**I. Giới thiệu**

Tấn công Smurf là một dạng tấn công từ chối dịch vụ (DoS - Denial of Service) khai thác giao thức ICMP (Internet Control Message Protocol). Kẻ tấn công gửi các gói tin ICMP Echo Request đến địa chỉ phát sóng (broadcast) của một mạng, giả mạo địa chỉ nguồn (source IP) thành địa chỉ của nạn nhân. Các thiết bị trong mạng phản hồi lại địa chỉ giả mạo này, tạo ra lưu lượng lớn làm quá tải hệ thống mục tiêu. Mặc dù hiện nay Smurf Attack ít phổ biến hơn nhờ các biện pháp bảo mật hiện đại, nó vẫn là mối đe dọa với các hệ thống chưa được cấu hình đúng cách. Báo cáo này trình bày ba biện pháp cụ thể để phòng chống tấn công Smurf.

**II. Các biện pháp phòng chống tấn công Smurf**

**1. Cấu hình các máy trong mạng và router không trả lời các yêu cầu ICMP**

Mô tả:

- Tấn công Smurf phụ thuộc vào việc các thiết bị trong mạng phản hồi ICMP Echo Request gửi đến địa chỉ broadcast. Nếu các máy chủ và router được cấu hình để không trả lời các yêu cầu ICMP, lưu lượng phản hồi sẽ không được tạo ra, làm mất hiệu quả của cuộc tấn công.

- Vô hiệu hóa phản hồi ICMP Echo trên máy chủ và router.

- Chặn phản hồi đối với gói tin ICMP gửi đến địa chỉ broadcast.

- Có thể giới hạn băng thông ICMP để giảm tác động nếu cần.

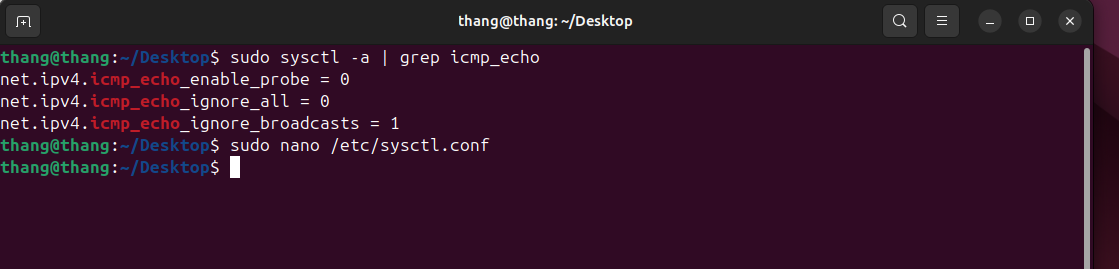
***\* Cách thực hiện:***

**- Trên Linux:**

* Kiểm tra trạng thái:

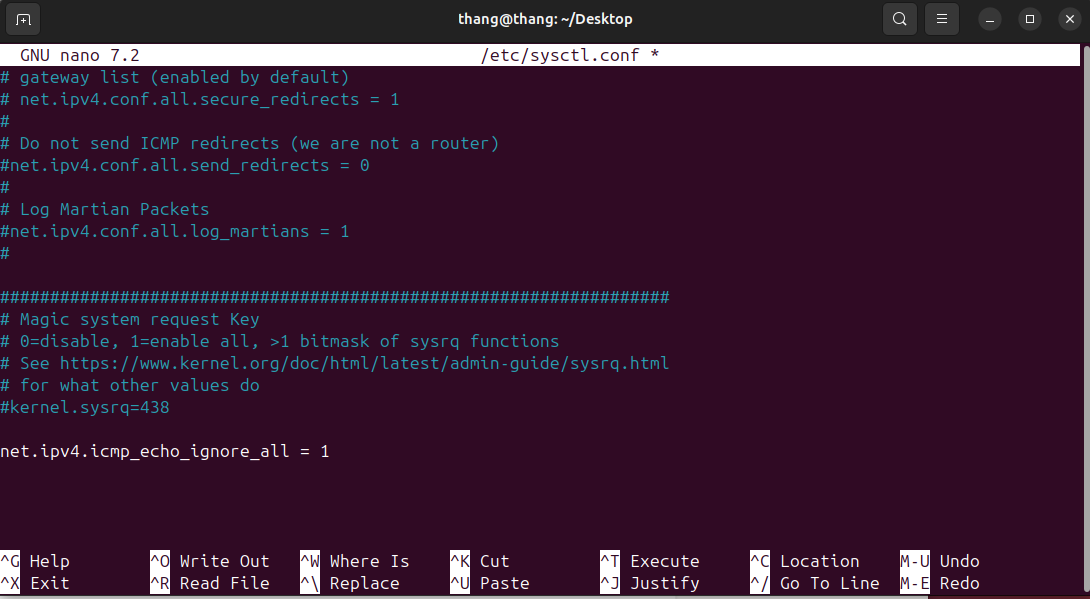
*sysctl net.ipv4.icmp\_echo\_ignore\_all*

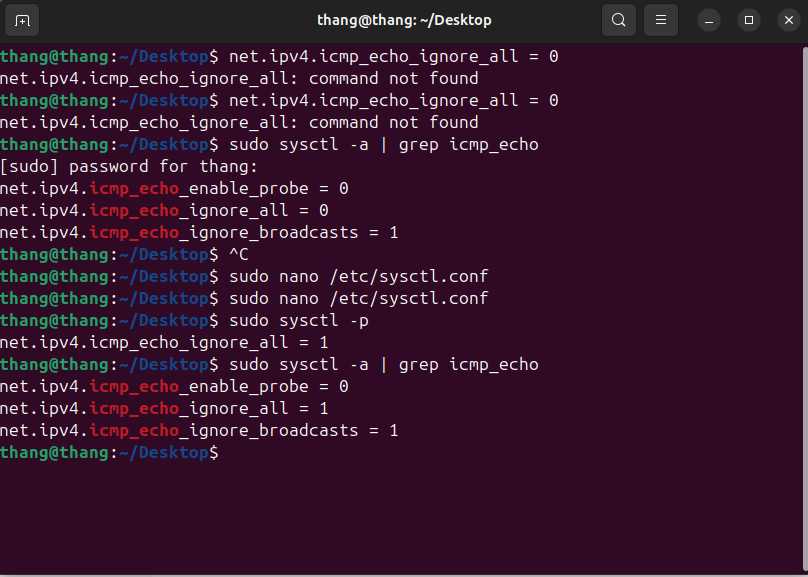
*sysctl net.ipv4.icmp\_echo\_ignore\_broadcasts*

* Nếu *kết quả là 0*, phản hồi ICMP đang được phép.
* Cấu hình:
* Mở file /etc/sysctl.conf bằng câu lệnh *sudo nano /etc/sysctl.conf*, thêm:
* **

1. *net.ipv4.icmp\_echo\_ignore\_all = 1*
2. *net.ipv4.icmp\_echo\_ignore\_broadcasts = 1*

* Áp dụng cấu hình bằng lệnh : sudo sysctl -p.
* Kiểm tra: cat /proc/sys/net/ipv4/icmp\_echo\_ignore\_all nếu trả về 1 nghĩa là đã cấu hình thành công.





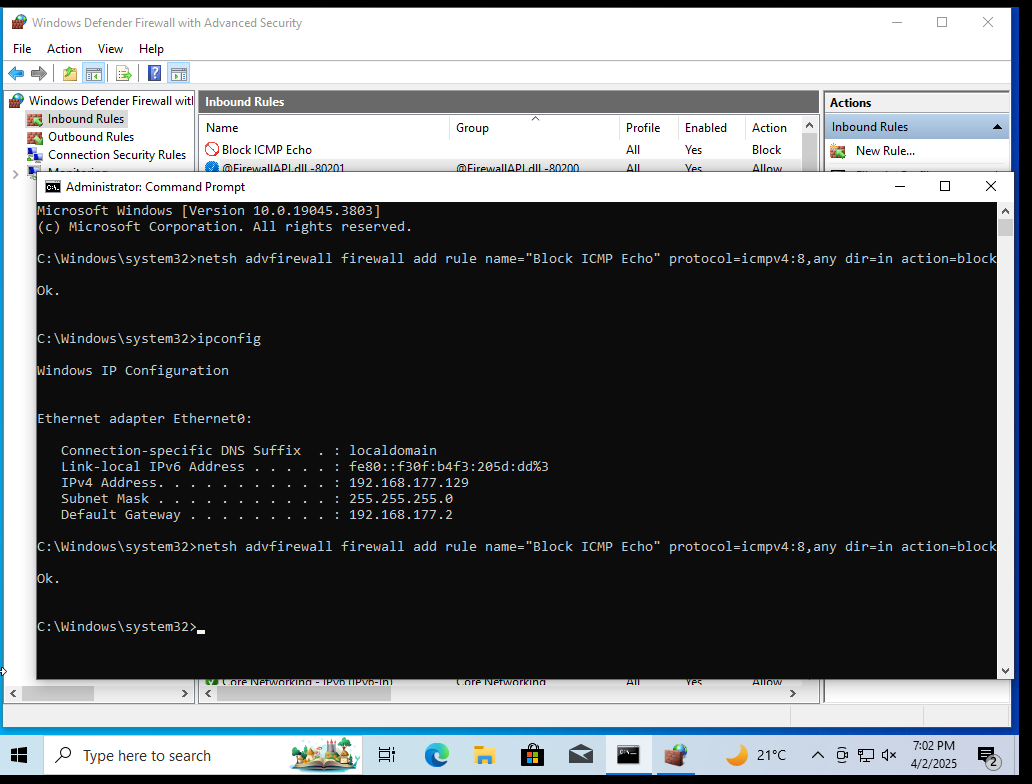
* Giới hạn băng thông (tùy chọn):

*sudo tc qdisc add dev eth0 root tbf rate 100kbit burst 10kb latency 50ms*

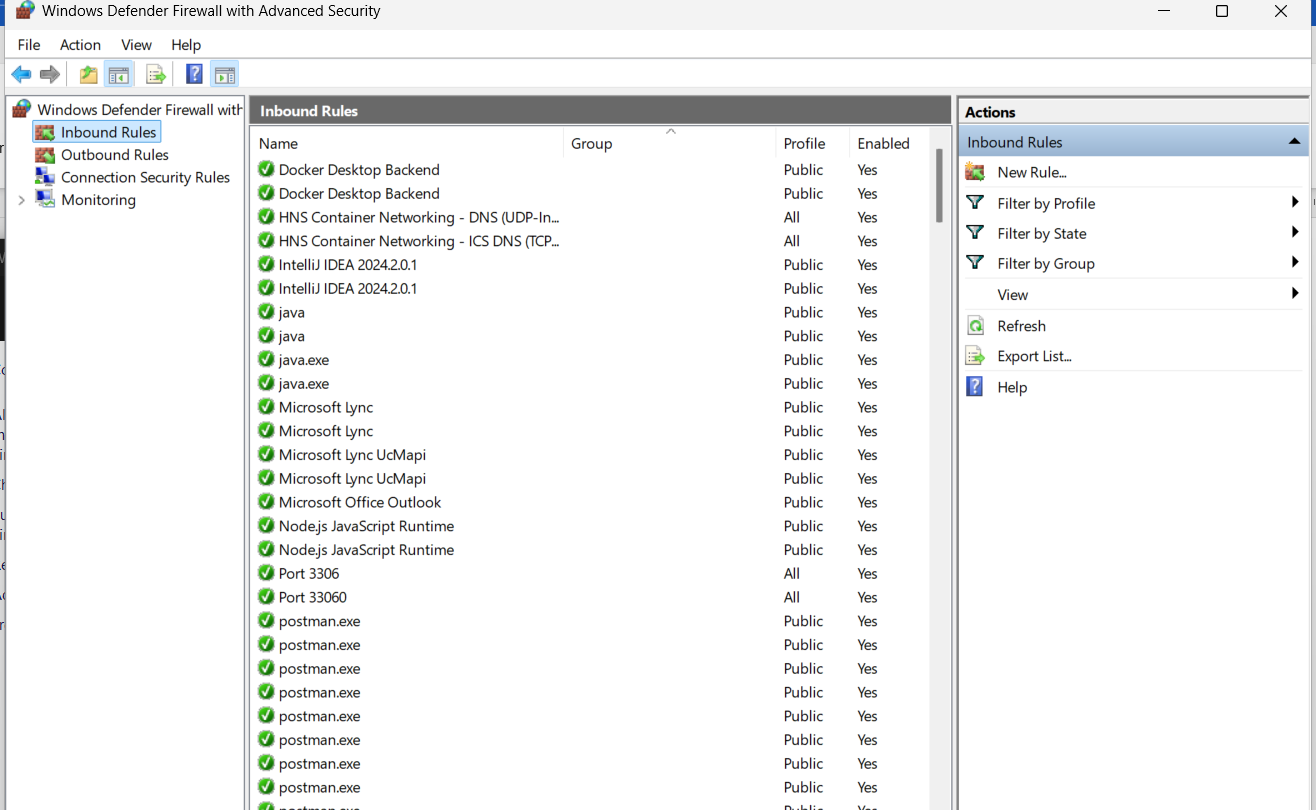
**- Trên Windows:**

* Dùng lệnh:

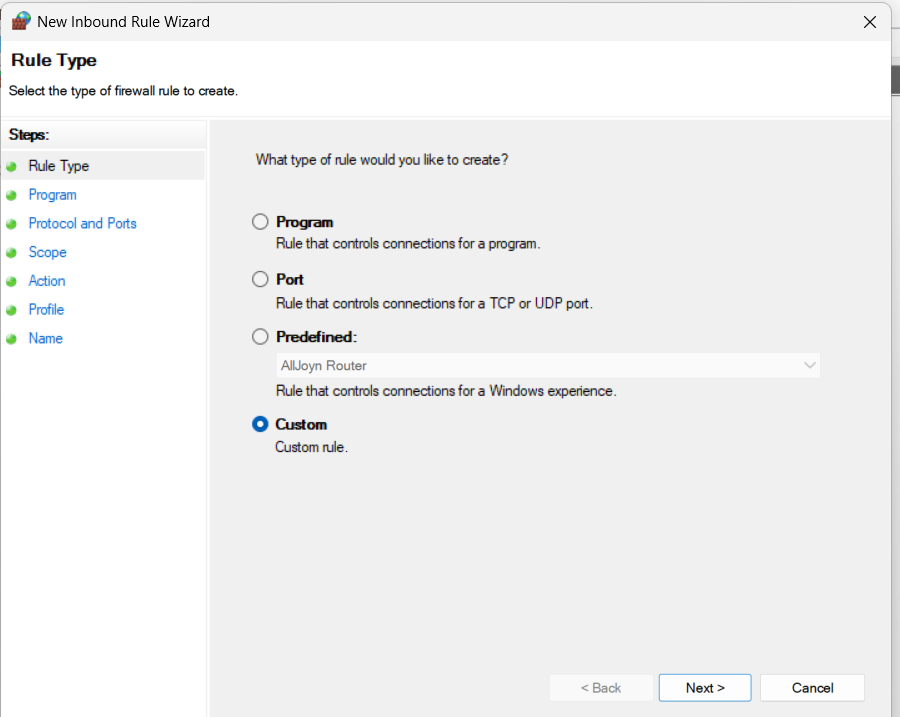
*netsh advfirewall firewall add rule name="Block ICMP Echo" protocol=icmpv4:8,any dir=in action=block*



* Tạo block ICMP Echo thủ công:

****

* *Mở Windows Defender Firewall > Advanced Settings > Inbound Rules > New Rule* chọn:
* *Rule Type: Custom*
* *Protocol Type: ICMPv4*
* *Specific ICMP Types: Echo Request*
* *Action: Block the connection*
* *Profile: All*
* *Name: "Block ICMP Echo"*



Kiểm tra: Từ máy khác, dùng ping [IP]. Nếu thấy "Request timed out", cấu hình thành công.

**Lợi ích:**

- Ngăn chặn thiết bị trong mạng tham gia vào việc khuếch đại lưu lượng Smurf.

- Giảm thiểu rủi ro mà không cần thay đổi cấu trúc mạng.

**Hạn chế:**

- Gây gián đoạn cho các công cụ chẩn đoán như ping hoặc traceroute.

- Không ngăn được tấn công nếu kẻ tấn công khai thác mạng khác làm trung gian.

**2. Cấu hình các router không chuyển tiếp yêu cầu ICMP gửi đến các địa chỉ quảng bá**

***Mô tả:***

* Trong Smurf Attack, router chuyển tiếp gói ICMP Echo Request đến địa chỉ broadcast sẽ khiến tất cả thiết bị trong mạng nhận được và phản hồi, tạo hiệu ứng khuếch đại
* Việc tắt tính năng chuyển tiếp broadcast trên router ngăn chặn gói tin đến các thiết bị, vô hiệu hóa cơ chế tấn công.
* Tắt tính năng chuyển tiếp IP directed broadcast.
* Router từ chối chuyển gói tin có đích là địa chỉ broadcast.
* Ngăn mạng bị lợi dụng làm bộ khuếch đại.

***Cách thực hiện:***

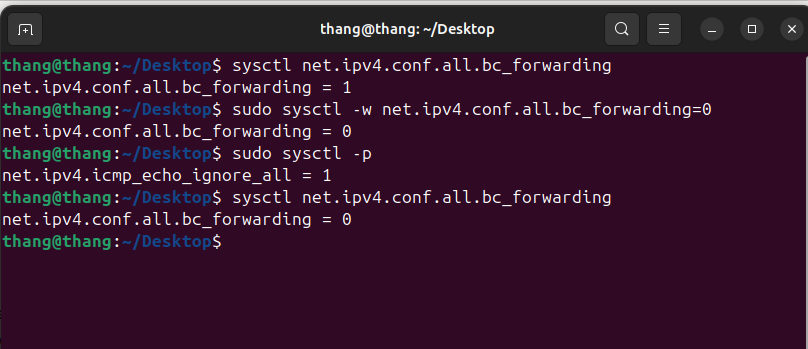
1. **Trên Ubuntu (dùng làm router):**

*- Kiểm tra: sysctl net.ipv4.conf.all.bc\_forwarding. Nếu là 1, chuyển tiếp broadcast đang bật.*

- Tắt:

*sudo sysctl -w net.ipv4.conf.all.bc\_forwarding=0*

*sudo sysctl -p*

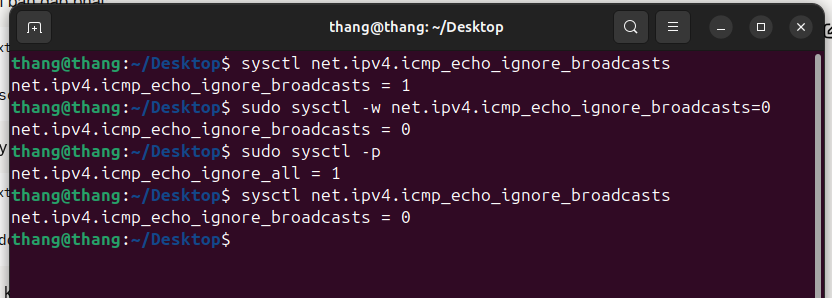
**

Hoặc có thể kiểm tra qua: *net.ipv4.icmp\_echo\_ignore\_broadcasts. Nếu là 1 thì chuyển tiếp broadcast đang bật.*

- Tắt:

sudo sysctl -w net.ipv4.icmp\_echo\_ignore\_broadcasts=0

*sudo sysctl -p*

**

1. **Trên Router Cisco:**

- Truy cập router qua SSH/Telnet dùng các lệnh:

* *enable*
* *configure terminal*
* *interface GigabitEthernet0/0*
* *no ip directed-broadcast*
* *exit*
* *write memory*

1. **Trên router phổ thông ( ví dụ:TP-Link ):**

* *Đăng nhập giao diện web (thường là 192.168.0.1).*
* *Vào "Advanced > Network > LAN Settings" hoặc "Firewall".*
* *Tìm và tắt "Enable IP Directed Broadcast" (nếu có), lưu và khởi động lại.*
* **Lợi ích:**

- Ngăn chặn khuếch đại lưu lượng ngay tại router, bảo vệ mạng nội bộ.

- Không ảnh hưởng đến các yêu cầu ICMP hợp lệ không gửi đến broadcast.

- Giảm tải xử lý cho router.

* **Hạn chế:**

- Có thể ảnh hưởng đến các ứng dụng hiếm hoi dùng broadcast (như Wake-on-LAN).

- Không hiệu quả nếu kẻ tấn công khai thác mạng khác có broadcast bật.

**3. Sử dụng tường lửa để lọc các gói tin với địa chỉ giả mạo trong mạng**

***Mô tả:***

* Smurf Attack giả mạo source IP thành địa chỉ của nạn nhân để đánh lừa các máy trong mạng phản hồi.
* Tường lửa có thể được cấu hình để kiểm tra tính hợp lệ của địa chỉ nguồn, chặn các gói tin giả mạo từ bên ngoài nhưng có nguồn thuộc mạng nội bộ.
* Phát hiện và chặn gói tin có source IP không hợp lệ.
* Kiểm tra tính hợp lệ bằng kỹ thuật anti-spoofing.
* Ngăn lưu lượng giả mạo đến từ bên ngoài mạng.

***Cách thực hiện:***

1. **Trên Ubuntu (iptables):**

* Bật Reverse Path Filtering:

sudo sysctl -w net.ipv4.conf.all.rp\_filter=1

sudo sysctl -w net.ipv4.conf.eth0.rp\_filter=1

sudo sysctl -p

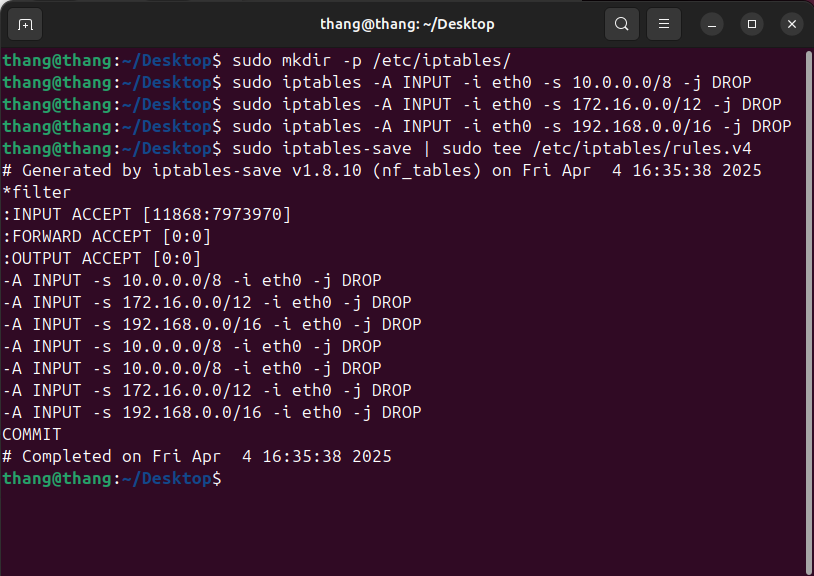
* Chặn gói tin giả mạo:

sudo iptables -A INPUT -i eth0 -s 192.168.1.0/24 -j DROP

sudo iptables -A INPUT -i eth0 -s 10.0.0.0/8 -j DROP

sudo iptables -A INPUT -i eth0 -s 172.16.0.0/12 -j DROP

sudo iptables-save | sudo tee /etc/iptables/rules.v4



1. **Trên Windows:**

- Sử dụng Windows Firewall:

+ Mở Windows Defender Firewall with Advanced Security.

+ Chọn Inbound Rules > New Rule.

+ Cấu hình:

+ Rule Type: Custom

+ Protocol Type: ICMPv4

+ Scope:

. Local IP: Any

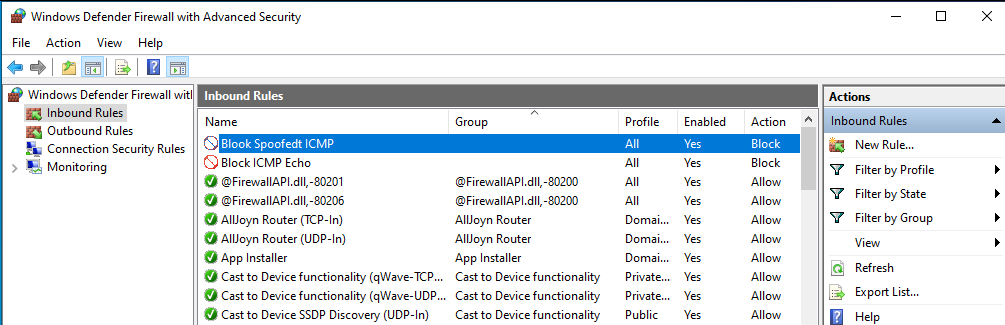
. Remote IP: Chọn "These IP addresses" và thêm dải IP nội bộ (ví dụ: 192.168.1.0-192.168.1.255)

+ Action: Block the connection

+ Profile: Tất cả

+ Name: "Block Spoofed ICMP"

+ Nhấn Finish.



1. **Trên Router Cisso:**

+ Dùng Access Control List (ACL):

* *Enable*
* *configure terminal*
* *access-list 101 deny ip 192.168.1.0 0.0.0.255 any*
* *interface [WAN\_interface]*
* *ip access-group 101 in exit*
* *write memory*
* **Lợi ích:**

- Bảo vệ mạng khỏi bị lợi dụng trong Smurf và các tấn công giả mạo khác.

- Tăng cường an ninh tổng thể chống spoofing.

* **Hạn chế:**

- Yêu cầu cấu hình chính xác, nếu sai có thể chặn nhầm lưu lượng hợp lệ.

- Không ngăn được tấn công nếu kẻ tấn công dùng source IP hợp lệ từ mạng khác.

* Như vậy, khi bị tấn công Smurf chúng ta cần thực hiện các quy trình sau:

1. Phát hiện: Theo dõi lưu lượng bằng công cụ như Wireshark, nhận diện tăng đột biến ICMP Echo Request.
2. Phản ứng: Áp dụng các biện pháp trên (chặn ICMP, tắt broadcast, lọc spoofing).
3. Phối hợp: Liên hệ ISP để lọc lưu lượng ở cấp độ mạng lõi nếu tấn công vượt khả năng xử lý nội bộ.
4. Đánh giá: Sau khi xử lý, phân tích nguyên nhân và cải thiện cấu hình để ngăn tái diễn.

***Kết luận:***

Tấn công Smurf tuy không còn phổ biến nhưng vẫn nguy hiểm với các mạng chưa được bảo vệ. Việc kết hợp ba biện pháp trên – chặn phản hồi ICMP, tắt chuyển tiếp broadcast, và lọc gói tin giả mạo – tạo thành một chiến lược phòng thủ toàn diện. Tuy nhiên, cần cân nhắc các hạn chế để tránh ảnh hưởng đến hoạt động hợp lệ của mạng. Giám sát liên tục và cập nhật hệ thống là yếu tố then chốt để duy trì an ninh mạng trước các mối đe dọa như Smurf