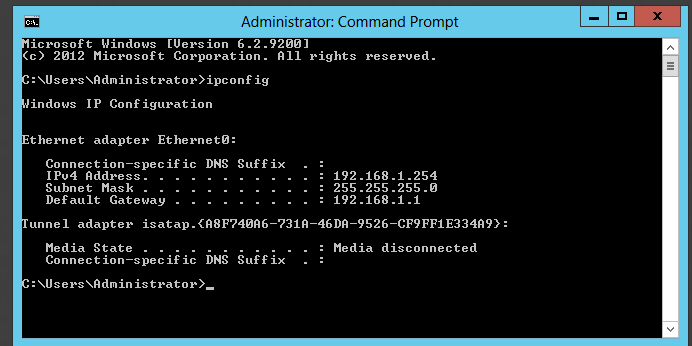
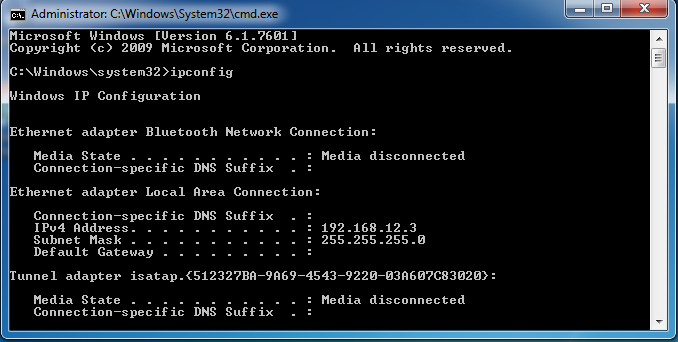
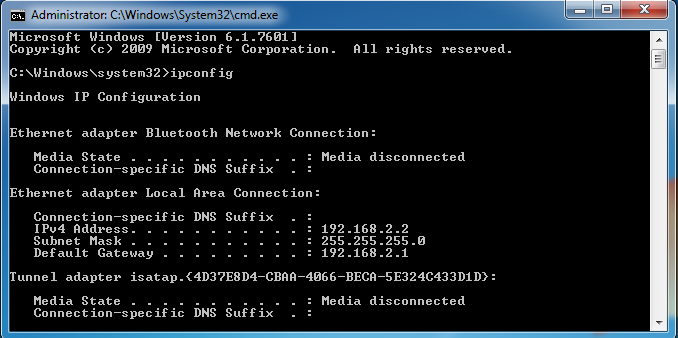


PC-1 :



PC-2 : 

PC-3 :

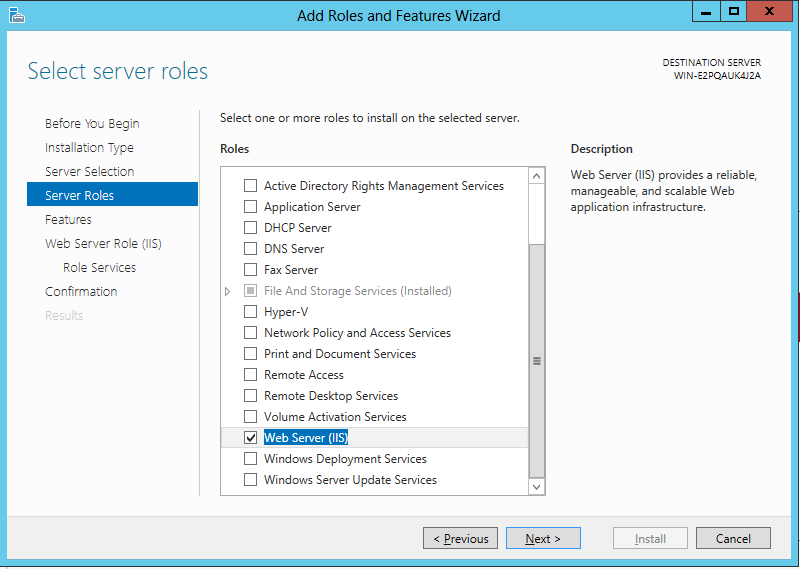


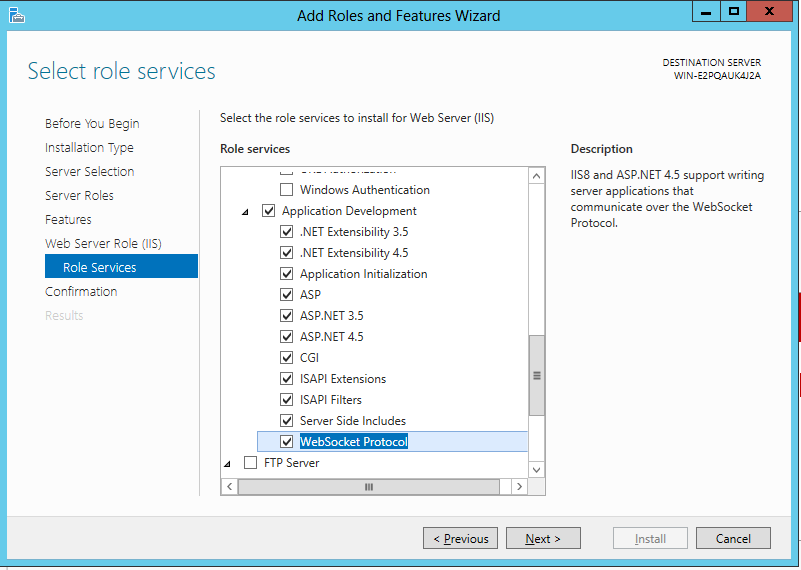




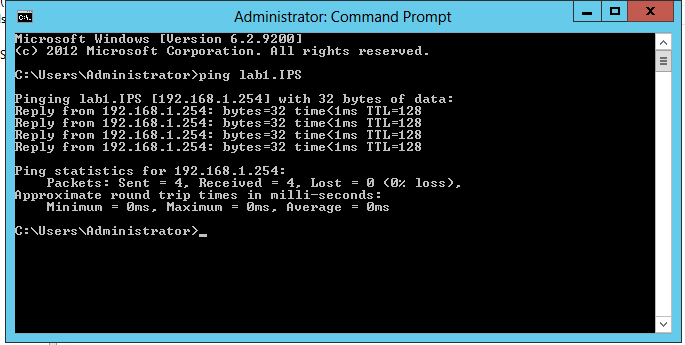


Cài đặt webserver:

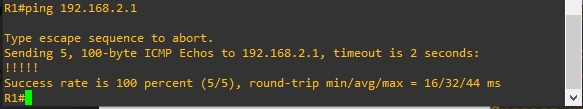




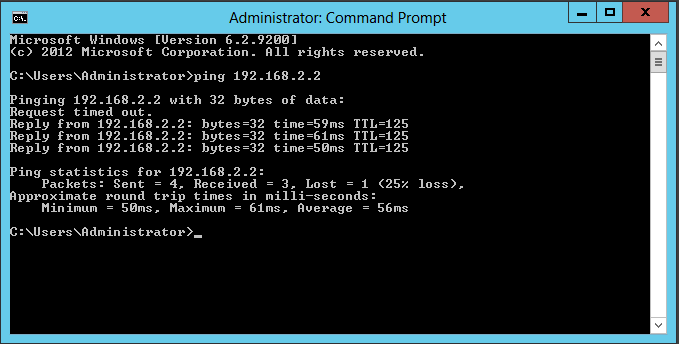
Ping thành công đến webserver đã tạo



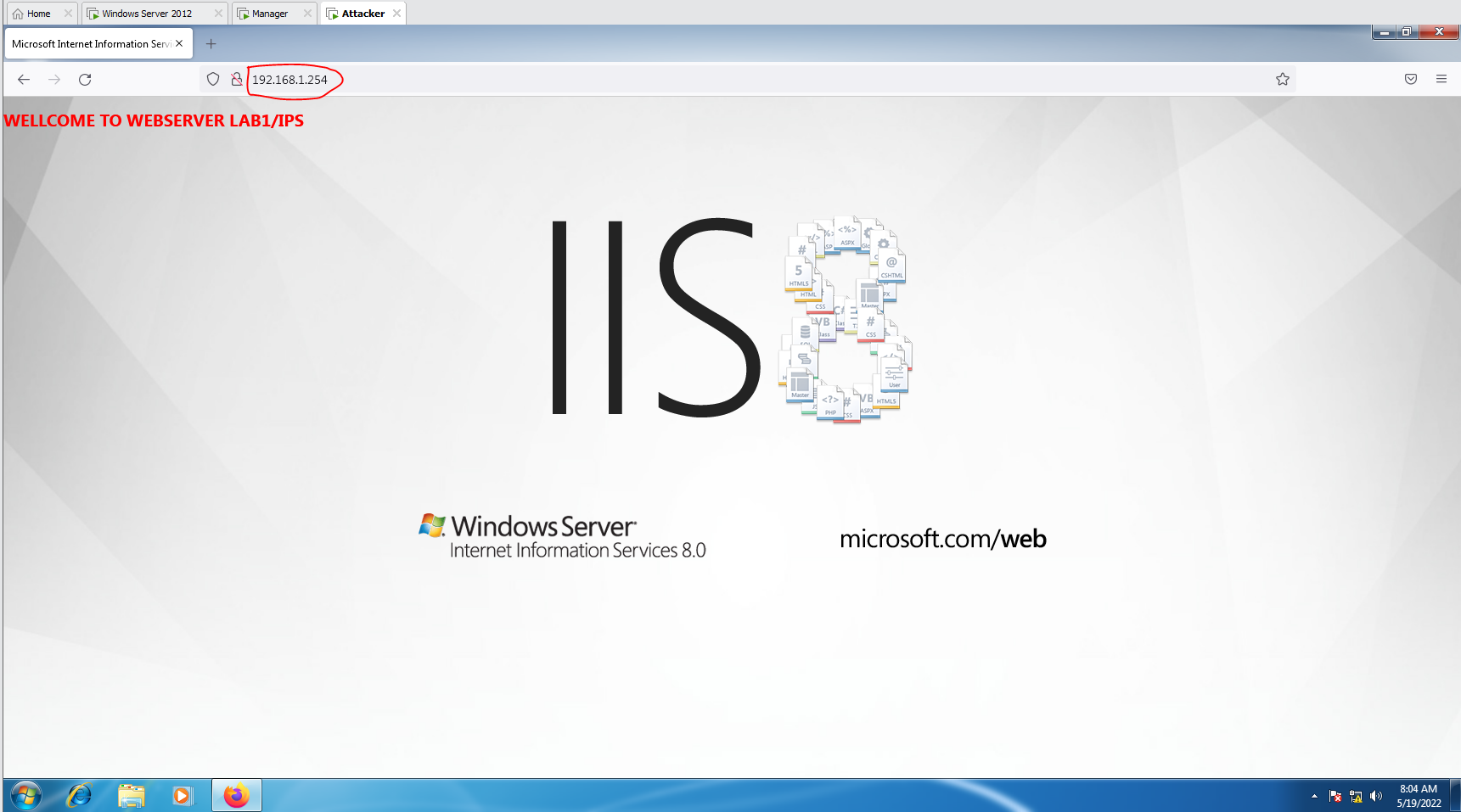
PING THÀNH CÔNG TỪ R1 ĐẾN R3 :



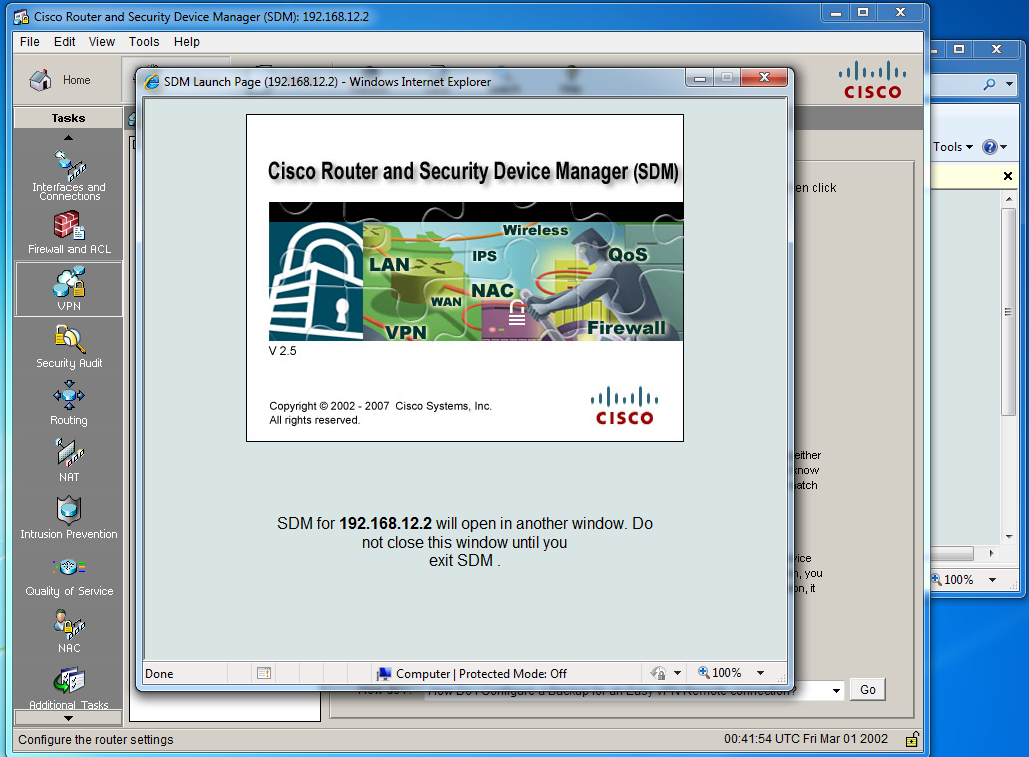
PING THÀNH CÔNG TỪ PC-1 ĐẾN PC-3 :



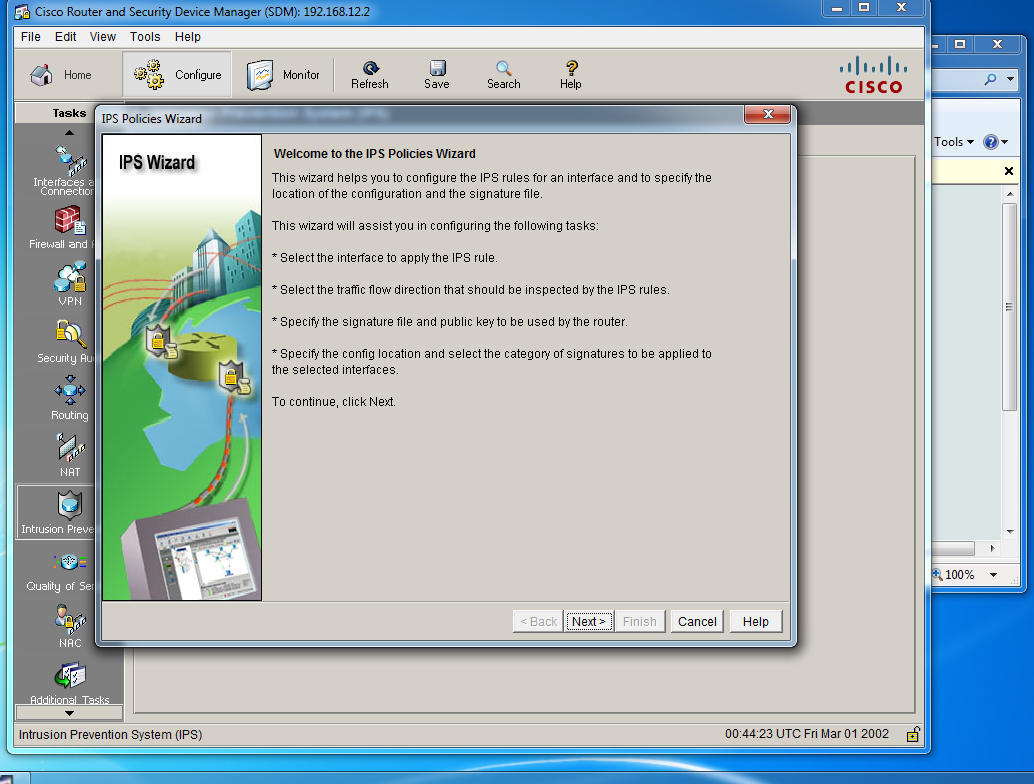
Truy cập vào webserver

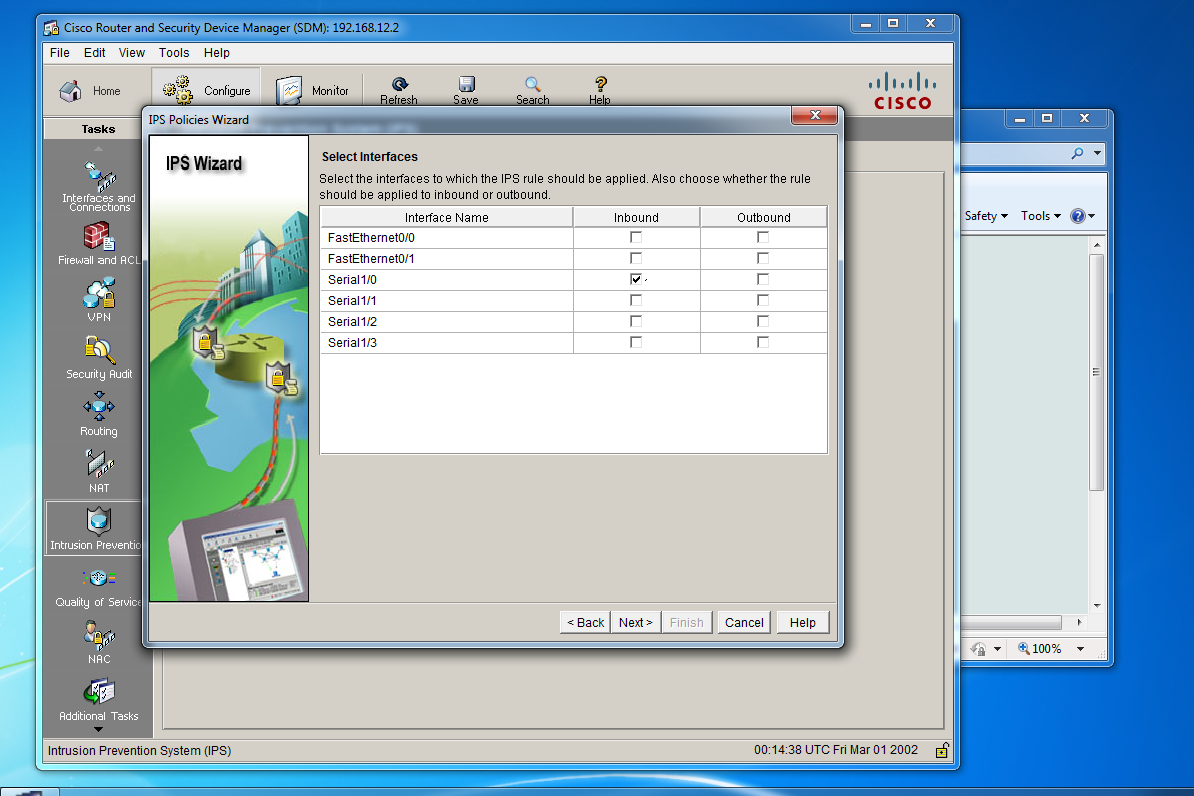


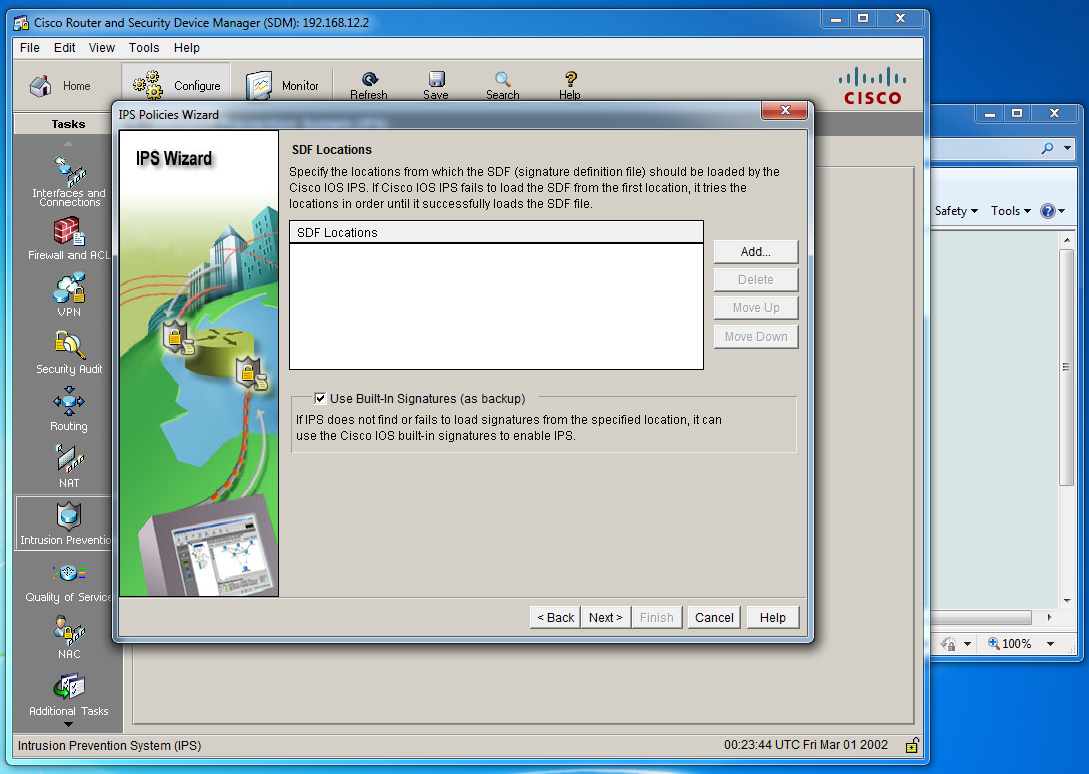
Truy cập vào SDM



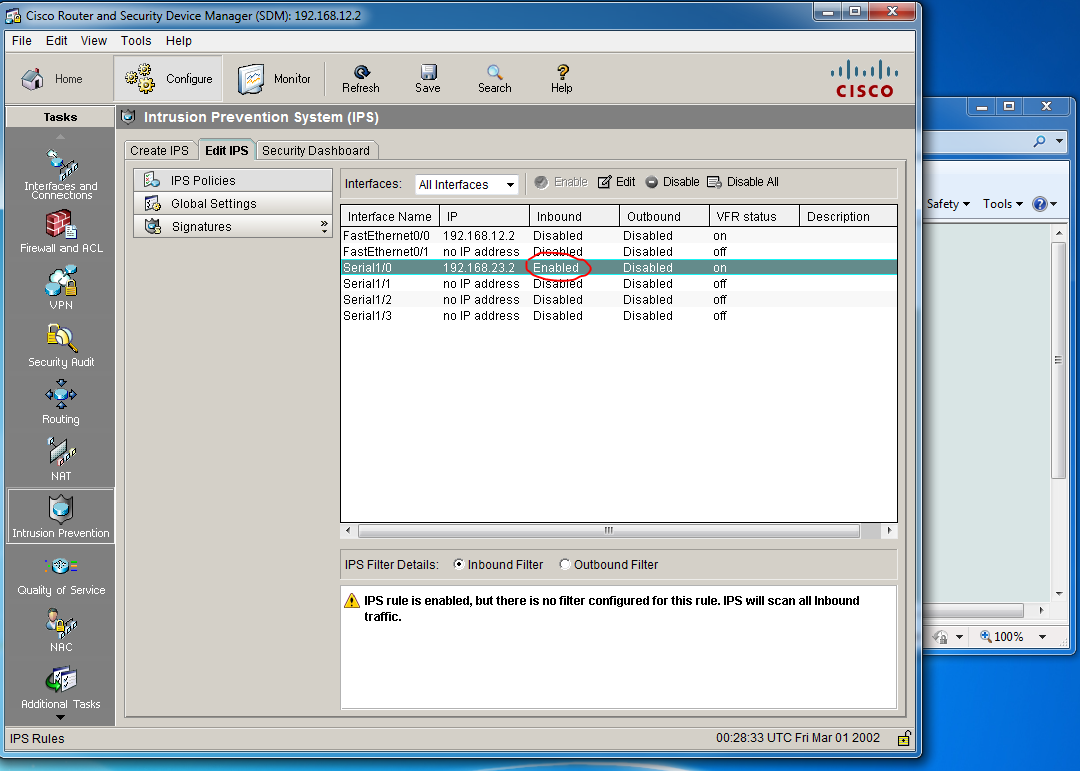
Cấu hình Policies Ips Wizrad



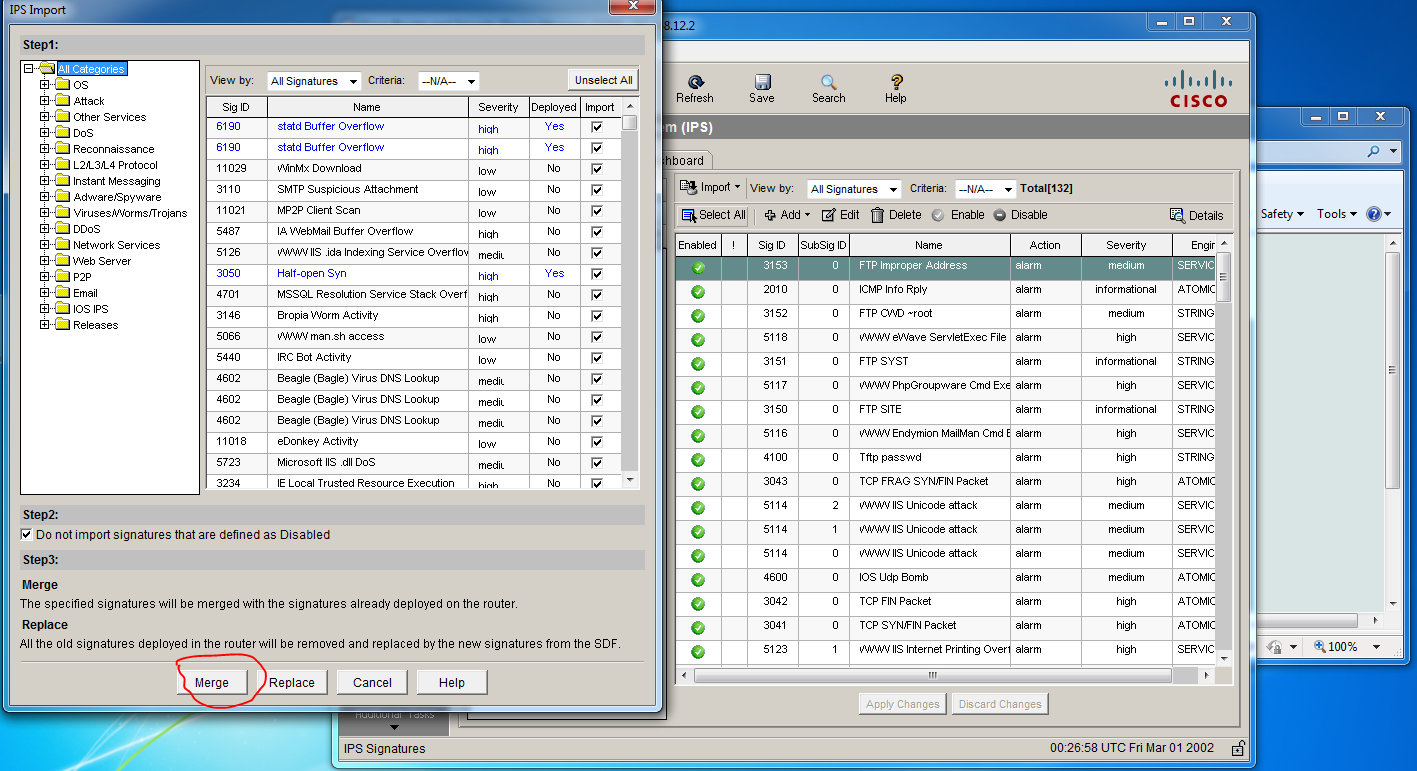




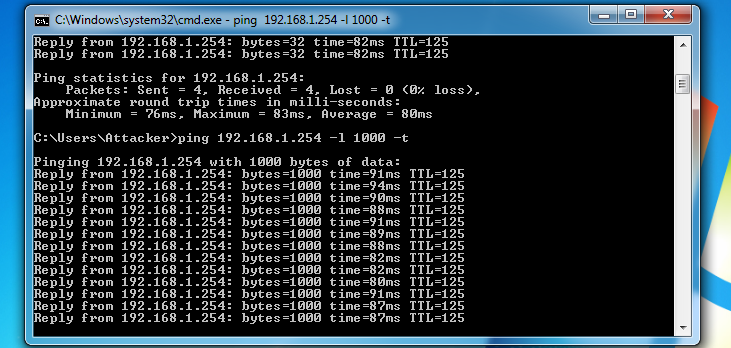
Sau khi Wizrad xong thì cổng s1/0 đã được inbound enable các Signatures



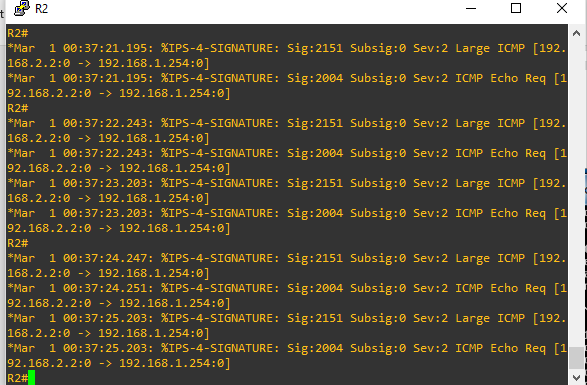
Ta tiến hành cài gói signature 256 cho các signature ở cổng S1/0



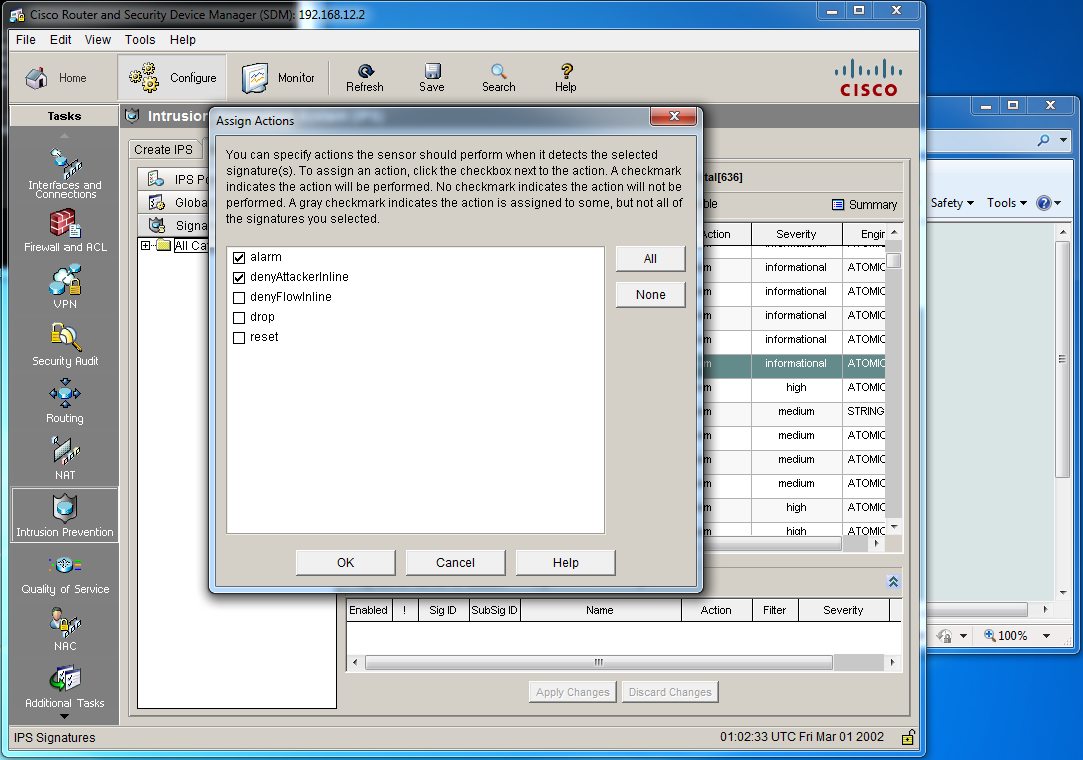
Ta thực hiện ping of dead webserver bằng máy attacker



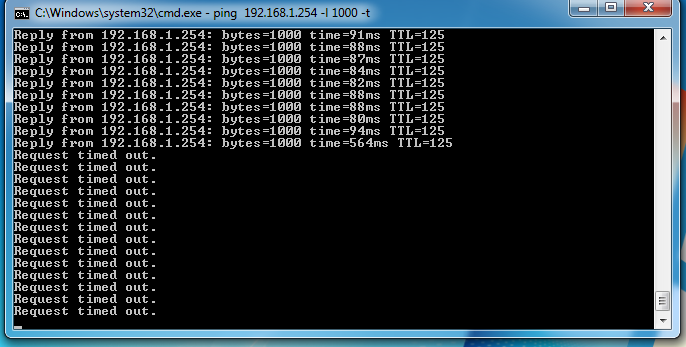
R2 cảnh báo signature khi bị ping quá nhiều gói Icmp lớn tới



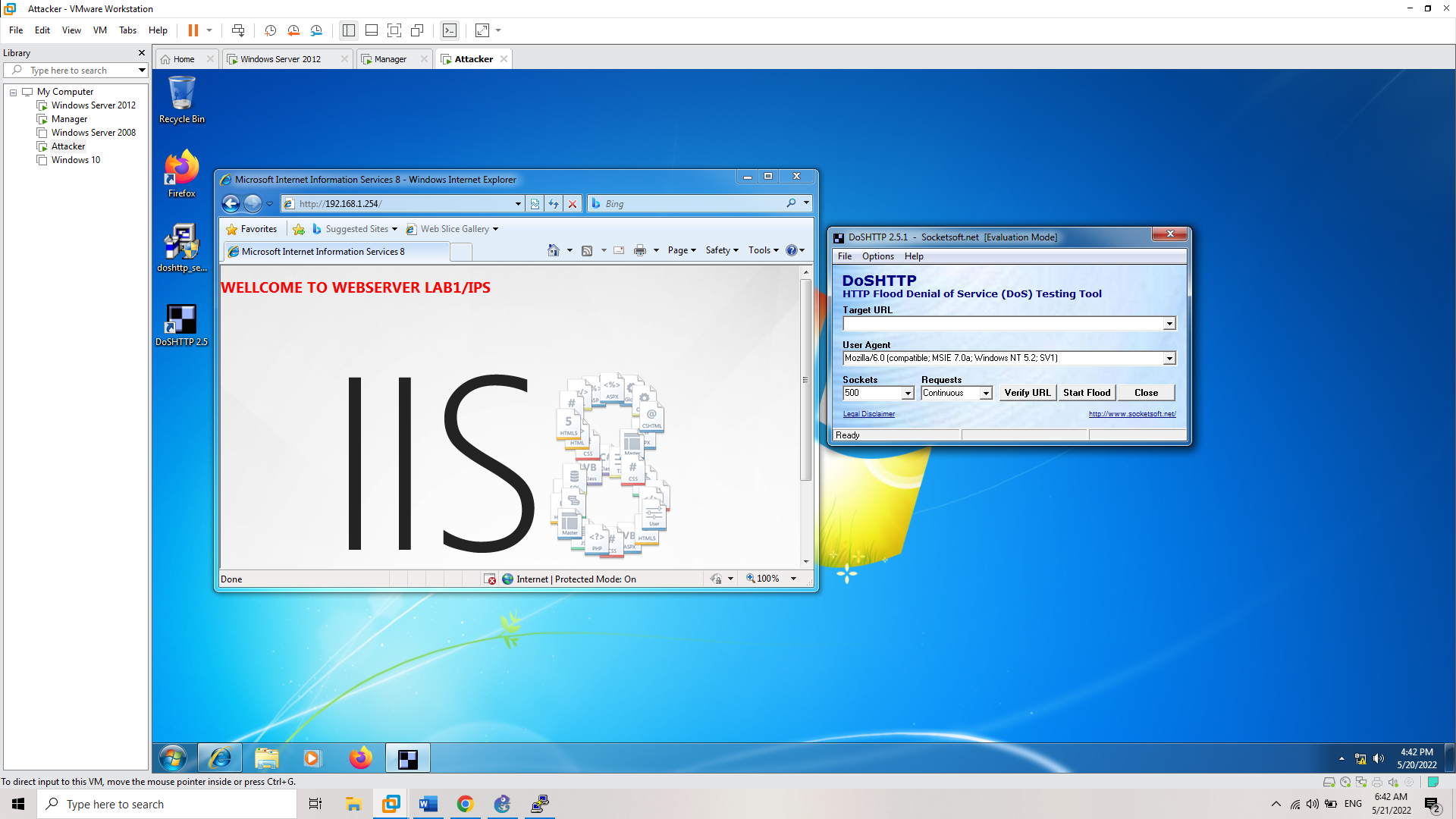
Ta tiến hành bật rule 2151 chặn việc ping of death trên máy manager



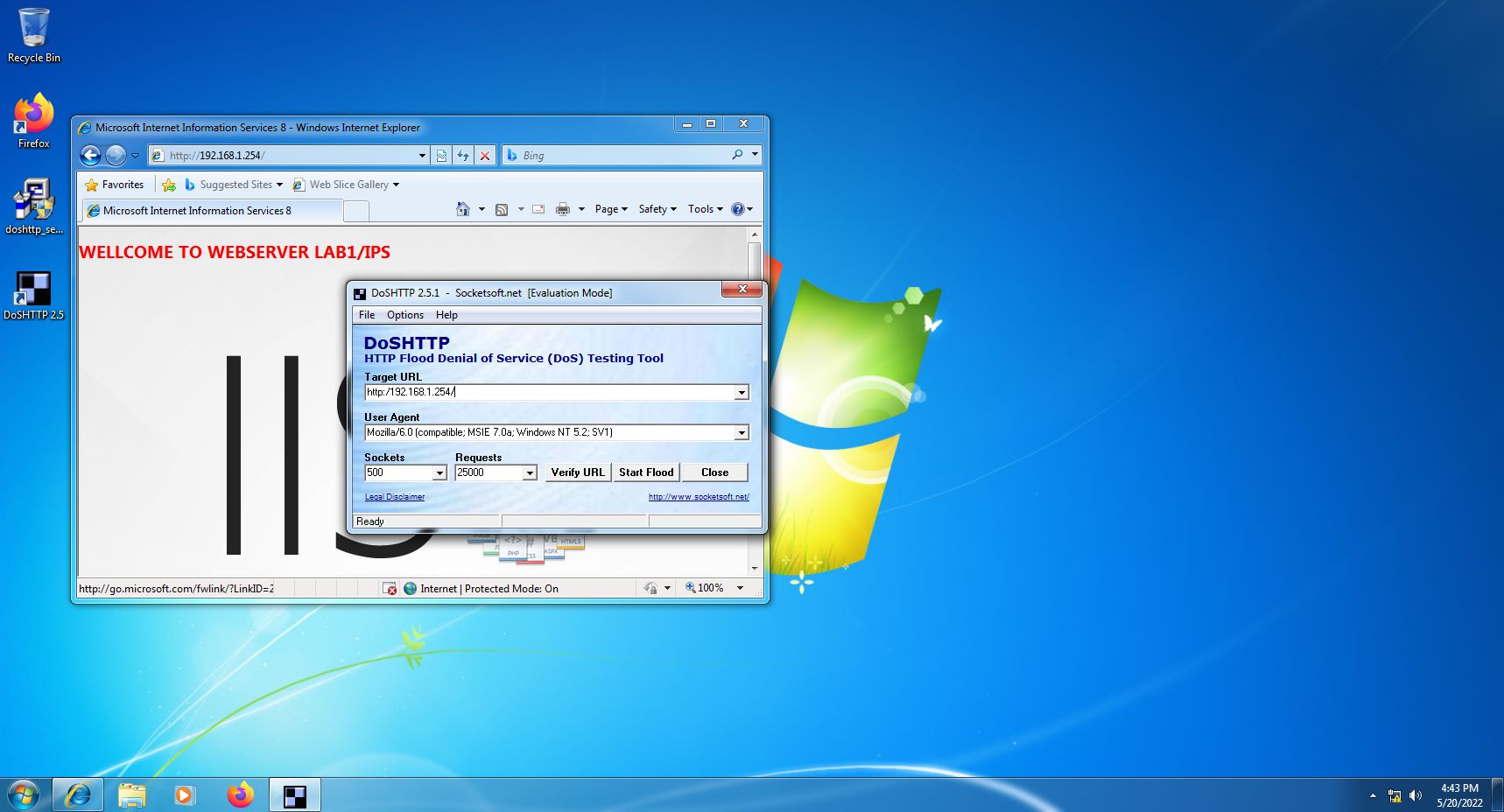
Sau đó thì máy attacker đã không thể ping gói icmp tới máy webserver được nữa



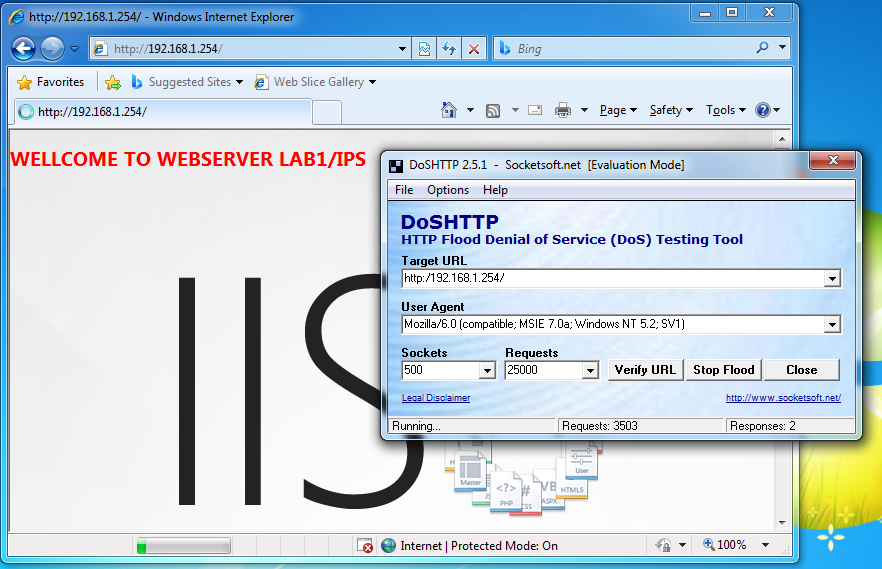
Tình trạng webserver bình thường trước khi ta tiến hành Ddos nó



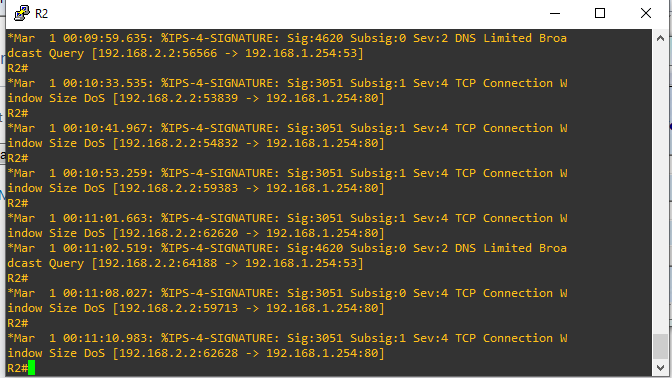
Ta bắt đầu tiến hành Ddos webserver



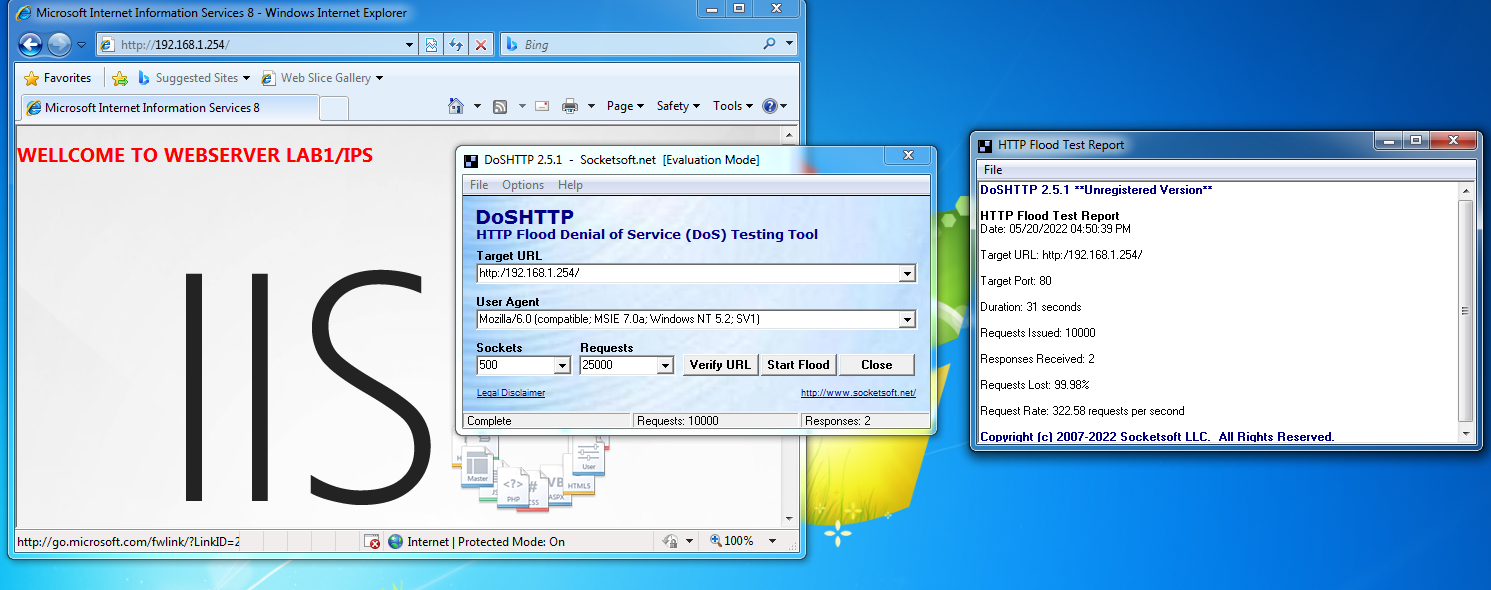
Khi đang bị Ddos thì ta thử reload lại trang web thì thấy là load rất lâu



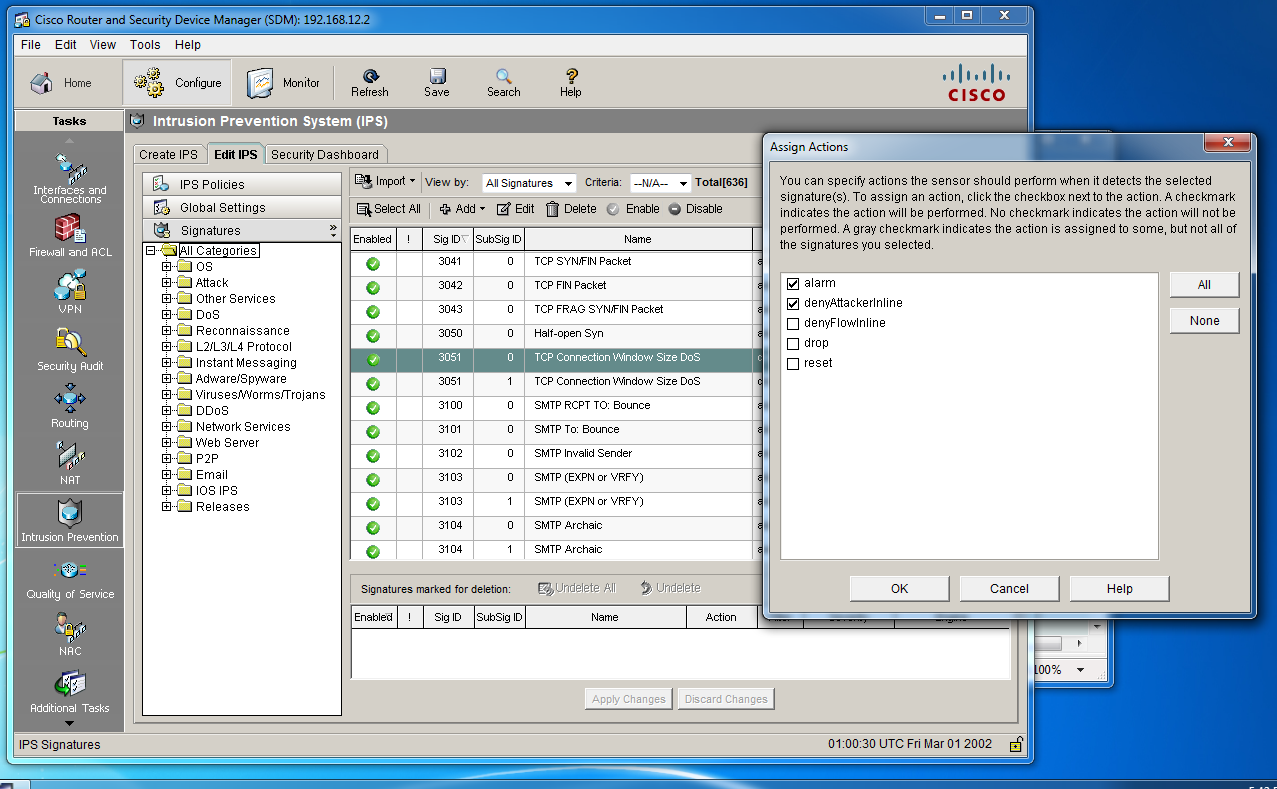
R2 có báo các signature khi các gói TCP 3051 Ddos



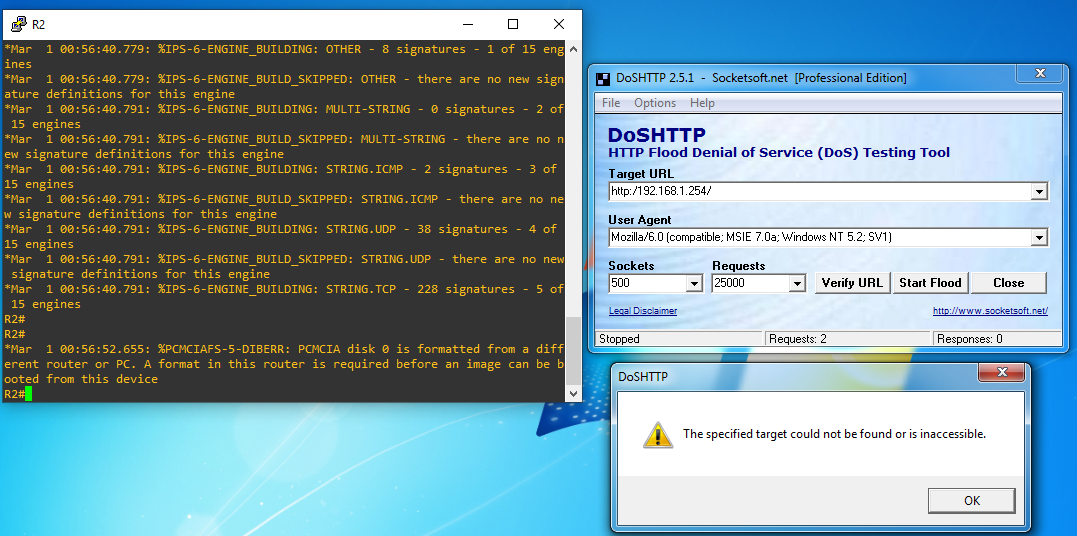
Sau khi đừng Ddos thì đã truy cập webserver lại 1 cách bình thường



Ta tiến hành bật rule chặn Ddos 3051



Sau khi ta tiến hành bật rule chặn Ddos thì Công cụ đã không thể Ddos tới máy webserver được nữa và request trả về ở mức rất thấp



Ta tiến hành scanport của webserver và thấy R2 báo log về



Thực hiện ngăn chặn scanport trên máy manager



Máy attacker đã không thể scan được port của máy webserver

