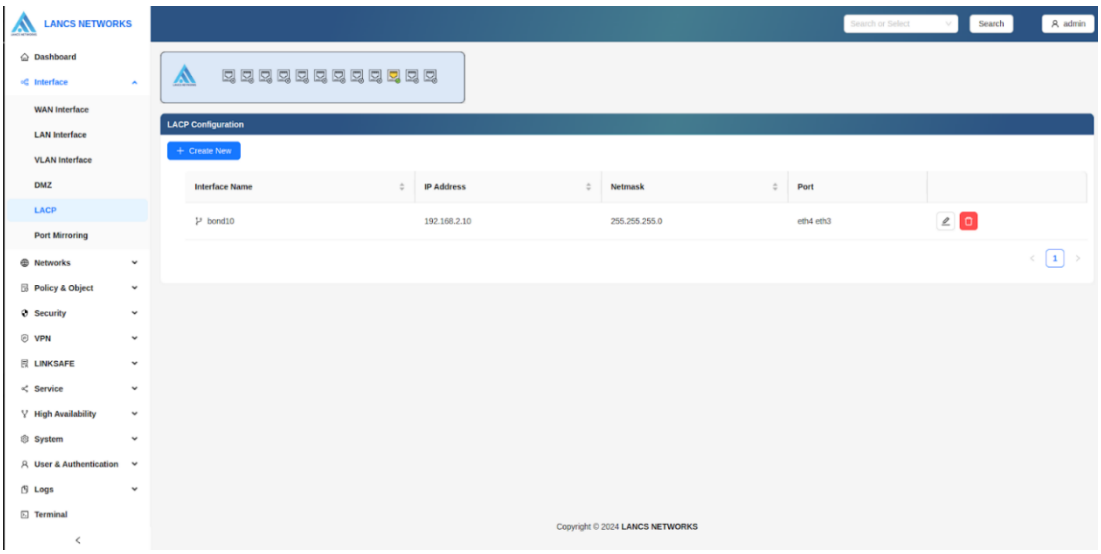


Hình 19: Giao diện cấu hình tính năng liên kết link LACP

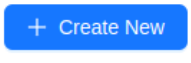
Giao diện cấu hình và hiển thị thông tin tính năng liên kết LACP:

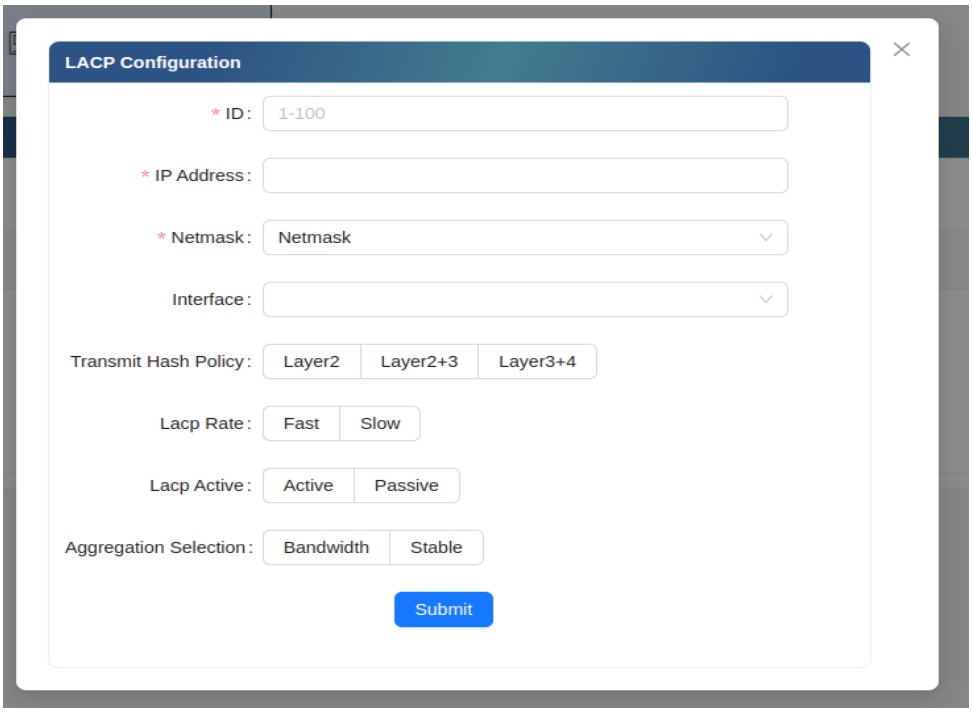
Bước 1: Từ giao diện quản lý → Interface → LACP.

- ❖ Trong mục này người dùng gồm nhiều cổng mạng lại với nhau nhằm tăng tốc độ đường truyền và nâng cao độ ổn định cho hệ thống:



Hình 20: Giao diện hiển thị thông tin LACP

Bước 2: Kích chuột vào  thực hiện thêm cấu hình cổng LACP:



Hình 21: Giao diện cấu hình LACP

❖ Trong đó:

- **ID**: Tạo Interface LACP với giá trị từ 0-9.
- **IP Address**: Đặt địa chỉ IP cho interface LACP.
- **Netmask**: Chọn mặt nạ mạng
- **Interface**: Lựa chọn các interface của trên thiết bị khi muốn gán vào cổng danh sách liên kết link.
- **Transmit Hash Policy**: Chọn chính sách phân phối
- **LACP Rate**: Tốc độ gửi các gói LACP.
- **LACP: Active**: Chế độ hoạt động LACP.
- **Aggregation Selection**: Chọn cách thức các cổng liên kết với nhau.
- **Submit**: *Lưu cấu hình.*

Bước 3: Thực hiện các thao tác khác:

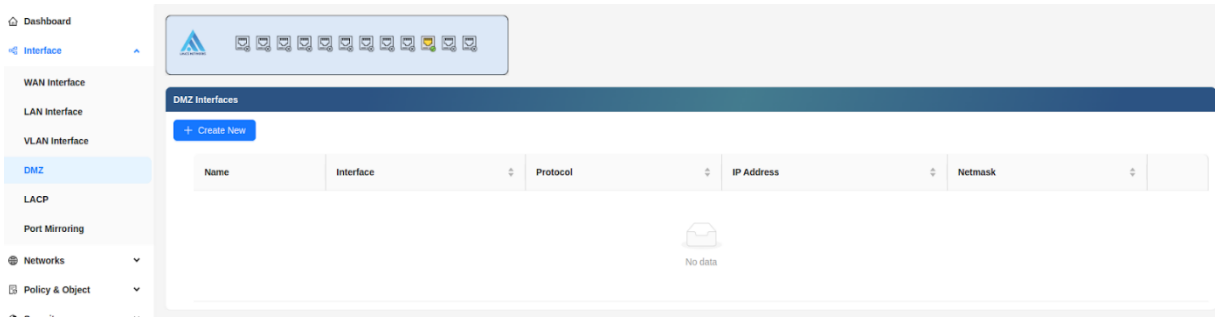
❖ Kích chuột vào thực hiện thao tác thay đổi thông tin cấu hình trong LAG.

❖ Kích chuột vào thực hiện thao tác xóa cấu hình LAG.

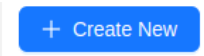
2.9 Cấu hình tính năng liên kết link DMZ trên NGFW

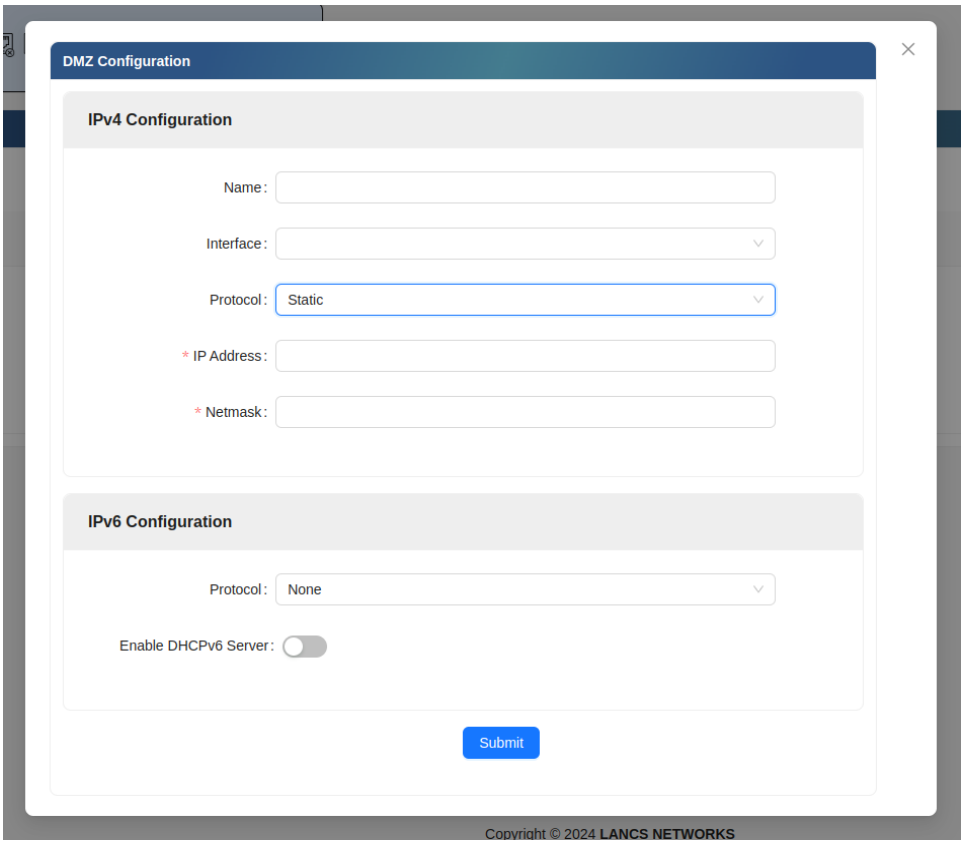
Giao diện hiển thị và cấu hình DMZ:

Bước 1: Từ giao diện quản lý → Interface → DMZ.



Hình 22: Giao diện hiển thị thông tin DMZ

Bước 2: Kích chuột vào  thực hiện thêm hoặc cấu hình cổng DMZ.



Hình 23: Giao diện cấu hình tính năng DMZ

- Trong đó:
  - **Name:** Tên DMZ.

- **Interface:** Chọn cổng mạng.
- **Protocol:** Chọn giao thức Static hoặc DHCP.
- **IP Address**: Nhập giá trị IP.
- **Netmask**: Nhập giá trị Netmask.
- **Submit**: Lưu cấu hình.

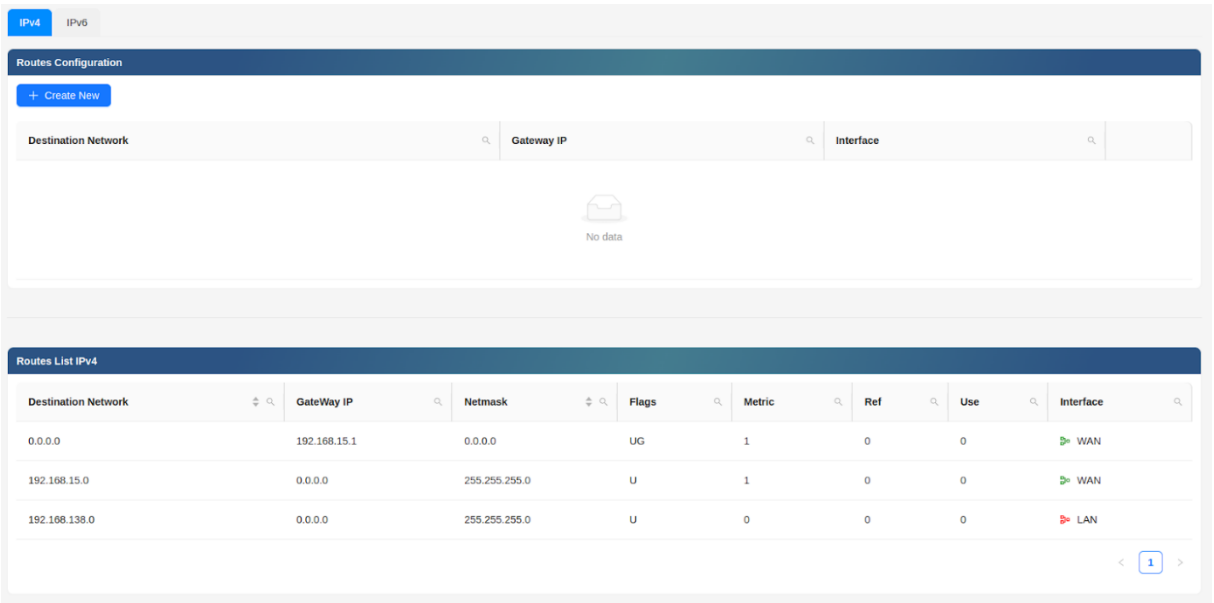
3 Cấu hình các tính năng mạng cơ bản (Network)

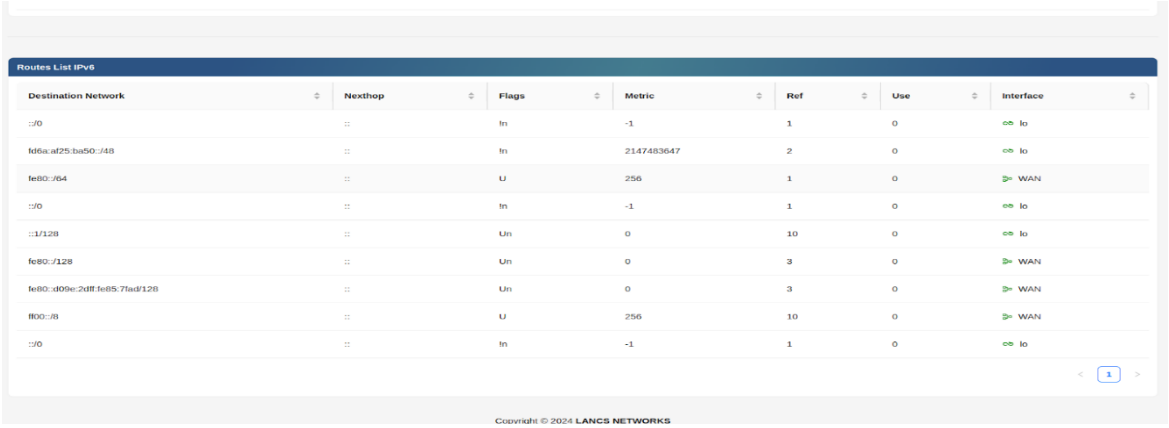
Đối với những giao thức định tuyến động (OSPF, BGP, RIP, IS-IS) cần phải cấu hình chính sách tường lửa tương ứng.

3.1 Cấu hình tính năng định tuyến tĩnh (Static) trên NGFW

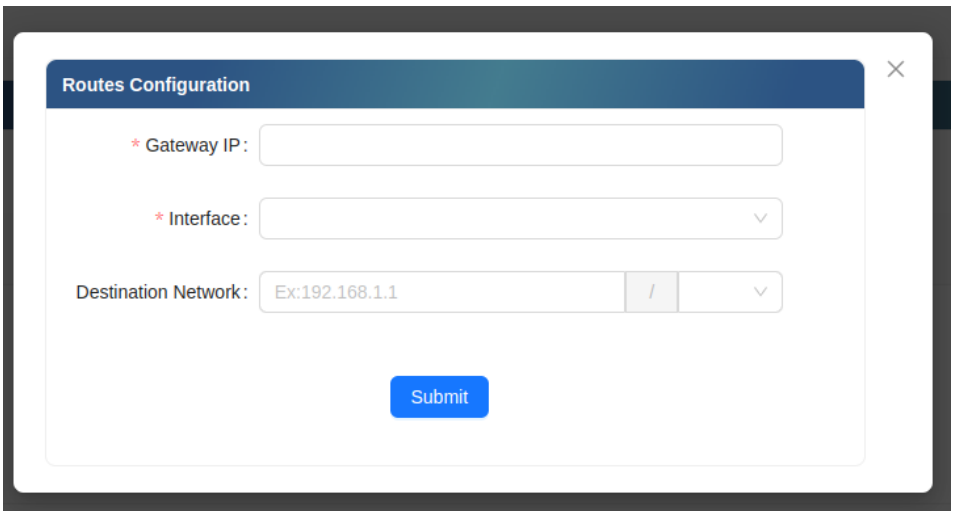
Giao diện hiển thị thông tin định tuyến tĩnh:

Bước 1: Từ giao diện quản lý Network → Static Routes → IPv4 hoặc IPv6: hiển thị thông tin các đường định tuyến mặc định và được cấu hình trên NGFW:





Hình 24: Giao diện hiển thị thông tin định tuyến tĩnh

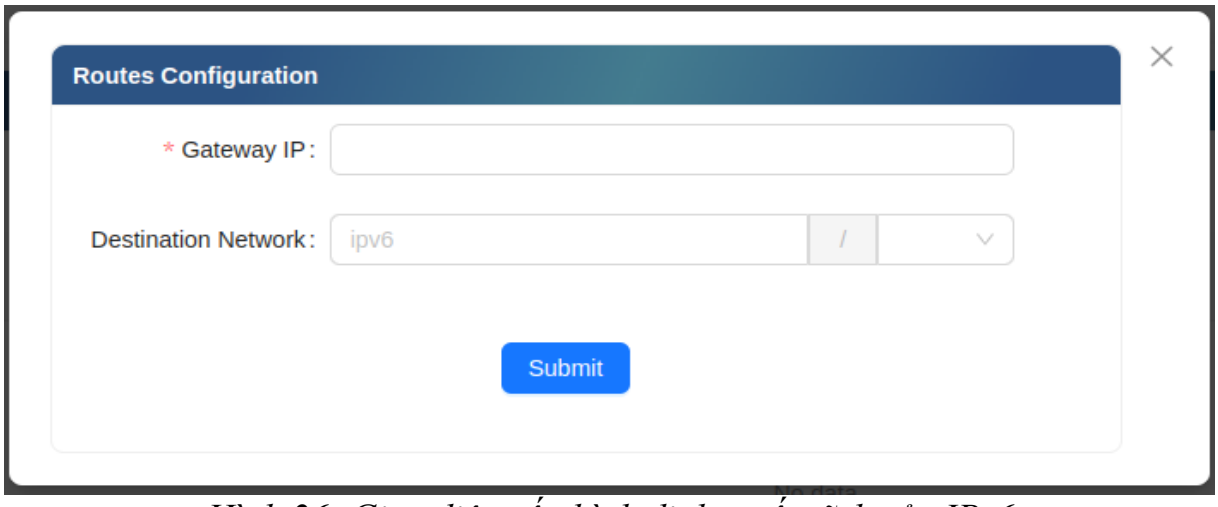


Hình 25: Giao diện cấu hình định tuyến tĩnh của IPv4

Bước 2: Kích chuột vào + Create New thực hiện cấu hình định tuyến tĩnh.

❖ Trong đó:

- **Interface (WAN / LAN):** Chọn Interface WAN.
- **Destination Network:** Miền mạng muốn thiết bị nhìn thấy thông qua IP Gateway (IP Gateway đã cấu hình ở trên).
- **Gateway:** IP cổng mà Interface WAN nhìn thấy.
- **Submit:** Lưu cấu hình.



Hình 26: Giao diện cấu hình định tuyến tĩnh của IPv6

Bước 3: Kích chuột vào + Create New thực hiện cấu hình định tuyến tĩnh.

❖ Trong đó:

- **Destination Network:** Miền mạng muốn thiết bị nhìn thấy thông qua IP Gateway (IP Gateway đã cấu hình ở trên).
- **Gateway:** IP cổng mà Interface WAN nhìn thấy.
- **Submit:** Lưu cấu hình.

3.2 Cấu hình tính năng định tuyến RIP trên NGFW

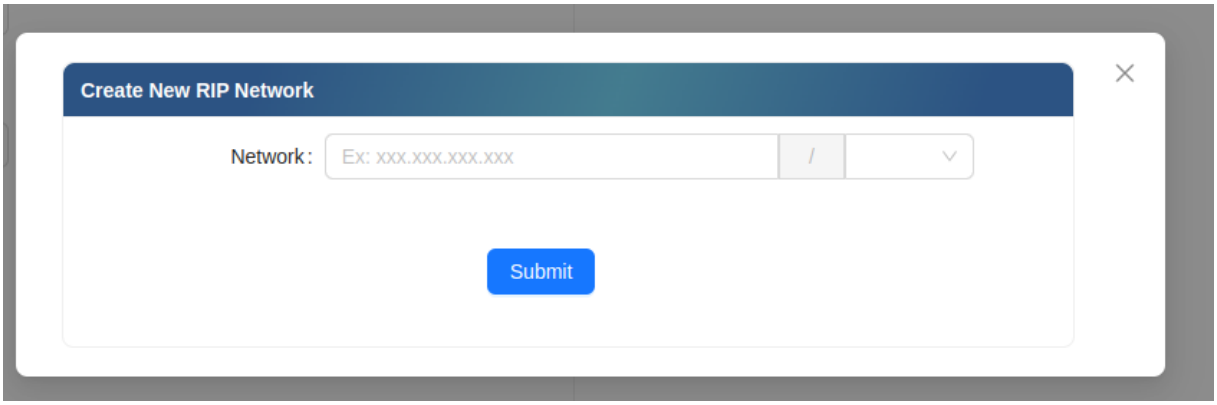
3.2.1 Giao diện hiển thị thông tin đường định tuyến động theo giao thức RIP

Bước 1: Giao diện hiển thị thông tin đường định tuyến động theo giao thức RIP: Từ giao diện quản lý =>Network => RIP => RIP.

Hình 27: Giao diện hiển thị thông tin đường định tuyến động theo giao thức RIP

- Trong đó:
  - **Redistribute (phân phối lại)**: phân phối lại thông tin định tuyến giữa các giao thức khác nhau. **Redistribution** cho phép router **chuyển thông tin định tuyến từ một giao thức này sang một giao thức khác** để đảm bảo khả năng kết nối giữa các mạng.
  - Để hiển thị cấu hình **Redistribute** => kích chuột vào + Redistribute . Sau khi hoàn thành cấu hình thì kích chuột vào Apply để lưu cấu hình

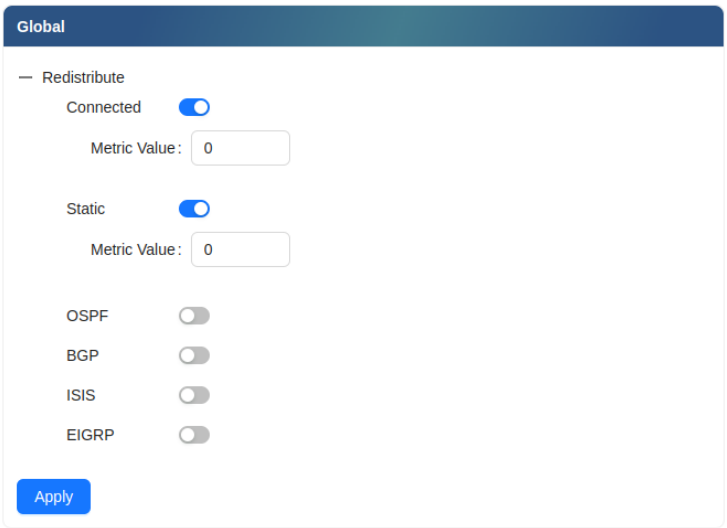
Bước 2: Kích chuột vào + Create New thực hiện cấu hình định tuyến động với giao thức RIP:



Hình 28: Giao diện cấu hình RIP

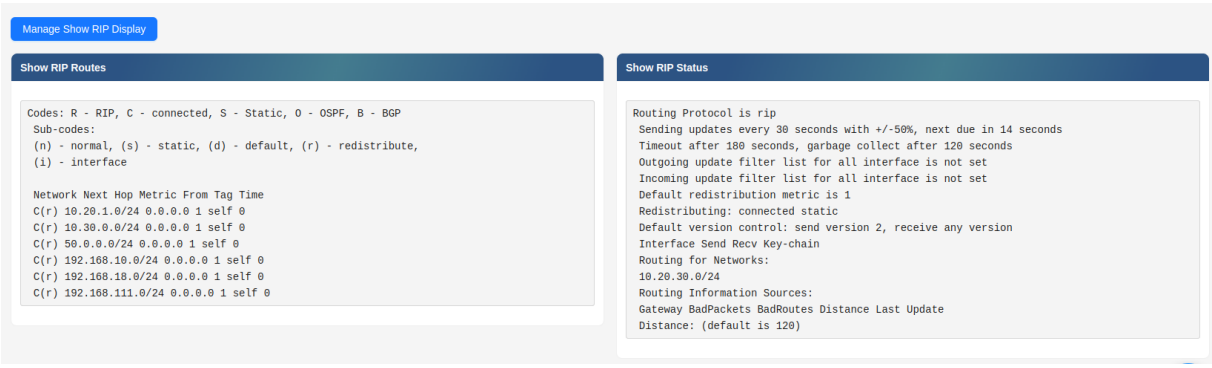
❖ Trong đó:

- **Network:** Quảng bá miền mạng trên thiết bị.
- **Submit:** Lưu cấu hình.



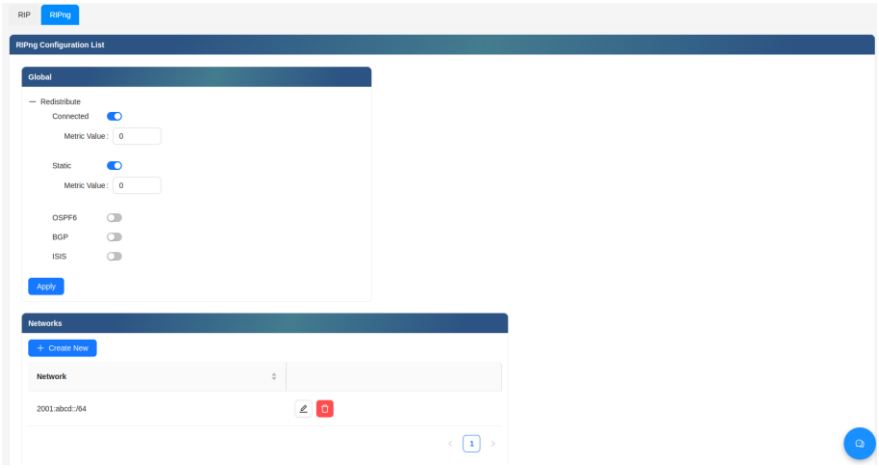
Hình 29: Giao diện hiển thị các tính năng nâng cao trong giao thức RIP

3.2.2 Giao diện hiển thị thông tin định tuyến RIP



Hình 30: Giao diện hiển thị thông tin định tuyến RIP

Bước 1: Tương tự với IPv6, người dung chọn mode IPv4/IPv6 trên RIP:



Hình 31: Giao diện hiển thị cấu hình IPv4/IPv6 trong định tuyến RIP

Bước 2: Thực hiện các thao tác khác:

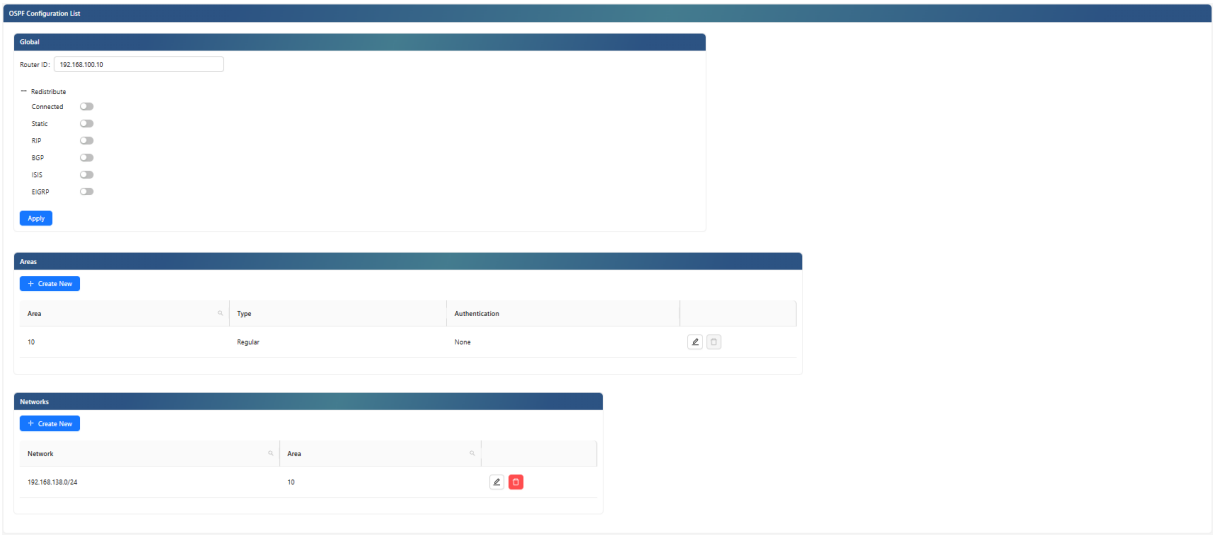
- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong định tuyến RIP.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình RIP.

3.3 Cấu hình tính năng định tuyến OSPF trên NGFW

3.3.1 Giao thức OSPFv4

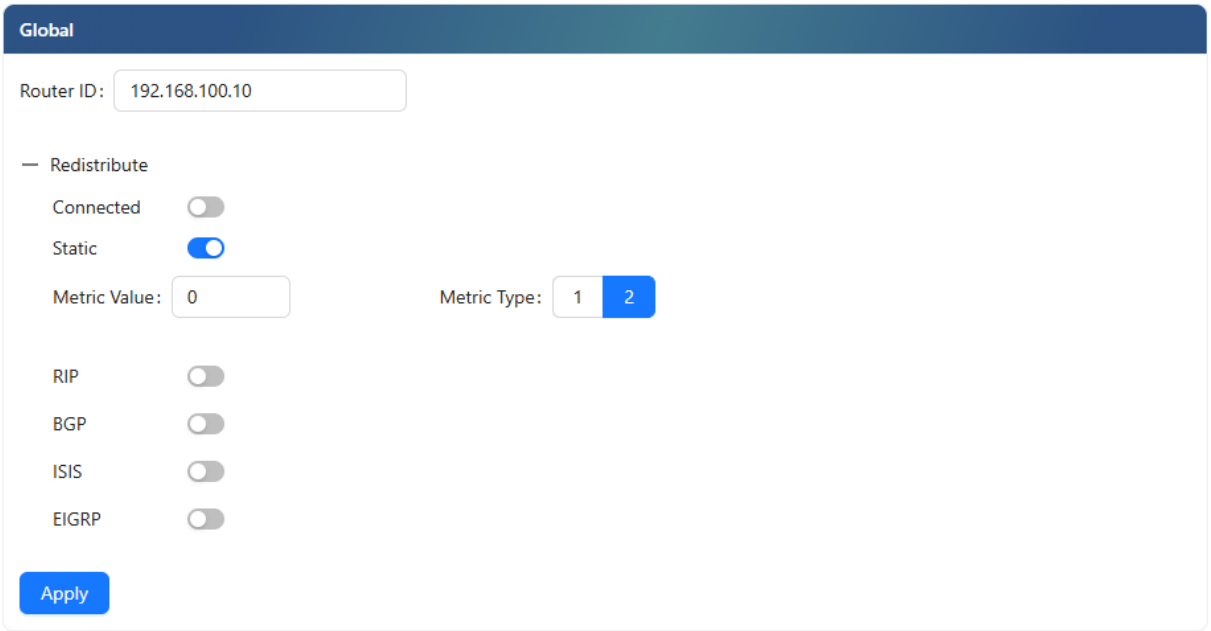
3.3.1.1 Cấu hình

Bước 1: Từ giao diện quản lý → Network → OSPF → OSPFv4: Người dùng thực hiện các tác vụ thêm/sửa/xóa các đường định tuyến động.

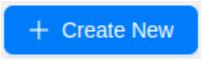


Hình 32: Giao diện hiển thị thông tin cấu hình OSPFv4

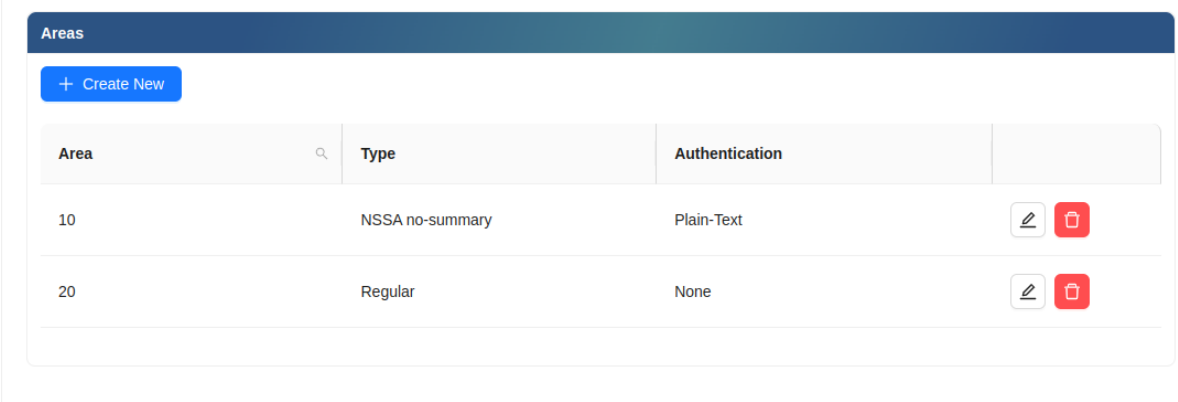
Bước 2: Thực hiện cấu hình Router ID bằng cách nhập ID vào ô tương ứng; **:** Thực hiện cấu hình redistribute bằng cách kích chuột vào + Redistribute để hiển thị giao diện cấu hình. Kích chuột vào biểu tượng switch (nghĩa là đang tắt; nghĩa là đã bật) để bật redistribute tương ứng; Cuối cùng kích chuột vào Apply để áp dụng cấu hình



Hình 33: Giao diện cấu hình Router ID và redistribute

Bước 3: Kích chuột vào 

trong bảng Areas để thực hiện tạo một cấu hình area mới:



Hình 34: Giao diện hiển thị cấu hình areas

Hình 35: Giao diện cấu hình area

❖ Trong đó:

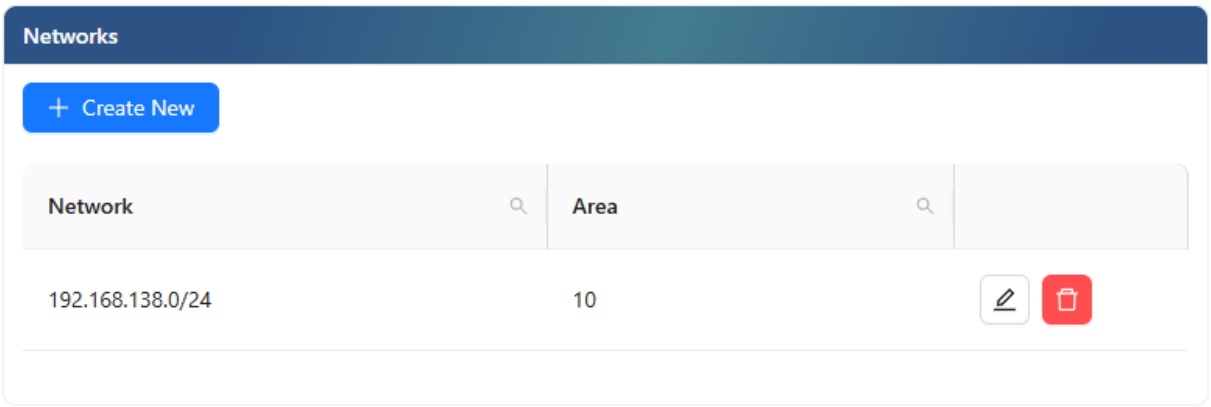
- **Area:** Chỉ định area cụ thể cho mỗi cấu hình.
- **Type:** Cài đặt loại cho mỗi area.

- **Regular** (mặc định): Lưu giữ tất cả thông tin định tuyến, bao gồm LSA (Link-State Advertisement) loại 1 đến loại 5.
- **NSSA:** Cho phép một số routes từ bên ngoài OSPF được đưa vào (External LSA loại 7); Sử dụng LSA loại 7 trong NSSA, được chuyển đổi thành LSA loại 5 khi ra khỏi NSSA.
- **Stub:** Không cho phép LSA loại 4 và loại 5 (external routes); Sử dụng một default route (0.0.0.0) để thay thế cho các external routes.

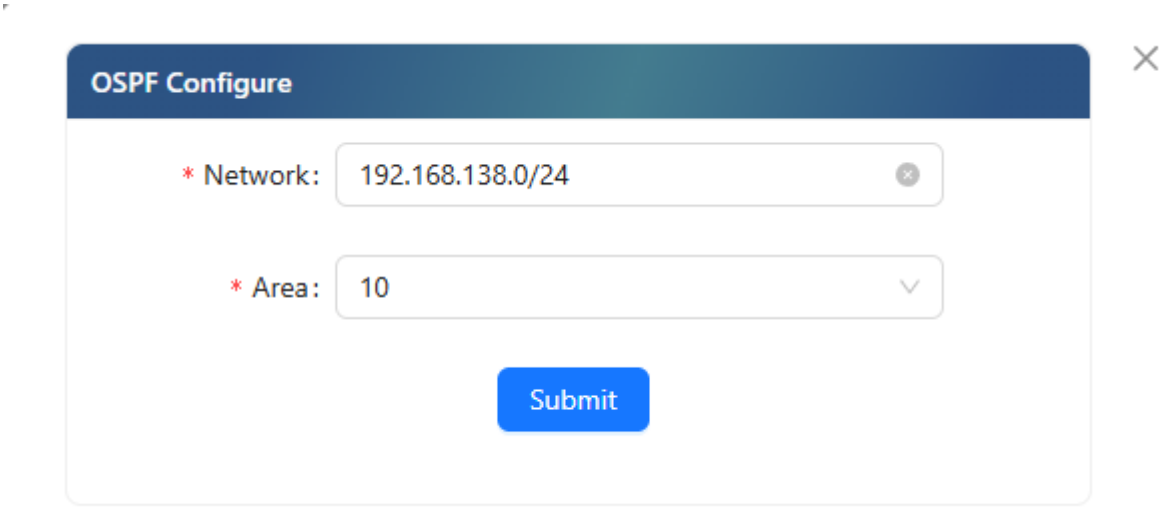
- **Authentication:** Cài đặt loại xác thực (OSPF hỗ trợ xác thực để đảm bảo rằng chỉ các router đáng tin cậy mới có thể tham gia và trao đổi thông tin định tuyến)
  - **None** (mặc định): Không sử dụng xác thực.
  - **Plain-Text**: Sử dụng mật khẩu dạng văn bản thuần túy (Ít an toàn do mật khẩu được gửi không mã hóa)
  - **Message-Digest**: Sử dụng thuật toán băm MD5 để bảo vệ mật khẩu

❖ Sau khi cài đặt xong, kích chuột vào Submit để tiến hành lưu cấu hình

Bước 4: Kích chuột vào + Create New trong bảng Networks để tạo một cấu hình mới cho quảng bá miền mạng:



Hình 36: Giao diện hiển thị các cấu hình network



Hình 37: Giao diện cấu hình cho network

- Trong đó:
  - **Network**: miền mạng muốn quảng bá
  - **Area**: vùng mà miền mạng tham gia
- Sau khi cài đặt xong, kích chuột vào Submit để tiến hành lưu cấu hình

3.3.1.2 Sửa, xóa cấu hình

- Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình.
- Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình.

3.3.1.3 Giao diện hiển thị thông tin định tuyến OSPF trên NGFW

Hình 38: Giao diện hiển thị thông tin định tuyến OSPFv4

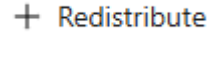
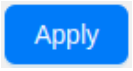
- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong định tuyến OSPF.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình OSPF.

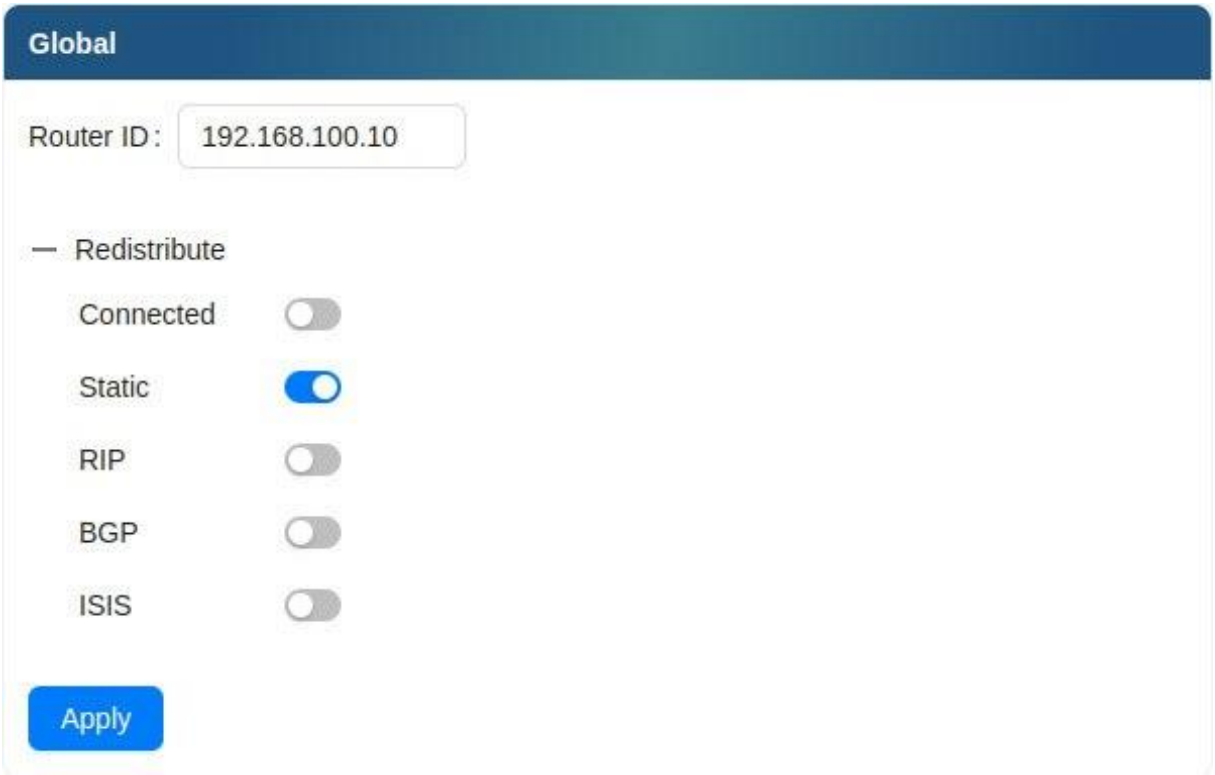
3.3.2 Giao thức OSPFv6

3.3.2.1 Cấu hình

Bước 1: Từ giao diện quản lý → Network → OSPF → OSPFv6: Người dùng thực hiện các tác vụ thêm/sửa/xóa các đường định tuyến động.

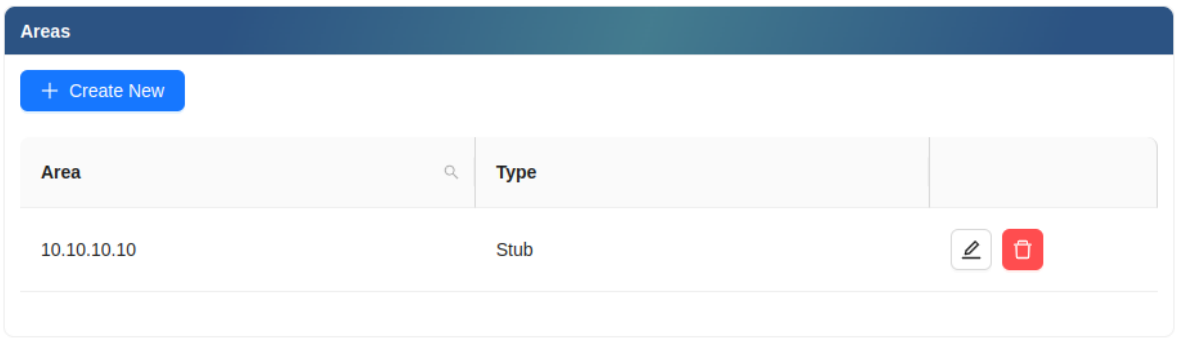
Hình 39: Giao diện hiển thị thông tin cấu hình OSPFv6

Bước 2: Thực hiện cấu hình Router ID bằng cách nhập ID vào ô tương ứng; **:** Thực hiện cấu hình redistribute bằng cách kích chuột vào  để hiển thị giao diện cấu hình. Kích chuột vào biểu tượng switch ( nghĩa là đang tắt;  nghĩa là đã bật) để bật redistribute tương ứng; Cuối cùng kích chuột vào  để áp dụng cấu hình

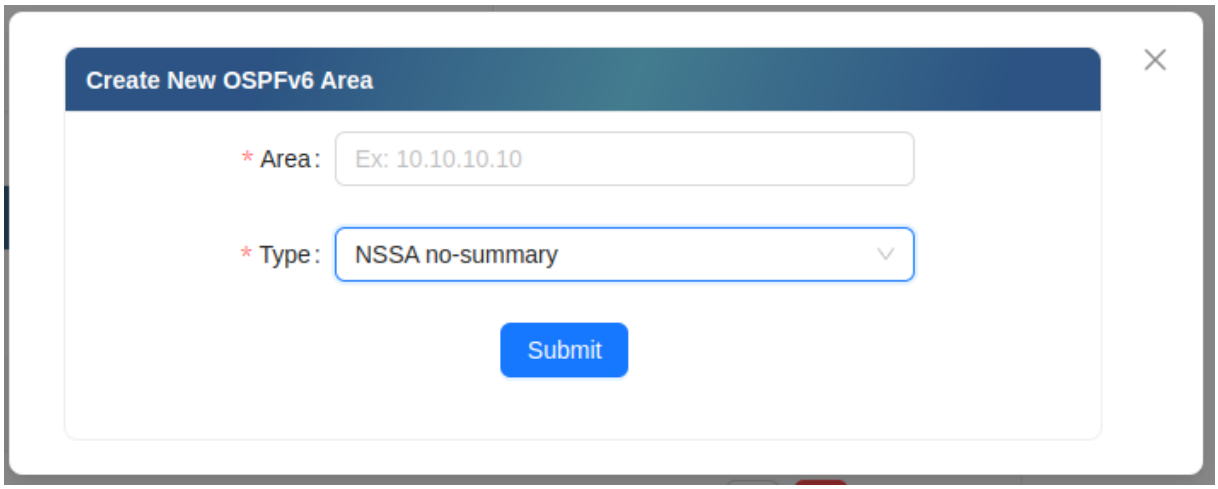


Hình 40: Giao diện cấu hình Router ID và redistribute

Bước 3: Kích chuột vào + Create New trong bảng Areas để thực hiện tạo một cấu hình area mới:



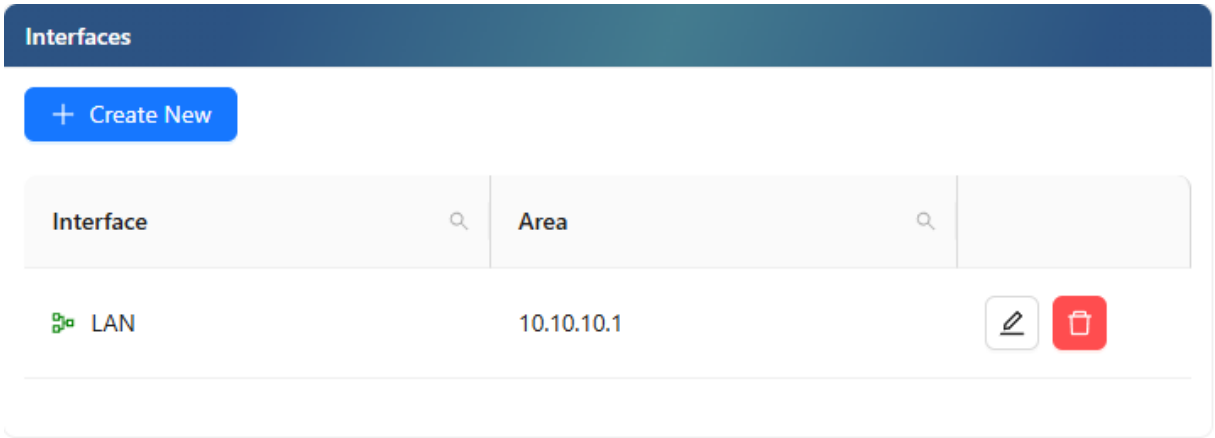
Hình 41:Giao diện hiển thị thông tin các cấu hình area



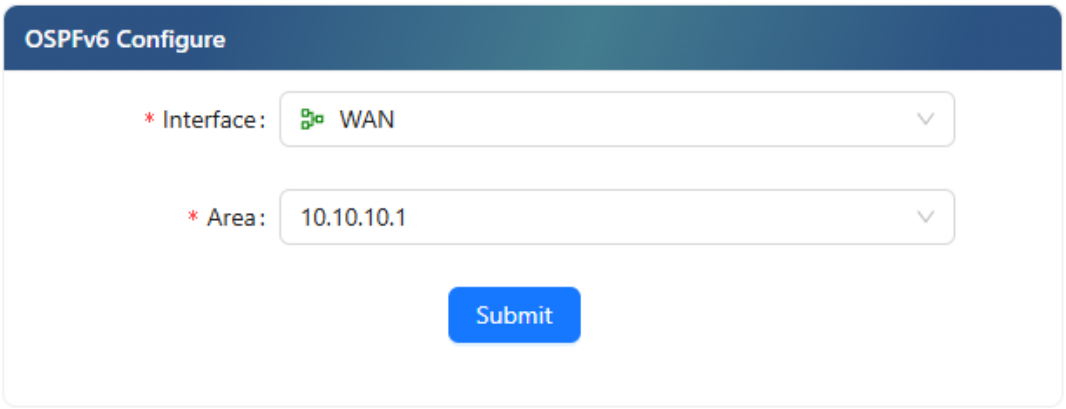
Hình 42: Giao diện cấu hình area

- Trong đó:
  - **Area**: Chỉ định một area cụ thể
  - **Range**: Cấu hình range cho area
- Sau khi cài đặt xong, kích chuột vào Submit để tiến hành lưu cấu hình

Bước 4: Kích chuột vào + Create New trong bảng Interfaces để thực hiện tạo một cấu hình mới:



Hình 43:Giao diện hiển thị thông tin các cấu hình OSPFv6 cho mỗi interface



Hình 44:Giao diện cấu hình OSPFv6 cho một interface

- Trong đó:
  - **Interface**: Lựa chọn giao diện để kích hoạt OSPFv6
  - **Area**: vùng mà interrface tham gia
- Sau khi cài đặt xong, kích chuột vào Submit để tiến hành lưu cấu hình

3.3.2.2 Sửa, xóa cấu hình

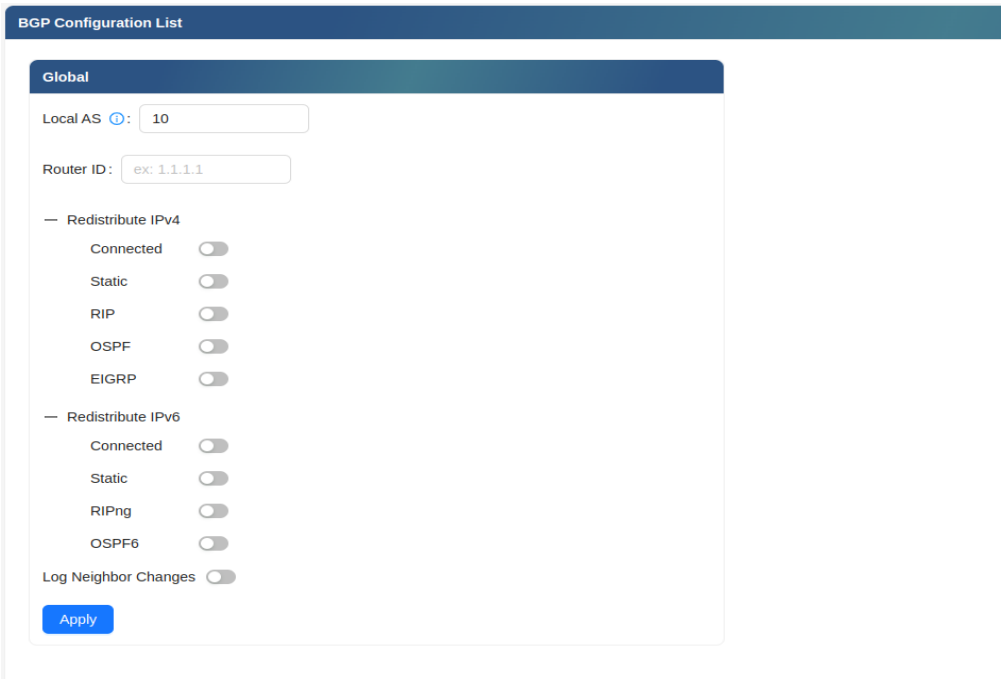
- Giống như OSPFv4

3.4 Cấu hình tính năng định tuyến BGP trên NGFW

Giao diện hiển thị thông tin đường định tuyến động theo giao thức BGP:

Bước 1: Từ giao diện quản lý → Network → BGP Config: Người dùng thực hiện các tác vụ thêm/sửa/xóa các đường định tuyến động.

Bước 2: Kích chuột vào Create thực hiện cấu hình giá trị vùng cho định tuyến BGP:



Hình 45: Giao diện cấu hình giá trị Router ID (Vùng định tuyến BGP)

Trong đó:

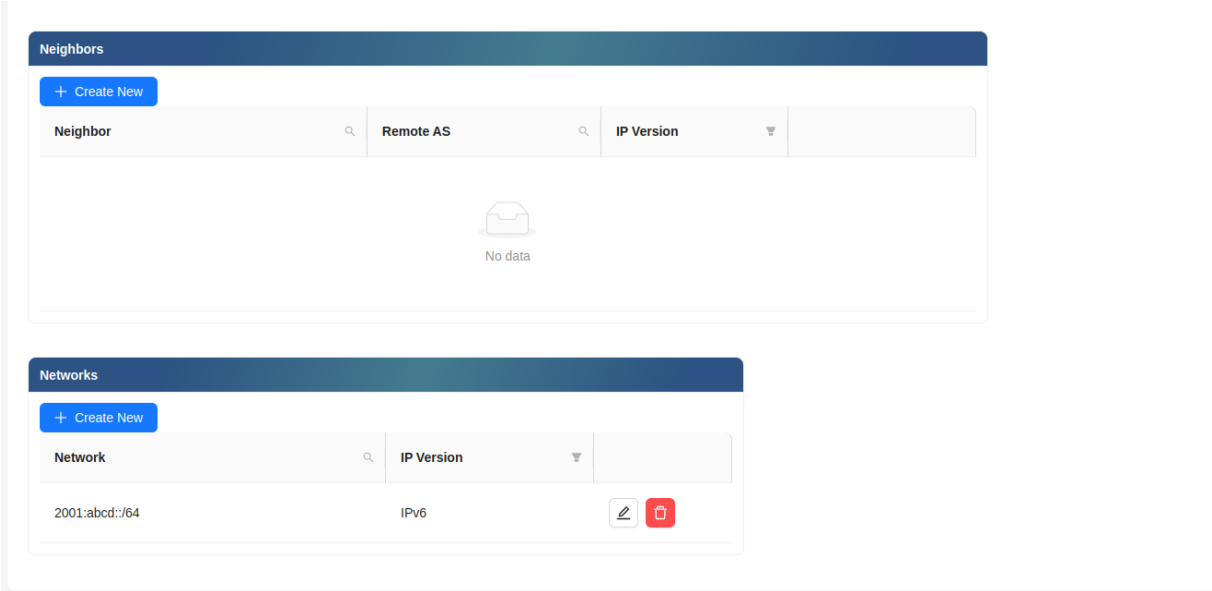
+ **Local AS:** Xác định AS Number (ASN) cục bộ mà router sử dụng khi tham gia BGP. Nếu trường này bỏ trống có nghĩa giao thức BGP sẽ không hoạt động. Nếu muốn thay đổi Local AS thì sẽ phải cấu hình lại từ đầu.

+ **Router ID**: Xác định Router ID duy nhất trong hệ thống BGP. Nếu không thiết lập thì router sẽ tự động chọn theo địa chỉ cao nhất trong các interface

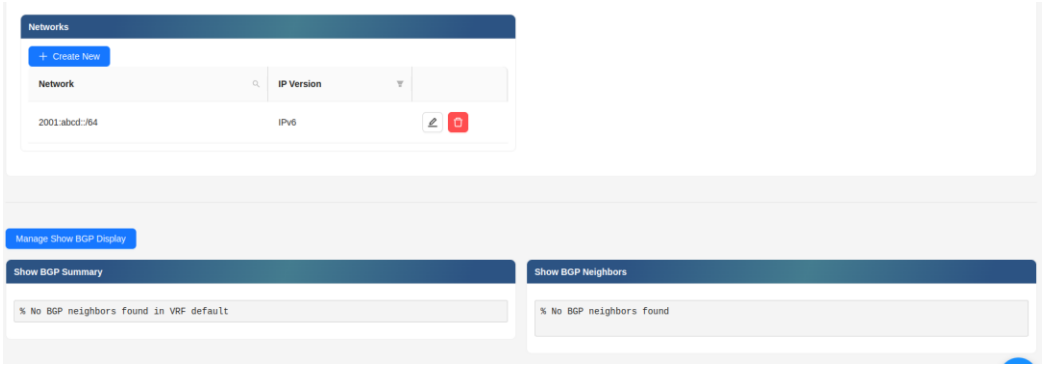
+ **Redistribute**: Chuyển đổi các tuyến từ một giao thức định tuyến khác (OSPF, EIGRP, RIP, Static) vào BGP. BGP có thể quản lý chung cho IPv4 và IPv6

+ **Log Neighbor changes:** Ghi lại sự thay đổi trạng thái của BGP Neighbors vào log hệ thống.

- Sau khi cấu hình xong thì nhấn **Apply** để lưu cấu hình. **Chú ý:** Khi thay đổi Local AS thì sẽ xóa hết tất cả cấu hình BGP hiện tại và phải thiết lập lại từ đầu.



Hình 46: Giao diện thông tin vùng định tuyến trên NGFW theo định tuyến BGP



Hình 47: Giao diện hiển thị thông tin định tuyến BGP

Bước 3: Kích chuột vào Create thực hiện cấu hình định tuyến động với giao thức BGP.

Hình 48: Giao diện cấu hình BGP

Trong đó:

+ **IP Version:** Chọn phiên bản IP mà BGP sẽ sử dụng để thiết lập kết nối với neighbor.

- IPv4: Neighbor sử dụng địa chỉ IPv4
- IPv6: Neighbor sử dụng địa chỉ IPv6

+ **Neighbor**: Địa chỉ IP của BGP Neighbor mà router sẽ thiết lập kết nối. Giá trị hợp lệ là IPv4 hoặc IPv6 tùy theo lựa chọn ở IP Version.

+ **Remote AS:** Xác định AS Number của neighbor BGP. Giá trị hợp lệ là số nguyên từ 1 - 4,294,967,295

- IBGP (Internal BGP) -> remote-as phải trùng với local AS.

+ EBGP (External BGP) -> remote-as phải khác local AS.

+ Activate IPv4 / Activate IPv6: Kích hoạt hoặc vô hiệu hóa giao tiếp BGP trên IPv4/IPv6. Nếu **Activate IPv4** được bật, neighbor sẽ được kích hoạt trên “address-family ipv4”. Nếu **Activate IPv6** được bật, neighbor sẽ hoạt động trên “address-family ipv6”. Nếu **chỉ có IPv4 hoặc IPv6 được kích hoạt**, neighbor sẽ không trao đổi tuyến của phiên bản IP còn lại

Hình 49: Giao diện hiển thị thông tin BGP

- Trong đó:
  - **IP Version:** Chọn phiên bản IP của mạng sẽ được quảng bá trong BGP.
    - IPv4: Chỉ định mạng IPv4 để quảng bá trong BGP.
    - IPv6: Chỉ định mạng IPv6 để quảng bá trong BGP.
  - **Network**: Xác định mạng (prefix) mà router sẽ quảng bá qua BGP.

Bước 3: Thực hiện các thao tác khác:

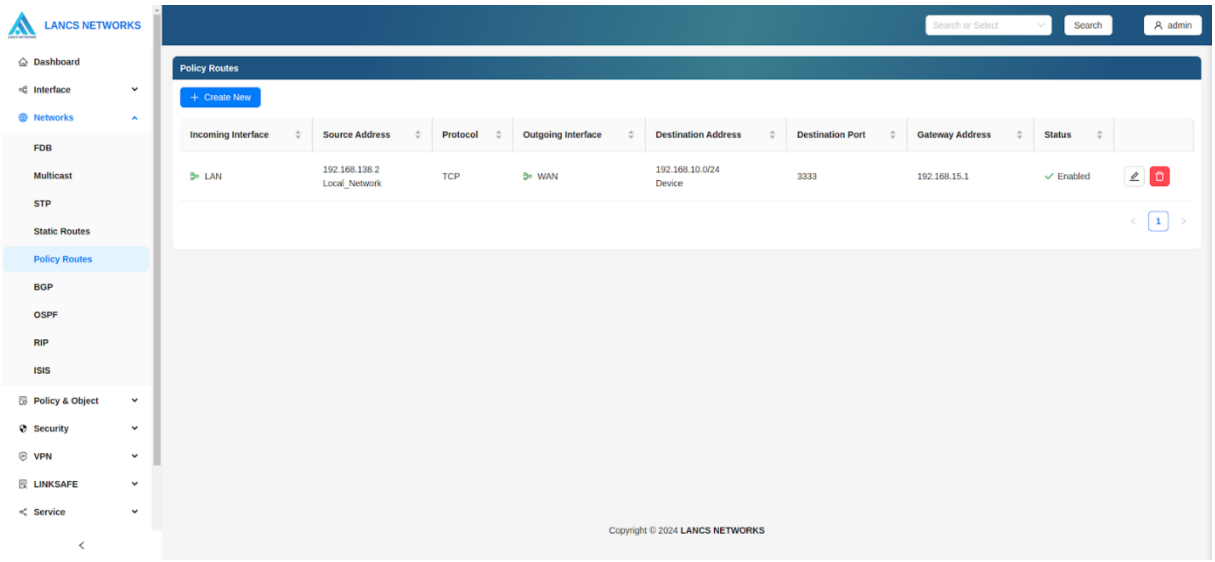
- Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong định tuyến BGP.
- Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình BGP.

3.5 Cấu hình tính năng định tuyến IS-IS trên NGFW

Tính năng update sau

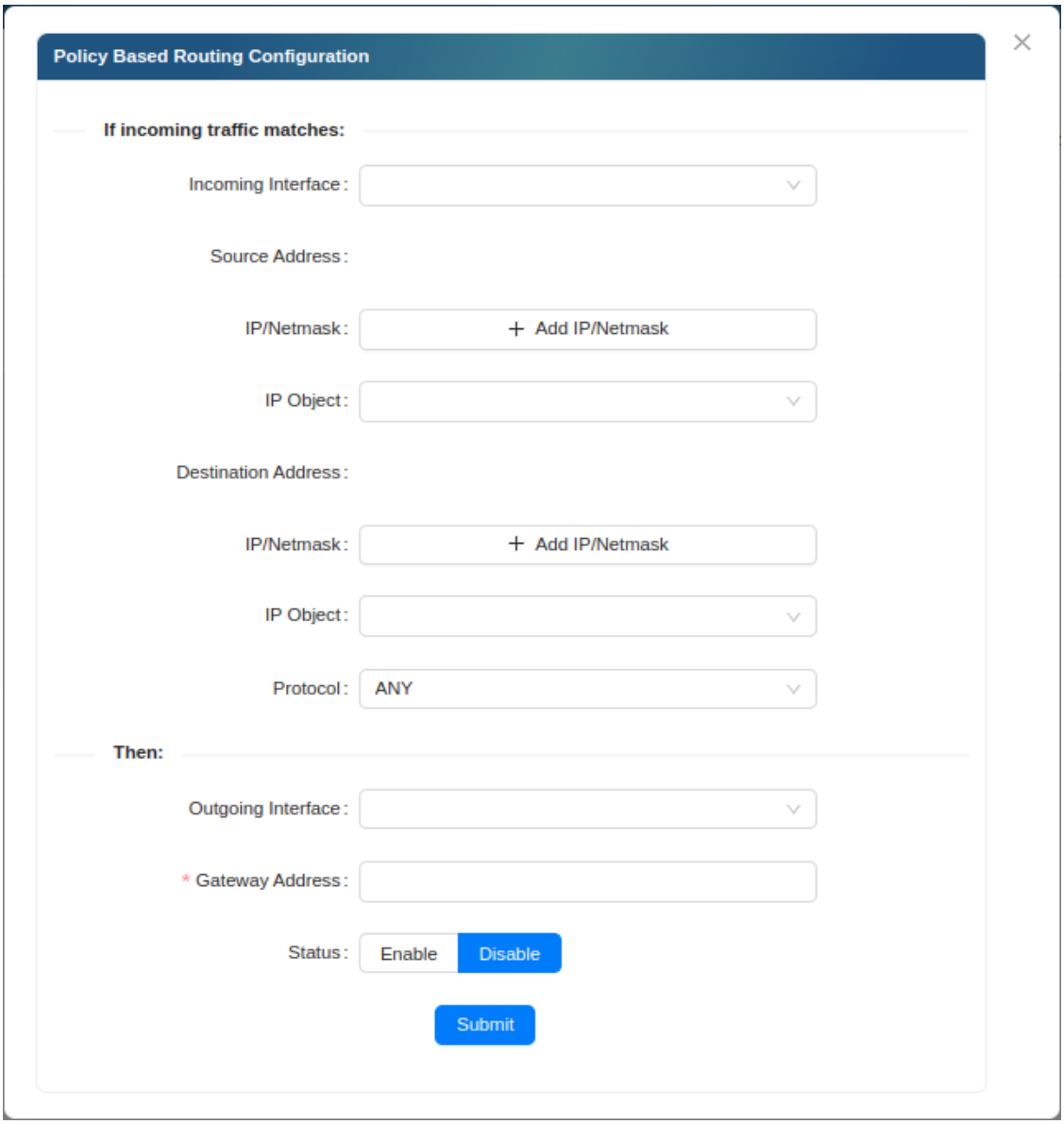
3.6 Tính năng Policy Based Routing

Giao diện chính của tính năng Policy Based Routing:



Hình 50: Giao diện chính tính năng Policy Based Routing

❖ Kích chuột vào + Create New để thực hiện tạo mới một cấu hình:



Hình 51: Giao diện cấu hình Policy Based Routing

❖ Trong đó:

- **Incoming Interface:** Chính sách sẽ khớp với các gói dữ liệu đi vào NGFW từ giao diện mạng này
- **Source Address:** Chính sách sẽ khớp với các gói dữ liệu có địa chỉ nguồn khớp với địa chỉ được cài đặt.
  - ***IP/Netmask:*** Sử dụng dạng địa chỉ IP (x.x.x.x) hoặc IP/mask (x.x.x.x/x)

- ***IP Object:*** Sử dụng các address hoặc address group được thiết lập sẵn ở nhóm tính năng Policy&Object (xem ở mục 2.4.3 - chỉ áp dụng cho IPv4)

- **Destination Address:** Chính sách sẽ khớp với các gói dữ liệu có địa chỉ nguồn khớp với địa chỉ được cài đặt. (các lựa chọn giống với Source Addres)
- **Protocol:** Chính sách sẽ khớp với các gói dữ liệu có giao thức khớp giao thức được cài đặt.
  - ***TCP/UDP/SCTP:*** là những giao thức cần cấu hình thêm port.
  - ***Specify:*** sử dụng protocol number theo chuẩn IANA.
  - ***any:*** khớp với tất cả giao thức.
- **Outgoing Interface:** Chính sách sẽ phân phối các gói dữ liệu khớp với các cài đặt ở phía trên đi ra ngoài NGFW từ giao diện mạng này.
- **Gateway Address:** Cài đặt gateway cho gói dữ liệu đầu ra.
- **Status:** Cài đặt trạng thái cho chính sách.

❖ Sau khi cài đặt xong thì kích chuột vào Submit để lưu cấu hình.

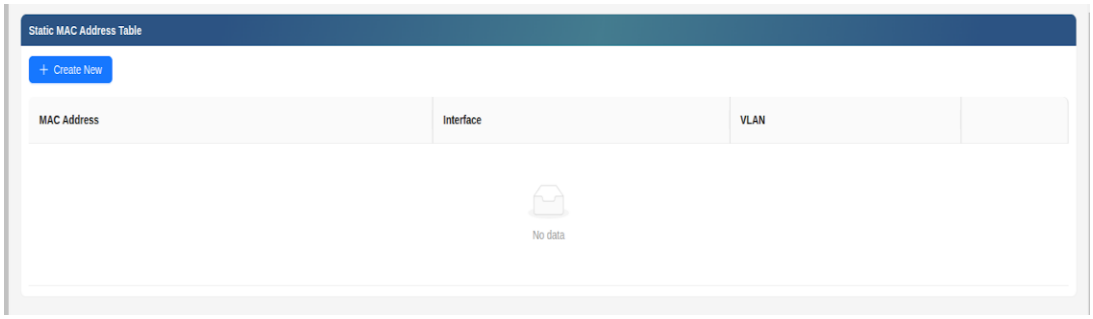
❖ Kích chuột vào để thực hiện chỉnh sửa cấu hình.

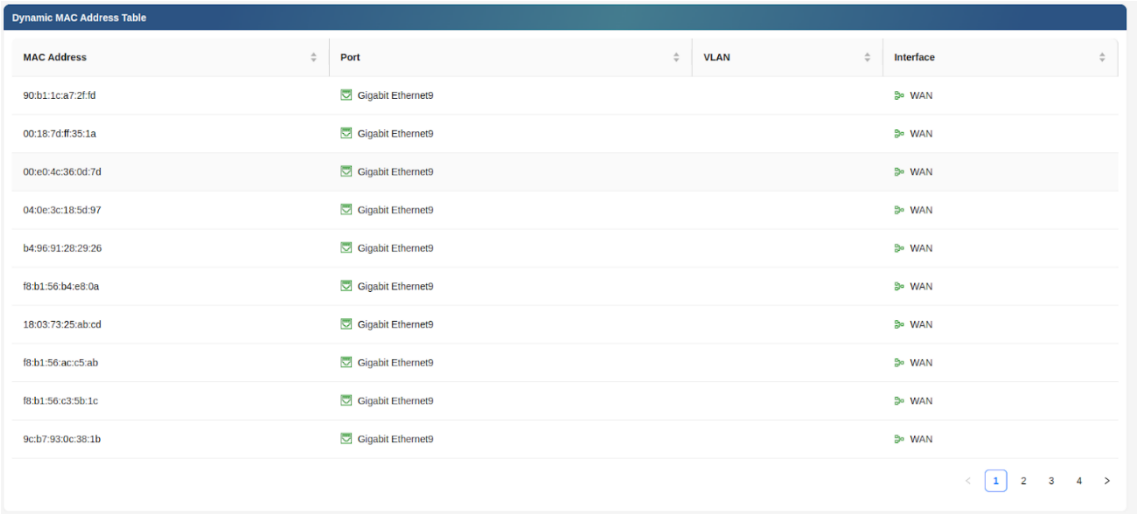
❖ Kích chuột vào để thực hiện xóa cấu hình.

3.7 Tính năng FDB

Giao diện hiển thị MAC Table:

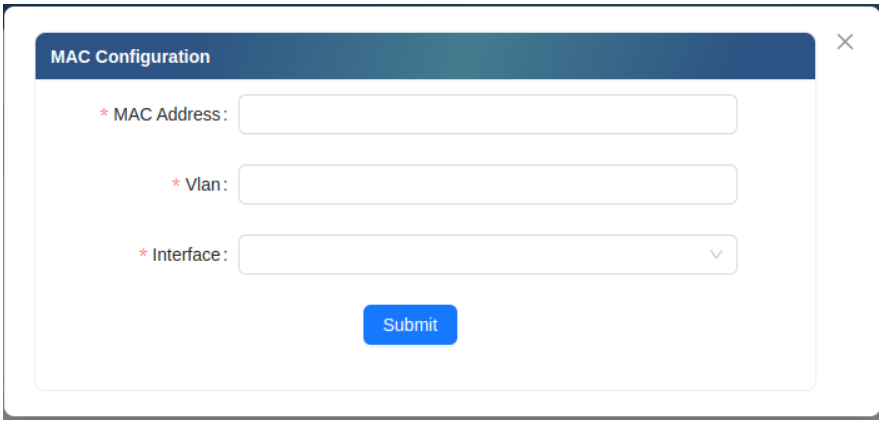
❖ Gồm config Static MAC Address Table và Dynamic MAC Address Table.





Hình 52: Bảng tính năng MAC động và tĩnh

❖ Click vào + Create New để tạo cấu hình MAC tĩnh.



Hình 53: Giao diện cấu hình tính năng MAC

❖ Trong đó:

- **MAC Address:** nhập địa chỉ MAC tĩnh vào
- **VLAN:** Nhập VLAN ID
- **Interface:** chọn cổng để add MAC
- **Submit:** Lưu cấu hình.

❖ Người dùng có thể click để sửa cấu hình.

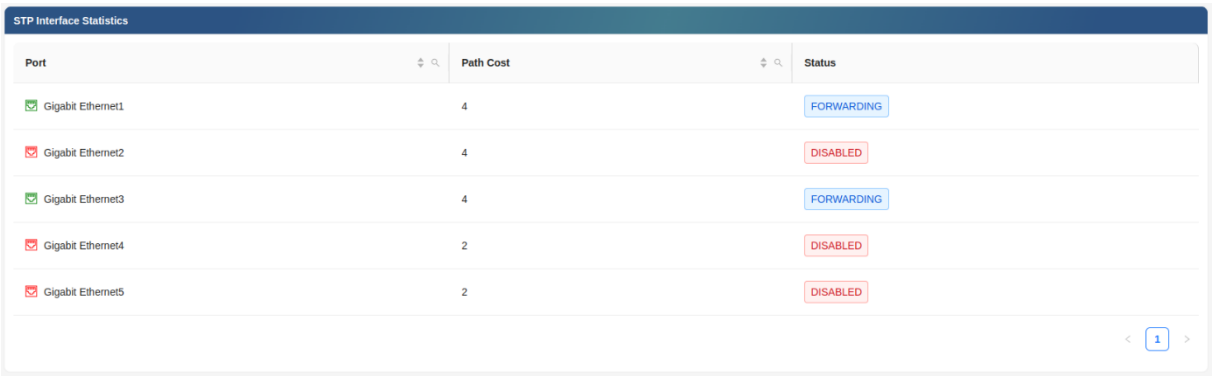
❖ Người dùng có thể click để xóa cấu hình.

3.8 Tính năng STP

Spanning Tree Protocol (STP) là một giao thức mạng tiêu chuẩn IEEE 802.1D được thiết kế để ngăn chặn các vòng lặp (loop) trong mạng Layer 2. Các

vòng lặp xảy ra khi có nhiều đường kết nối giữa các switch, có thể gây ra hiện tượng broadcast storm, xung đột địa chỉ MAC, và làm tê liệt toàn bộ mạng. STP trong thiết bị chạy tự động theo cơ chế bình bầu ngẫu nhiên dựa theo trọng số path cost.

❖ Từ giao diện trang chủ: Click Network → STP:



Hình 54: Giao diện STP

4 Cấu hình nhóm tính năng Policy & Object

4.1 Cấu hình tính năng Firewall Zone

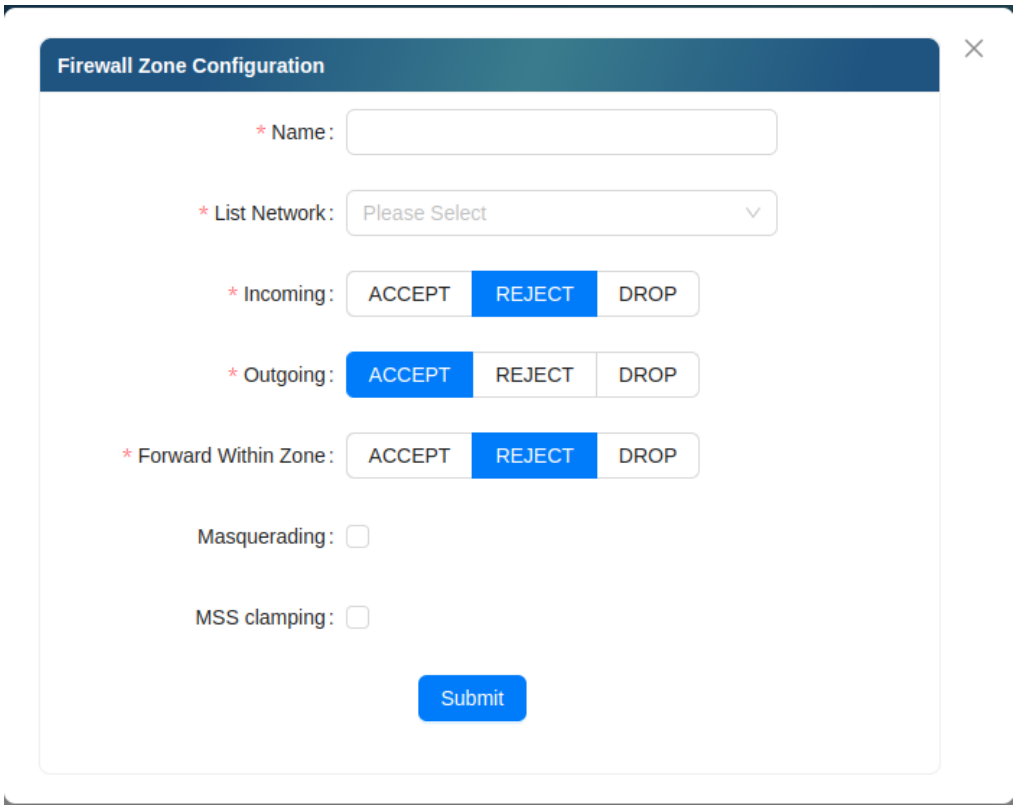
Firewall Zone trong NGFW của Lancs hoạt động như những container chứa các chính sách bảo mật. Mỗi zone đại diện cho một khu vực mạng riêng biệt, và các chính sách bên trong zone xác định cách mà traffic đi vào hoặc đi ra khỏi khu vực đó, có thể là cả việc chuyển tiếp giữa các network trong cùng một khu vực. Khi một gói tin di chuyển qua tường lửa, nó sẽ được kiểm tra để xem nó thuộc zone nào. Sau đó, các quy tắc trong policy của zone đó sẽ được áp dụng để quyết định cách mà hệ thống sẽ xử lý gói tin.

Các tham số chính của Firewall Zone:

❖ Firewall zone mặc định gồm 4 cấu hình, tuy nhiên chỉ có cấu hình LAN được bổ sung network tương ứng. Các cấu hình zone khác chưa có cấu hình network.

❖ Mặc định, traffic của các network chưa được cấu hình quản lý bởi zone sẽ bị chặn toàn bộ.

❖ Trong hệ thống, mặc định các network bị cô lập và sẽ không tương tác với các network khác. Trong trường hợp chúng được đặt trong cùng một zone và được bật chế độ Forwarding within zone, chúng có thể forwarding tới nhau thông qua L3.



Hình 55: Giao diện cấu hình Firewall Zone

Incoming	Quản lý traffic được gửi tới zone này (zone là đích đến).
Outgoing	Quản lý traffic được gửi ra từ zone này (zone là nguồn gửi).
Forwarding within zone	Quản lý forwarding traffic giữa các network trong zone.
Masquerading	Cấu hình sử dụng địa chỉ IP public thay cho các địa chỉ IP của các network trong mạng nội bộ khi giao tiếp với mạng bên ngoài.
MSS clamping	Tự động điều chỉnh kích thước gói TCP (MSS) giúp chống phân mảnh gói tin khi truyền trong mạng có MTU nhỏ, cải thiện hiệu suất.

Với các traffic được quản lý bởi zone, có thể thực hiện một trong ba hành động là accept, reject và drop, trong đó accept cho phép traffic đi qua, reject và drop đều không cho traffic đi qua, tuy nhiên khác với drop loại bỏ gói trong im lặng, reject có gửi lại phản hồi từ chối tới nguồn traffic.

❖ Người dùng có thể click để sửa cấu hình.

❖ Người dùng có thể click  để xóa cấu hình.

4.2 Cấu hình các rules Firewall Policy

Hệ thống Firewall Policy bao gồm một loạt các quy tắc, trong đó mỗi quy tắc xác định các điều kiện mà một gói tin phải đáp ứng để được xử lý theo một cách cụ thể. Các điều kiện này có thể dựa trên địa chỉ IP, cổng, giao thức, và zone nguồn đích.

Các tham số chính của một policy:

Để quản lý traffic, các điều kiện mà một policy có thể được thiết lập bao gồm:

❖ Source Zone
❖ Destination Zone
❖ IP Object
❖ Port Object
❖ Target

Các traffic được so sánh với các trường tham số của policy được cấu hình, nếu traffic không trùng khớp với bất kỳ policy đã được cấu hình nào, nó sẽ bị loại bỏ.

Policy quản lý traffic trên cả chiều đi và chiều về:

Một điều quan trọng cần lưu ý là việc cho phép traffic đi từ zone A đến zone B trên một port cụ thể không có nghĩa rằng traffic cũng có thể đi theo chiều ngược lại. Mỗi hướng lưu lượng (incoming và outgoing) đều cần được cấu hình chính sách riêng biệt. Tuy nhiên, NGFW cung cấp tính năng linh hoạt cho phép bạn cấu hình các quy tắc "accept" chung cho tất cả traffic đi vào hoặc đi ra khỏi một zone, giúp đơn giản hóa quá trình cấu hình.

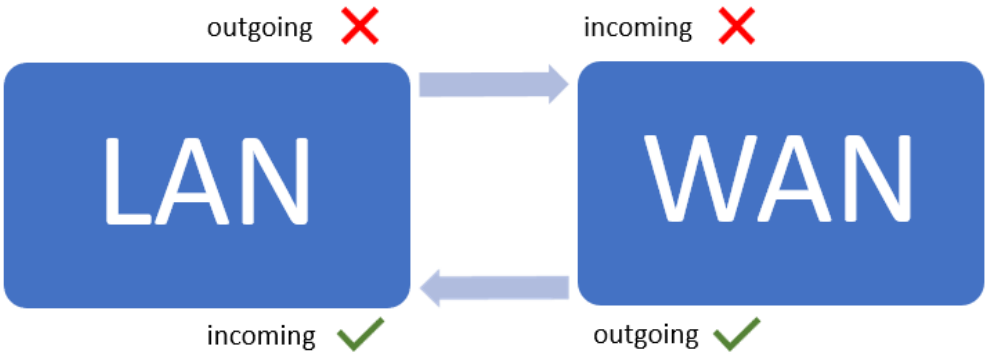
Điều này làm cho cấu hình firewall policy và firewall zone có mối liên hệ mật thiết với nhau.

Ví dụ: muốn cho phép traffic qua lại giữa 2 zone A và B, thông thường ta cần thực hiện các bước sau:

❖ Xác định các zone: Đảm bảo rằng zone A và zone B đã được tạo và cấu hình đúng list network mong muốn.
❖ Quy tắc cho traffic đi từ A tới B: Tạo các quy tắc "accept" cụ thể để cho phép traffic đi từ zone A đến zone B trên cổng X của firewall policy.

❖ Quy tắc cho traffic đi từ B tới A: Nếu bạn muốn cho phép tất cả traffic đi ra khỏi zone B, hãy "accept" trường outgoing của zone B.

Trong trường hợp cụ thể như hai miền mạng LAN và WAN, với nhu cầu quản lý traffic tới hệ thống (incoming WAN) và quản lý các traffic từ nội bộ đi ra ngoài (outgoing LAN).

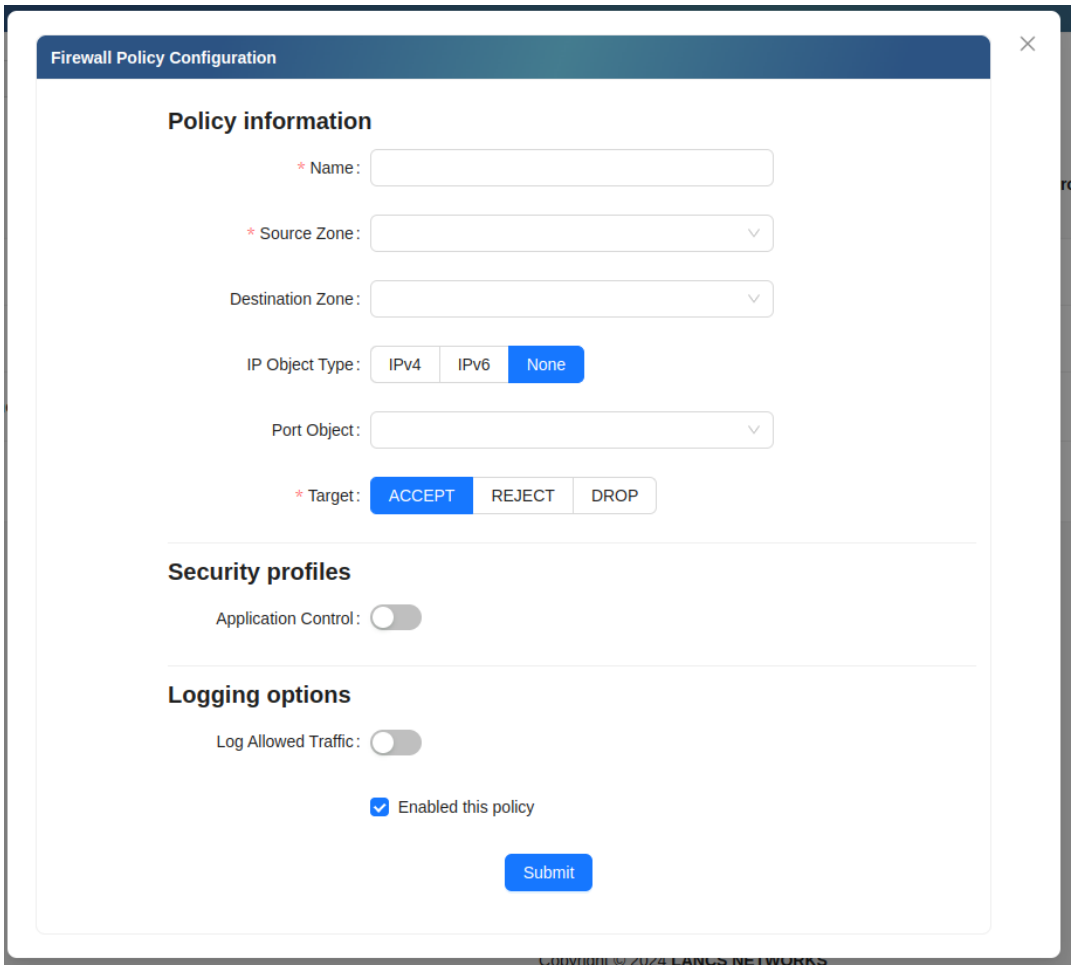


Hình 56: Ví dụ cấu hình cụ thể

Trong trường hợp này với việc outgoing LAN và incoming WAN cần được quản lý vì vậy được cấu hình drop trong firewall zone. Lúc này để cấu hình giúp traffic qua lại giữa LAN và WAN, cần thiết phải có một cấu hình policy cho phép traffic di chuyển với nguồn được match với zone LAN và đích là zone WAN.

4.2.1 Giao diện

Bước 1: Truy cập giao diện Dashboard → Policy & Object → Firewall Policy.



Hình 57: Giao diện cấu hình Firewall Policy

❖ Các policy quản lý các traffic được cấu thành từ các trường sau:

Source zone	Chỉ định vùng đầu tiên mà traffic đi vào thiết bị NGFW, hay vùng nguồn nguồn của traffic.
Destination Zone	Chỉ định vùng đích mà traffic hướng tới sau khi được NGFW xử lý. Vùng này có thể chính là bản thân thiết bị và được mô tả là "this device"
IP Object Type	Chỉ định định dạng địa chỉ nguồn hoặc đích của traffic, giữa 2 dạng IPv4 và IPv6 trước khi chọn cụ thể một object.
Source	Chỉ định địa chỉ IP nguồn cụ thể của traffic.
Destination	Chỉ định địa chỉ IP đích cụ thể của traffic.
Port Object Type	Chỉ định giao thức mà các traffic incoming sử dụng. Có thể là TCP/IP, UDP/IP, ICMP hoặc một dạng protocol IP khác.

Port Object	Chỉ định một hoặc nhiều các Object cụ thể của các giao thức sử dụng. Với TCP/UDP là các port dịch vụ đích cụ thể. Với ICMP là các loại ICMP và với type là IP thì port object là các protocol IP khác ngoài các protocol đã kể trên.
Target	Chỉ định hành động của firewall khi tìm được các traffic thỏa mãn hết các chỉ số phía trên, với 3 dạng hành động bao gồm: accept, reject và drop.

Bước 2: Thực hiện các thao tác:

- Người dung có thể click để sửa cấu hình Firewall Policy.
- Người dùng có thể click để xóa cấu hình.
- Người dùng có thể click để sao chép cấu hình. Các cấu hình bản sao sẽ được sửa lại tên với đuôi _copy. Công cụ này rất hữu ích trong việc tạo các policy chỉ khác một vài tham số.

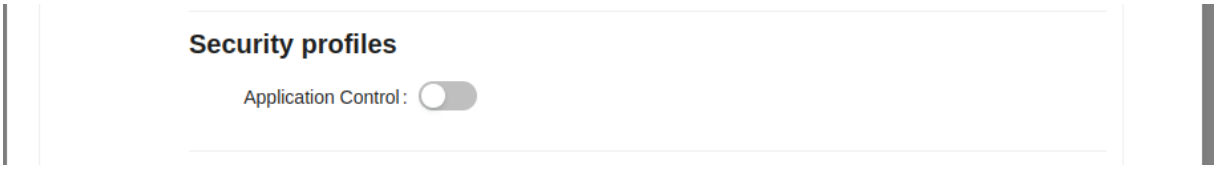
Bước 3: Các policy đã được cấu hình sẽ được cập nhật vào bảng firewall policy.

	Policy Name	Source Zone	Destination Zone	Source	Destination
⋮⋮	Allow-DHCP-Renew-wan	wan	This Device	ALL	ALL
⋮⋮	Allow-DHCP-Renew-wan1	wan1	This Device	ALL	ALL
⋮⋮	Allow-DHCP-Renew-wan2	wan2	This Device	ALL	ALL

Hình 58: Cấu hình không được áp dụng bị làm mờ trong firewall policy

- Với các dòng policy bị làm mở đi, đây là các policy được tạo ra nhưng không được áp dụng trên hệ thống.

4.2.2 Bật tính năng application control



Hình 59: Phân đoạn cấu hình application control trong policy firewall

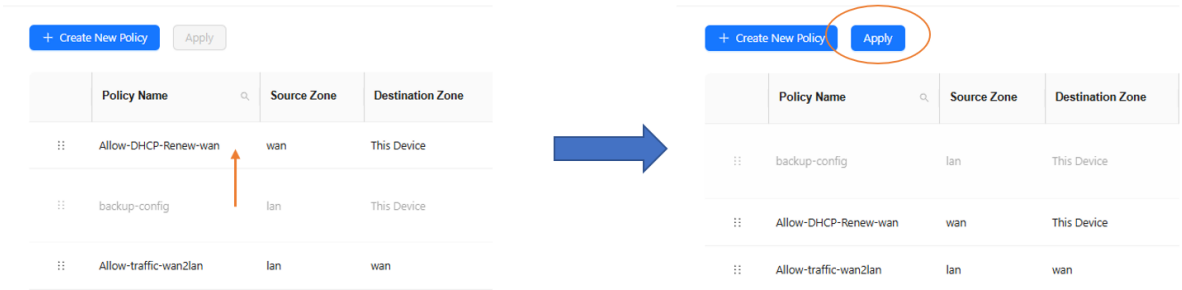
Khi chỉ định hành động của firewall với traffic là accept, có thể sử dụng tính năng application control như một bộ lọc thứ 2, kiểm soát các dịch vụ như app, website cụ thể có được phép di chuyển qua firewall hay không.

4.2.3 Cấu hình priority cho firewall policy

Bước 1: Các cấu hình priority được xếp theo thứ tự ưu tiên từ trên xuống dưới. Policy phía trên sẽ có mức độ ưu tiên thực hiện cao hơn các policy phía dưới.

Bước 2: Sử dụng thanh kéo ở đầu mỗi dòng, cho phép điều chỉnh vị trí của policy từ đó điều chỉnh priority cho toàn bộ policy.

Bước 3: Sau khi hoàn thành chỉnh sửa priority chọn apply để lưu lại các chỉnh sửa.



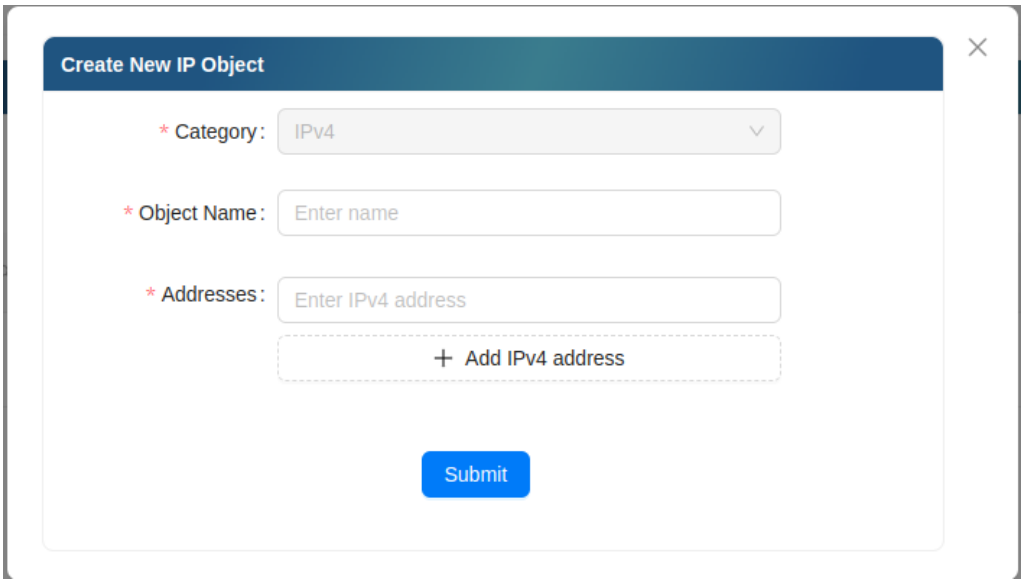
Hình 60: Cấu hình priority cho firewall policy

4.3 Cấu hình IPv4 object

4.3.1 IP Address

Từ giao diện trang chủ: Click Policy & Object → IP object.

❖ Click vào trên bảng IPv4 Address để tạo cấu hình:



Hình 61: Giao diện cấu hình IP Object

❖ Trong đó:

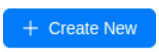
- **Category:** chỉ định cho IPv4 hoặc IPv6
- **Object Name:** đặt tên gợi nhớ
- **Submit:** Lưu cấu hình

❖ Người dùng có thể click  để sửa cấu hình.

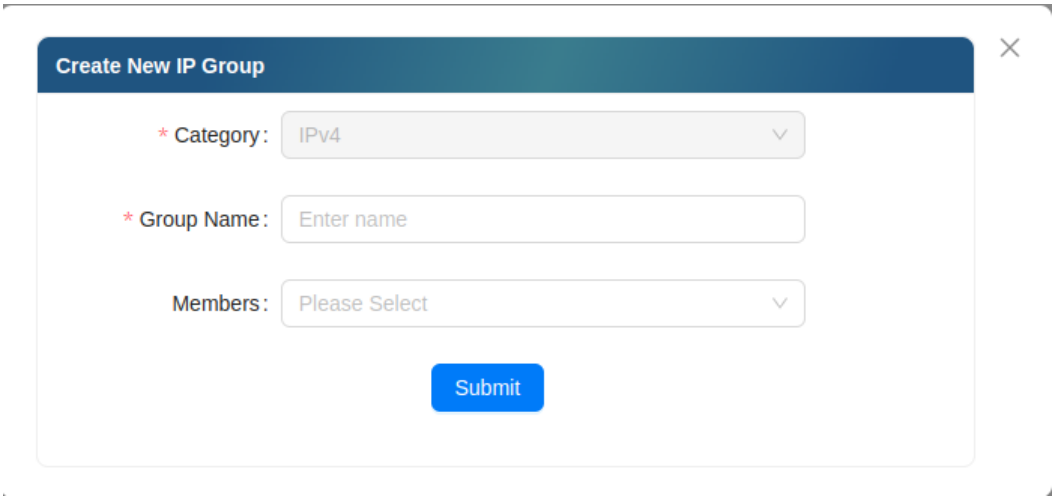
❖ Người dùng có thể click  để xóa cấu hình.

4.3.2 IP Address Group

Từ giao diện trang chủ : Click Policy & Object → IP object.

❖ Click vào 

trên bảng IPv4 Address Group để tạo cấu hình:



Hình 62: Giao diện tạo mới IP Group

- Trong đó:
  - **Category:** Chỉ định cho IPv4 hoặc IPv6
  - **Group Name:** Đặt tên gợi nhớ
  - **Members:** Lựa chọn các thành viên IPv4 Object để thêm vào group
  - **Submit:** Lưu cấu hình
- Người dùng có thể click  để sửa cấu hình.
- Người dùng có thể click  để xóa cấu hình.

4.4 Cấu hình IPv6 Object

- Tương tự như cấu hình IPv4 Object.

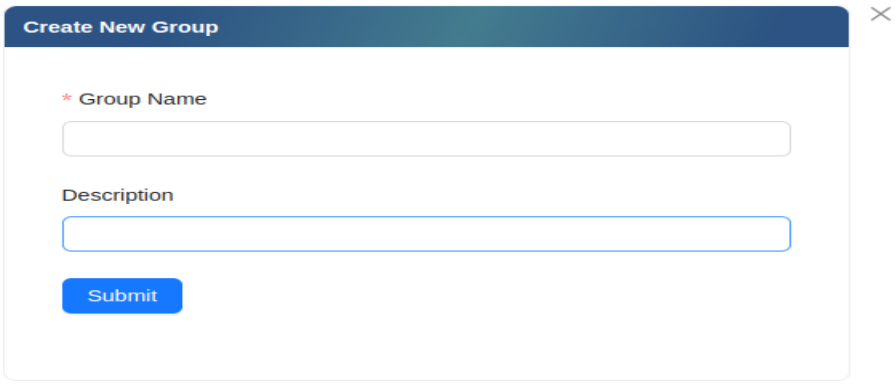
4.5 Cấu hình các dịch vụ Port Object

Từ giao diện trang chủ: Click Policy & Object → Port Object:

4.5.1 New group object

- Click vào 

để tạo cấu hình group cho từng Port Object:



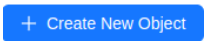
Hình 63: Giao diện cấu hình Group Port-Object

❖ Trong đó:
- **Group Name:** Đặt tên nhằm gợi nhớ nhóm
- **Description:** Mô tả thêm để người dùng hiểu rõ hơn về nhiệm vụ của nhóm
- **Submit:** Lưu cấu hình

❖ Người dùng có thể click  để sửa cấu hình.

❖ Người dùng có thể click  để xóa cấu hình.

4.5.2 New Port Object

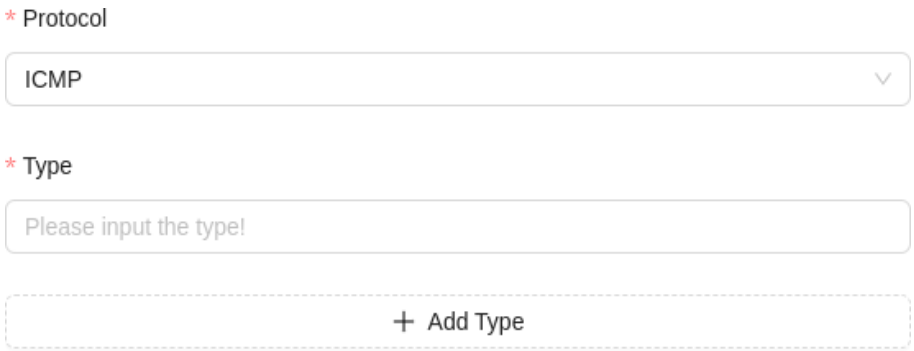
❖ Click vào 

để tạo cấu hình cho từng Port Object.

Hình 64: Giao diện cấu hình Port-Object mới

❖ Trong đó:
- **Name:** Tên cho từng Port Object
- **Group Name:** Chọn các nhóm đã tạo sẵn trước đó

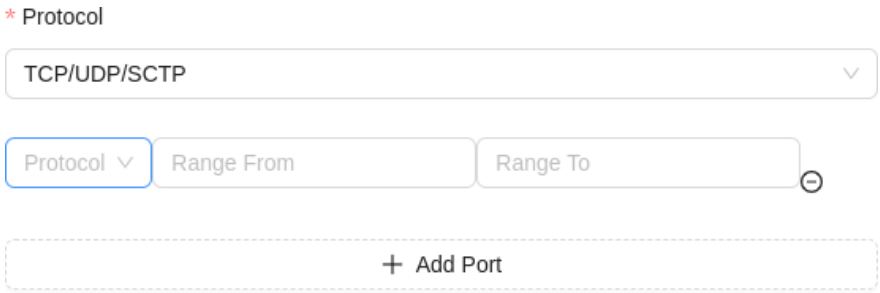
- Protocol bao gồm 2 phần:
  - TCP/UDP/SCTP
  - ICMP
- **Protocol:** ICMP



Hình 65: Giao diện cấu hình giao thức ICMP

❖ Trong đó:

- **Type:** Cấu hình loại giao thức, thường chọn là any
- **Protocol:** TCP/UDP/SCTP



Hình 66: Giao diện cấu hình giao thức TCP/UDP/SCTP

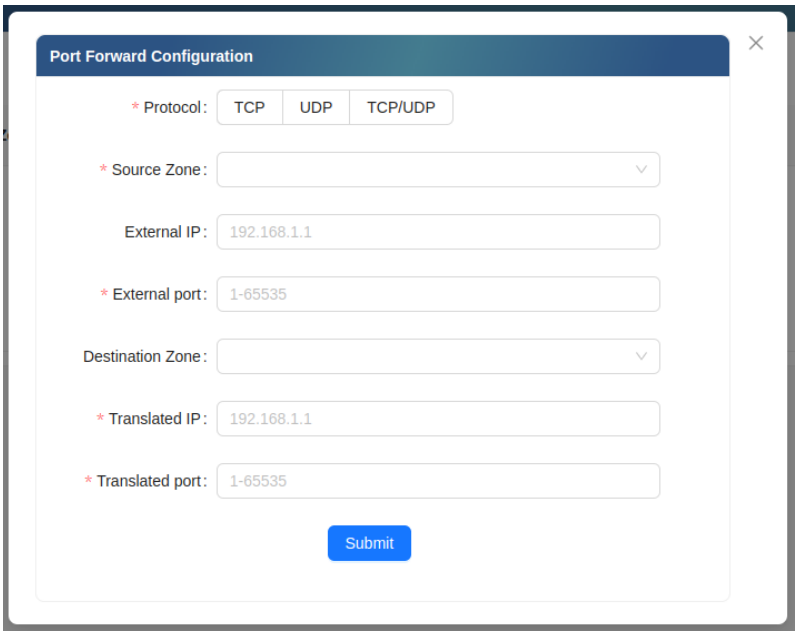
❖ Trong đó:

- **Protocol:** Có thể chọn một trong 3 giao thức: TCP/UDP/SCTP
- **Range from:** Chọn cổng bắt đầu
- **Rang to:** Chọn cổng kết thúc

4.6 Cấu hình tính năng Port Forwarding

Từ giao diện trang chủ: Click Policy & Object → Port Forwarding.

❖ Click vào Create để tạo cấu hình group cho từng Port Forwarding.



Hình 67: Giao diện cấu hình Port Forwarding

❖ Trong đó:

- **Protocol:** Có thể chọn 1 trong 2 giao thức TCP/UDP
- **Source Zone:** Chọn các vùng Zone nguồn là LAN/WAN
- **Destination Zone:** Chọn các vùng Zone đích LAN/WAN
- **Wan IP:** Cấu hình Wan cho thiết bị ngoài mạng có thể truy cập vào.
- **Wan Port:** Cấu hình mở cổng cho thiết bị ngoài mạng truy cập vào nội bộ.
- **LAN IP:** Cấu hình IP nội bộ mà thiết bị mạng ngoài muốn truy cập vào.
- **LAN Port:** Cấu hình mở cổng cho thiết bị.
- **Submit:** Lưu cấu hình.

❖ Người dùng có thể click để sửa cấu hình.

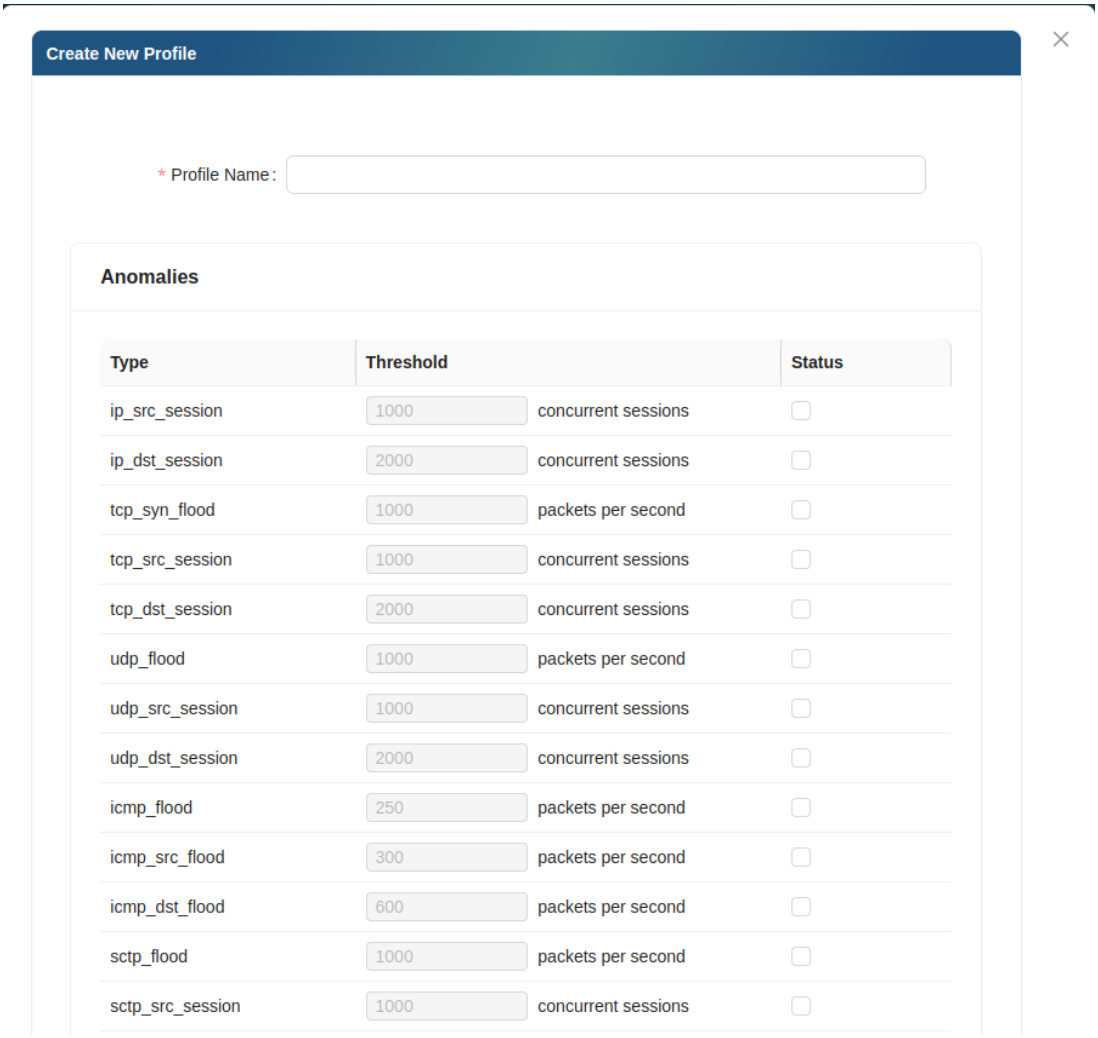
❖ Người dùng có thể click để xóa cấu hình.

4.7 Cấu hình tính năng DoS protection

4.7.1 DoS profile

Từ giao diện trang chủ: Click Policy & Object → DoS protection → DoS Profile:

❖ Click vào + Create New để tạo cấu hình cho từng DoS profile:



Hình 68: Giao diện cấu hình DoS Profile

❖ Trong đó:

- **Profile name:** Đặt tên profile gợi nhớ
- **Anomalies:**
  - ***Type:*** Chọn loại
  - ***Threshold:*** Thiết lập ngưỡng
  - ***Status:*** Trạng thái bật/tắt để áp dụng các gói.

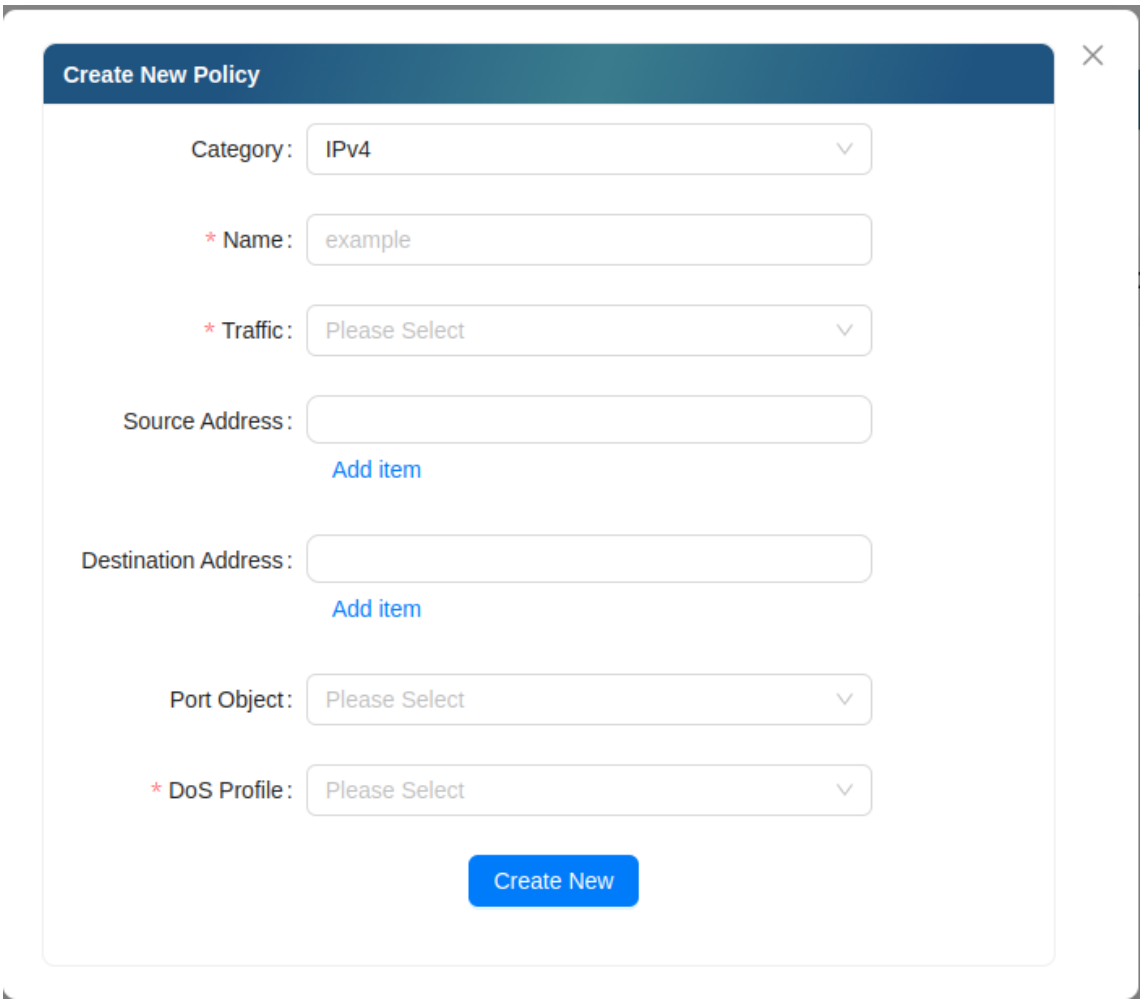
❖ Người dùng có thể click để sửa cấu hình.

❖ Người dùng có thể click để xóa cấu hình.

4.7.2 DoS Policy

Từ giao diện trang chủ: Click Policy & Object → DoS protection → DoS Policy:

❖ Click vào + Create New để tạo cấu hình cho từng DoS policy:



Hình 69: Giao diện cấu hình DoS Policy

❖ Trong đó:

- **Category:** Chọn cấu hình cho IPv4 hoặc IPv6
- **Name:** Đặt tên gợi nhớ cho chính sách
- **Traffic:** Chọn Incoming/Forwarding (sau khi chon traffic thì sẽ cấu hình thêm source zone và dest zone tương ứng)
  - ***Incoming:*** Áp dụng cho những luồng dữ liệu đi vào trong NGFW từ vùng nguồn (Source Zone)

- ***Forwarding:*** Áp dụng cho những luồng dữ liệu đi qua NGFW từ vùng nguồn (Source Zone) đến vùng đích (Destination Zone)

- **Port Object:** Áp dụng chính sách đối với những dịch vụ được cài đặt
- **Source Address:** Áp dụng chính sách đối với gói tin có địa chỉ nguồn được cài đặt
- **Destination Address:** Áp dụng chính sách đối với gói tin có địa chỉ đích được cài đặt
- **DoS Profile:** Chọn profile đã được thiết lập sẵn để áp dụng vào các luồng dữ liệu khớp với các cài đặt ở trên

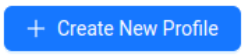
❖ Người dùng có thể click  để sửa cấu hình

❖ Người dùng có thể click  để xóa cấu hình

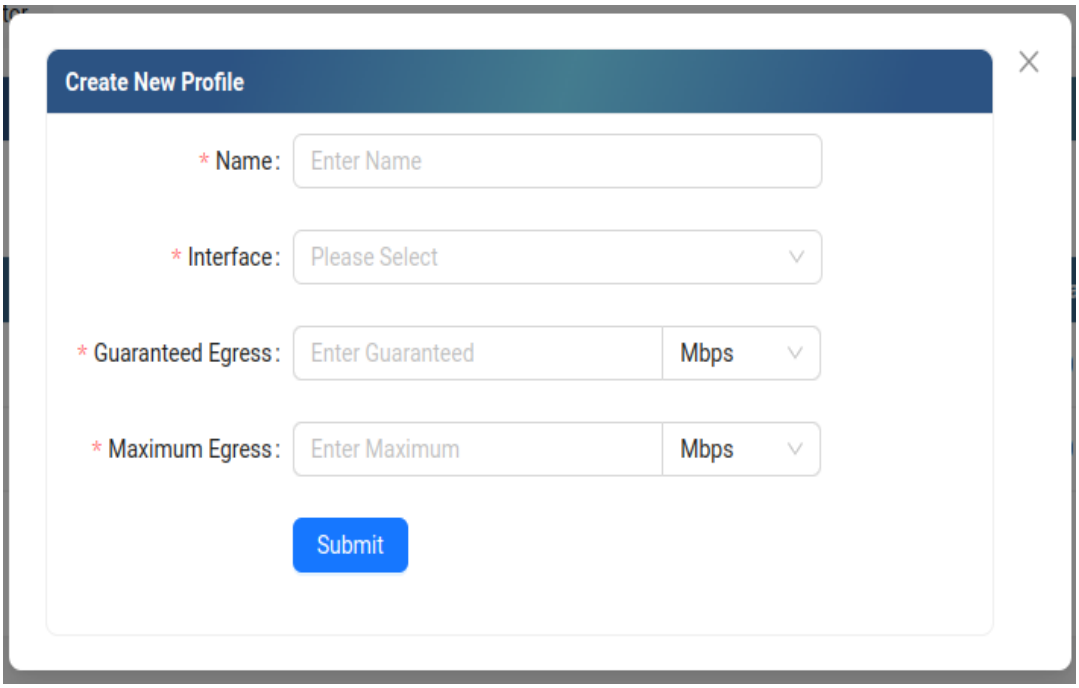
4.8 Cấu hình tính năng QoS

4.8.1 QoS Profile

Từ giao diện trang chủ: Click Policy & Object → QoS → QoS Profile:

❖ Click vào 

để tạo cấu hình cho từng QoS profile:



❖ Trong đó:

- **Name:** Đặt tên cho profile
- **Interface:** Lựa chọn các interface sẵn có trên hệ thống
- **Guarantee Egress:** Băng thông cam kết tối thiểu cho profile
- **Maximum Egress:** Băng thông tối đa cho profile
- Lựa chọn đơn vị Kbps/Mbps/Gbps

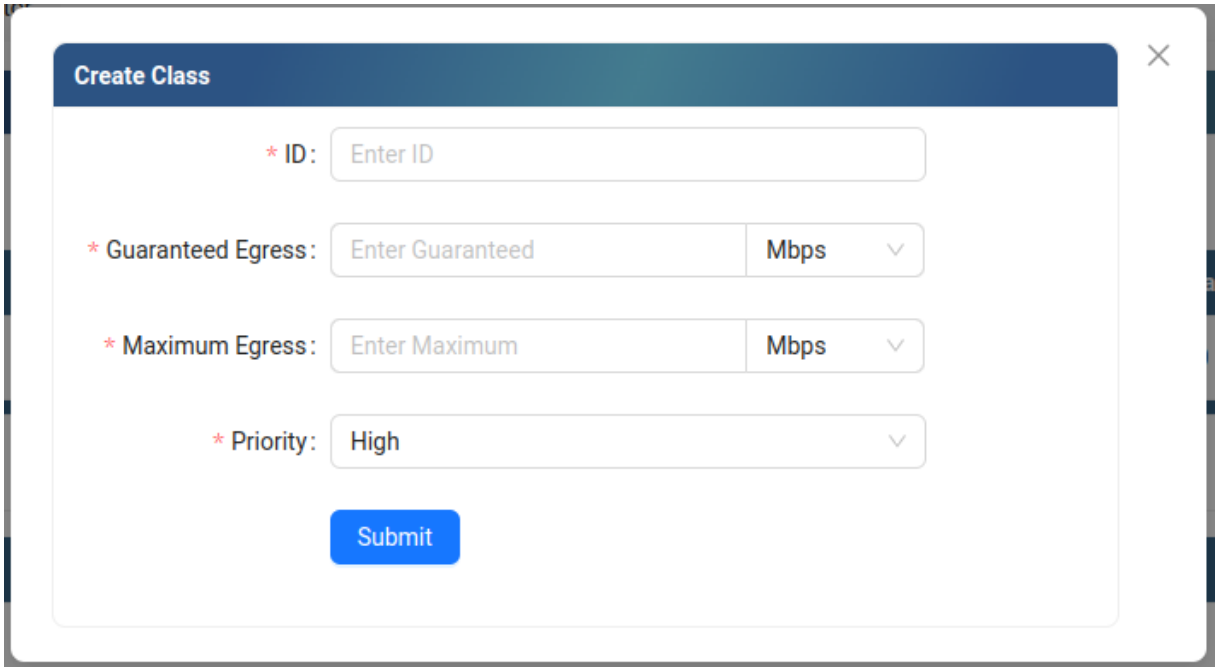
❖ Người dùng có thể click để sửa cấu hình.

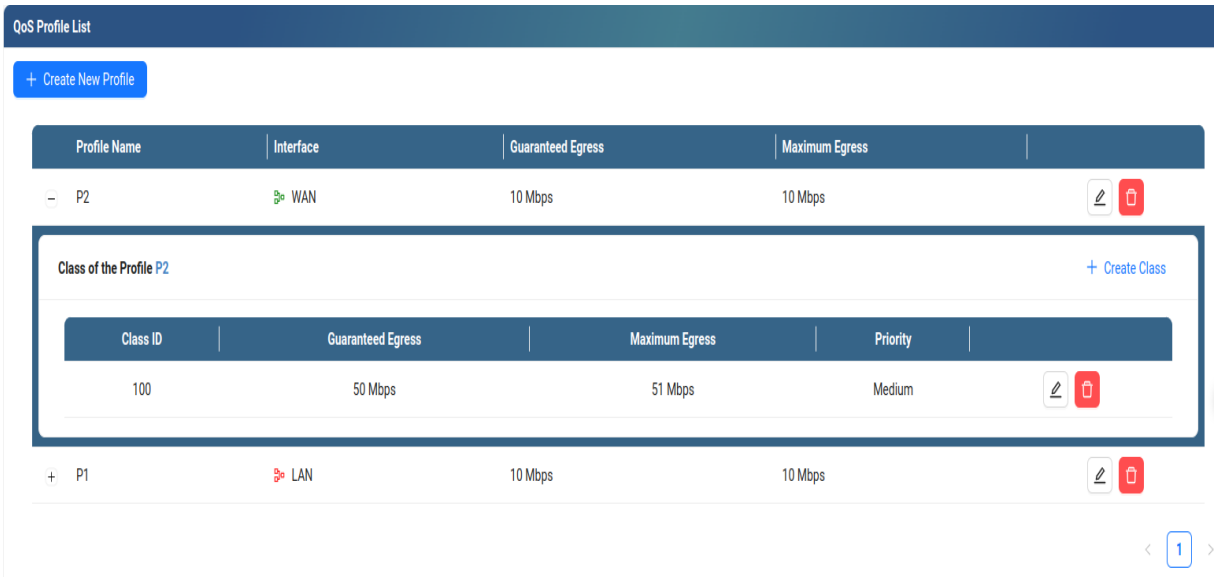
❖ Người dùng có thể click để xóa cấu hình, khi xóa profile thì tất cả class thuộc profile cũng sẽ bị xóa.

4.8.2 QoS Class

Từ giao diện trang chủ: Click Policy & Object → QoS → QoS Profile → của profile sẽ hiện ra các class thuộc profile:

❖ Click vào + Create Class để tạo class thuộc profile:

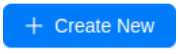


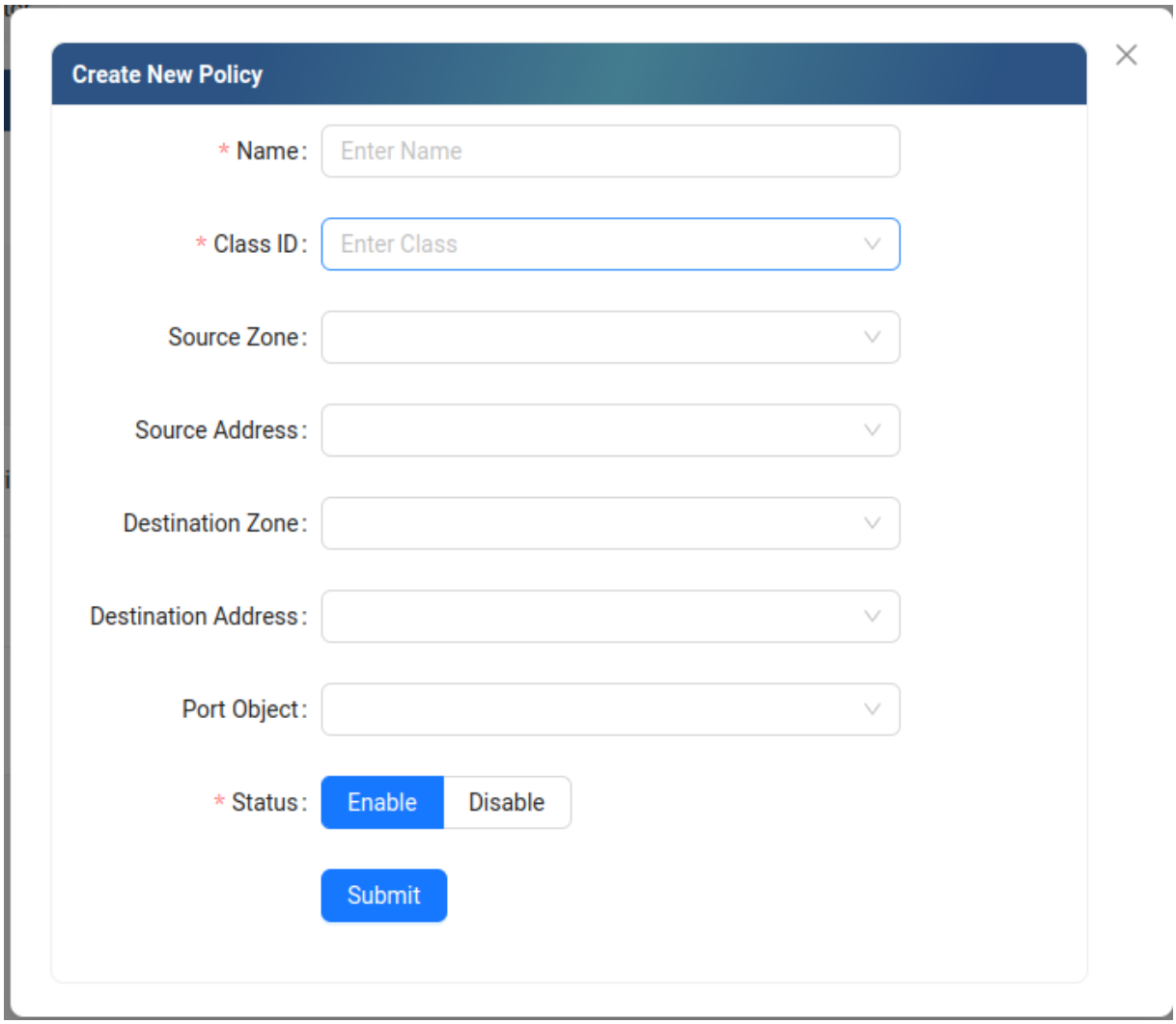


- Trong đó:
  - **ID:** ID của class
  - **Guarantee Egress:** Băng thông cam kết tối thiểu cho class, tổng guarantee egress của các class thuộc profile phải nhỏ hơn Maximum egress của profile
  - **Maximum Egress:** Băng thông tối đa cho class, tổng các maximum egress của các class thuộc profile phải nhỏ hơn Maximum egress của profile
  - Lựa chọn đơn vị Kbps/Mbps/Gbps
  - **Priority:** Lựa chọn priority cho class, prio càng cao thì traffic của class đó sẽ được ưu tiên hơn trong trường hợp nghẽn mạng
- Người dùng có thể click  để sửa cấu hình.
- Người dùng có thể click  để xóa cấu hình, cần loại bỏ các policy sử dụng class trước khi xóa class đó

4.8.3 QoS Policy

Từ giao diện trang chủ: Click Policy & Object → QoS → QoS Policy:

- Click vào  để tạo cấu hình policy:



❖ Trong đó:

- **Name:** Tên của policy
- **Class ID:** ID của class muốn sử dụng, tương ứng với việc băng thông của traffic match với policy sẽ bị kiểm soát bởi class.
- **Source Zone:** Zone nguồn của gói tin, lựa chọn các zone sẵn có
- **Destination Zone:** Zone đích của gói tin, lựa chọn các zone sẵn có
- **Source Address:** Địa chỉ nguồn của gói tin, chính là IP Object
- **Destination Address:** Địa chỉ đích của gói tin, chính là IP Object
- **Port Object:** Lựa chọn các Port Object sẵn có và có thể chọn nhiều giá trị
- **Status:** Bật hoặc tắt cấu hình policy

❖ Người dùng có thể click để sửa cấu hình.

❖ Người dùng có thể click  để xóa cấu hình.

5 Cấu hình các tính năng bảo mật cho thiết bị (Security)

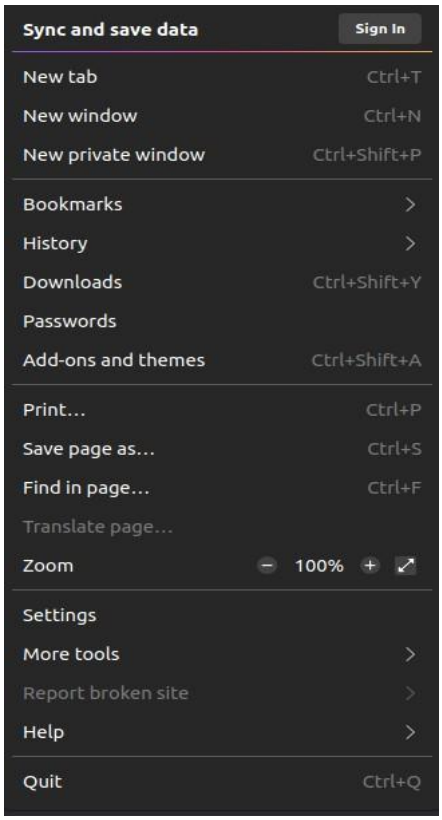
Lưu ý: Trước khi chạy tính năng mở port 8080 (chi tiết hướng dẫn trong mục 2.4.4 Port-Object). Truy cập vào Policy & Object → Firewall Policy, chọn Create new policy và cấu hình:

❖ **Source Zone:** WAN
❖ **Destination Zone:** This device
❖ **Port Object:** Cổng 8080 vừa tạo.
❖ **Target:** ACCEPT
❖ **Status:** Enable

5.1 Thực hiện cấu hình certificate trên trình duyệt

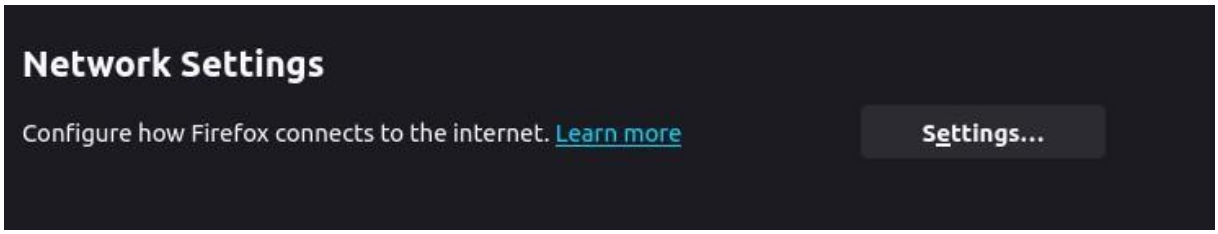
Thực hiện tải chứng chỉ theo các bước dưới đây:

Bước 1: Truy cập setting của Firefox:



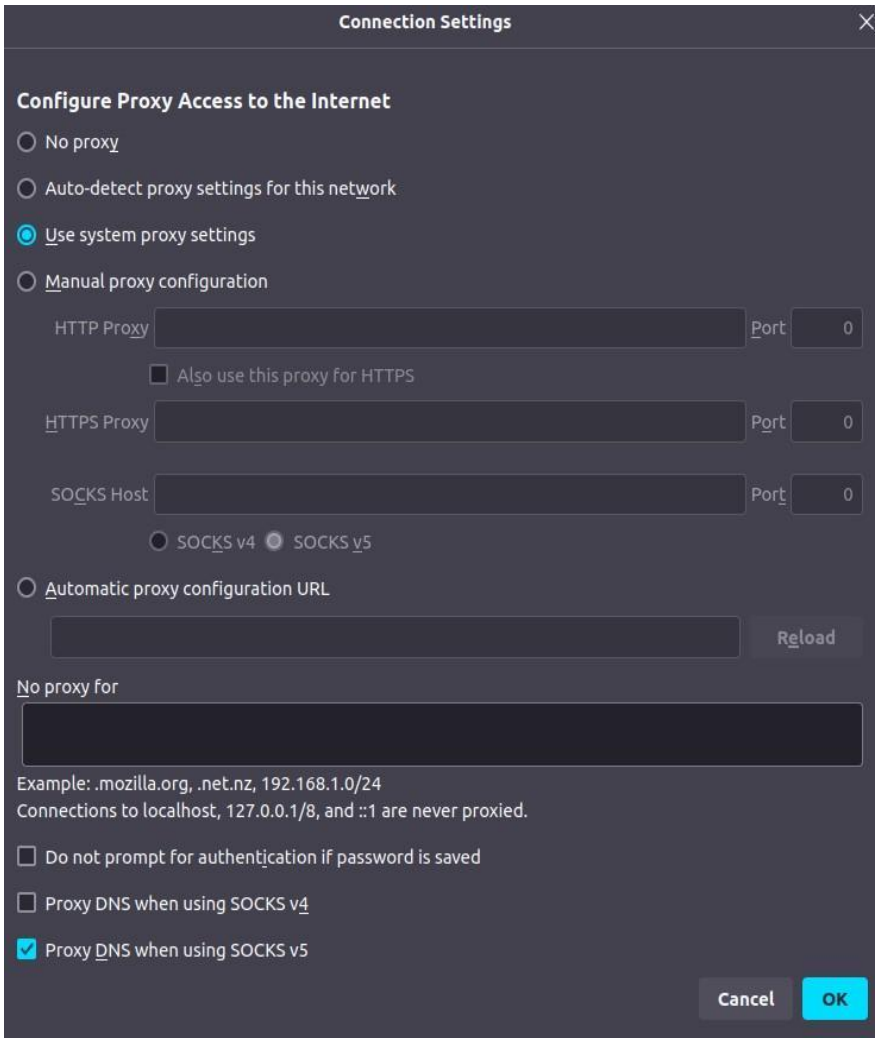
Hình 70: Truy cập vào Setting trên Firefox

Bước 2: Truy cập General → Setting → Network setting.



Hình 71: Mục Network Setting

Bước 3: Trong mục Setting, Manual proxy configuration, sau đó nhập địa chỉ IP của máy chạy proxy, nhập port 8080, tích vào also use this proxy for HTTPS và OK để lưu.



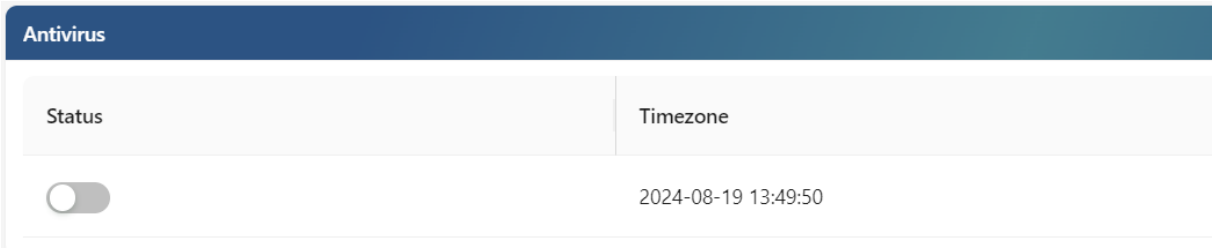
Hình 72: Cấu hình địa chỉ server proxy

Bước 4: Truy cập phần Privacy & Security, trong đây tìm phần Certificates, đó click vào ViewCertificates → Chọn sang Authorities và click vào import → Chọn file myroot_CA.crt và nhấn "OK".

Hình 73: Import Certificate vào trình duyệt

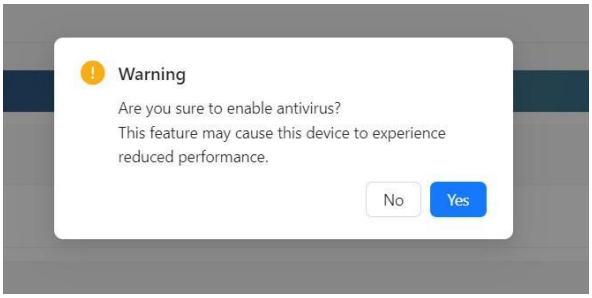
5.2 Cấu hình tính năng chống Anti Virus

Bước 1: Truy cập vào Security → Anti Virus → Click chọn enable để mở tính năng.



Hình 74: Bật/Tắt tính năng AV

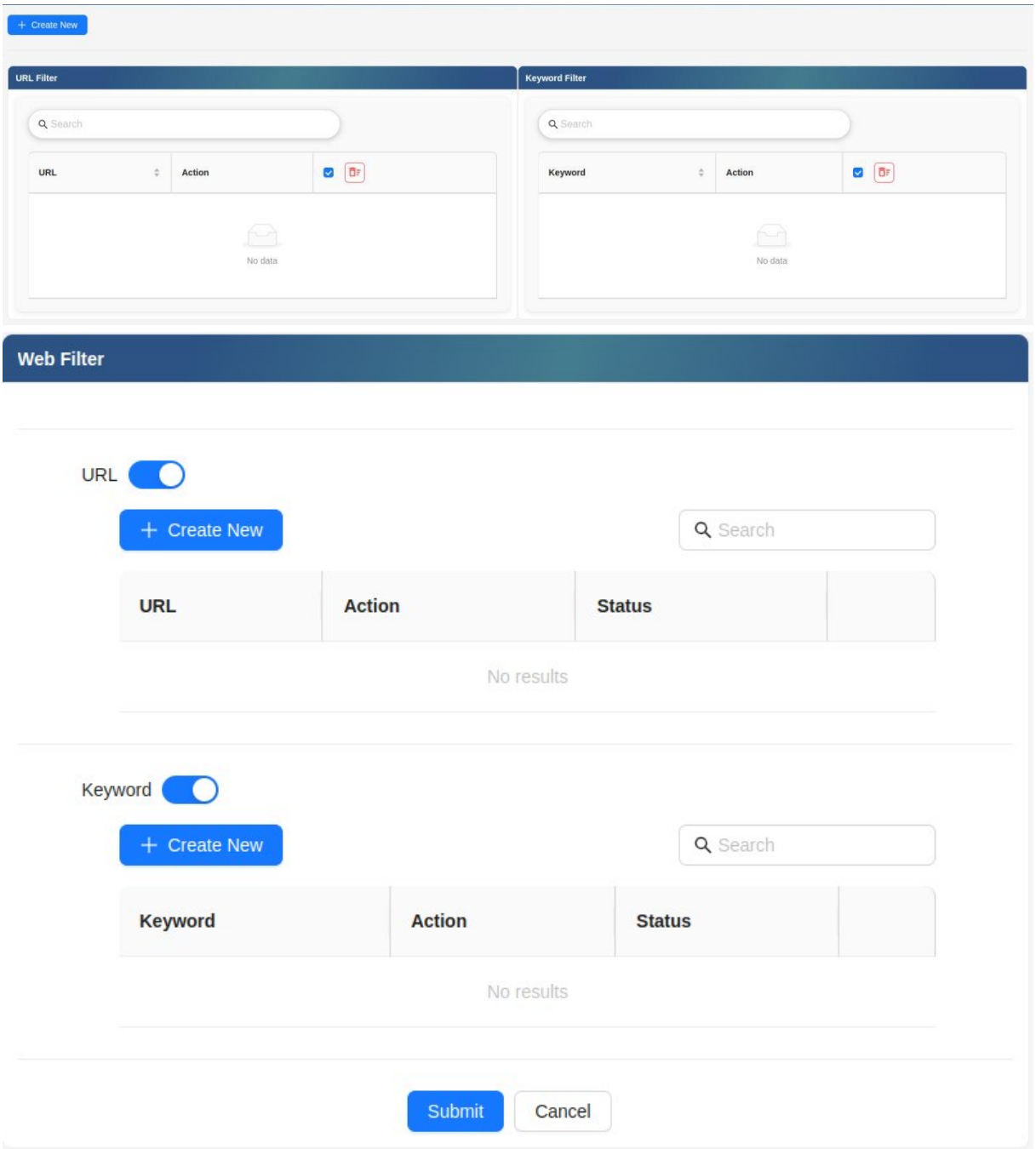
Bước 2: Hiển thị thông báo, chọn Yes để xác nhận.



Hình 75: Xác nhận bật tính năng

5.3 Cấu hình tính năng chặn Web filter

❖ Chọn + Create để tạo filter mới.



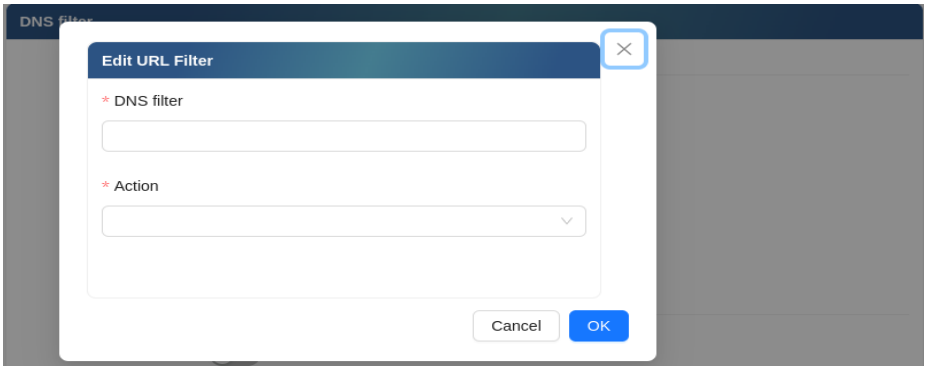
Hình 76: Giao diện cấu hình Web filter

❖ Trong đó:

- **Mode URL filter:** Thêm các đường dẫn Url và các action kèm theo
- **Mode keyword filter:** Thêm các keyword khi thực hiện search và các action kèm theo
- **Block list default:** Đặt filter làm

5.4 Cấu hình tính năng chặn DNS filter

❖ Chọn + Create để tạo filter mới.



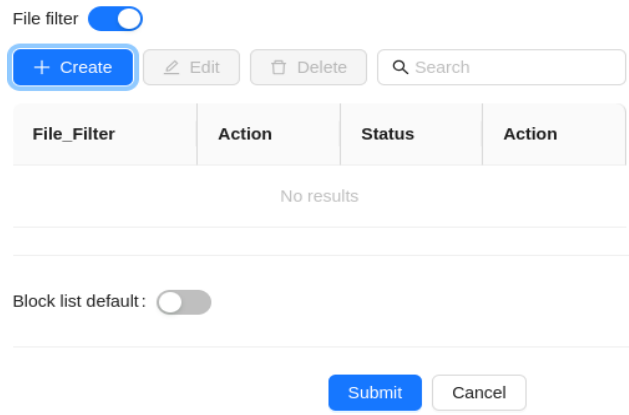
Hình 77: Giao diện cấu hình DNS filter

❖ Trong đó:

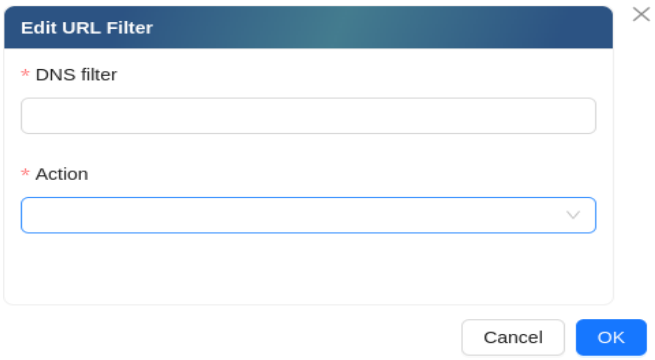
- **DNS filter:** đường dẫn DNS
- **Action:** Chọn loại action: Block/Unblock

5.5 Cấu hình tính năng chặn File filter

❖ Chọn + Create để tạo filter mới.

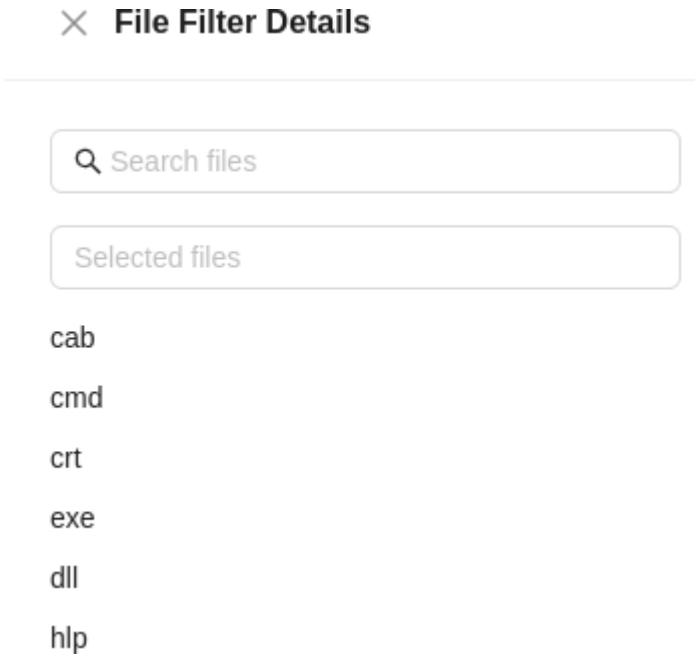


Hình 78: Giao diện cấu hình File filter



Hình 79: Giao diện cấu hình chi tiết File filter

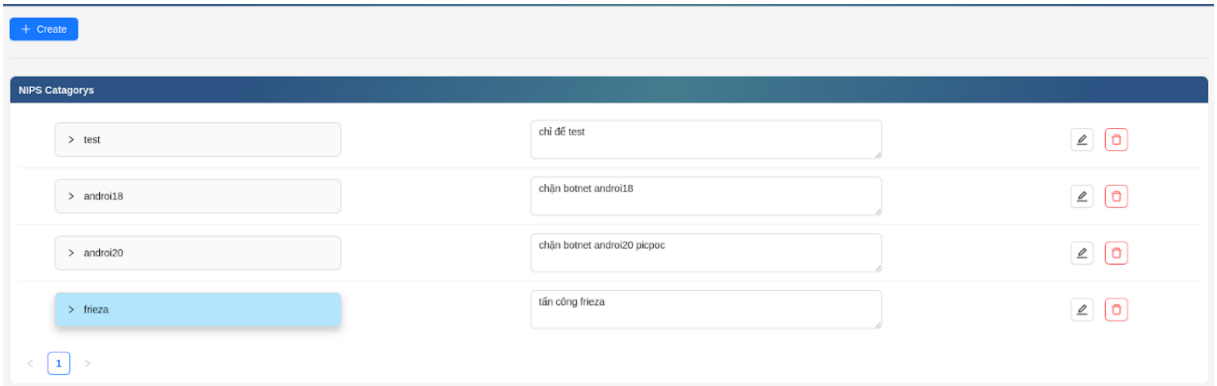
- Trong đó:
  - **File filter:** Tên đuôi file cần kiểm tra
  - **Action:** Chọn loại action: Block/Unblock
  - **List file:** Danh sách các đuôi file mà thiết bị hỗ trợ



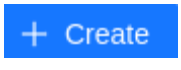
Hình 80: Danh sách các file hỗ trợ

5.6 Cấu hình tính năng chặn NIPS

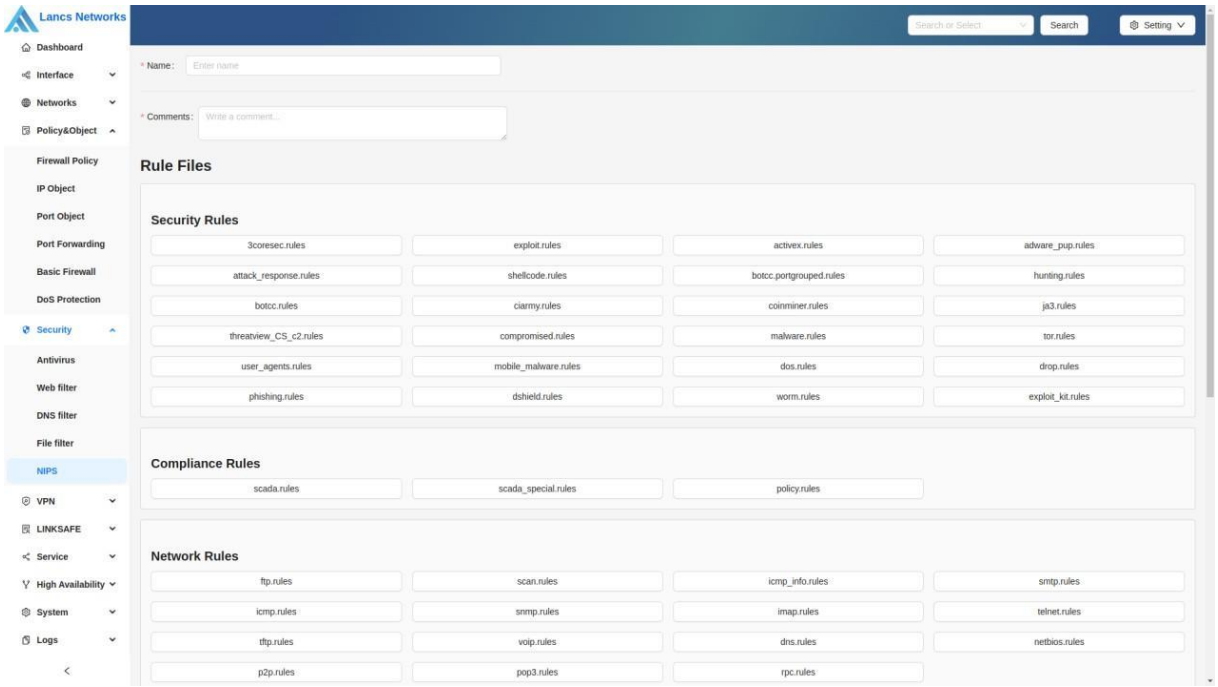
NIPS cho phép cấu hình các rule theo các Catagorys tùy chọn theo ý người dùng.



Hình 81: Danh sách category của NIPS

- Chọn 

để tạo filter mới.



Hình 82: Danh sách các tập rule NIPS

❖ Trong đó:

- **Name:** Tên của category
- **Description:** Mô tả về category
- **Danh sách các bộ rule theo các chủ đề:** Security rule, Compliance Rules…

6 Cấu hình tính năng VPN trên NGFW

Để cấu hình các tính năng trong nhóm VPN, người dùng thực hiện lựa chọn vào mục "VPN".

Nhóm tính năng VPN bao gồm các cấu hình VPN như: IPSec.

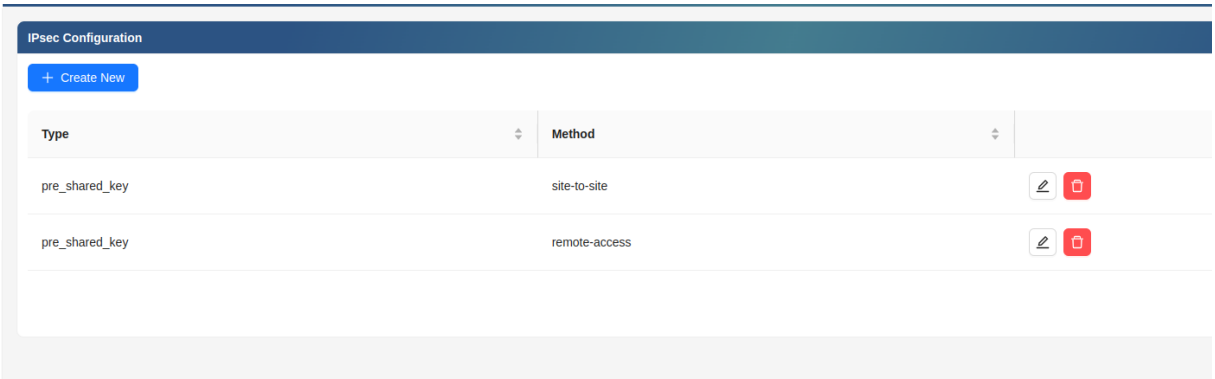
6.1 Cấu hình tính năng IPSec trên NGFW

Tính năng IPSec trên thiết bị NGFW làm việc ở hai chế độ đó là Site-to-Site và Remote Access. Site-to-Site là chế độ làm việc tạo đường hầm (tunnel) giữa hai mạng LAN tức là giữa hai thiết bị Gateway. Còn chế độ Remote Access là chế độ làm việc tạo đường hầm (tunnel) giữ thiết bị End-User như là PC, Laptop hoặc SmartPhone với một thiết bị Gateway.

Cấu hình Site-to-Site

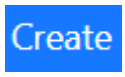
Bước 1: Từ giao diện quản lý → VPN → General → Tunnel.

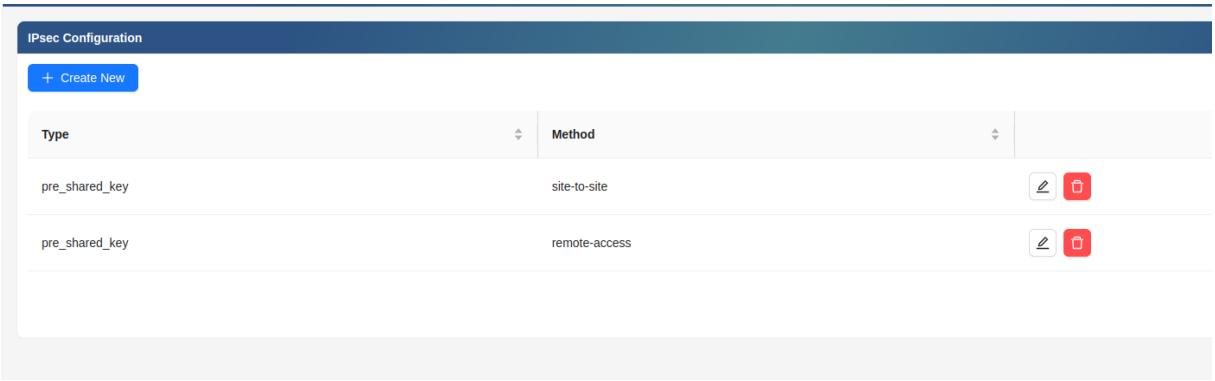
Bước 2: Cấu hình các đường tunnel được hiển thị ở hình ảnh sau. Chế độ Site-to-Site sử dụng IKE để làm giao thức trao đổi khóa, có hai phương thức xác thực hỗ trợ đó là xác thực bằng Pre-Shared Key và xác thực bằng Certificate.



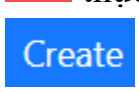
Hình 83: Giao diện hiển thị thông tin cấu hình IPsec

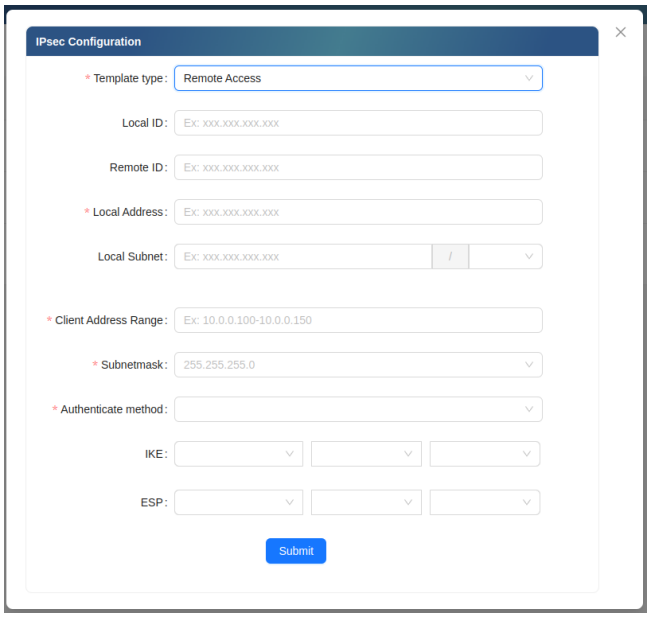
Bước 3: Thực hiện các thao tác khác:

- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong IPSec.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình IPSec.
- Kích chuột vào  thực hiện cấu hình với giao thức IPSec.



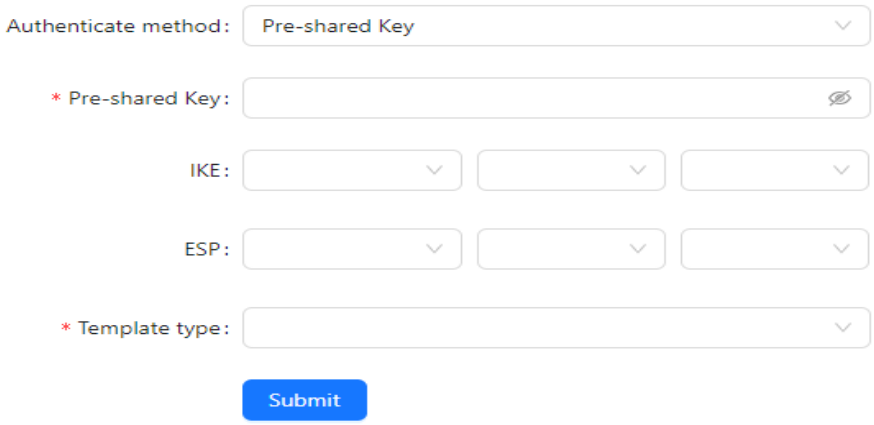
Hình 84: Giao diện hiển thị thông tin cấu hình IPsec

- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong IPSec.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình IPSec.
- Kích chuột vào  thực hiện cấu hình với giao thức IPSec.



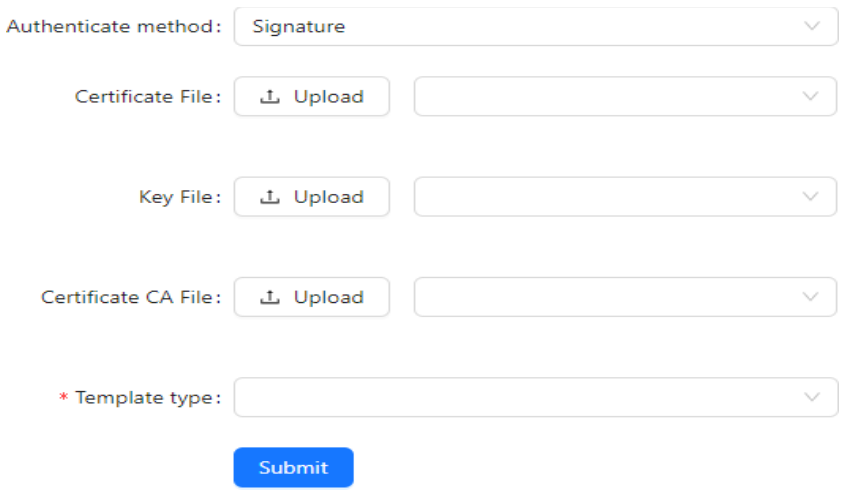
Hình 85: Giao diện cấu hình IPSec

- Trong đó:
  - **Local ID:** Tích chọn IP tương ứng cho cổng WAN thiết lập đường VPN.
  - **Remote ID:** Điền thông tin IP của site remote thiết lập đường VPN.
  - **Local Address:** Địa chỉ IP tương ứng của thiết bị tại vị trí đang setup đường VPN.
  - **Remote Address:** Địa chỉ IP tương ứng của thiết bị tại vị trí remote thiết lập đường VPN.
  - **Authenticate method:** Hỗ trợ hai chế độ Pre-Shared Key và Signature.
  - **Template type:** Hỗ trợ hai chế độ: Site to Site và Remote Access.
  - **Mode Pre - shared Key:**

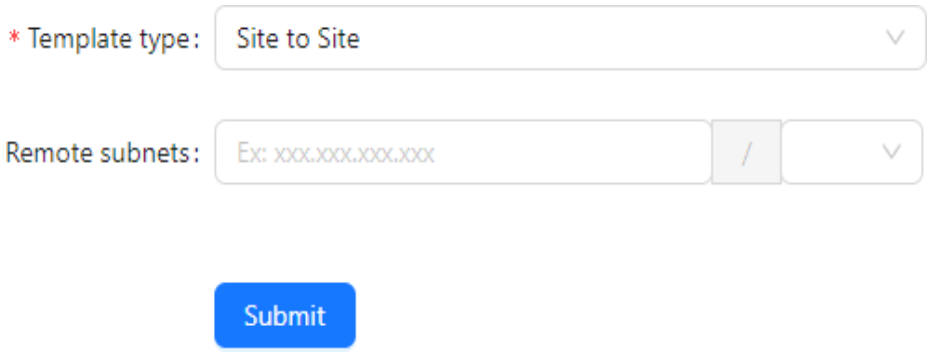


Hình 86: Giao diện cấu hình Mode Pre - shared Key

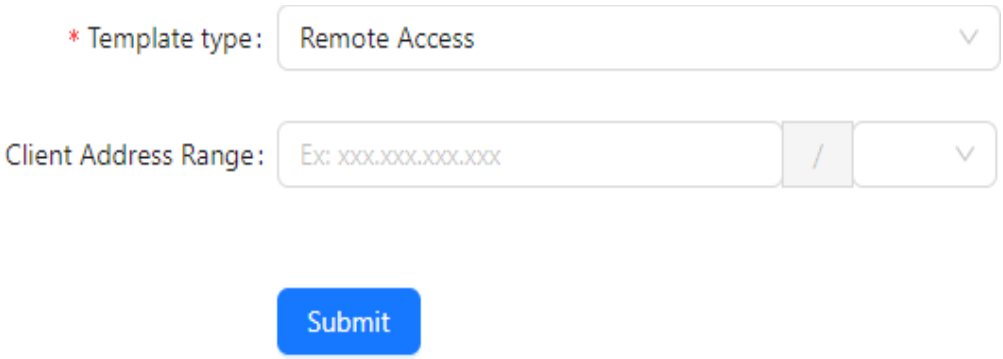
- **Pre-shared Key:** Tạo key cho Tunnel (ví dụ: test123456).
- **IKE & ESP:** Đưa ra các mode mã hóa & khóa để thiết lập tunnel trên NGFW: IKE & ESP hỗ trợ các mode Encryption, hash và diffie-hellman exponentiation.
- **Encryption:** các mode mã hóa được hỗ trợ: ase128/ ase128ctr/ ase128mac/ ase192/ ase192ctr/ ase192gcm/ ase256/ ase256gcm/ ase256gmac/ 3des.
- **Mode Signature:**



Hình 87: Giao diện cấu hình mode Signature

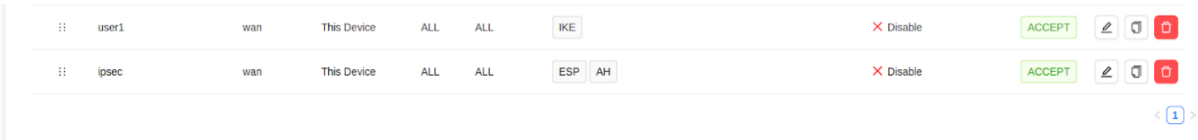


Hình 88: Giao diện cấu hình Template type Site to Site



Hình 89: Giao diện cấu hình Template type Client to Site

Note: Để chạy với thiết bị NGFW thì cần tạo rule cho Firewall policy và Firewall Zone.



Hình 90: Thêm rule vào firewall policy

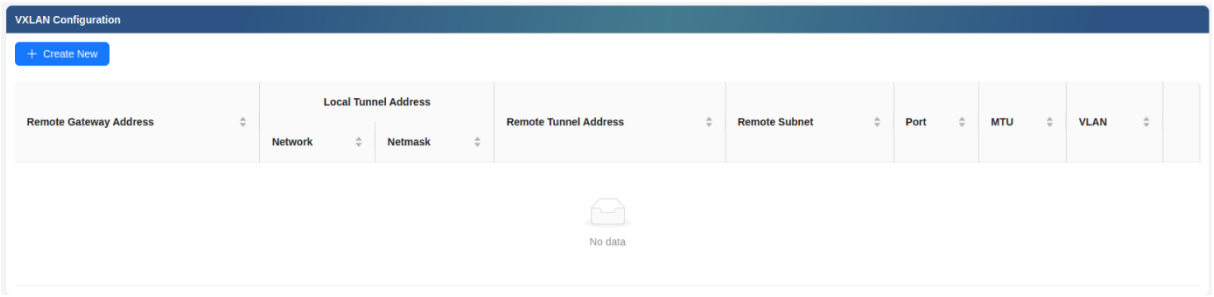
Note: Cần thêm rule allow các port trên firewall policy.
allow allow traffic ISAKMP/IKE (UDP port 500)
allow traffic ESP (IP protocol 50)
allow traffic AH (IP protocol 51)
add rule forward traffic vào mạng nội bộ

6.2 Tính năng VXLAN trên NGFW

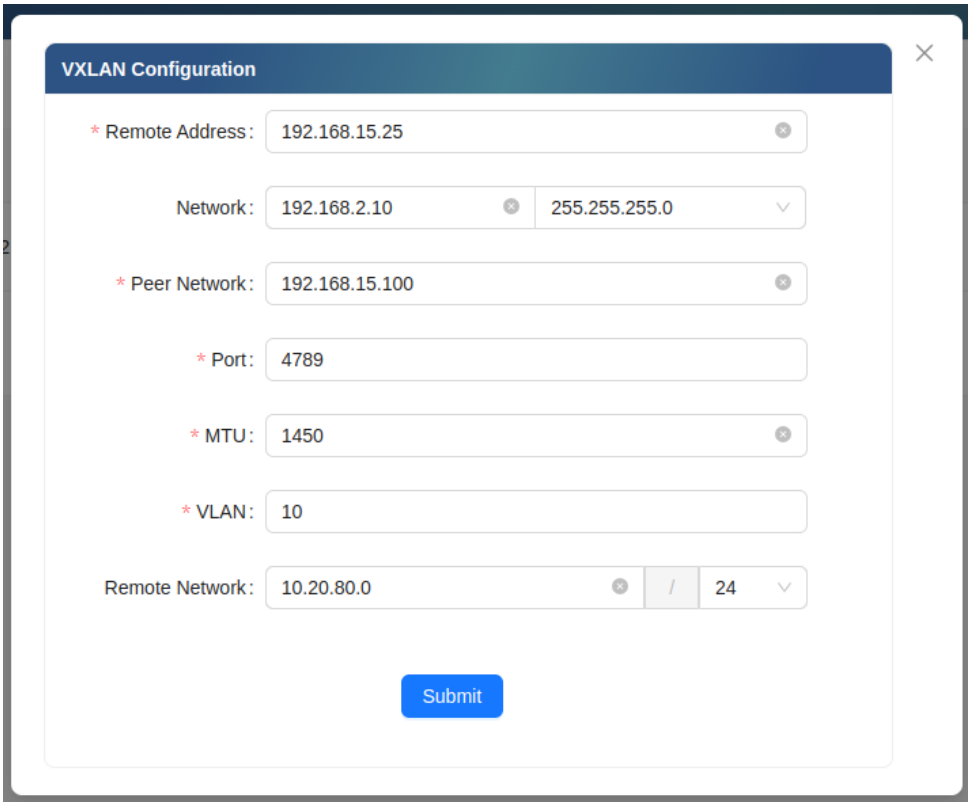
VXLAN (Virtual Extensible LAN): là một công nghệ mạng ảo hóa lớp 2, được thiết kế để khắc phục các hạn chế của mạng VLAN truyền thống trong môi trường trung tâm dữ liệu và mạng quy mô lớn. VXLAN cho phép tạo các mạng

ảo trên cơ sở hạ tầng IP hiện có, mở rộng khả năng phân đoạn mạng và cải thiện tính linh hoạt trong quản lý.

Bước 1: Từ giao diện quản lý → VPN → VXLAN.



Hình 91: Giao diện hiển thị cấu hình VXLAN

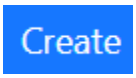


Hình 92: Giao diện cấu hình và giao diện hiển thị của VXLAN

- Trong đó:
  - **Remote Address:** Địa chỉ của IP Wan muốn tunnel đến
  - **Network:** Địa chỉ IP tunnel của thiết bị
  - **Peer Network:** Là IP tunnel của thiết bị lân cận
  - **Port:** Ưu tiên port 4789

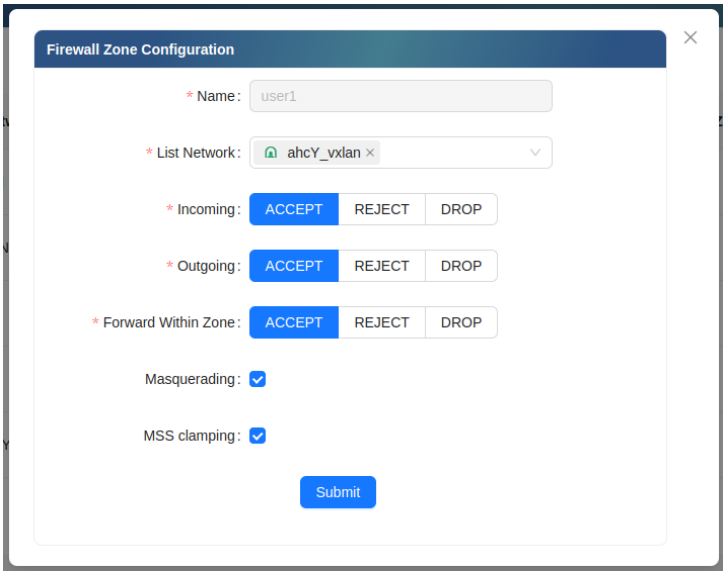
- **MTU:** Ưu tiên port 1450
- **VLAN:** Trong khoảng 1 -100
- **Remote Network:** địa chỉ br-lan của thiết bị lân cận

Bước 2: Thực hiện các thao tác:

- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong VXLAN.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình VXLAN.
- Kích chuột vào 

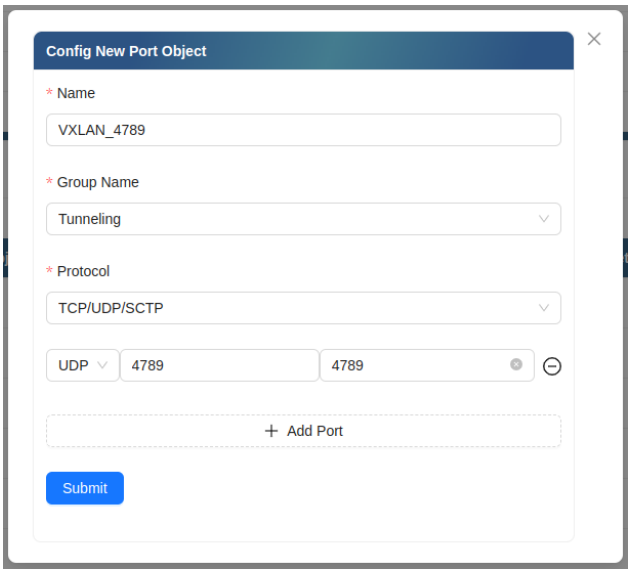
thực hiện cấu hình với giao thức VXLAN

Bước 3: Đối với NGFW thì ta cần allow port và accept tunnel vào firewall zone và firewall policy.



Hình 93: Firewall Zone add tun_vxlan

Bước 4: Add firewall zone accept cho tunnel vxlan giống như 1 cổng interface.



Hình 94: Cấu hình trong Port Object

- Cần tạo port object vxlan UDP port, chọn thường 4789.

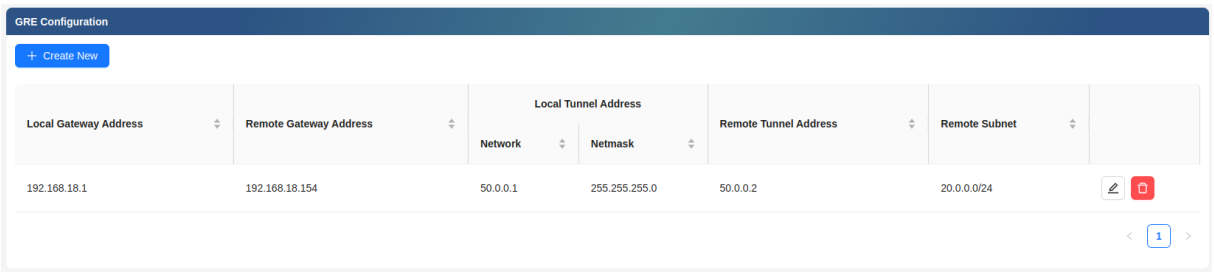
Note: Cần thực hiện 3 rule

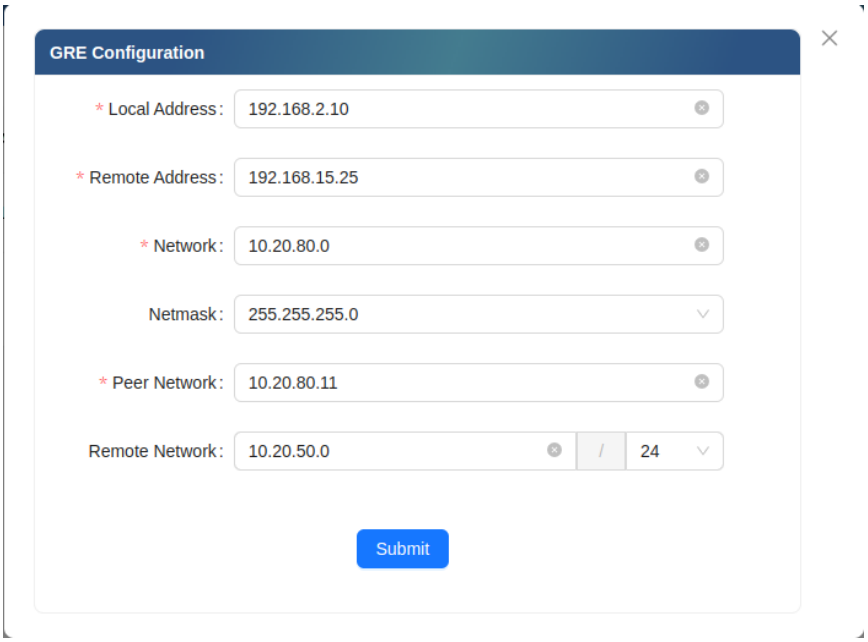
- allow traffic VXLAN proto (UDP port ...)
- add zone for interface VXLAN
- add rule forward traffic from zone VXLAN to zone wan

6.3 Tính năng GRE trên NGFW

Cấu hình GRE:

Bước 1: Từ giao diện quản lý → VPN → VXLAN.





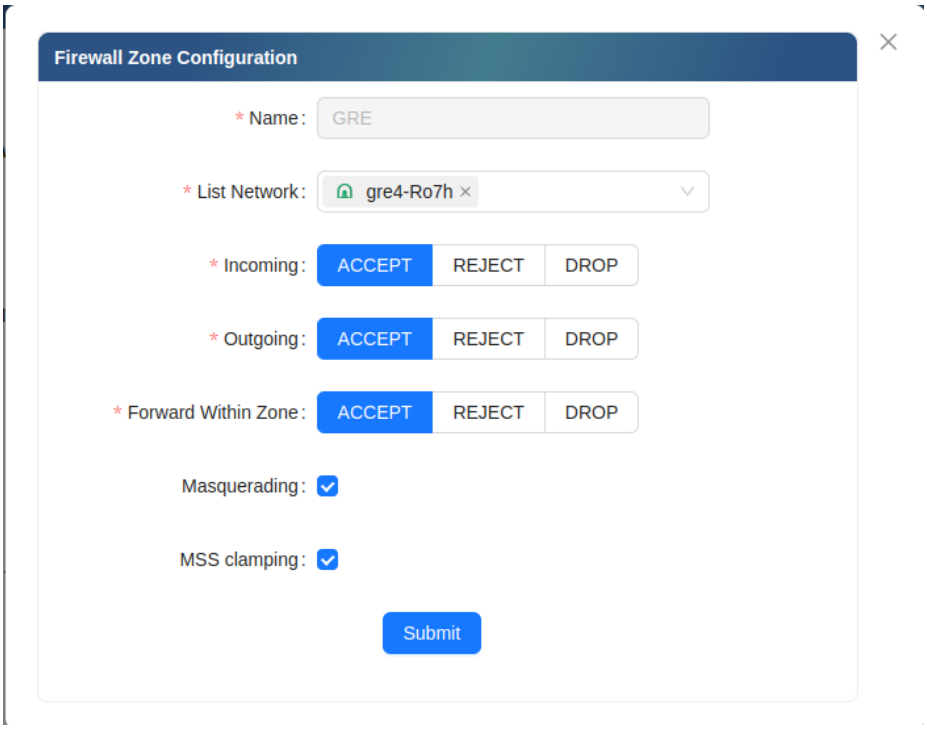
Hình 95: Giao diện hiển thị và giao diện cấu hình GRE

- Trong đó:
  - **Local Address:** Địa chỉ IP Wan của thiết bị
  - **Remote Address:** Địa chỉ IP Wan của Thiết bị muốn tunnel
  - **Network:** Địa chỉ IP tunnel của thiết bị
  - **Netmask:** Địa chỉ Netmask của tunnel của thiết bị
  - **Peer Network:** Địa chỉ tunnel bên kia
  - **Remote Network:** Địa chỉ br-lan bên muốn kết nối

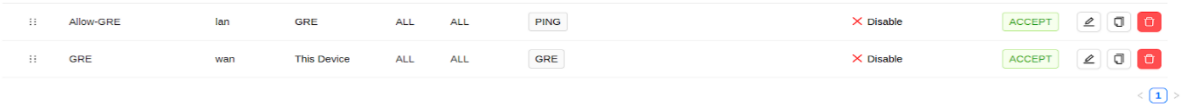
Bước 2: Thực hiện các thao tác:

- Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong VXLAN.
- Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình VXLAN.
- Kích chuột vào Create thực hiện cấu hình với giao thức VXLAN

Bước 3: Đối với Thiết bị NGFW thì cần add rule cho Firewall policy và Firewall zone ở 2 bên



Hình 96: Add rule trên Firewall ZONE



Hình 97: Tạo 2 rule để add cấu hình lên firewall policy

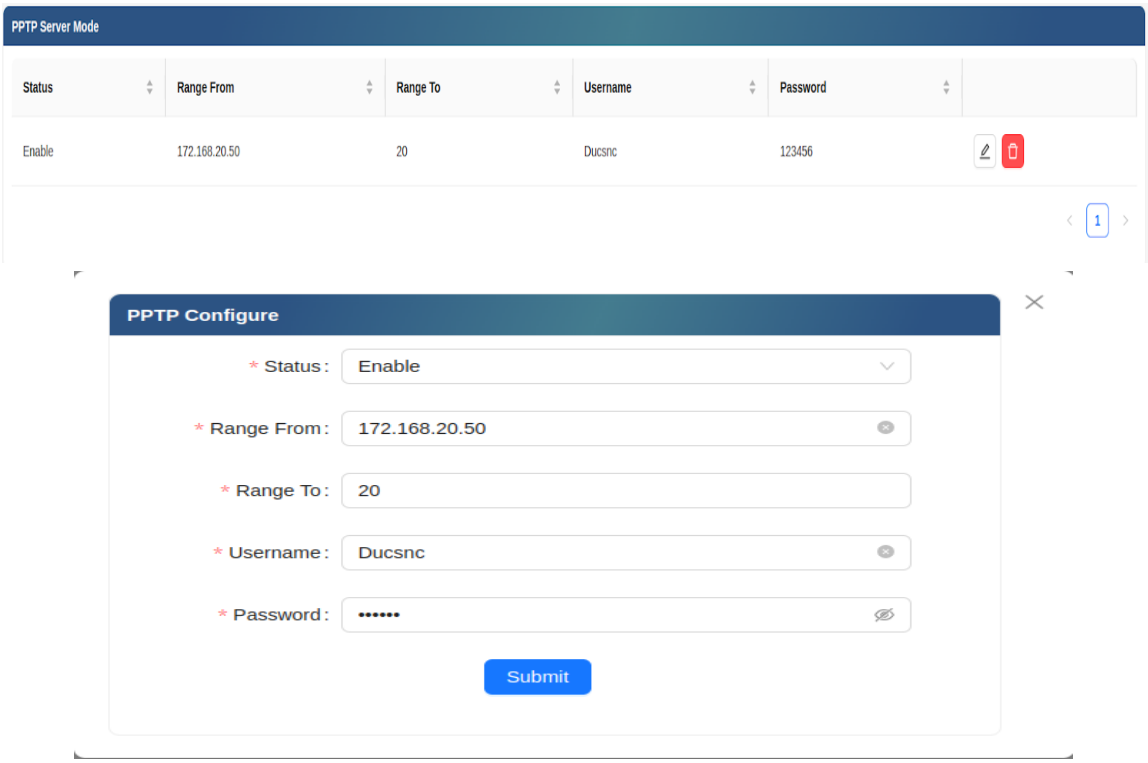
Note:

- allow traffic INPUT protocol GRE (proto 47)
- add zone cho interface GRE (ACCEPT all hoặc tùy chỉnh)
- add rule forward traffic src zone LAN, dest zone GRE

6.4 Tính năng PPTP trên NGFW

PPTP (Point-to-Point Tunneling Protocol) là một giao thức mạng được sử dụng để tạo các kết nối VPN (Virtual Private Network). PPTP cho phép người dùng từ xa kết nối an toàn đến mạng nội bộ của tổ chức qua Internet.

PPTP chia làm 2 phần **PPTP server**

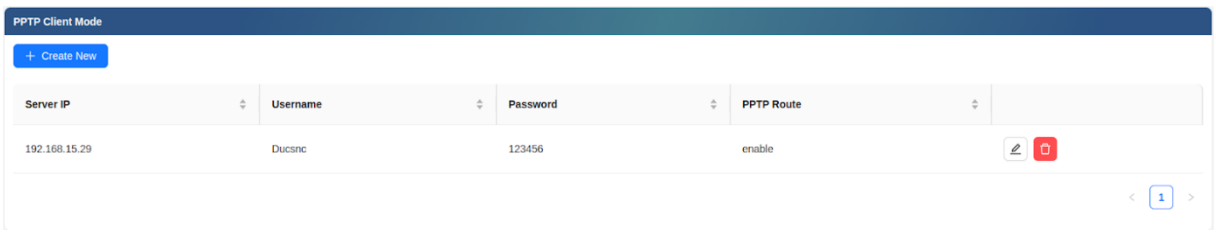


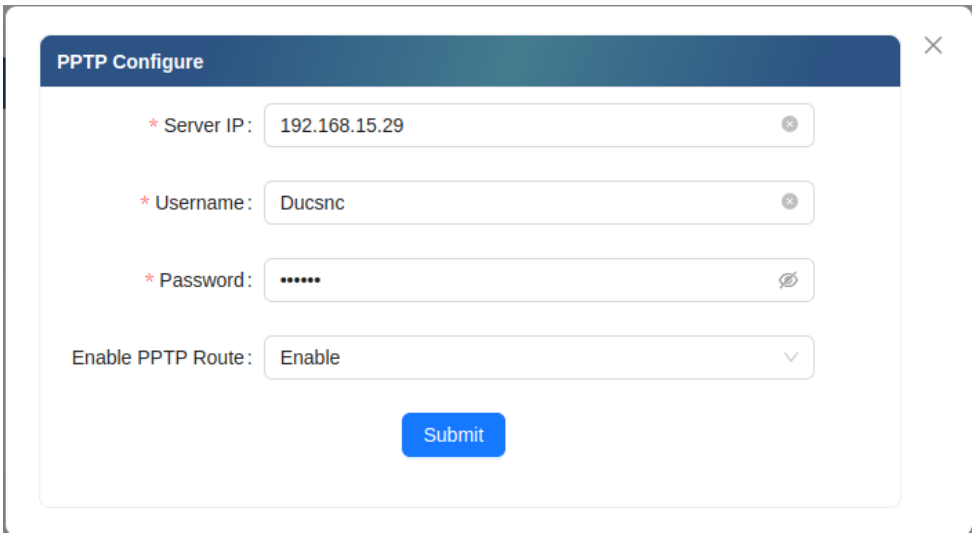
Hình 98: Giao diện cấu hình PPTP

❖ Trong Config PPTP server:

- **Status:** Trạng thái Enable hoặc Disable server.
- **Range From:** Địa chỉ IP
- **Range To:** Khoảng địa chỉ
- **Username:** Nhập username
- **Password:** Nhập password

PPTP Client:



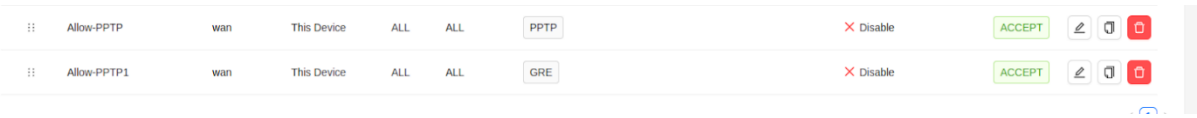


Hình 99: Giao diện cấu hình PPTP Client

- Trong Config PPTP client:
  - **Server IP:** Nhập IP Wan của PPTP server
  - **Username:** Nhập username
  - **Password:** Nhập password
  - Enable PPTP Route

Trong thiết bị NGFW cần cấu hình rule Firewall policy để cho phép allow ra bên ngoài kết nối tunnel:

- allow traffic PPTP (TCP port 1723)
- allow traffic GRE (IP protocol 47)
- add zone for interface PPTP
- add rule forward traffic from zone PPTP to Zone WAN



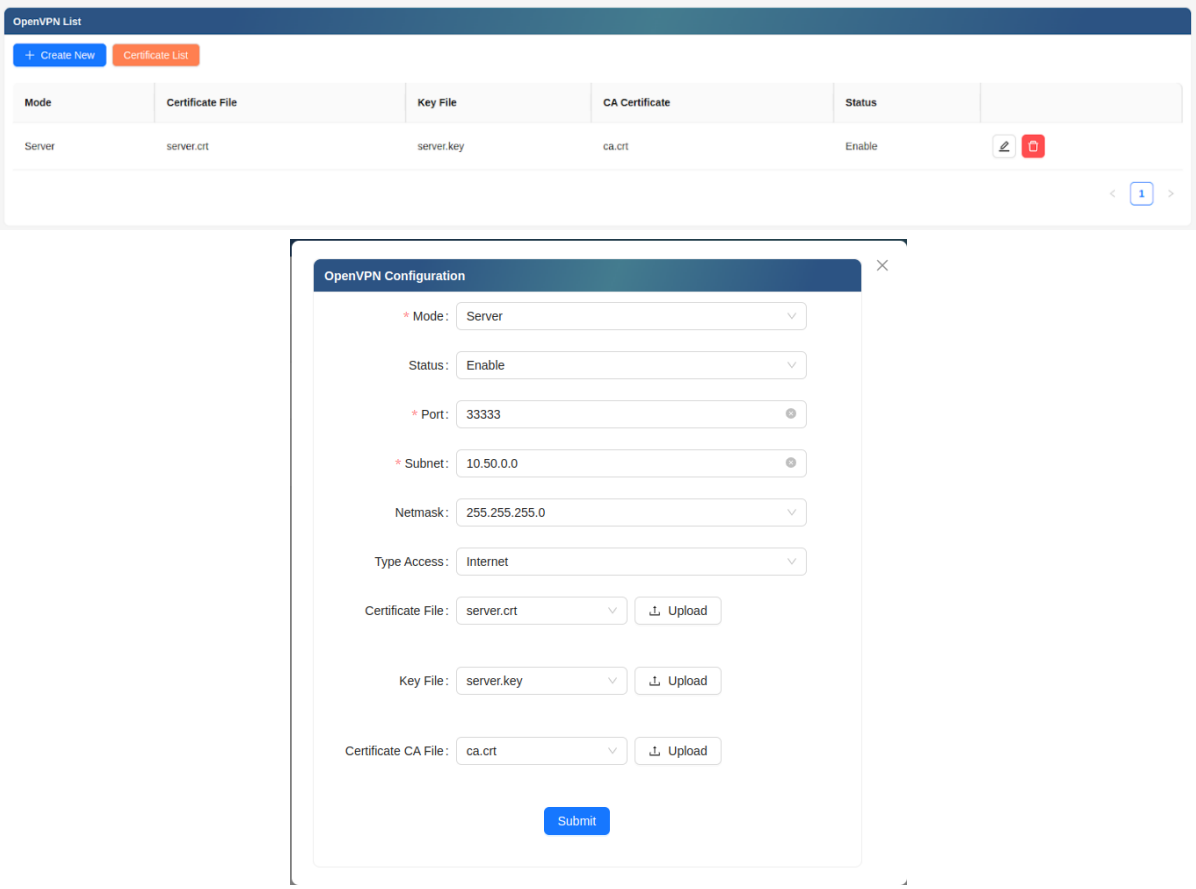
Hình 100:Cấu hình Rule Policy

6.5 Tính năng OpenVPN trong NGFW

OpenVPN là một phần mềm mã nguồn mở được sử dụng để tạo các kết nối mạng riêng ảo (VPN) an toàn và mạnh mẽ.

- Từ giao diện quản lý → VPN → OPENVPN
- Giao diện chia làm 2: OPENVPN server và OPENVPN client

6.5.1 OPENVPN server

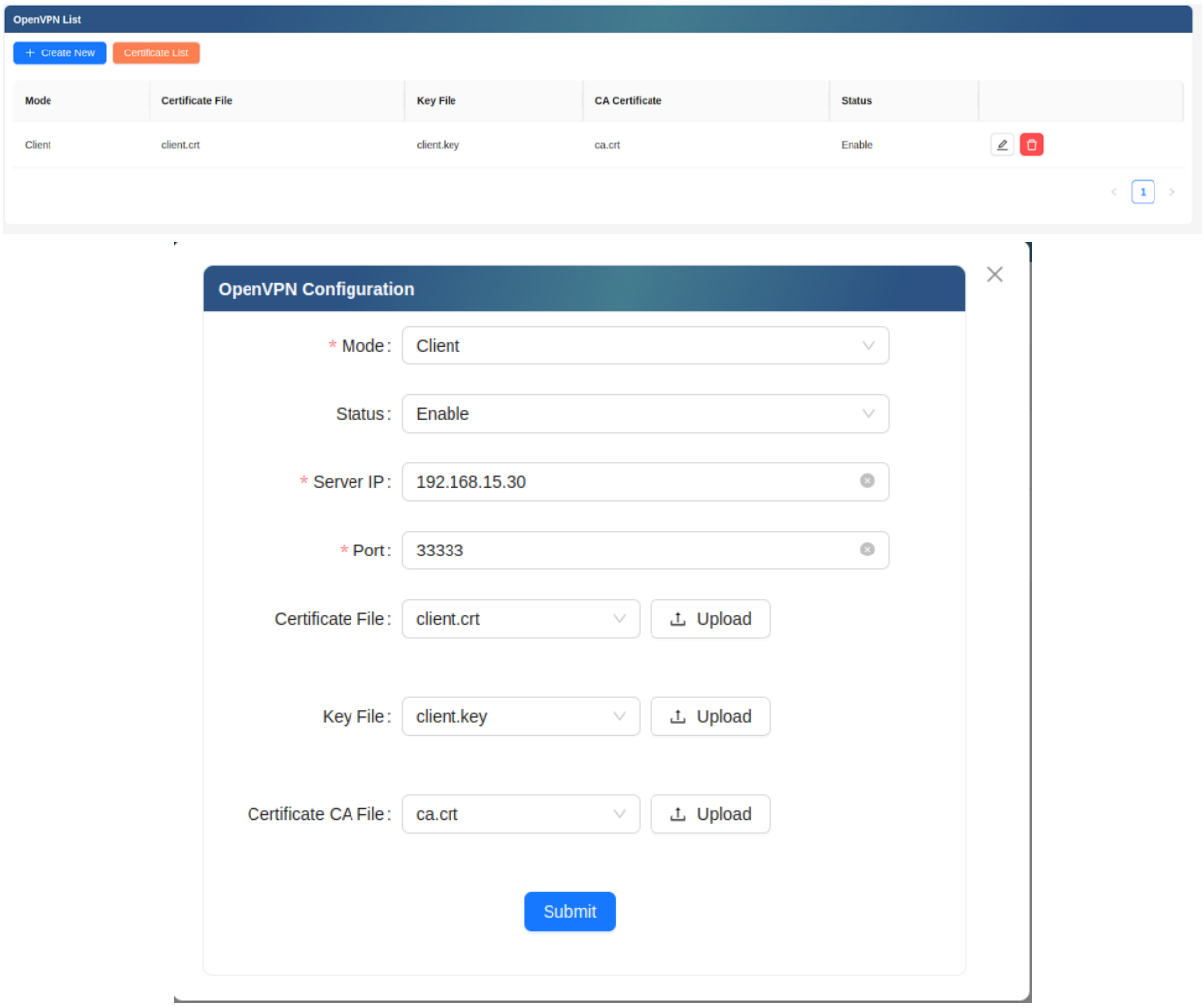


Hình 101: Cấu hình và config của OPENVPN

❖ Trong đó:

- **Mode:** Server và client
- **Status:** Enable và Disable
- **Port:** Nhập Port 1-65535
- **Subnet:** Nhập IP cho tunnel
- **Netmask:** Nhập IP netmask
- **Type Access:** Gồm home và internet: Khi cần tất cả lưu lượng mạng đi qua máy chủ VPN
- **Certificate File:** update crt
- **Key File:** update key
- **Certificate CA File:** update CA

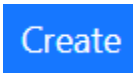
6.5.2 OPENVPN client

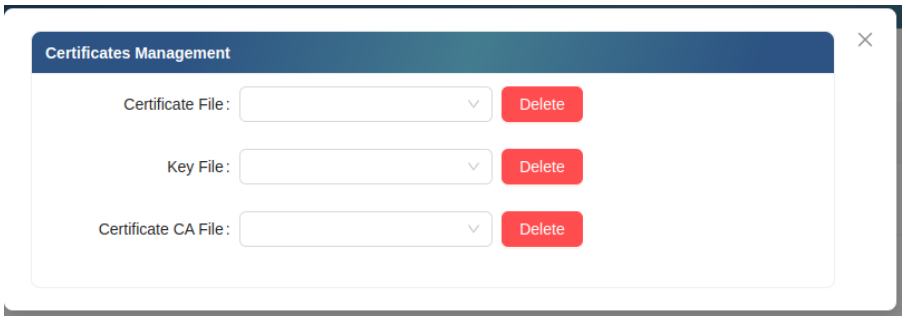


Hình 102: Giao diện cấu hình OPENVPN client

❖ Trong đó:

- **Mode:** Server và client
- **Status:** Enable và Disable
- **Server IP:** nhập IP server
- **Port:** nhập Port 1-65535
- **Certificate File:** update crt
- **Key File:** update key
- **Certificate CA File**: update CA

- Kích chuột vào  thực hiện tác vụ thay đổi thông tin cấu hình trong OPENVPN.
- Kích chuột vào  thực hiện tác vụ xóa thông tin cấu hình OPENVPN.
- Kích chuột vào  thực hiện cấu hình với giao thức OPENVPN.
- Để xóa các Certificate sử dụng giao diện:



Hình 103: Giao diện xóa certificate

Note: Để config OPENVPN cho thiết bị NGFW cần allow firewall policy và Firewall Zone.

- Cấu hình trên router server:
  - allow traffic INPUT protocol UDP và TCP port (theo cấu hình VPN).
  - add zone cho interface OpenVPN (ACCEPT all hoặc tùy chỉnh).
- Cấu hình trên router client:
  - allow traffic INPUT (UDP, TCP port ...)

(*) Nếu muốn router client truy cập mạng:

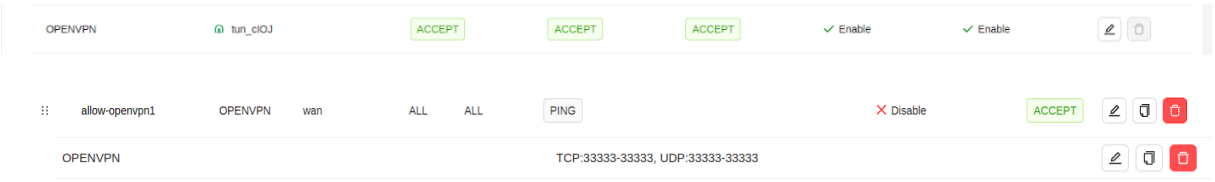
- Cấu hình trên router server:
  - add rule forward traffic src zone OpenVPN, dest zone WAN.

(*) Nếu muốn thiết bị phía sau router client truy cập mạng:

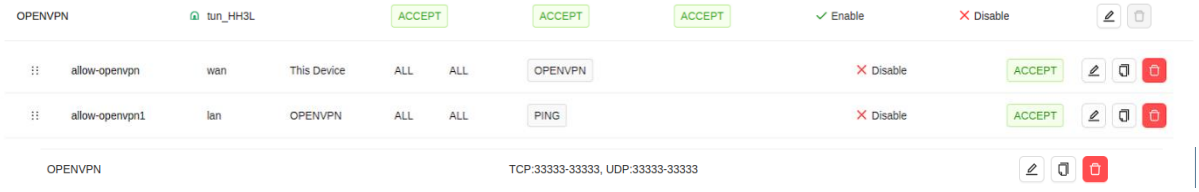
- Cấu hình trên router client:

- add zone cho interface OpenVPN, bật Masquerade.
- add rule forward traffic src zone LAN, dest zone OpenVPN.

Add rule OPENVPN-Server:



Add rule OPENVPN-client:

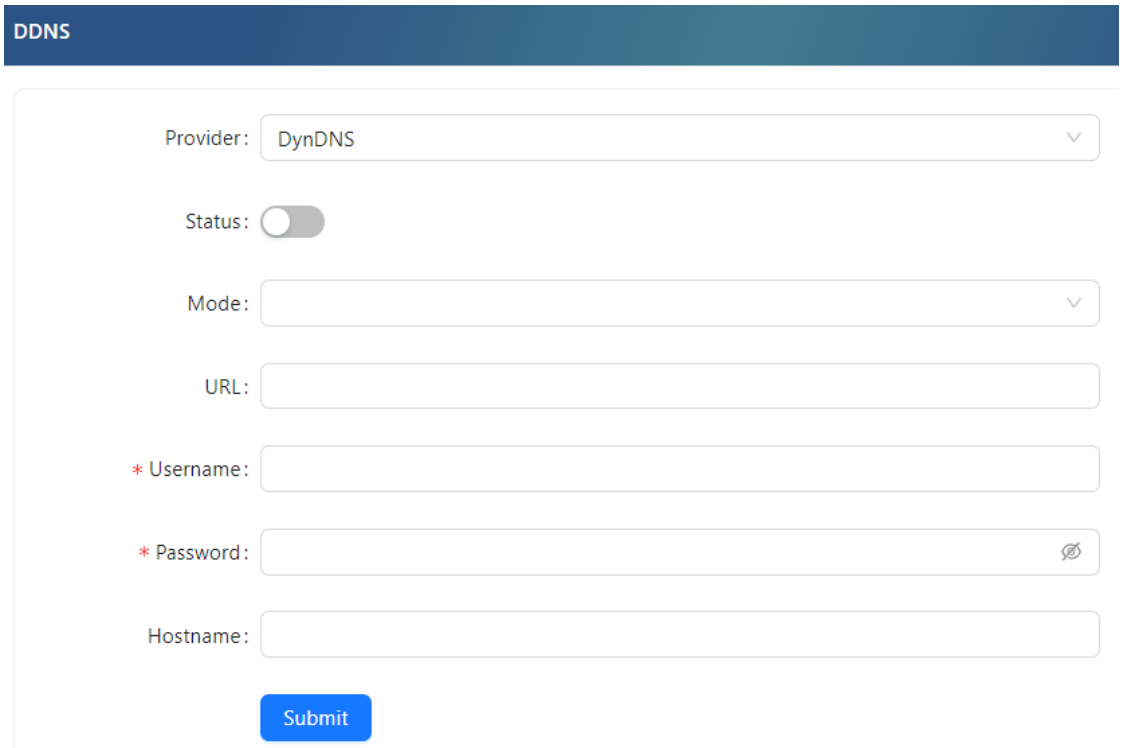


Tương tự như cấu hình rule firewall cho router server, router client, config rule ra mạng.

7 Cấu hình các dịch vụ (Service)

7.1 Cấu hình tính năng DDNS

❖ Từ giao diện quản lý → Service → Dynamic DNS:



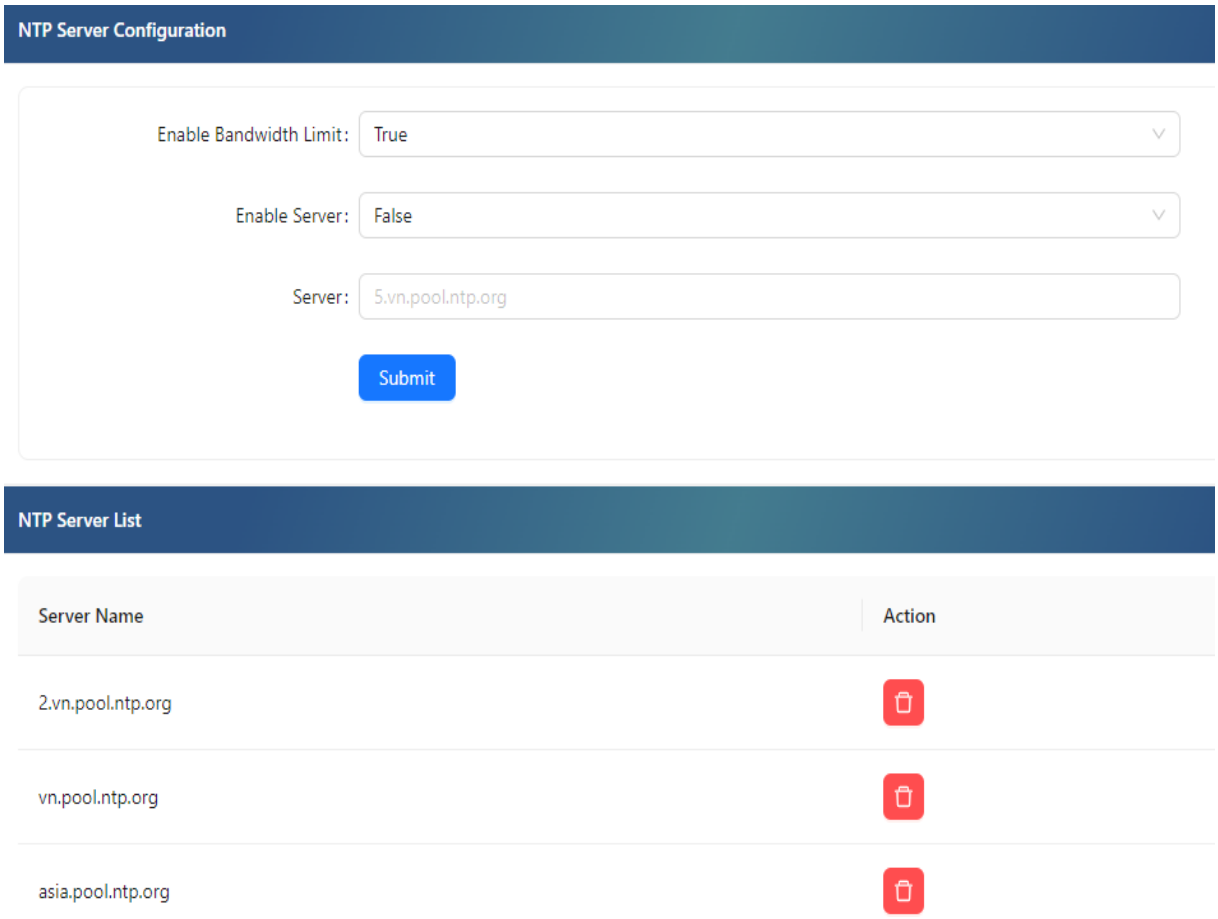
Hình 104: Giao diện cấu hình DDNS

❖ Trong đó:

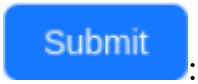
- **Enable:** Bật/tắt tính năng Dynamic DNS.
- **Username:** Tên đăng nhập của Dynamic DNS server.
- **Password:** Mật khẩu đăng nhập của Dynamic DNS.
- **Your domain:** Tên miền động muốn thiết lập cho thiết bị
- **Mode** (Provider URL/Customer URL)
- **Provider URL:** Cài đặt Dynamic DNS server:
- **Customer URL:** Cài đặt Dynamic DNS client:
- Điền thông tin URL tương ứng đối với Provider/Customer.
- **Submit:** Lưu cấu hình.

7.2 Cấu hình tính năng NTP

❖ Từ giao diện quản lý → Service → NTP:



Hình 105: Giao diện cấu hình NTP

❖ Kích chuột vào 

: Thực hiện thêm các miền DNS.

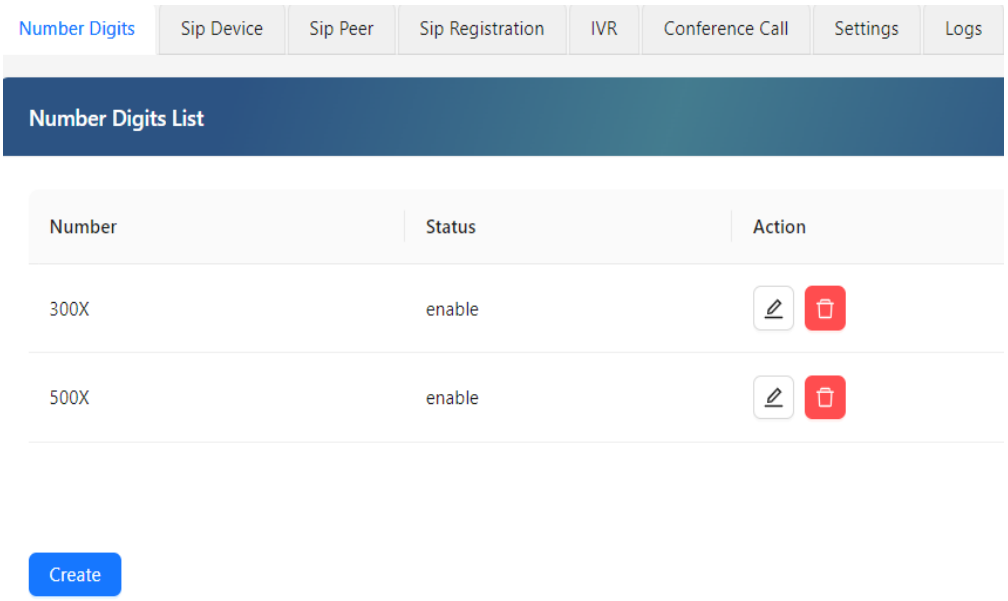
❖ Kích chuột vào  hiện xóa miền DNS.

7.3 Cấu hình tính năng Multimedia

Nhóm tính năng đa phương tiện bao gồm các dịch vụ call, video call, Message, voice mail, voice conferencing và dịch vụ tổng đài ảo IVR ở mục Service → MultiMedia:

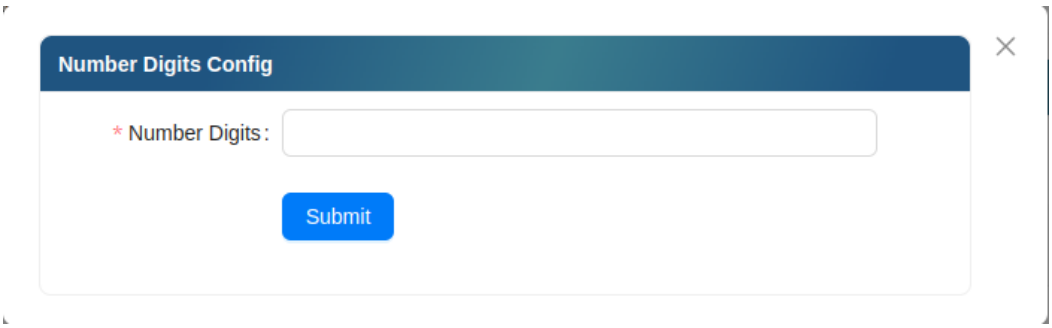
7.3.1 Cấu hình miền số trên NGFW (Number Digits)

❖ Kiểm tra trạng thái đầu số thuê bao đã được đăng ký trên NGFW bằng cách: Services → Multimedia → Number Digits:



Hình 106: Giao diện cấu hình tính năng Number Digits

- Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong Number Digits.
- Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình Number Digits.
- Kích chuột vào + Create New thực hiện cấu hình với giao thức Number Digits:

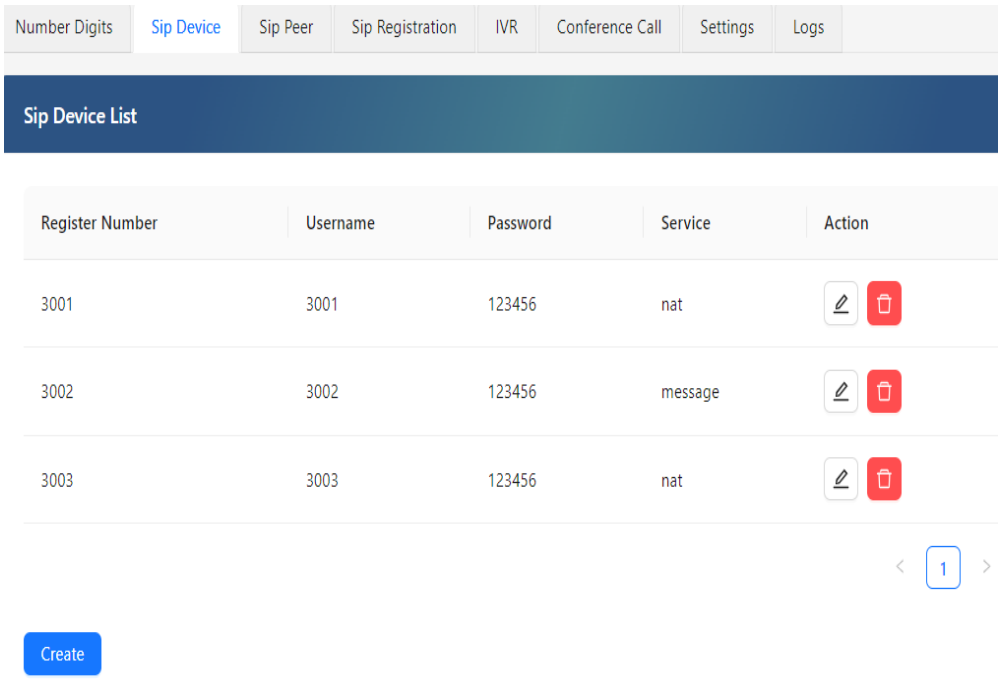


Hình 107: Giao diện cấu hình chi tiết Number Digits

- Trong đó:
  - **Number Digits:** Đầu số thuê bao đăng ký trên NGFW.
  - **Status (Enable/Disable):** Bật/tắt đầu số thuê bao đã đăng ký.

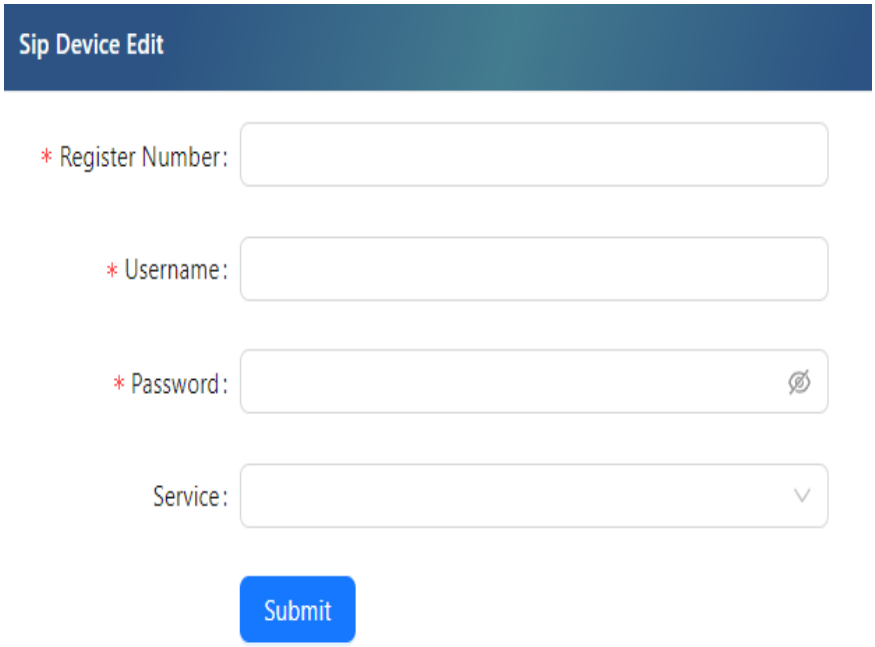
7.3.2 Cấu hình thuê bao cho người dùng trên NGFW quản lý (SIP Device)

Kiểm tra trạng thái thiết lập các số thuộc miền đầu số đã được đăng ký ở Number Digits trên NGFW ứng với từng user bằng cách: Services → Multimedia → SIP Device:



Hình 108: Giao diện cấu hình tính năng SIP Device

- Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong Sip Device.
- Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình Sip Device.
- Kích chuột vào Create thực hiện cấu hình với giao thức Sip Device:



Hình 109: Giao diện cấu hình chi tiết tính năng SIP Device

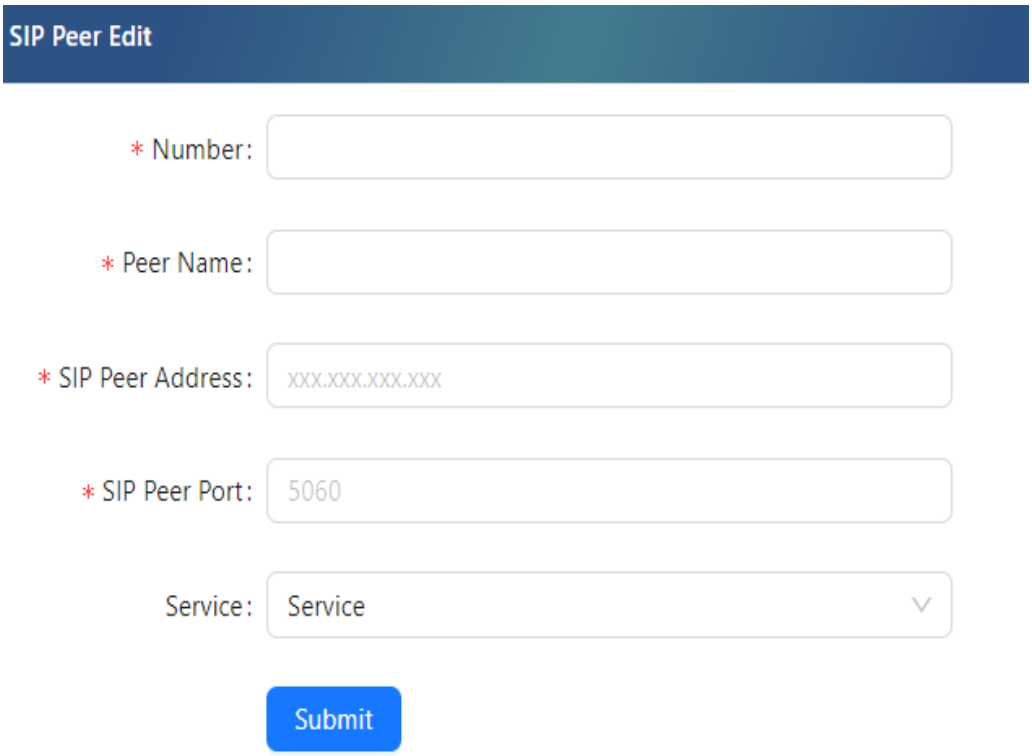
❖ Trong đó:

- **Register Number:** Đăng ký số cho người dùng (User) thuộc đầu số đã khai báo ở Number Digits.
- **Username:** Tên người dùng.
- **Password:** Thiết lập mật khẩu cho người dùng.
- **Service:** NAT/Message/Follow Me/All.
- **Submit:** Lưu cấu hinh

7.3.3 Thiết lập đường trung kế (TRUNK) trên một hay nhiều NGFW (SIP Peer)

❖ Kiểm tra trạng thái thiết lập đường trunk trên NGFW bằng cách: Từ giao diện quản lý → Service → Multimedia → Sip Peer:

❖ Kích chuột vào Create thực hiện thiết lập một đường Trunk trên LS-SMR-2506 E:



Hình 110: Giao diện cấu hình chi tiết tính năng SIP peer

❖ Trong đó:

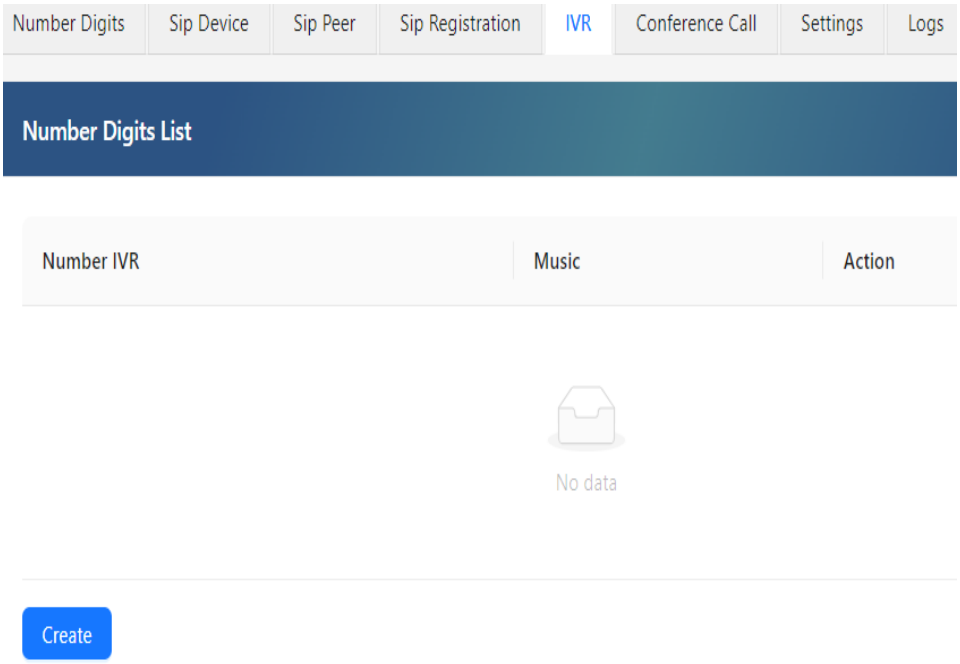
- **Number:** Đầu số thuê bao muốn thiết lập trên hai hay nhiều thiết bị với NGFW.

- **Peer Name:** Đặt tên cho đường trunk muốn thiết lập với LS-SMR-2506 E.
- **SIP Peer Address:** Địa chỉ IP của thiết bị muốn thiết lập đường Trunk với NGFW.
- **SIP Peer Port:** Default 5060.
- **Service:** NAT/Message/All:
- **Submit:** Lưu cấu hình.

7.4 Cấu hình dịch vụ tổng đài ảo (IVR) trên NGFW

Kiểm tra trạng thái IVR trên NGFW

❖ Từ giao diện quản lý → Services MultiMedia → IVR:

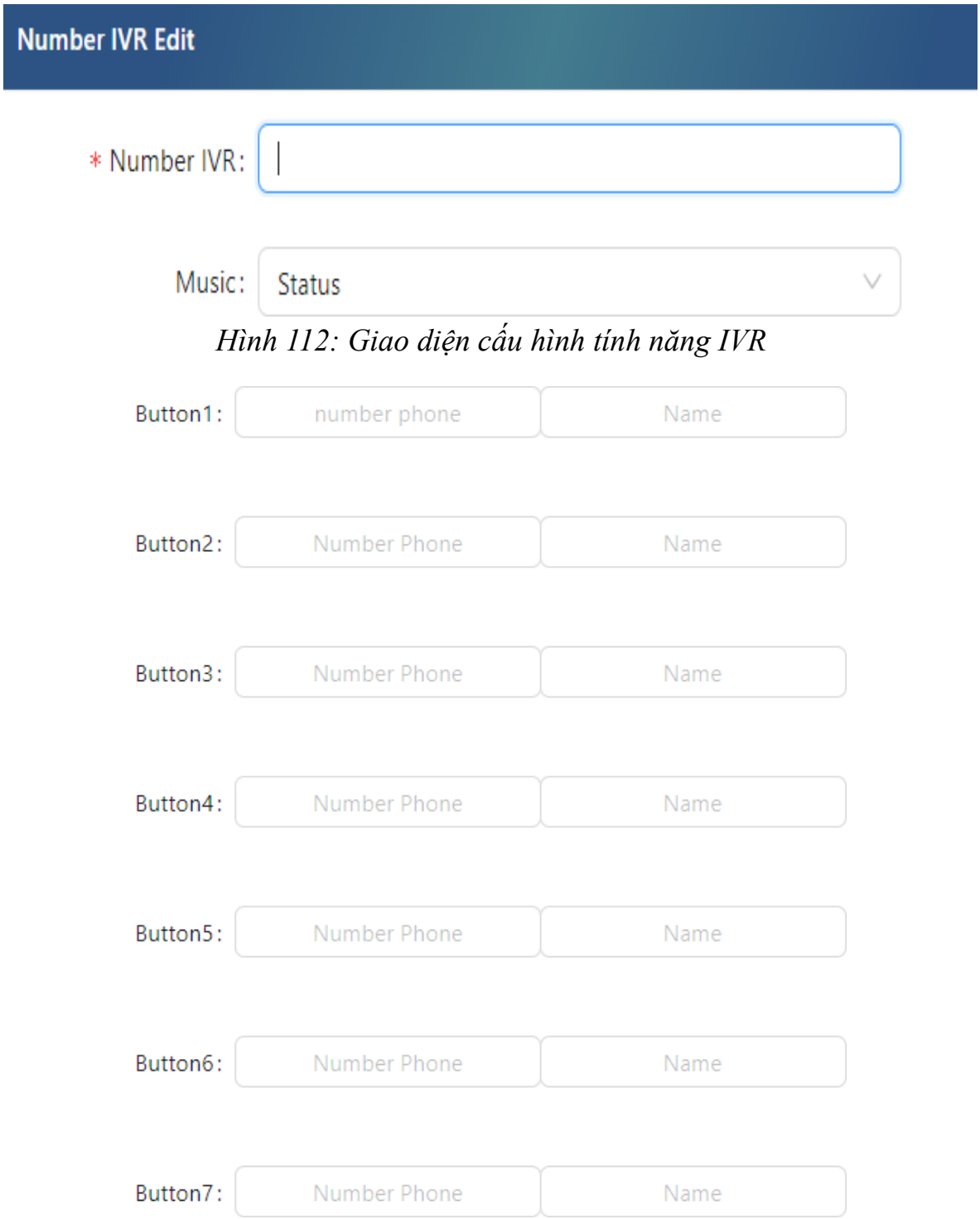


Hình 111: Giao diện hiển thị thông tin IVR

❖ Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong Sip Device.

❖ Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình Sip Device.

❖ Kích chuột vào Add thực hiện cấu hình với giao thức Sip Device:



Hình 112: Giao diện cấu hình tính năng IVR

Hình 113: Giao diện cấu hình chi tiết tính năng IVR

❖ Trong đó:

- **Number IVR:** Tạo số tổng đài IVR.
  - ***Status:*** Enabled để bật tính năng này.

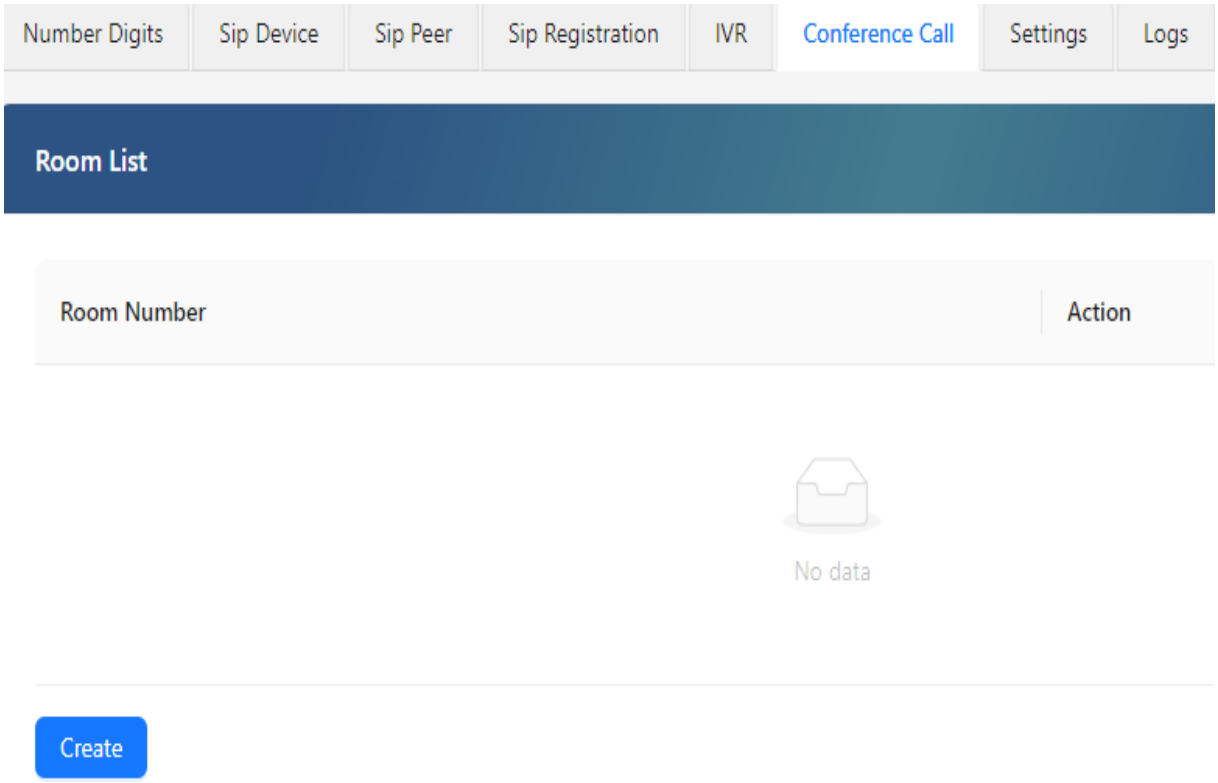
- ***Music:*** Thiết lập nhạc chờ, hướng dẫn người gọi thực hiện mong muốn theo thao tác phím.

- Tiếp theo thiết lập các đầu số user theo các phím tắt từ Button 1-Button 9.
- **Submit:** Lưu cấu hình.

7.5 Cấu hình dịch vụ gọi nhóm (Conference Call) trên NGFW

7.5.1 Kiểm tra trạng thái Conference Call trên NGFW

❖ Từ giao diện quản lý → Services → Multimedia → Conference Call:



Hình 114: Giao diện cấu hình tính năng Conference call

❖ Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong Conference Call.

❖ Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình Conference Call.

❖ Kích chuột vào Create thực hiện cấu hình với giao thức Conference Call.

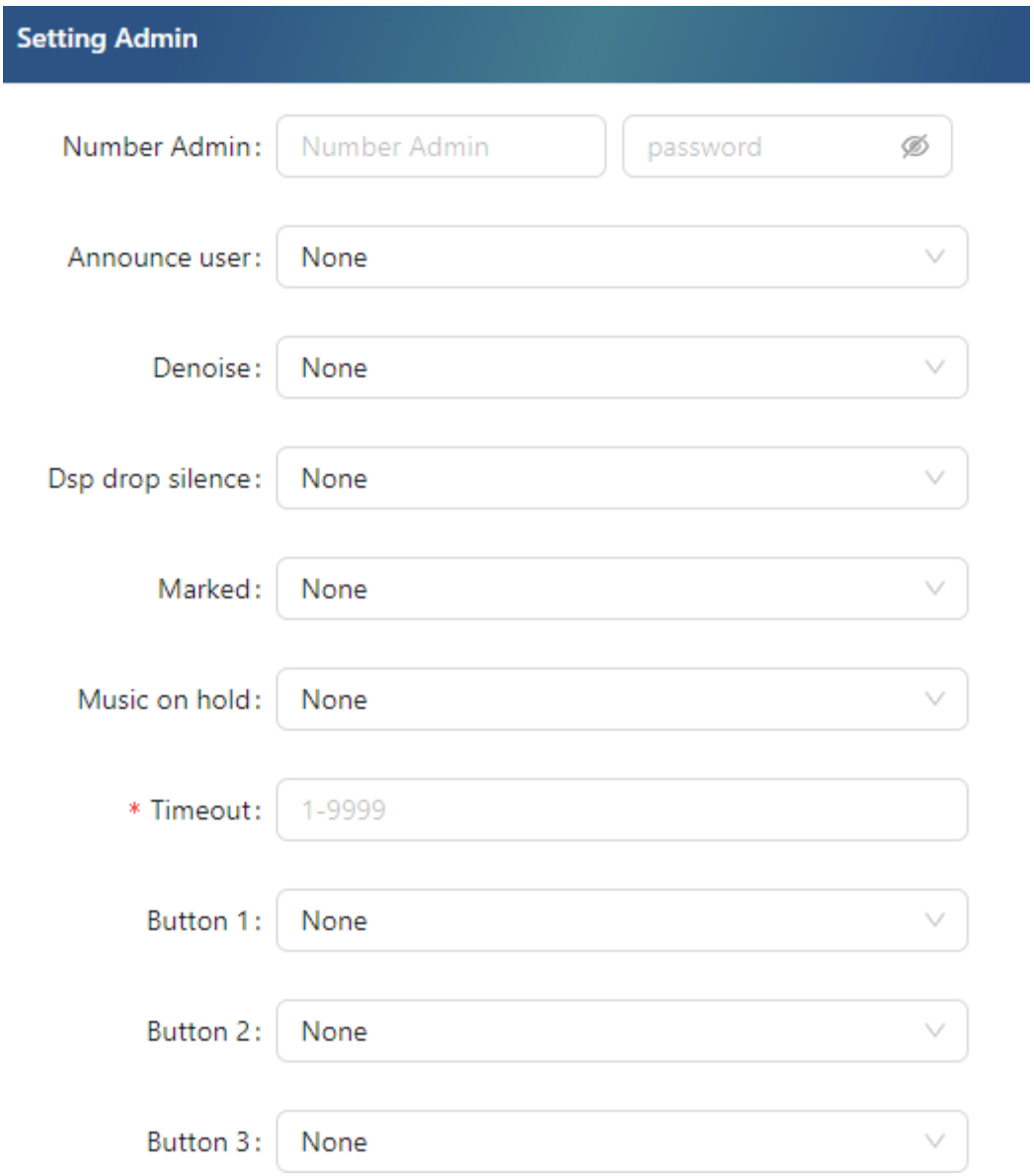
❖ Trong đó:

- **Room Number:** Số phòng.
- **Setting Room:** Thiết lập chính sách cho Root

❖ Trong đó:

- **Max members:** Số lượng thành viên tối đa một phòng.
- **Mixing Interval:** Đặt thời gian (ms) giúp âm thanh có độ trễ nhỏ nhất.
- **Interval sample rate:** Thiết lập tốc độ lấy mẫu gốc.
- **Record conference:** Bật/tắt ghi âm hội thoại.
- **Video mode:** Bật/tắt chế độ video cho phòng

7.5.2 Setting Admin: Thiết lập chính sách của Admin.

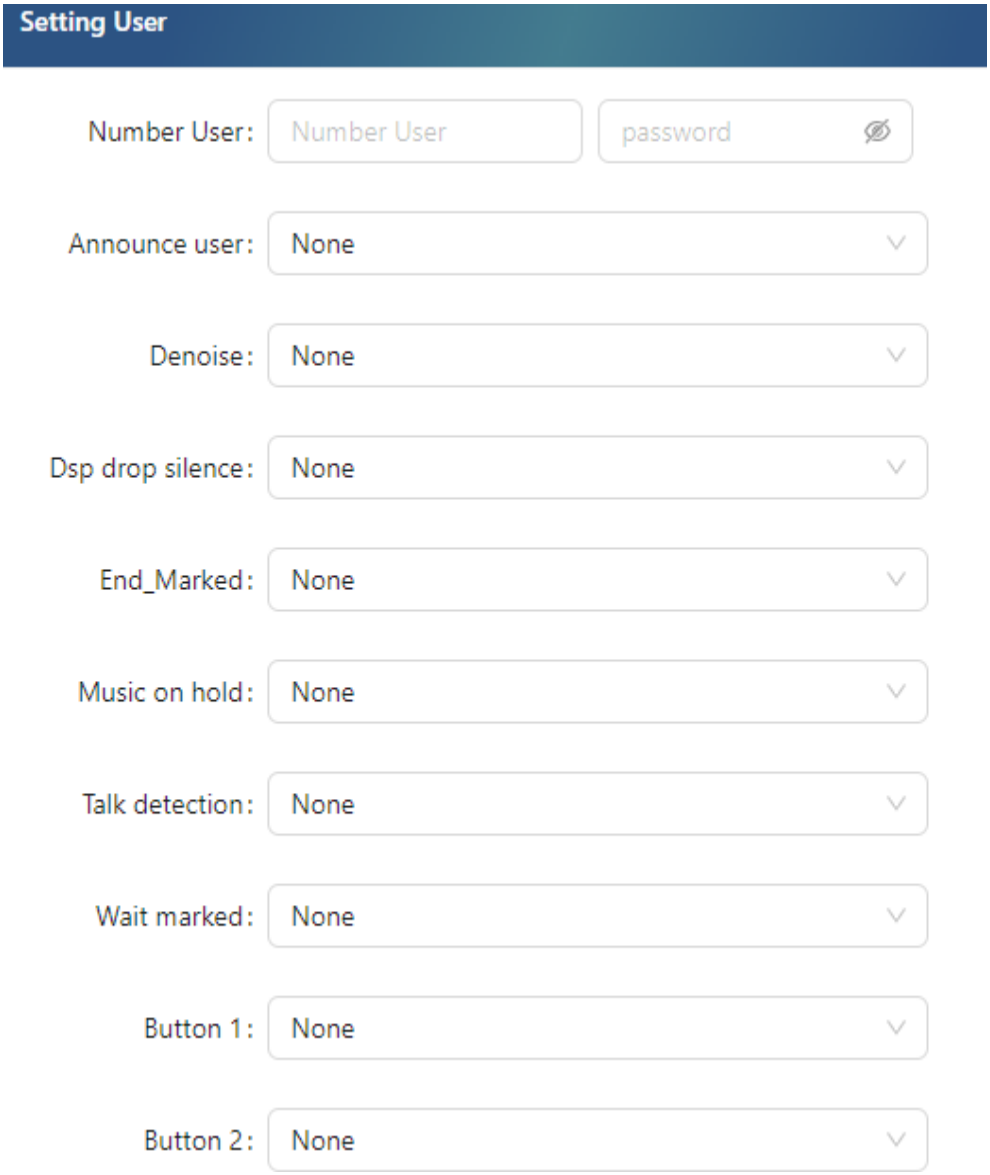


Hình 115: Giao diện cấu hình "Setting Admin"

❖ Trong đó:

- **Number Admin:** Thiết lập đầu số và password cho admin.
- **Announce user count (Enable/Disable):** Bật/tắt tính năng thông báo cho User trên NGFW.
- **Denoise (Enable/Disable):** Bật/tắt tính Denoise trên Conference Call.
- **Dsp drop silence (Enable/Disable):** Bật/tắt tính năng Dsp drop silence cho Conference Call.
- **Market (Enable/Disable):** Bật/tắt tính năng Mark trên Conference Call.
- **Music on hold when empty (Enable/Disable):** Bật/tắt tính năng Music on hold when empty trên Conference Call.
- **Timeout:** Thiết lập thời gian cho Conference Call.
- **Button:** Thiết lập các phím dành riêng cho admin: Enable/Disable - Bật/Tắt trên từng option từ Button 1 – 9.

7.5.3 Setting User: Thiết lập chính sách cho user khi tham gia vào Conference Call



Hình 116: Giao diện cấu hình "Setting User"

❖ Trong đó

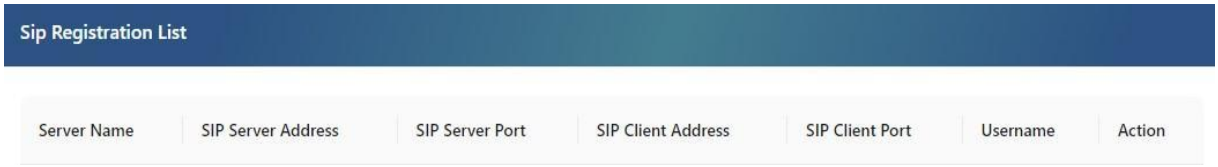
- **Number User:** Thiết lập đầu số và password cho admin.
- **Announce user count (Enable/Disable):** Bật/tắt tính năng thông báo cho User trên NGFW.
- **Denoise (Enable/Disable):** Bật/tắt Denoise trên Conference Call.
- **Dsp drop silence (Enable/Disable):** Bật/tắt tính năng Dsp drop silence cho Conference Call.

- **Markd (Enable/Disable):** Bật/tắt tính năng Markd trên Conference Call.
- **Music on hold when empty (Enable/Disable):** Bật/tắt tính năng Music on hold when empty trên Conference Call.
- **Talk detection events (Enable/Disable):** Bật/tắt tính năng Talk detection events trên trên Conference Call.
- **Wait_marked (Enable/Disable):** Bật/tắt tính năng Wait_marked trên trên Conference Call.
- **Button:** Thiết lập các phím dành riêng cho admin: Enable/Disable - Bật/Tắt trên từng option từ Button 1 – 9.
- **Submit:** Lưu cấu hình.

7.6 Cấu hình dịch vụ SIP Registration

Kiểm tra trạng thái SIP Registration trên NGFW

❖ Từ giao diện quản lý → Service → Multimedia → SIP Registration:

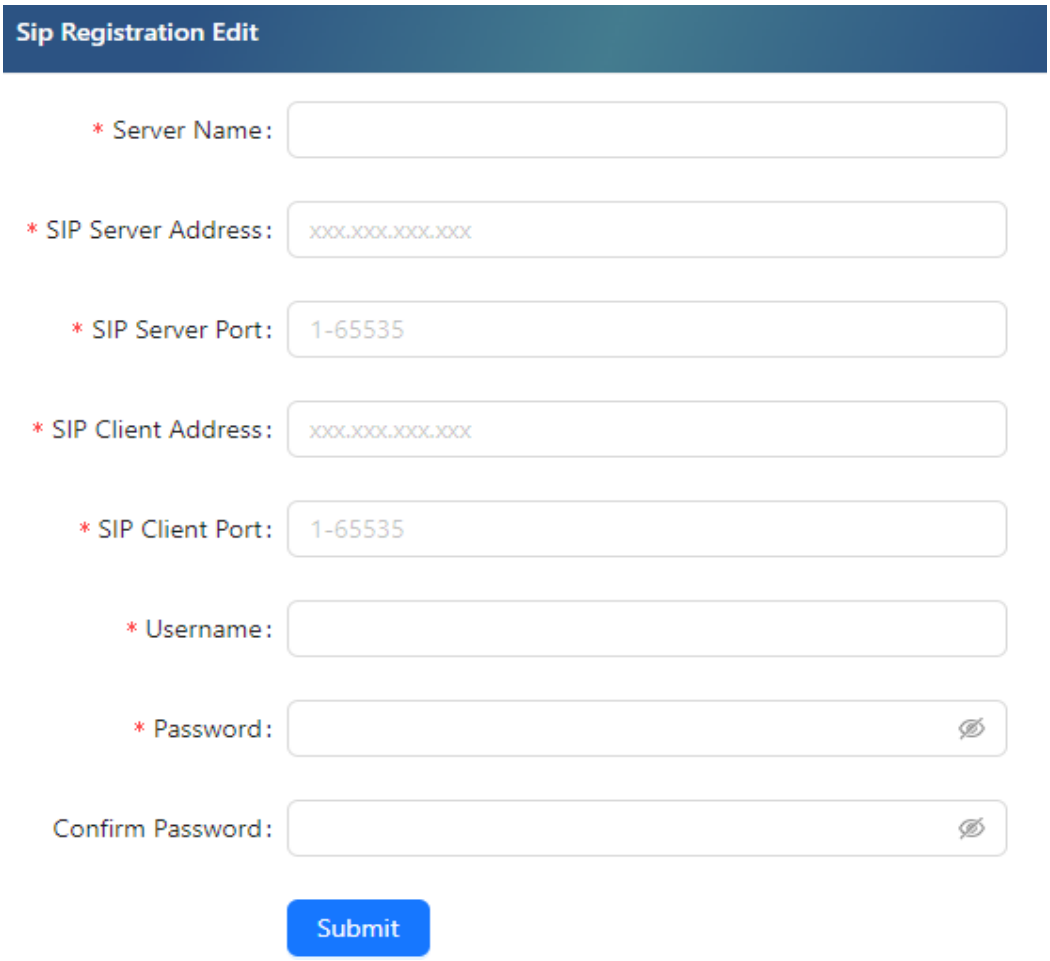


Hình 117: Giao diện hiển thị thông tin cấu hình SIP Registration

❖ Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong SIP Registration.

❖ Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình SIP Registration.

❖ Kích chuột vào Create thực hiện cấu hình với giao thức SIP Registration:



Hình 118: Giao diện cấu hình SIP Registration

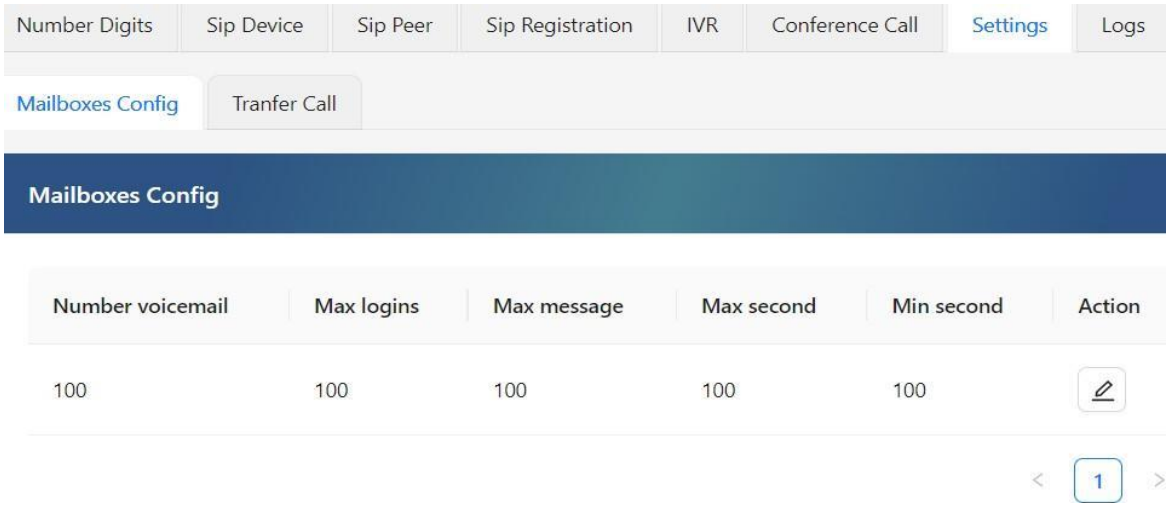
❖ Trong đó:

- **Status (Enable/Disable):** Bật/Tắt tính năng SIP Registration trên LS- SMR-2506 E.
- **Server Name:** Tên Server NGFW kết nối.
- **SIP Server Address:** Địa chỉ IP của Server.
- **SIP Server Port:** Giá trị Port SIP của Server.
- **SIP Client Address:** Địa chỉ IP của Client.
- **Username:** Tên người dùng.
- **Password:** Đặt mật khẩu cho người dùng.
- **Confirm Password:** Xác nhận mật khẩu vừa thiết lập cho người dùng
- **Submit:** Lưu cấu hình.

7.7 Cấu hình dịch vụ Mailboxes Digits (Settings)

Kiểm tra trạng thái Setting trên NGFW

❖ Từ giao diện quản lý → Services → Multimedia → Setting:



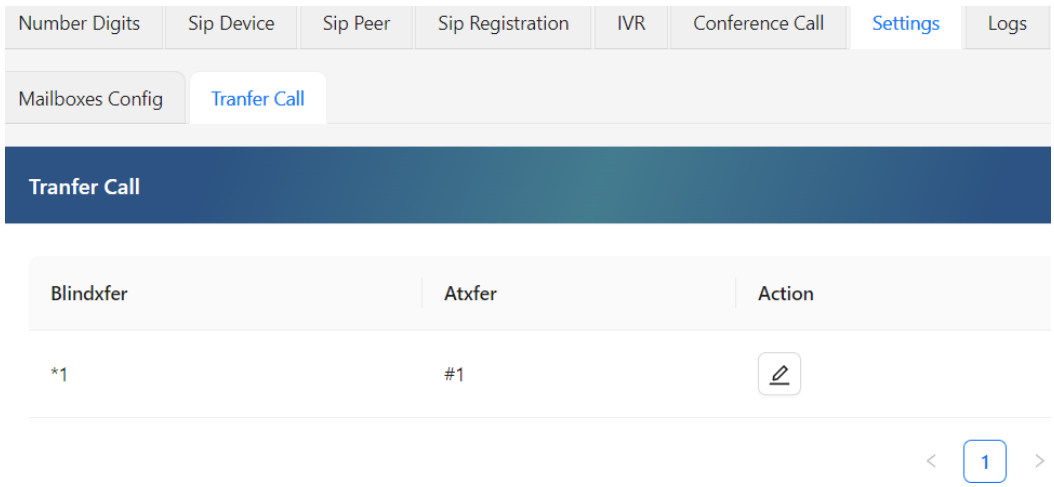
Hình 119: Giao diện hiển thị thông tin Transfer Call & Mailboxes

❖ Kích chuột vào thực hiện tác vụ thay đổi thông tin cấu hình trong Mailboxes Digits.

❖ Kích chuột vào thực hiện tác vụ xóa thông tin cấu hình Mailboxes Digits.

❖ Kích chuột vào Create thực hiện cấu hình với giao thức Mailboxes Digits.

7.7.1 Transfer Call

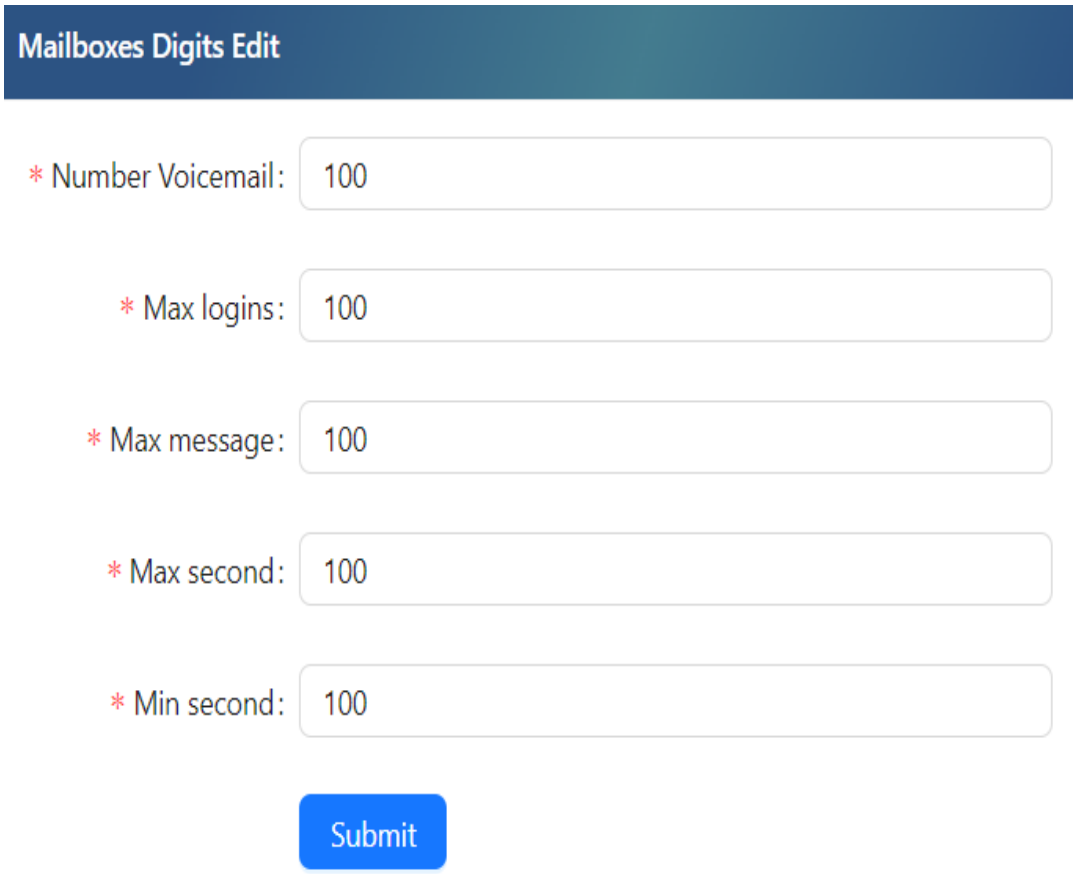


Giao diện cấu hình Transfer Call

❖ Trong đó:

- **Blindxfer:** Thiết lập đầu số chuyển hướng cuộc gọi.
- **Atxfer:** Thiết lập đầu số tham gia cuộc gọi.
- **Submit:** Lưu cấu hình.

7.7.2 Mailboxes Config



Hình 120: Giao diện cấu hình Mailboxes Config

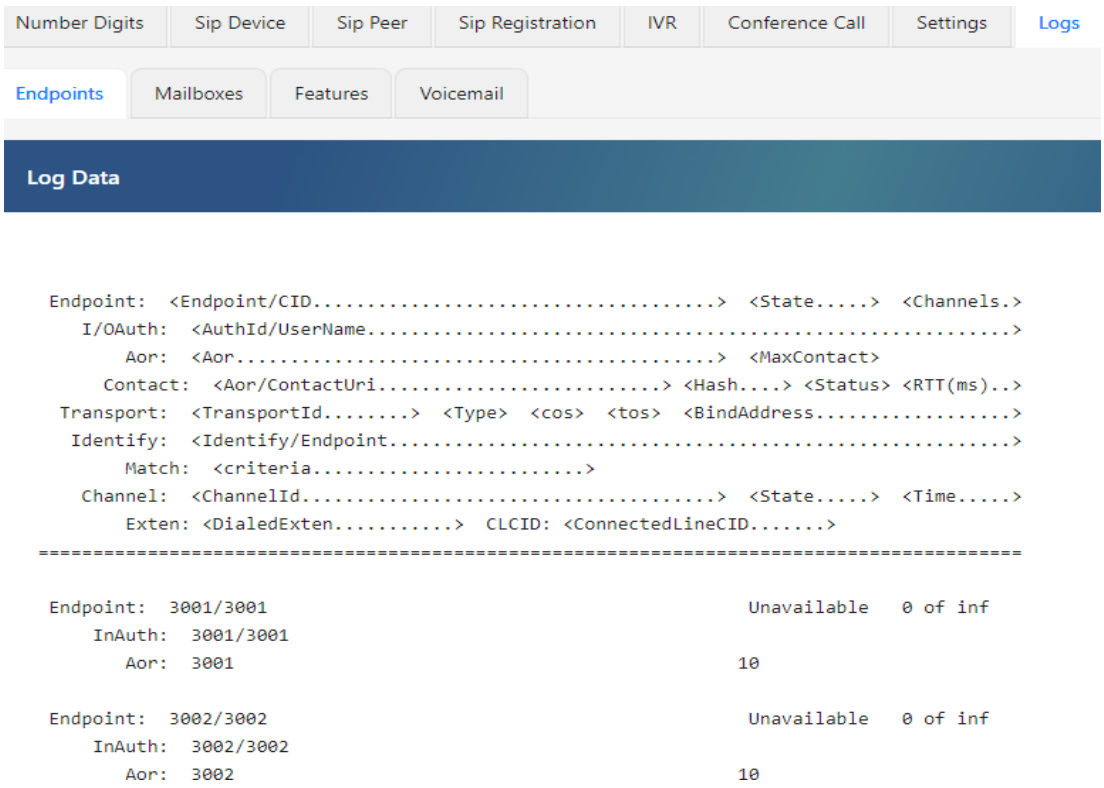
❖ Trong đó:

- **Status (Enable/Disable):** Bật/tắt tính năng Mailboxes Digits NGFW.
- **Number Voicemail:** Thiết lập số thực hiện tính năng Voicemail.
- Thực hiện các thiết lập với Max login, Max message, Max second & Min second.
- **Submit:** Lưu cấu hình.

7.8 Kiểm tra thông tin cấu hình đa phương tiện trên NGFW

Giao diện hiển thị thông tin các tham số đã cấu hình trên NGFW

❖ Từ giao diện quản lý Services → Multimedia → Log:

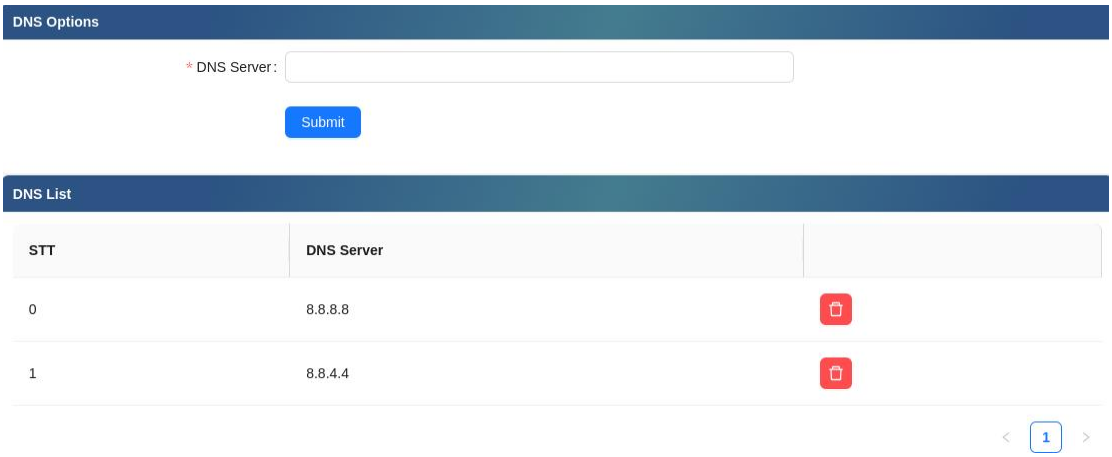


Hình 121: Giao diện hiển thị log

7.9 Cấu hình tính năng DNS

7.9.1 Giao diện cấu hình và hiển thị DNS

❖ Truy cập trình quản lý → Service → DNS:



Hình 122: Giao diện cấu hình DNS

❖ Kích chuột vào Submit: Thực hiện thêm các miền DNS.

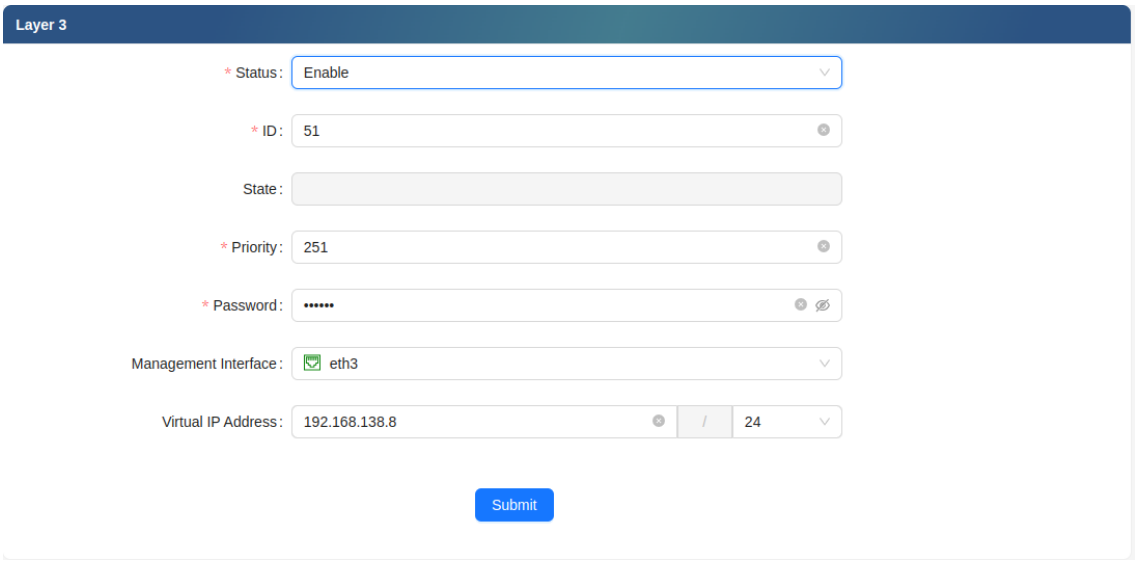
❖ Kích chuột vào  hiện xóa miền DNS.

8 Cấu hình tính năng High Availability

8.1 Cấu hình tính năng HA ở layer 3

Tính năng HA Layer 3 của NGFW được LANCS phát triển

❖ Truy cập vào HA → Layer 3.



Hình 123: Giao diện cấu hình HA Layer 3

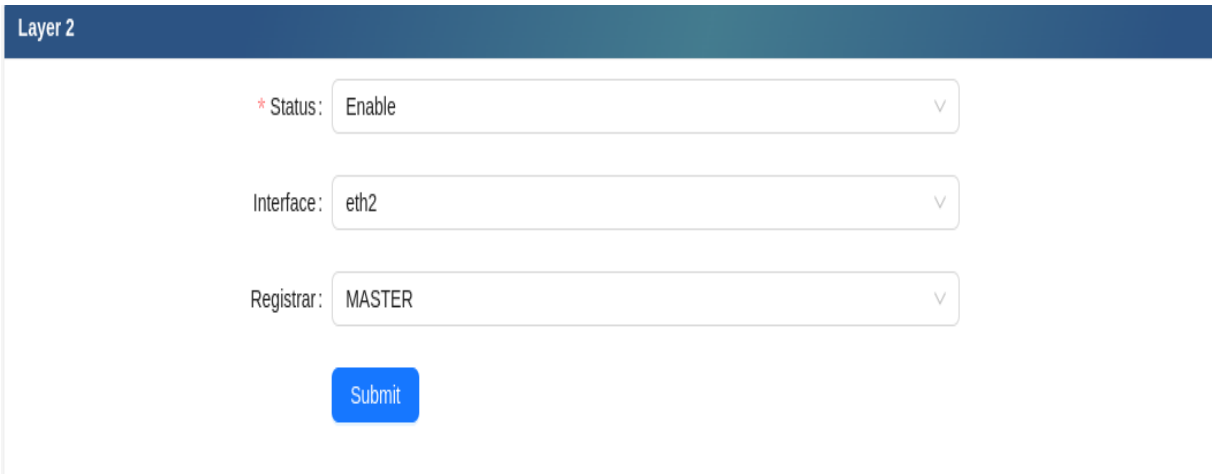
❖ Trong đó:

- **Enable/Disable**: Bật/tắt tính năng
- **ID**: Nhập giá trị ID
- **Priority**: Nhập giá trị ưu tiên
- **Password**: Nhập giá trị password
- **Management Interface**: Tên interface vật lý sử dụng
- **Virtual IP Address**: Nhập giá trị Virtual IP

8.2 Cấu hình tính năng HA ở layer 2

Tính năng HA Layer 2 của NGFW được LANCS phát triển tương ứng với mode Active-Passive

❖ Truy cập vào HA → Layer 2.



Hình 12420: Giao diện cấu hình HA Layer2

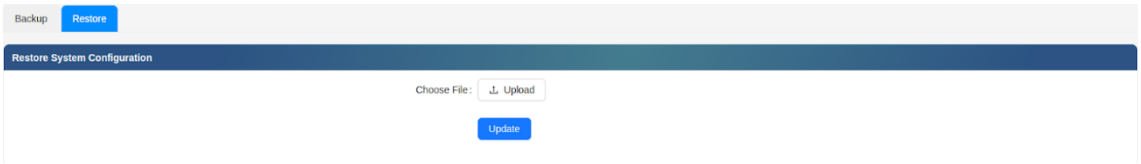
❖ Trong đó:

- **Enable/Disable:** Bật/tắt tính năng
- **Ifname:** Tên interface vật lý sử dụng
- **Registrar:** Đặt vai trò Master/Slave

9 Cấu hình nhóm tính năng System

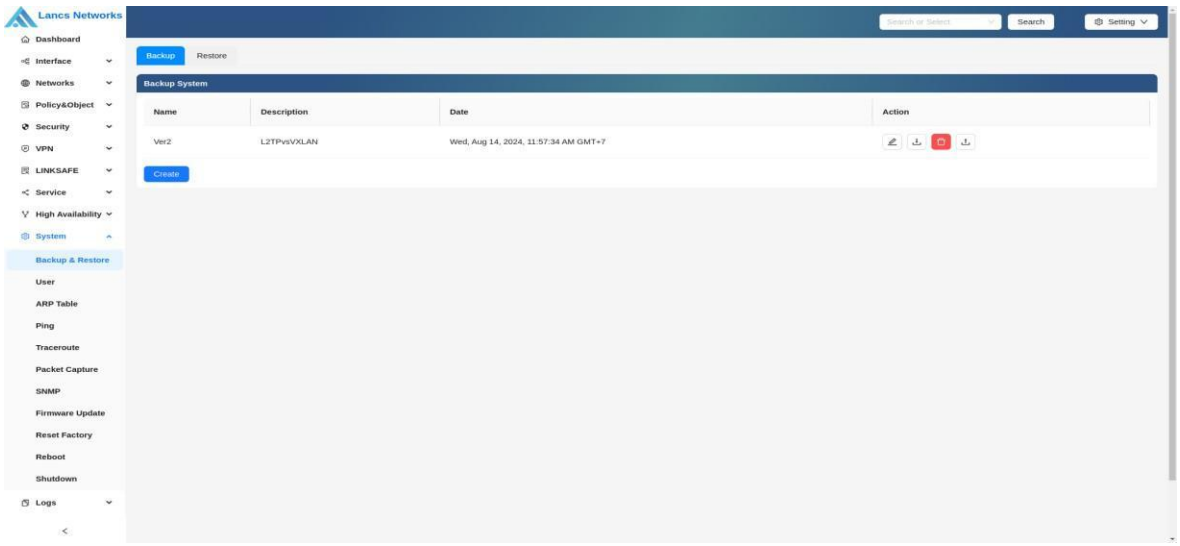
9.1 Cấu hình tính năng Backup & Restore

Tính năng lưu lại cấu hình Backup đề phòng khi thiết bị gặp lỗi và tính năng upload lại file cấu hình.



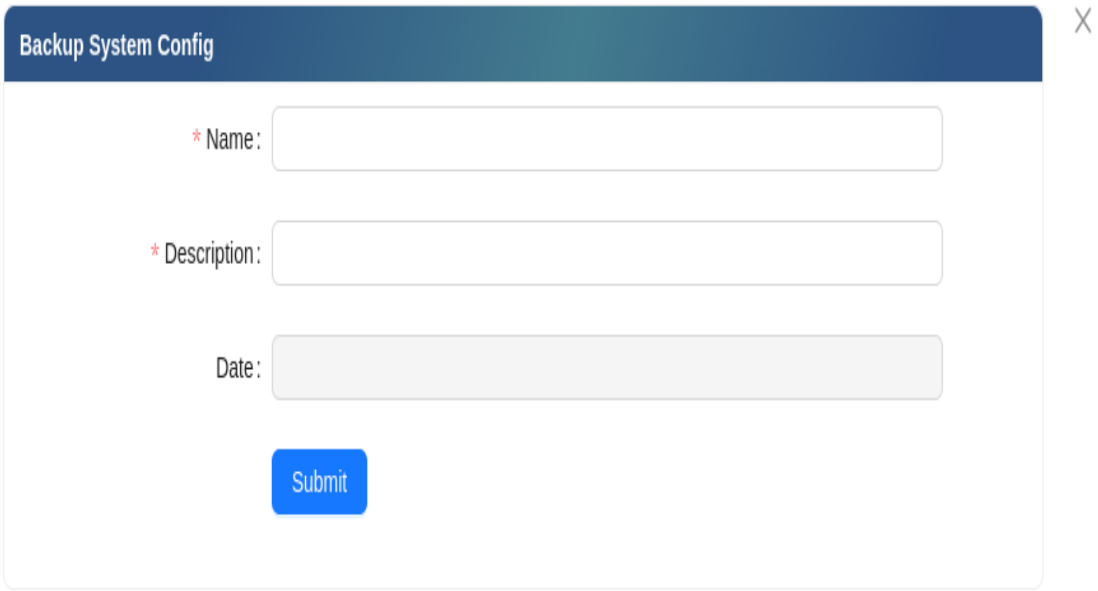
Hình 1251: Giao diện Restore

9.2 Cấu hình tính năng Backup



Hình 1262: Giao diện Backup

❖ Chọn + Create để tạo mới.



Hình 1273: Giao diện cấu hình chi tiết Backup

❖ Trong đó

- **Name:** Tên file config
- **Description:** Mô tả về file
- **Date:** Cập nhật tự động theo thời gian tạo file

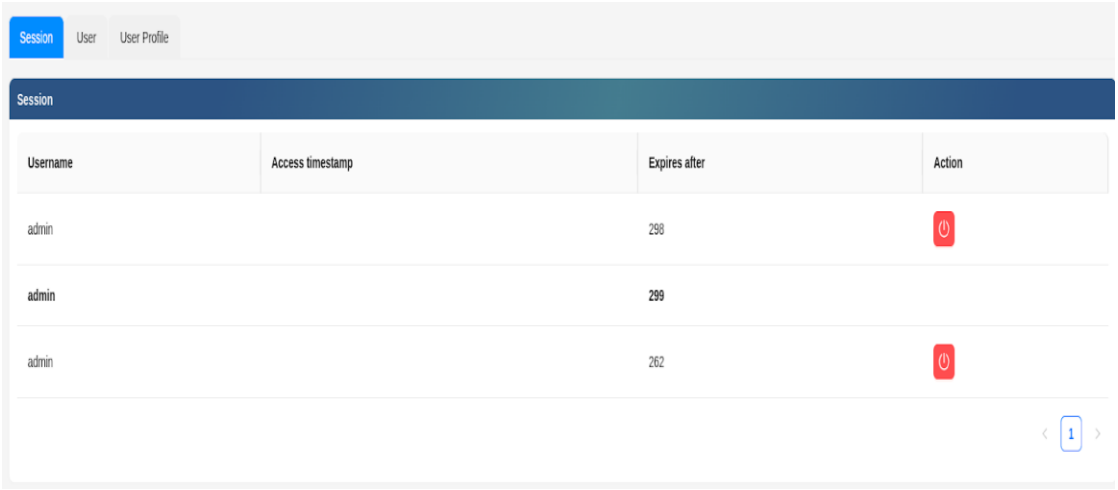
❖ Các nút bấm thao tác với file config:  lần lượt là Edit, Download file config, Delete file và Restore file.

9.3 Cấu hình tính năng phân quyền (User)

Tính năng phân quyền cho các tài khoản đăng nhập vào web quản trị, quản lý các session đăng nhập hiện thời của thiết bị.

9.3.1 Session

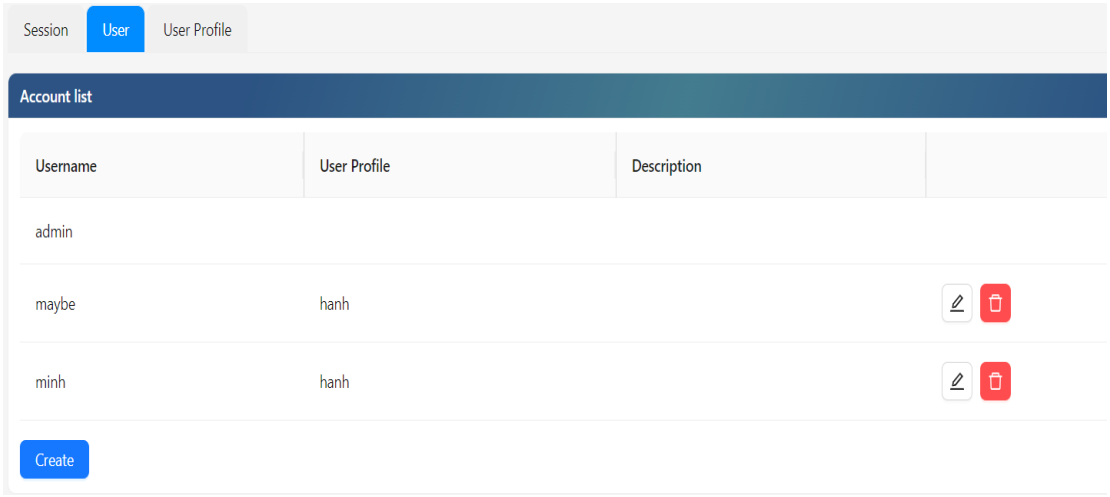
Tính năng quản lý Session đăng nhập của thiết bị, người dùng có thể theo dõi các phiên đăng nhập hiện thời, tài khoản đang đăng nhập cũng như có thể loại bỏ phiên đăng nhập với quyền admin.



Hình 1284: Giao diện quản lý Session

9.3.2 User & Authentication

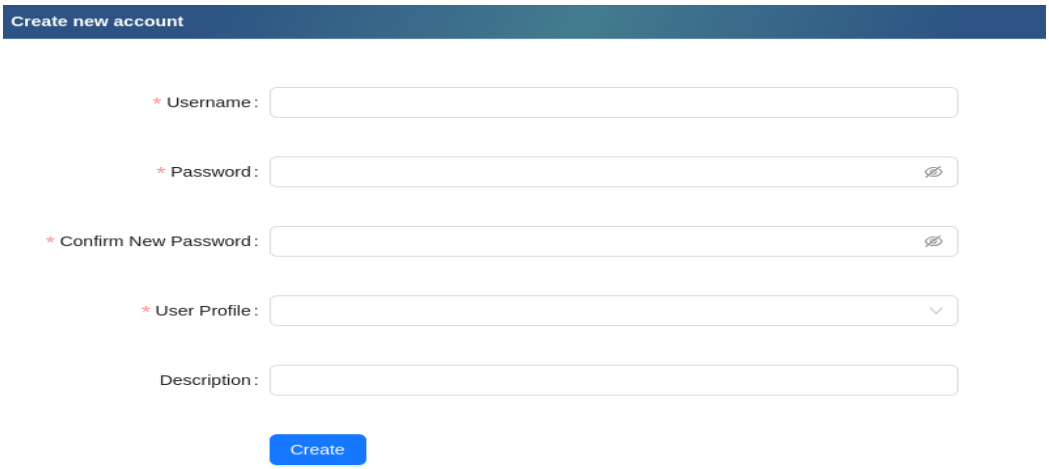
Tính năng quản lý các User sử dụng để đăng nhập tài khoản.



Hình 1295: Giao diện quản lý User

Tạo tài khoản mới:

❖ Chọn + Create để tạo mới:

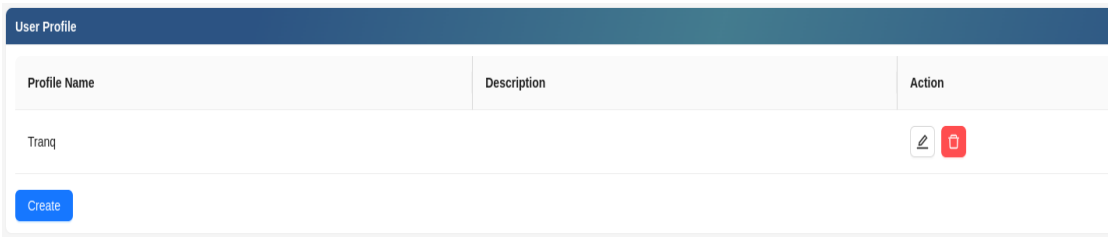


Hình 1306: Giao diện quản lý User

❖ Trong đó:
- **Username:** tên tài khoản đăng nhập
- **Password:** mật khẩu
- **Confirm New Password:** Xác nhận lại mật khẩu vừa đặt
- **User profile:** quyền truy cập
- **Description:** Mô tả về User

9.3.3 User profile

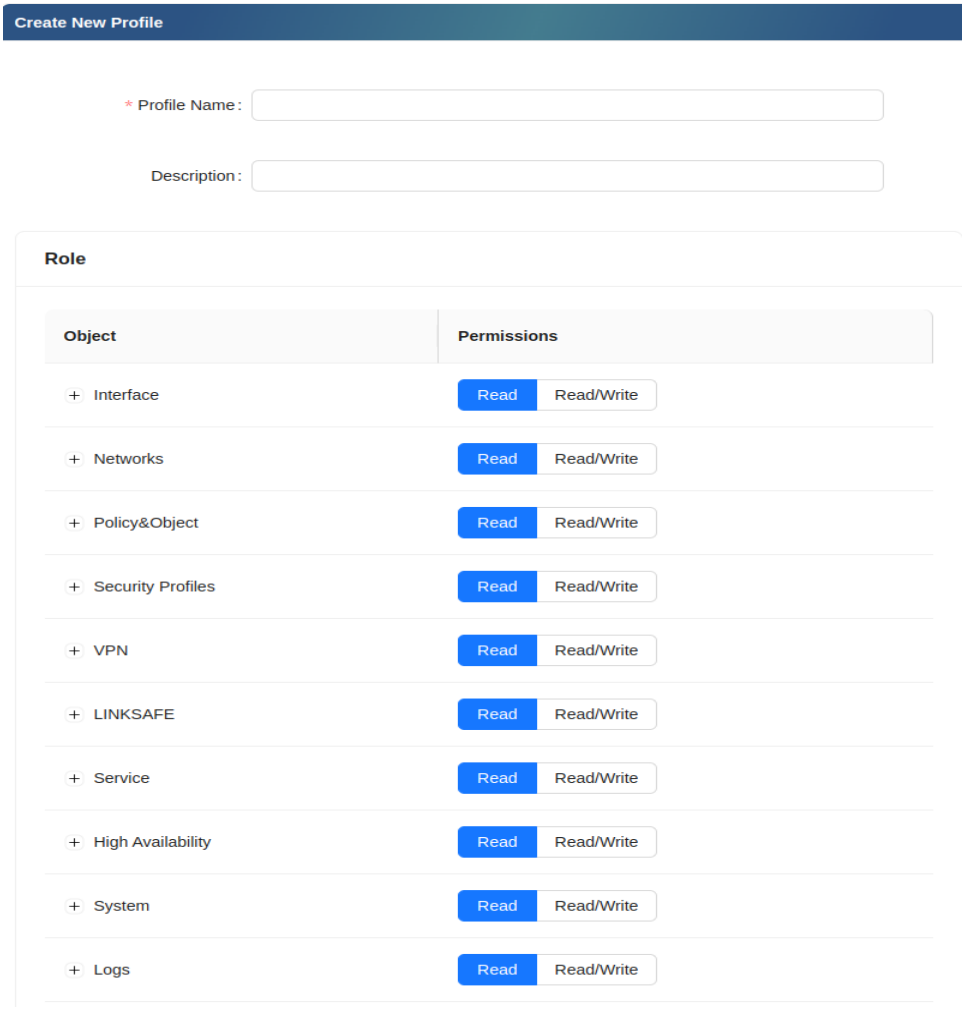
Tính năng tạo và quản lý các hồ sơ - quyền user theo lựa chọn của người dùng.



Hình 1317: Giao diện quản lý Profile

Tạo hồ sơ mới:

❖ Chọn + Create để tạo mới:



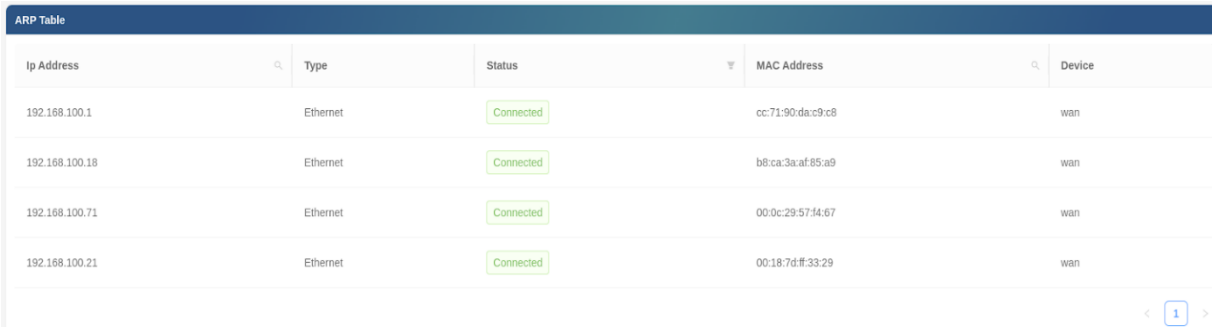
Hình 1328: Giao diện cấu hình chi tiết Profile

❖ Trong đó:

- **Profile name:** Tên của hồ sơ
- **Description:** Mô tả về hồ sơ
- **Role:** lựa chọn quyền Read/ Read and Write

9.4 ARP Table

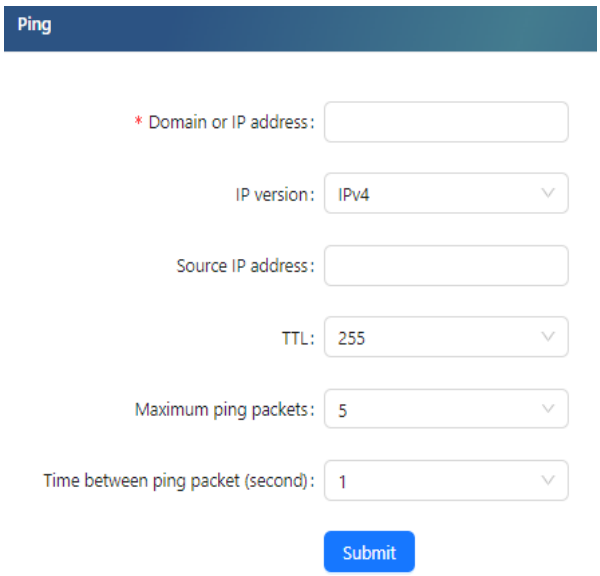
Tính năng lưu trữ các ánh xạ giữa địa chỉ IP và địa chỉ MAC của các thiết bị trong mạng theo dạng bảng.



Hình 1339: Giao diện ARP table

9.5 Cấu hình tính năng Ping

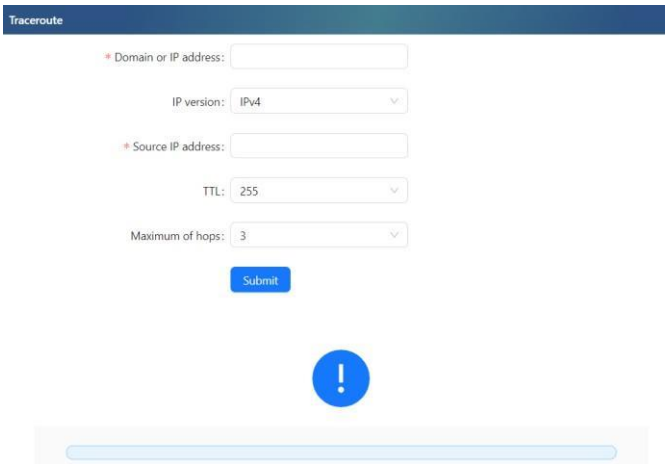
❖ Từ giao diện quản lý → System → Ping:



Hình 13430: Giao diện Ping

9.6 Công cụ Packet tracer

❖ Từ giao diện quản lý → System → Traceroute:



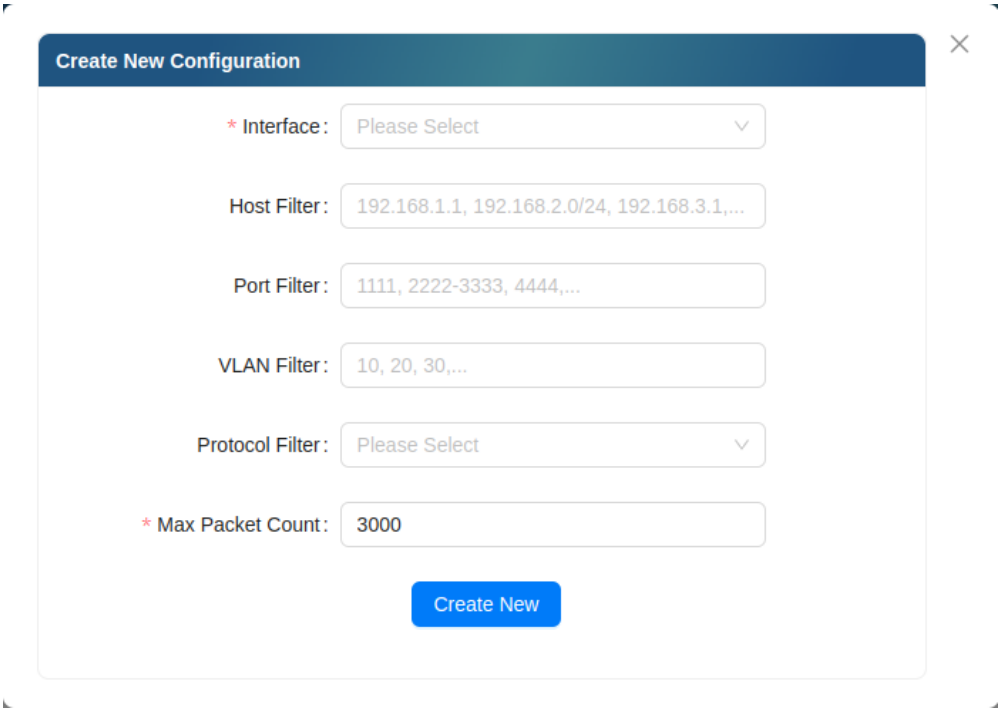
Hình 13531: Giao diện traceroute

9.7 Theo dõi lưu lượng mạng (Packet Capture)

Tính năng theo dõi lưu lượng mạng trên một interface vật lý cụ thể với các option tùy chỉnh theo người dùng.

Tạo capture mới:

❖ Chọn + Create để tạo mới:

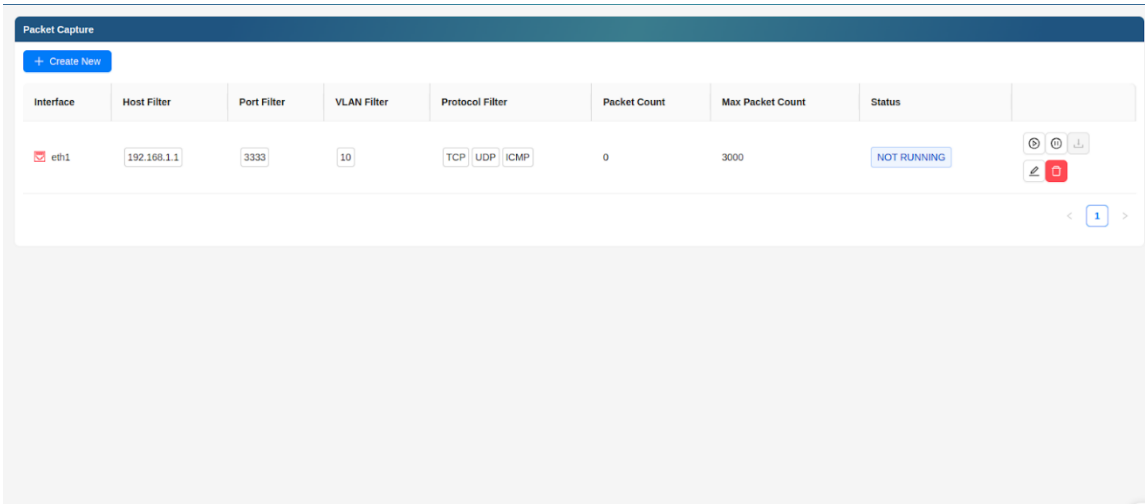


Hình 1362: Giao diện cài đặt Packet Capture

❖ Trong đó:

- **Interface:** Tên interface muốn theo dõi
- **Host filter:** Tên địa chỉ IP muốn theo dõi
- **Port Filter:** Tên port cần theo dõi
- **Vlan Filter:** Tag VLAN cần theo dõi
- **Protocol Filter:** Protocol cần theo dõi
- **Max packet Count:** Số gói tin theo dõi

❖ Sau khi tạo, cấu hình sẽ xuất hiện tại giao diện hiển thị:



Hình 1373: Giao diện quản lý Port Capture

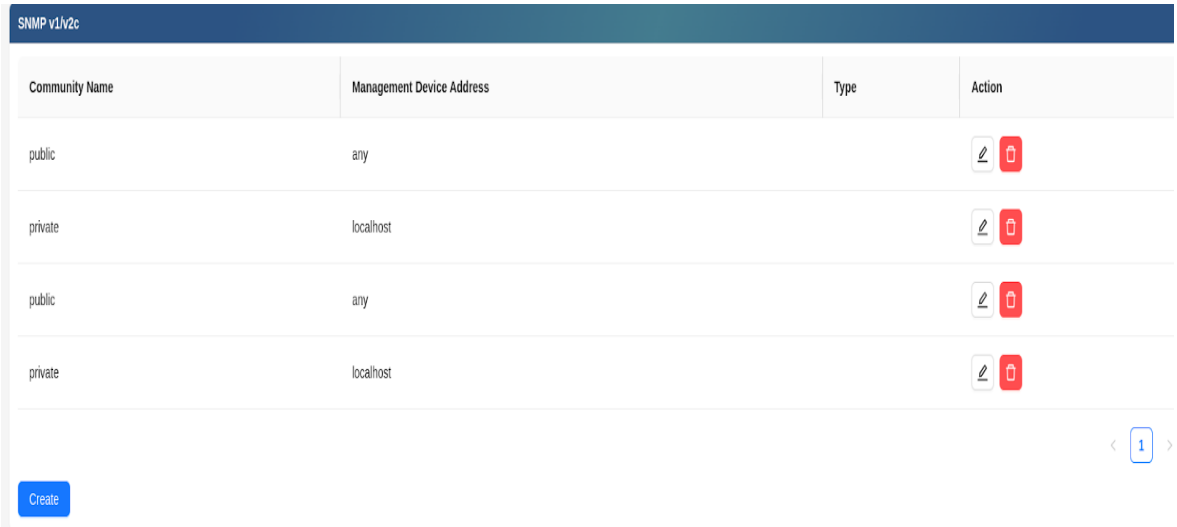
❖ Kích chuột vào  để bắt đầu "bắt" gói tin

❖ Kích chuột vào  để dừng việc "bắt" gói tin (nếu không thì việc "bắt" gói tin sẽ dừng lại sau khi đạt được số lượng đã chỉ định (Max packet Count)

❖ Kích chuột vào  để thực hiện tải file.pcap (lưu trữ các gói tin "bắt được") về máy tính sau khi quá trình "bắt" gói tin được dừng lại.

9.8 Cấu hình giao thức SNMP

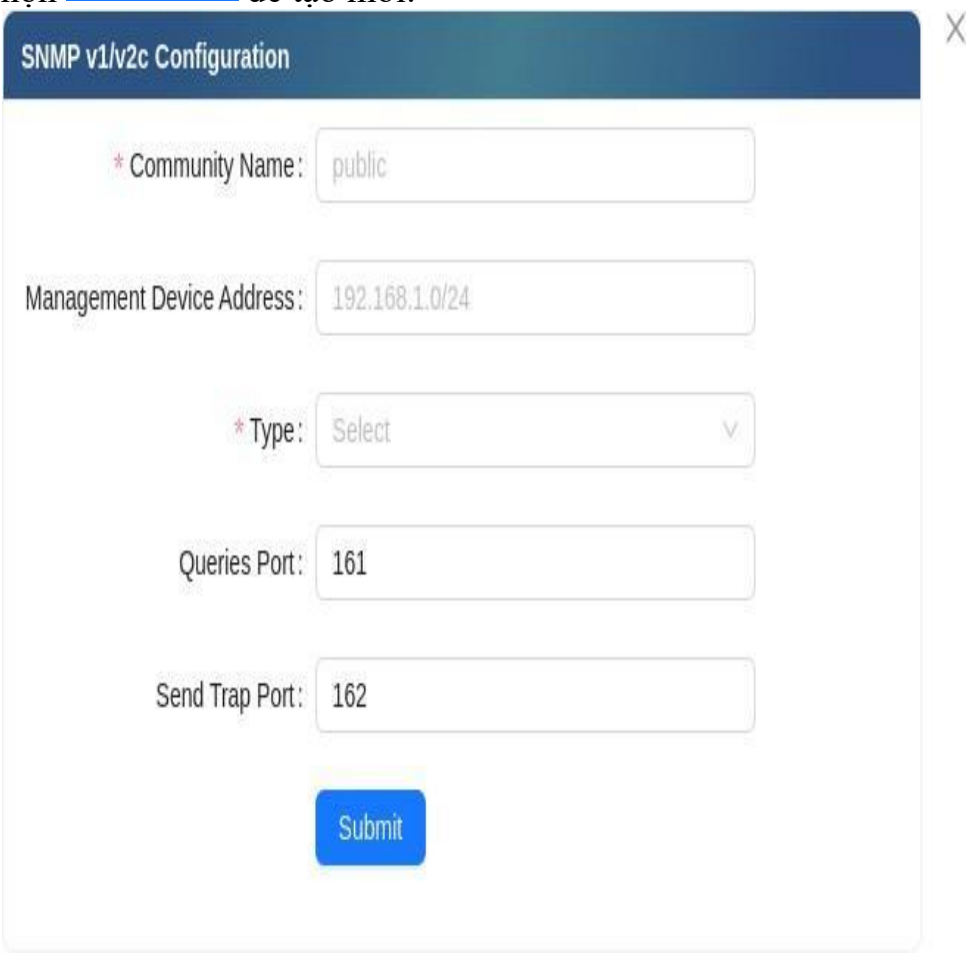
Tính năng cho phép quản trị viên mạng giám sát và quản lý các thiết bị mạng từ xa một cách hiệu quả. SNMP cung cấp khả năng thu thập dữ liệu từ các thiết bị mạng, theo dõi hiệu suất, và nhận các cảnh báo khi có sự cố xảy ra. Các thông tin quản lý này bao gồm trạng thái hệ thống, thông tin giao diện mạng, và các thông số quan trọng khác. Hỗ trợ cả SNMPv1/v2c và SNMPv3



Hình 1384: Giao diện quản lý Community

9.8.1 SMNPv1/v2c

❖ Chọn + Create để tạo mới.



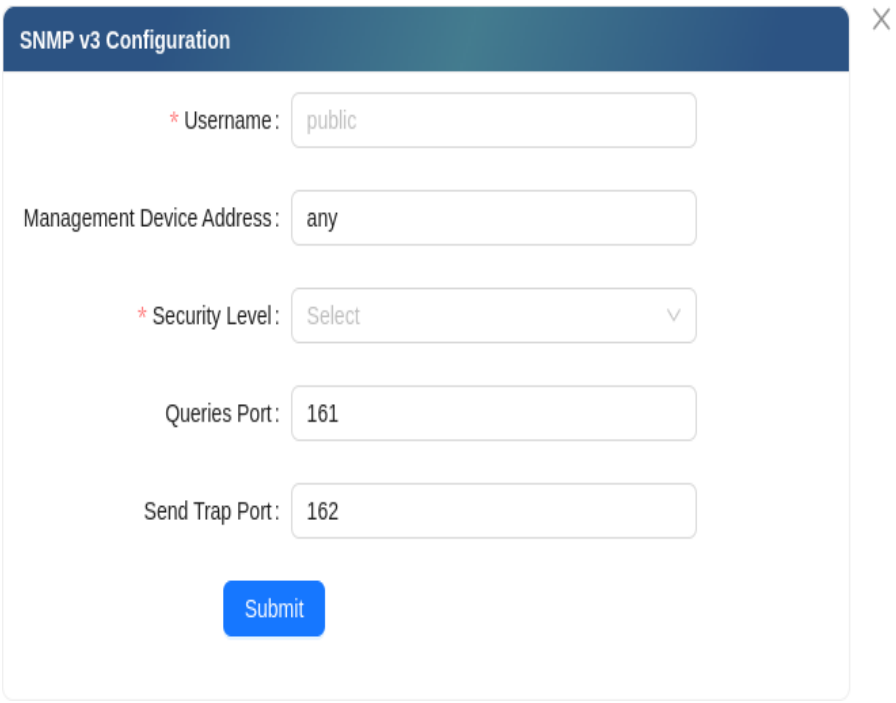
Hình 1395: Giao diện cấu hình chi tiết Community

- Trong đó
  - **Community Name:** Tên của comunity\
  - **Management Device Address:** IP của SNMP manager
  - **Type:** Kiểu dữ liệu gửi
  - **Queries Port:** Port gửi queries (Mặc đinh: 161)
  - **Send Trap Port:** Port gửi gói Trap (Mặc định 162)

9.8.2 SNMPv3

Tạo user mới:

- Chọn + Create để tạo mới:

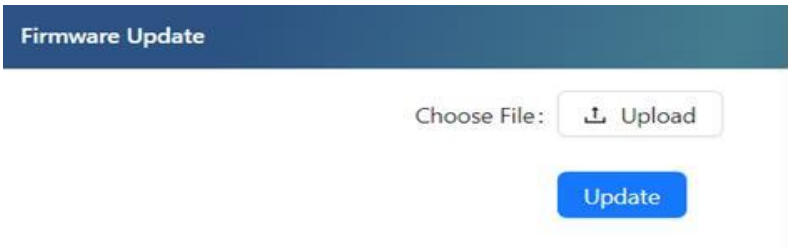


Hình 1406: Giao diện cấu hình chi tiết SNMPv3

- Trong đó
  - **Username:** Tên của Username
  - **Management Device Address:** IP của SNMP manager
  - **Type:** Kiểu dữ liệu gửi
  - **Queries Port:** Port gửi queries (Mặc đinh: 161)
  - **Send Trap Port:** Port gửi gói Trap (Mặc định 162)

9.9 Firmware update

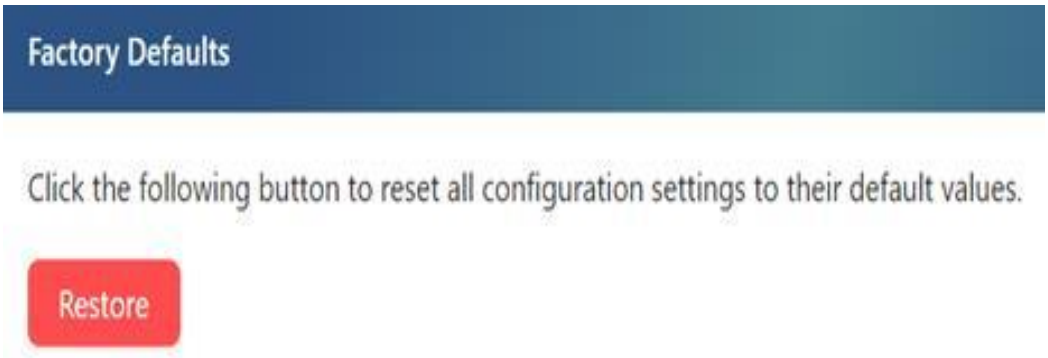
Từ giao diện quản lý → System → Update Firmware:



Hình 1417: Giao diện Update Firmware

9.10 Chuyển thiết bị về cấu hình mặc định (Reset Factory)

❖ Từ giao diện quản lý → System → Reset Factory: Người dùng chọn mode Reset Factory để chuyển thiết bị về cấu hình mặc định:



Hình 14238: Giao diện Factory Reset

9.11 Khởi động lại thiết bị (Reboot)

❖ Từ giao diện quản lý → System → Reboot: Người dùng Reboot lại thiết bị.

Hình 14339: Giao diện Reboot

9.12 Tắt nguồn thiết bị (Shutdown)

❖ Từ giao diện quản lý → System → Reboot: Người dùng Reboot lại thiết bị.

Hình 14440: Giao diện Shutdown

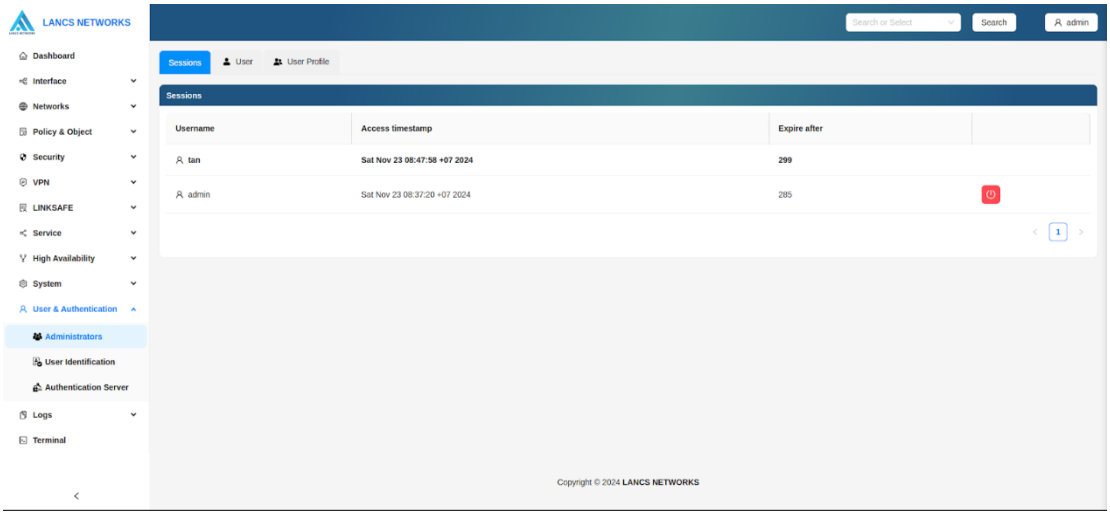
10 Cấu hình User & Authentication

10.1 Administrator

Mục đích dùng để tạo ra các tài khoản đăng nhập kèm theo các phân quyền cụ thể trên từng tính năng.

10.1.1 Sessions

Giao diện hiển thị những phiên đăng nhập hiện có:



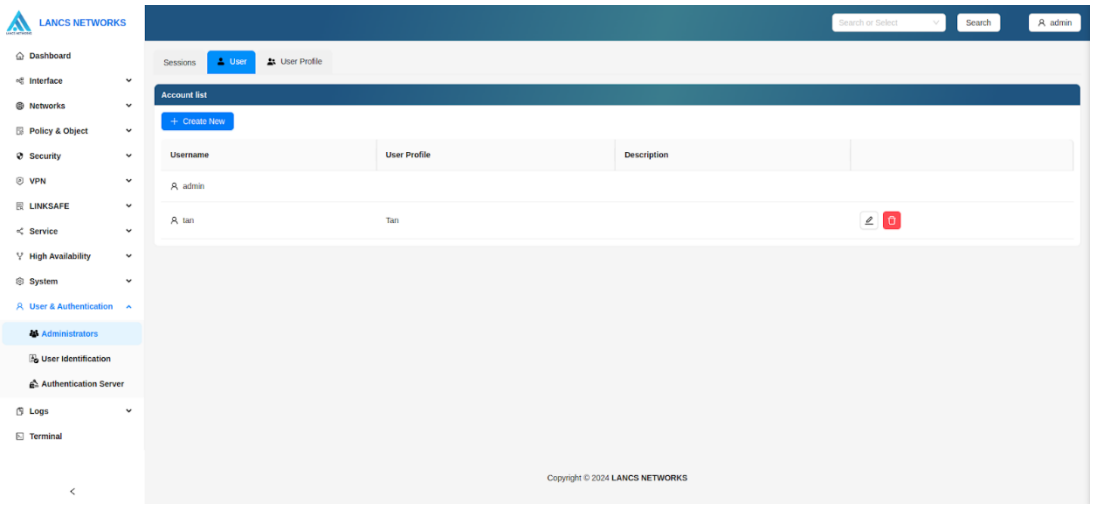
Hình 14541: Giao diện hiển thị các phiên đăng nhập hiện có

❖ Kích chuột vào  để thực hiện đóng phiên đăng nhập.

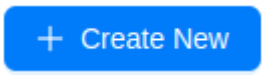
10.1.2 User

Thực hiện tạo các tài khoản đăng nhập với quyền truy cập cụ thể tại đây.

Giao diện hiển thị các tài khoản đăng nhập đã được tạo:

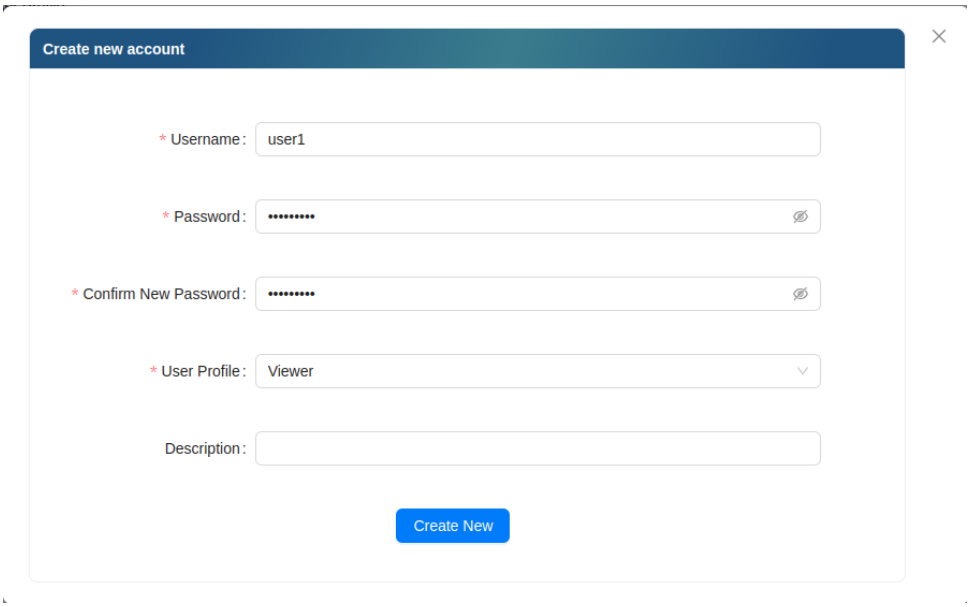


Hình 1462: Giao diện hiển thị các tài khoản đăng nhập đã được tạo

❖ Kích chuột vào 

để thực hiện tạo một tài khoản đăng nhập mới.

Giao diện cài đặt cho mỗi tài khoản cụ thể:



Hình 1473: Giao diện cài đặt cho mỗi tài khoản cụ thể

❖ Trong đó:

- **Username:** Tên đăng nhập
- **Password:** Mật khẩu đăng nhập
- **Confirm New Password:** Xác nhận lại mật khẩu

- **User Profile:** Chọn hồ sơ đã được cài đặt sẵn (xem ở mục User Profile phía dưới)
- **Description:** Thêm mô tả cho tài khoản

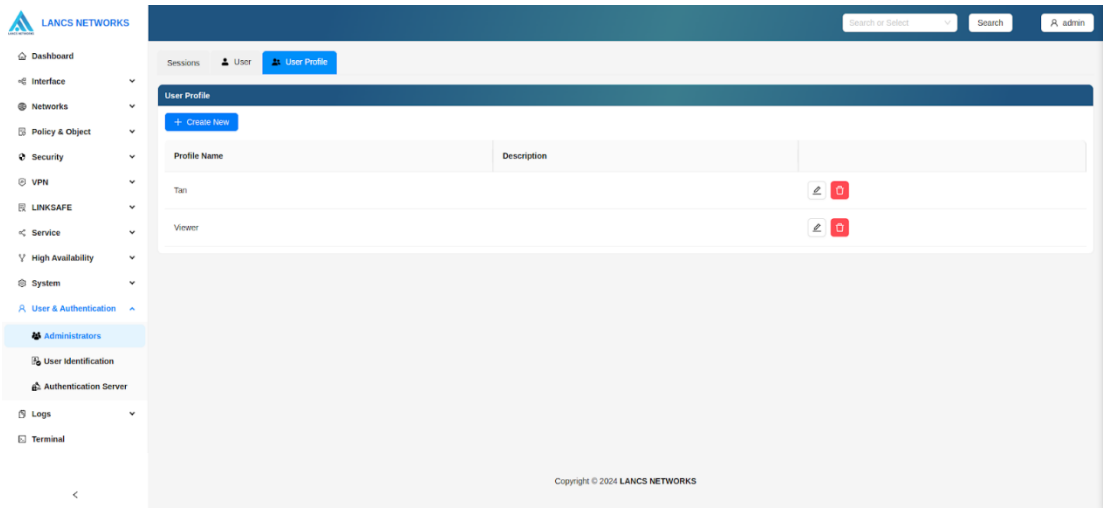
❖ Sau khi cài đặt xong, kích chuột vào Create New để lưu cài đặt.

❖ Kích chuột vào để thực hiện chỉnh sửa cài đặt cho mỗi tài khoản

❖ Kích chuột vào để thực hiện xóa tài khoản đăng nhập.

10.1.3 User Profile

Dùng để tạo các hồ sơ với mỗi hồ sơ sẽ được phân quyền truy cập cụ thể trên từng tính năng hoặc nhóm tính năng.



Hình 1484: Giao diện quản lý hồ sơ người dùng

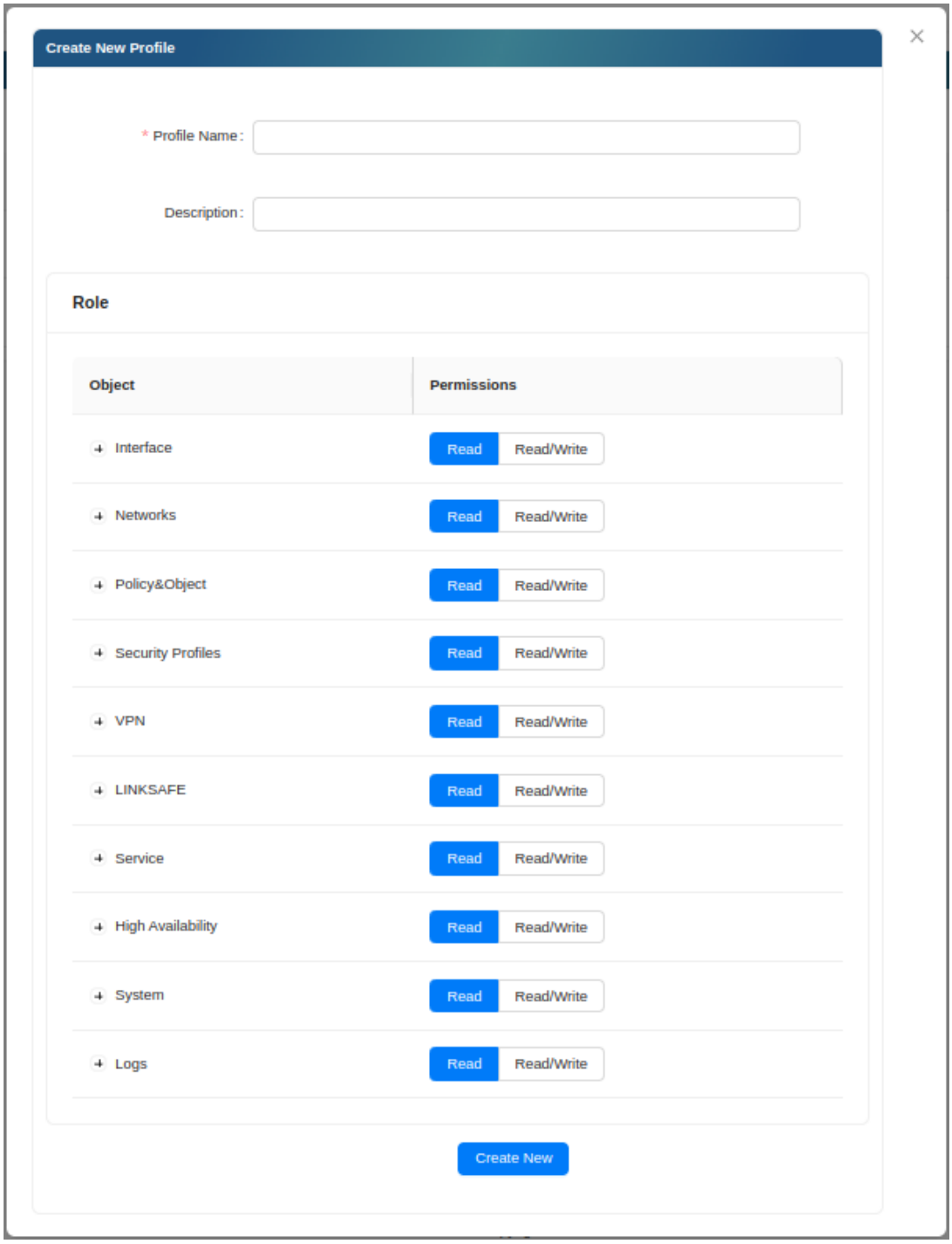
❖ Kích chuột vào nút Create New để thực hiện tạo một profile.

Giao diện cài đặt:

❖ Trong đó:

- **Profile Name**: Đặt tên cho profile
- **Description**: Thêm mô tả cho profile
- **Role**: Phân quyền truy cập vào mỗi tính năng cụ thể:
- **Read**: Chỉ có quyền xem
- **Read/Write**: Có quyền thêm, sửa

❖ Kích chuột vào **Create New** (đối với tạo mới một profile) hoặc **Confirm** (đối với chỉnh sửa một profile) để lưu cấu hình.



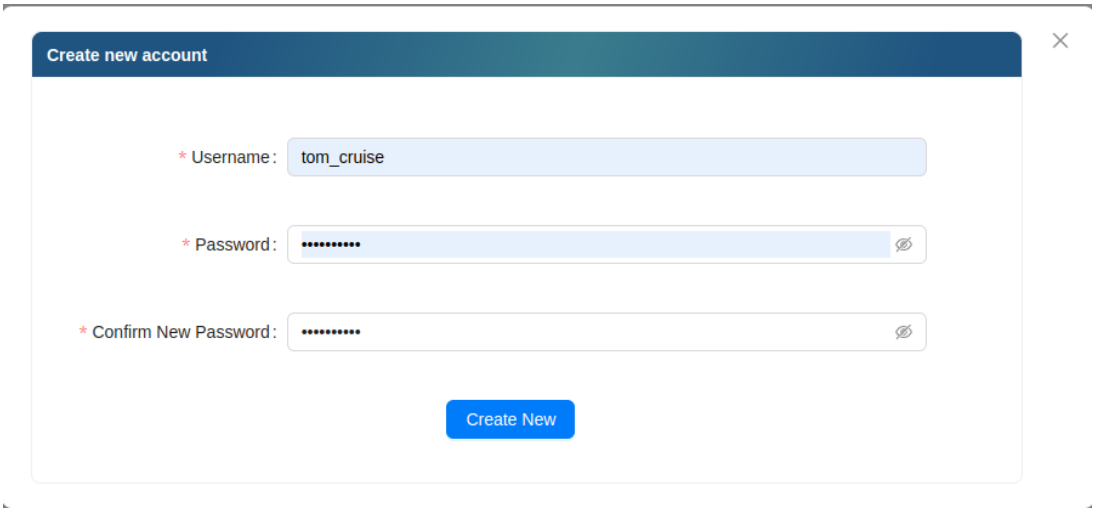
Hình 1495: Giao diện thêm mới hồ sơ người dùng

10.2 User Identification

Tạo ra các tài khoản dùng để định danh (xác thực) người dùng cuối (end device) trước khi cho phép truy cập vào tài nguyên mạng hoặc các dịch vụ cụ thể.

- Kích chuột vào **Create New** nếu muốn tạo một tài khoản mới
- Kích chuột vào nút có biểu tượng cây bút nếu muốn chỉnh sửa cài đặt của một tài khoản đã được tạo.

Giao diện cài đặt cho một tài khoản cụ thể:



Hình 1506: Giao diện cài đặt tài khoản

10.3 Authentication Server

Sử dụng các giao thức xác thực chuẩn để giao tiếp với các server xác thực bên ngoài để xác thực danh tính của người dùng hoặc thiết bị trước khi cho phép truy cập vào tài nguyên mạng hoặc các dịch vụ cụ thể.

10.3.1 LDAP Servers (Lightweight Directory Access Protocol)

Sử dụng giao thức LDAP (hoạt động trên nền tảng TCP/IP)

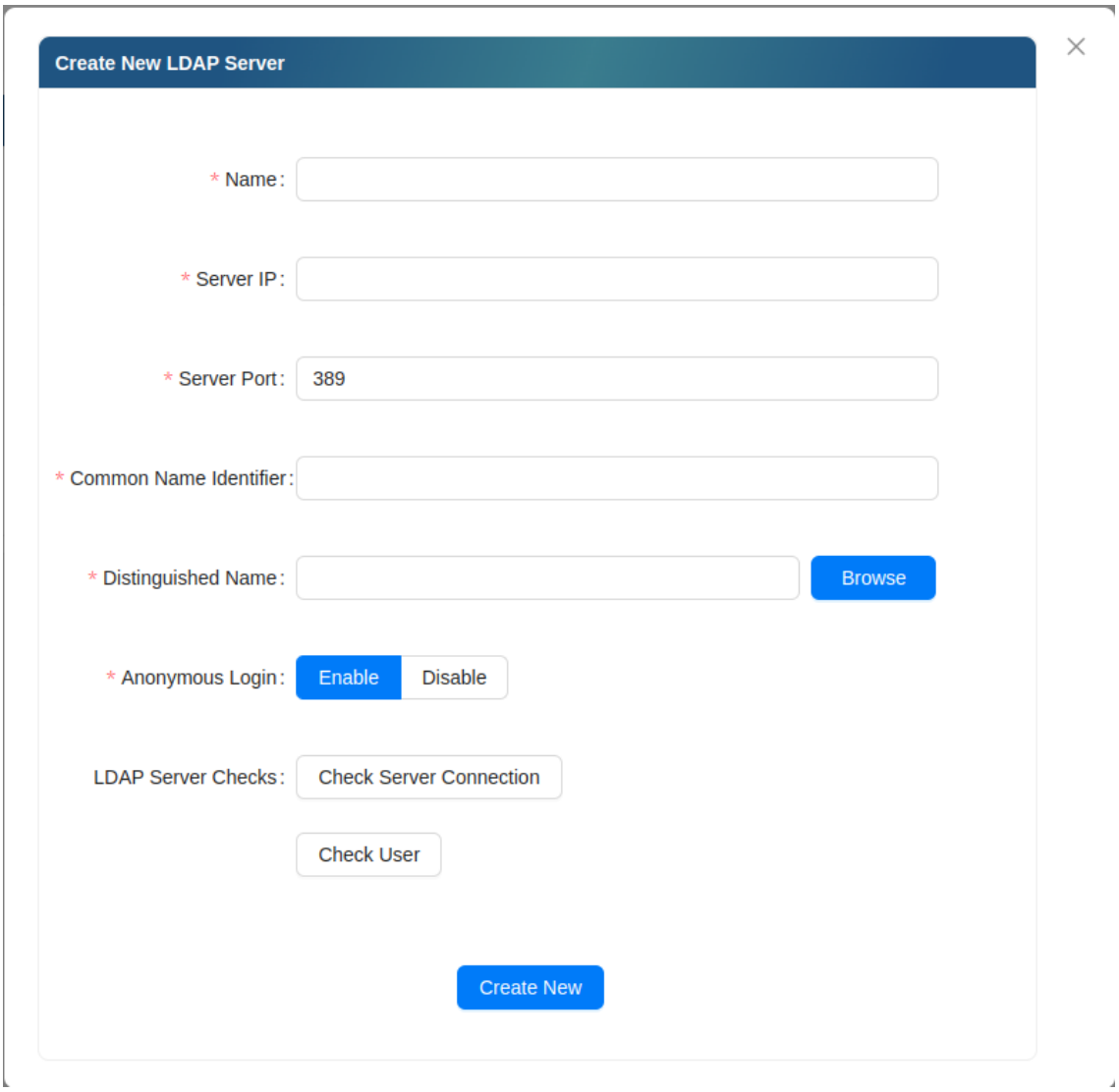
Giao diện cài đặt LDAP Server:

- Trong đó:
  - **Name**: Tên cấu hình
  - **Server IP**: Địa chỉ IP của server (khả dụng khi thiết bị có thể kết nối được tới địa chỉ này)
  - **Server Port**: Cổng để giao tiếp với server (mặc định là 389)

- **Common Name Identifier (CN)**: Trường thuộc tính của đối tượng trong LDAP mà NGFW sử dụng để xác định người dùng đang kết nối
- **Distinguished Name (DN)**: Một định danh duy nhất cho mỗi entry, giống như "địa chỉ" trong cây thư mục. Được sử dụng để tra cứu các mục nhập tài khoản người dùng trên máy chủ LDAP
- **Anonymous Login**:
- **Enable**: Để truy cập cơ sở dữ liệu thư mục mà không yêu cầu cung cấp thông tin xác thực (có nghĩa là người dùng hoặc ứng dụng có thể truy vấn thông tin từ LDAP server mà không cần phải "đăng nhập"
- **Disable**: Cần cung cấp thêm tên người dùng (Username) có đủ đặc quyền để truy cập máy chủ LDAP và mật khẩu (Password) kèm theo

10.3.2 LDAP Server Checks

Sử dụng để kiểm tra kết nối của NGFW tới server LDAP hoặc kiểm tra truy cập tới server với tên người dùng và mật khẩu cụ thể.

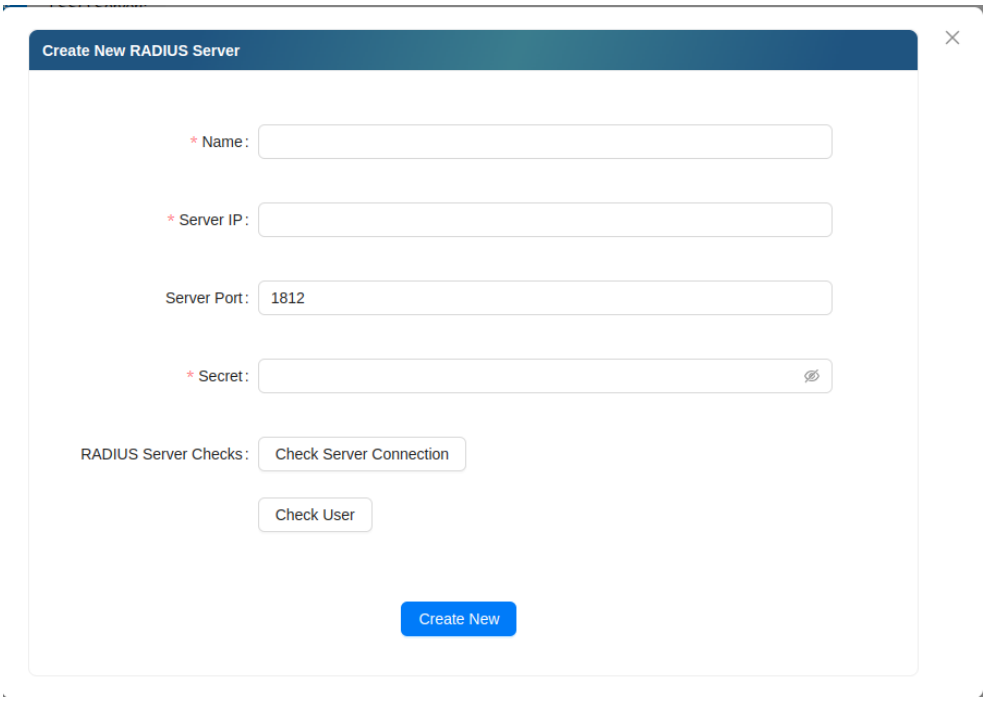


Hình 1517: Giao diện thêm mới LDAP Server

10.3.3 RADIUS Servers (Remote Authentication Dial-In User Service)

Sử dụng giao thức RADIUS (dùng UDP để truyền dữ liệu với cổng mặc định là 1812)

Giao diện cài đặt cấu hình RADIUS Servers:



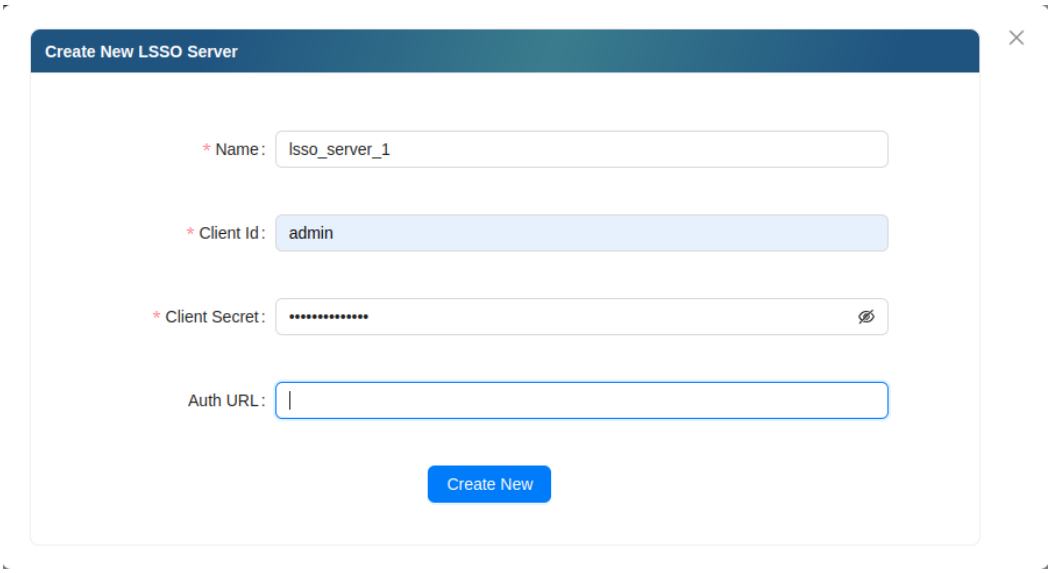
Hình 1528: Giao diện cài đặt cấu hình RADIUS Server

❖ Trong đó:

- **Name**: Tên cấu hình
- **Server IP**: Địa chỉ IP của server (khả dụng khi thiết bị có thể kết nối được tới địa chỉ này)
- **Server Port**: Cổng để giao tiếp với server (mặc định là 1812)
- **Serect**: Chuỗi ký tự (string) được sử dụng để bảo mật giao tiếp giữa RADIUS Server và RADIUS Client
- **RADIUS Server Checks**: Sử dụng để kiểm tra kết nối của NGFW tới server RADIUS hoặc kiểm tra truy cập tới server với tên người dùng và mật khẩu cụ thể

10.3.4 LSSO

Giao diện cài đặt LSSO:



Hình 1539: Giao diện cài đặt LSSO Server

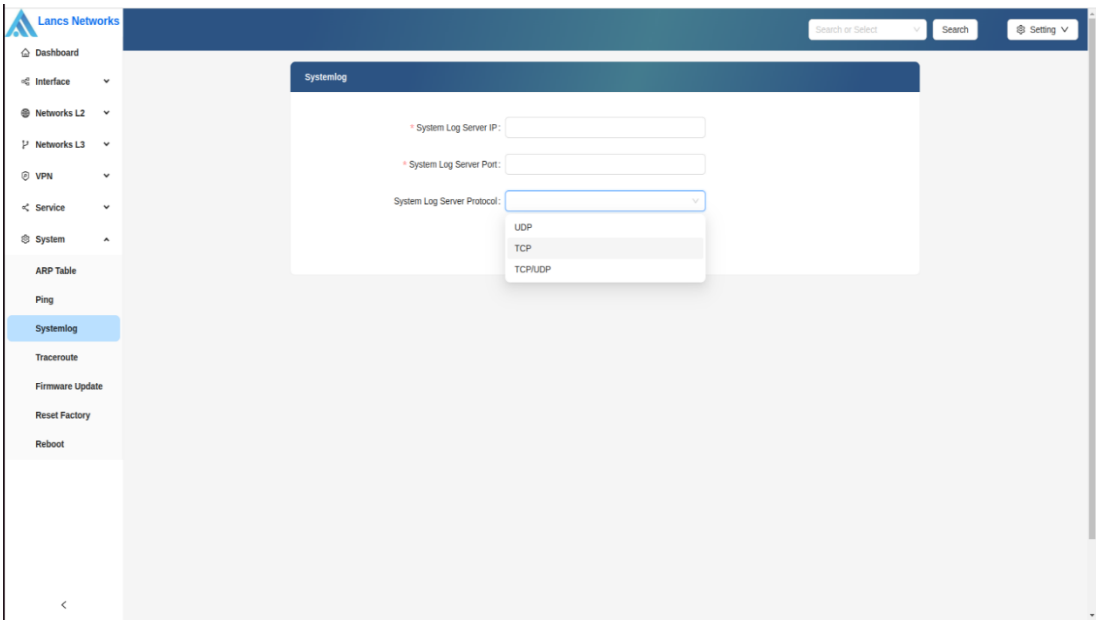
❖ Trong đó:

- **Name**: Tên cấu hình
- **Client id**:
- **Client Secrect**:
- **Auth URL**:

11 Theo dõi Log

11.1 Cấu hình Syslog

❖ Từ giao diện quản lý → System → System Log:



Hình 15450: Giao diện System Log.

- Trong đó:
  - **System log server ip:** điền thông tin ip server
  - **System log server port:** điền thông tin port server
  - **System log server protocol:** chọn UDP, TCP, TCP/UDP
- Bấm Submit để thực hiện gửi đến server.

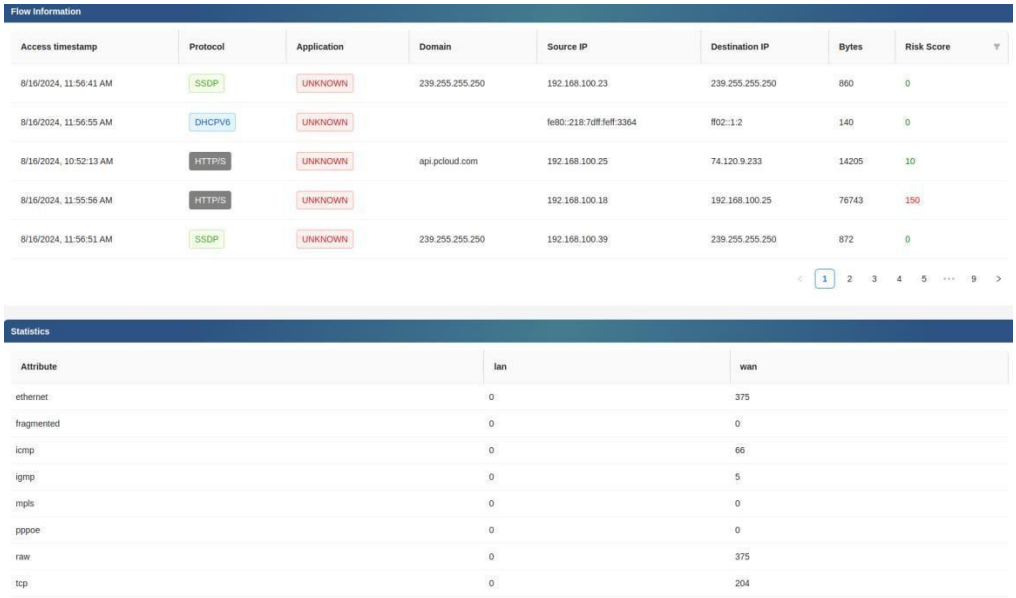
11.2 Theo dõi các kết nối trên thiết bị (Connections)

Log các connections đang kết nối nối tới thiết bị, hỗ trợ cả IPv4 và IPv6.

Hình 155: Giao diện Connection

11.3 Theo dõi và kiểm tra NIPS log

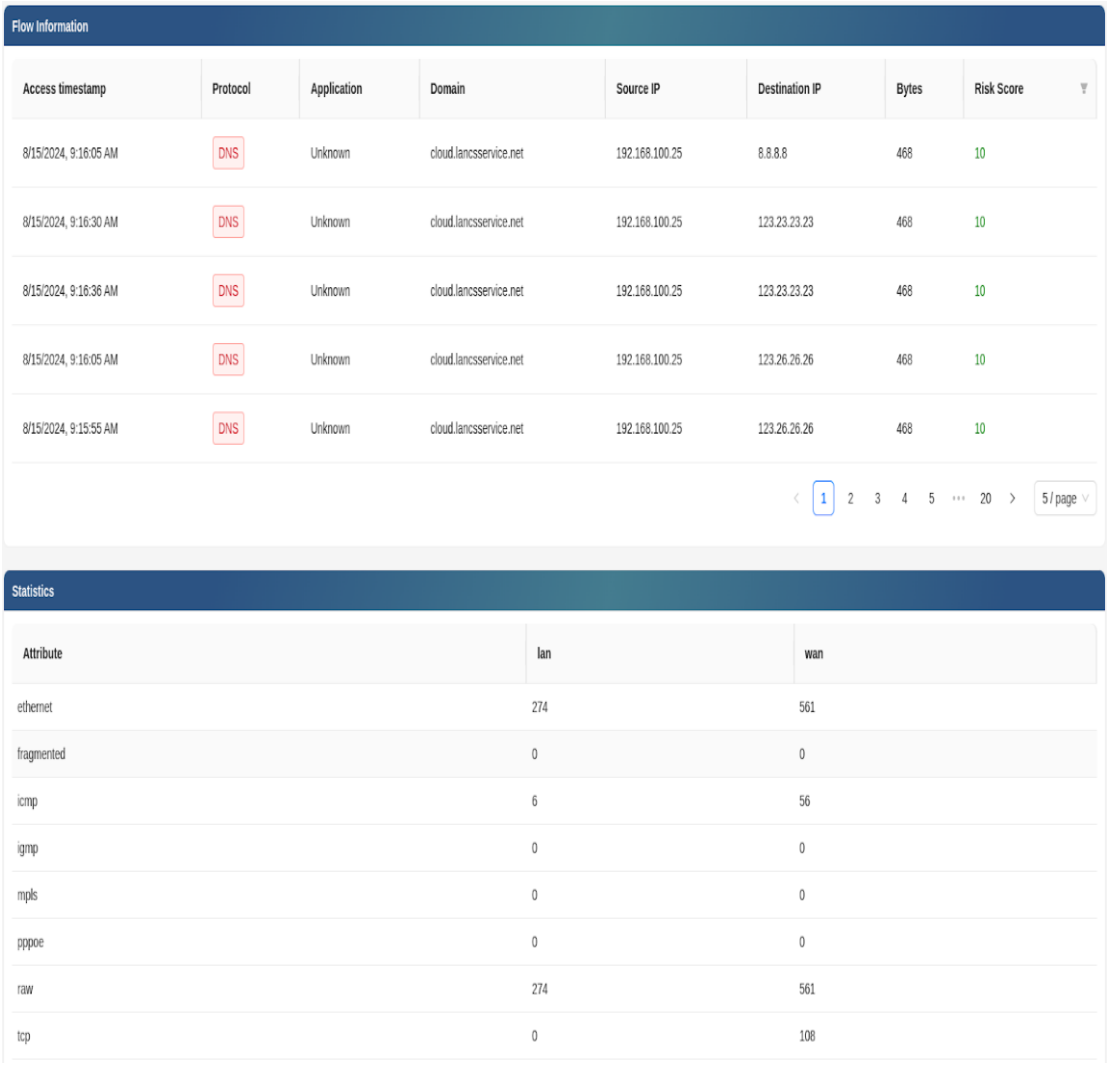
Là nơi lưu trữ các thông tin liên quan đến hoạt động và các sự kiện bảo mật mà hệ thống đã ghi nhận:



Hình 1562: Giao diện NIPS logs

11.4 Theo dõi và kiểm tra Network flow

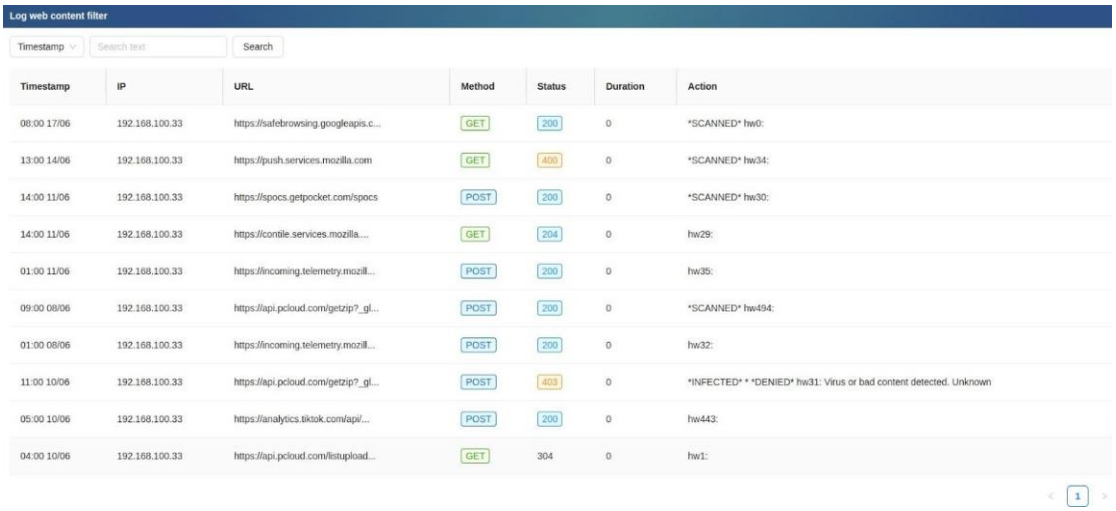
Là nơi lưu trữ thông tin chi tiết về lưu lượng mạng đi qua thiết bị. Những thông tin này giúp quản trị viên mạng theo dõi, phân tích, và tối ưu hóa hoạt động của mạng.



Hình 1573: Giao diện Network flow

11.5 Theo dõi và giám sát Web Content

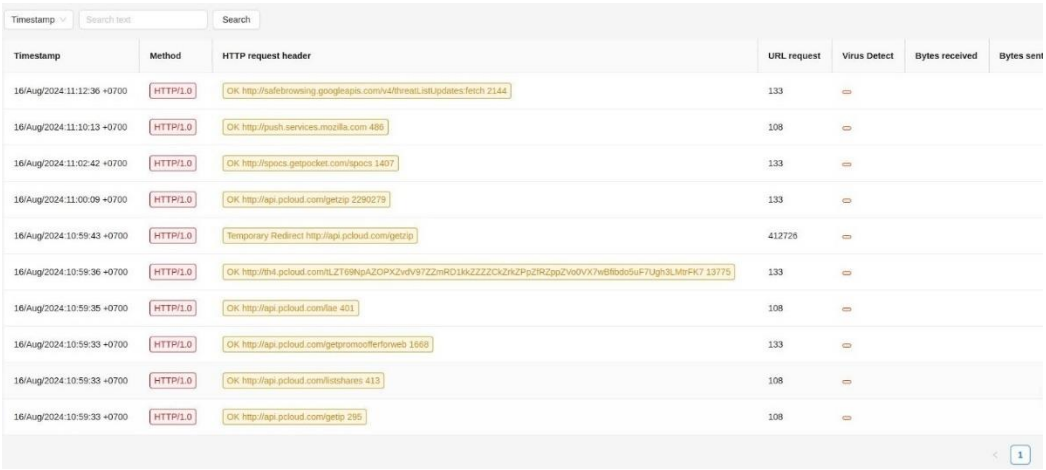
Là nơi ghi lại các thông tin liên quan đến việc truy cập và sử dụng nội dung web thông qua thiết bị.



Hình 1584: Giao diện Web Content

11.6 Theo dõi và kiểm tra Anti Virus log

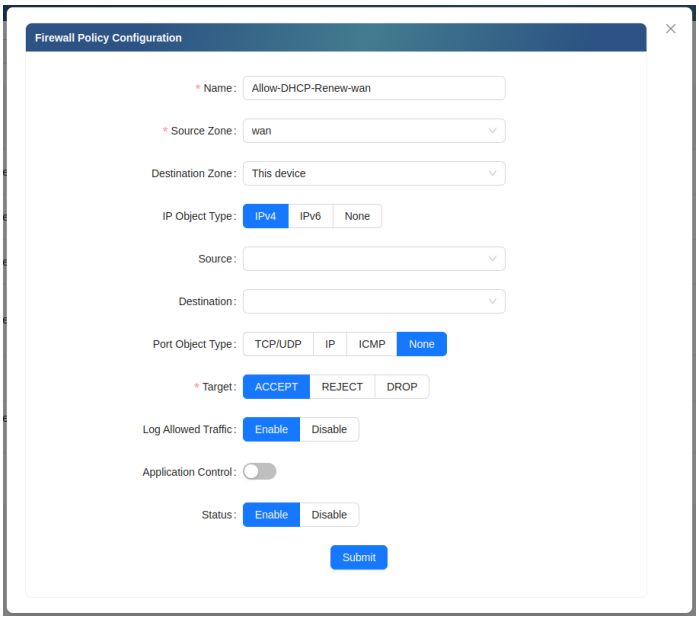
Là nơi lưu trữ các thông tin liên quan đến hoạt động và các sự kiện bảo mật mà hệ thống đã ghi nhận khi phát hiện được những payload được coi là virus:



Hình 1595: Giao diện AV logs

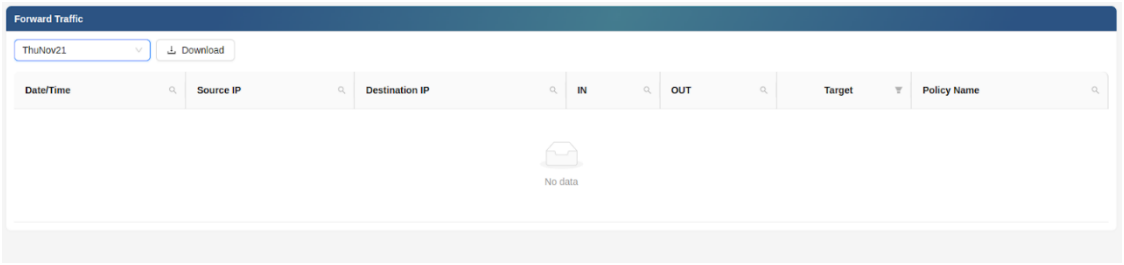
11.7 Theo dõi log firewall Forward Traffic

Đây là nơi lưu trữ các thông tin liên quan đến hoạt động của Firewall ghi lại các luồng dữ liệu đi qua để giám sát các luồng đi qua Firewall và có thể download Log Firewall.



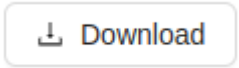
Hình 1606: Hình ảnh Log Allowed Traffic

❖ Cần truy cập vào Policy & Object → Firewall Policy → Enable trong phần edit hoặc tạo mới Log Allowed Traffic để hiển thị lên Log cho từng luồng.



Hình 1617: Hình ảnh Forward Traffic

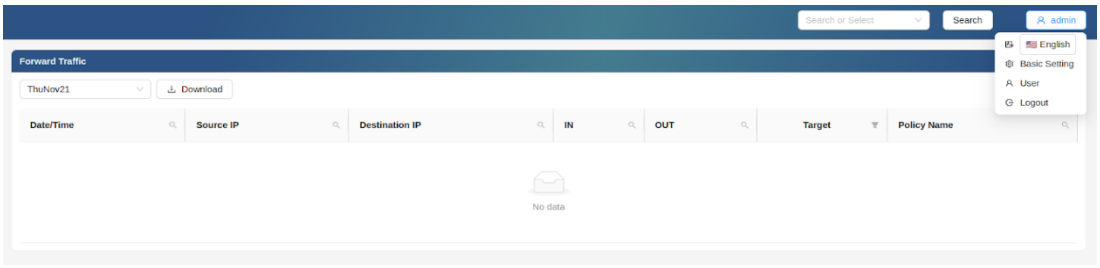
❖ Truy cập trên web Logs → Forward Traffic

❖ Có trạng thái 

: Download các log cũ hơi ở đây

12 Cấu hình quản trị thiết bị

Khi trỏ vào phần Admin ở góc phải màn hình ta hiển thị lên.



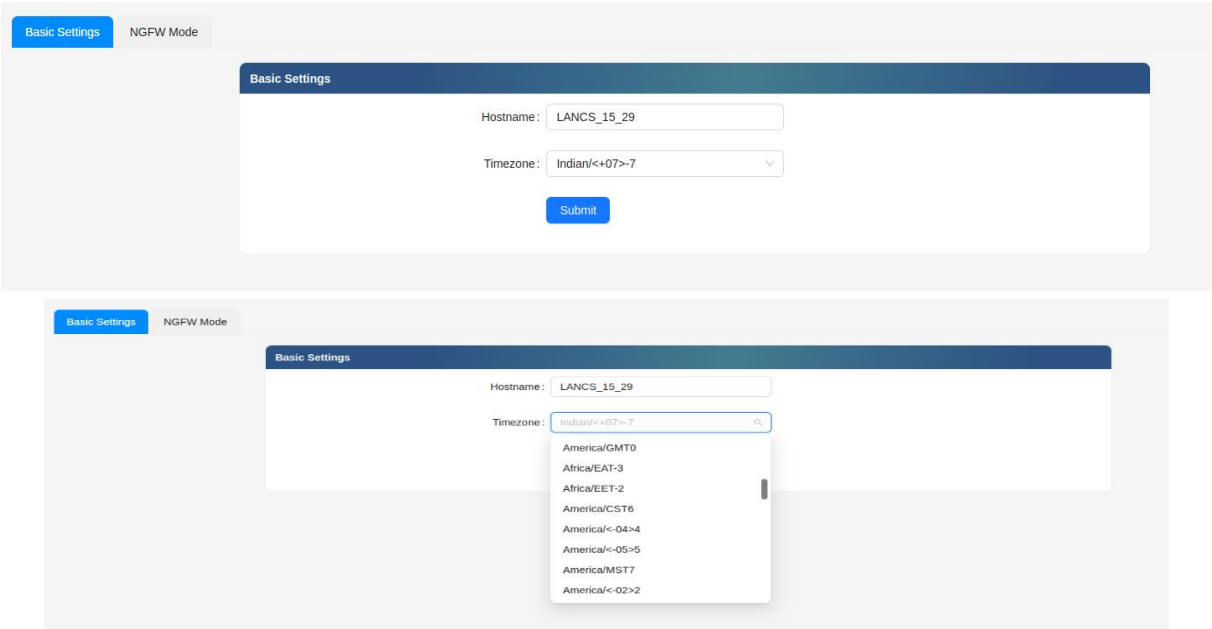
Hình 1628: Giao diện hiển thị trang quản thị thiết bị

❖ Trong đó bao gồm:

- **Translations:** EN vs VI
- **Basic Setting:** gồm 2 mục khi kích vào
- **User:** sẽ giúp thay đổi mật khẩu và tên đăng nhập
- **Logout:** ra ngoài màn hình đăng nhập

12.1 Thay đổi HostName và TimeZone

❖ Truy cập vào Setting → Basic Setting: Để thay đổi HostName và TimeZone.

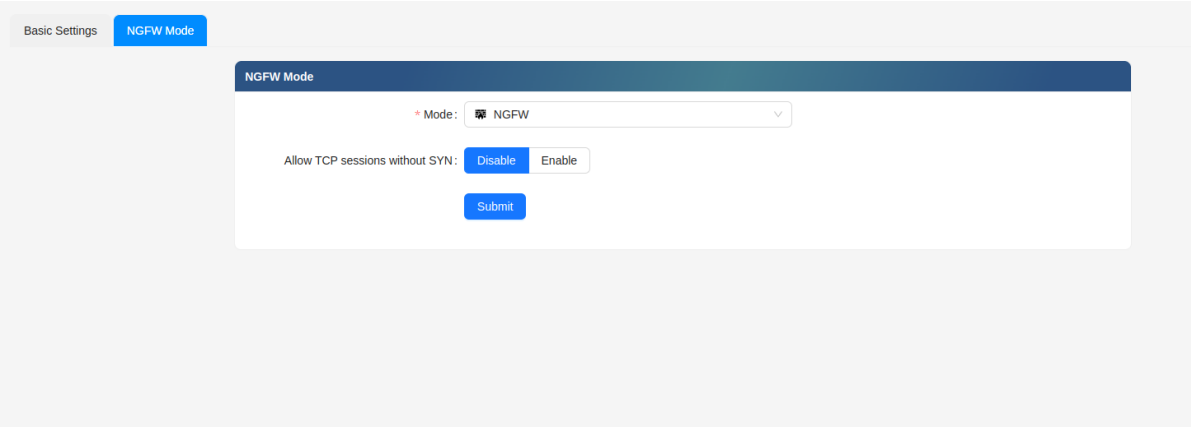


Hình 1639: Hình ảnh Basic Setting

❖ Có thể thay thế Hostname và timezone phù hợp với yêu cầu.

12.2 Thay đổi Mode từ NGFW sang Route

❖ Truy cập vào Setting → NGFW Mode: Để thay đổi Mode NGFW và Mode Router



Hình 16460: Giao diện Change Mode

❖ Trong đó:

- **Mode:** gồm 2 trạng thái NGFW và Router
- **Allow TCP sessions without SYN:** Enable và Disable