BAN CƠ YẾU CHÍNH PHỦ

HỌC VIỆN KỸ THUẬT MẬT MÃ

MODULE THỰC HÀNH

AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 01

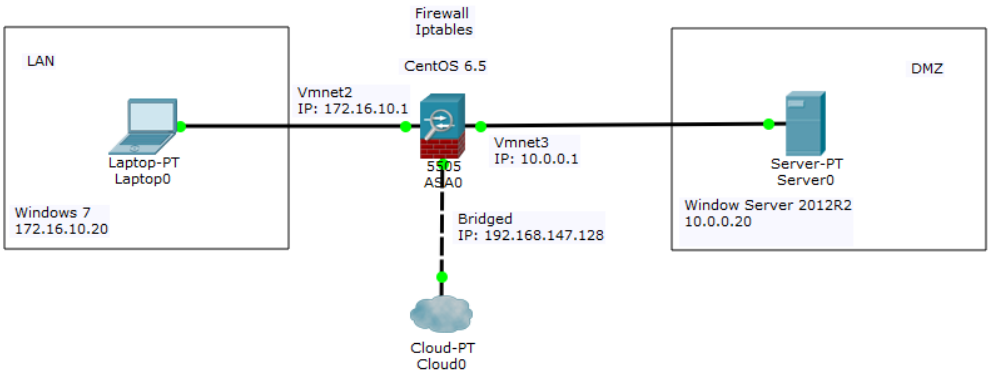
Thiết lập và cấu hình tường lửa Iptables

Sinh viên thực hiện:

Nguyễn Đức Mạnh - AT170432

1. CHUẨN BỊ

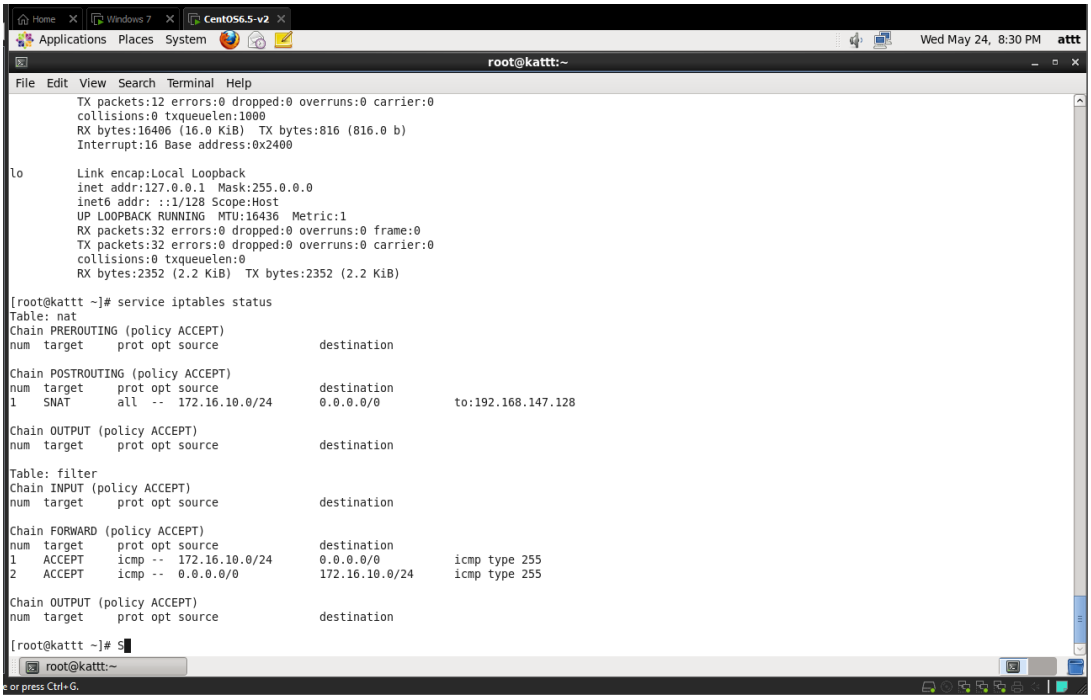
Vẽ lại mô hình mạng chuẩn bị thực hành *(bao gồm các kết nối, địa chỉ IP, hệ điều hành, tên máy, ứng dụng được cài đặt)* và dán vào bên dưới.



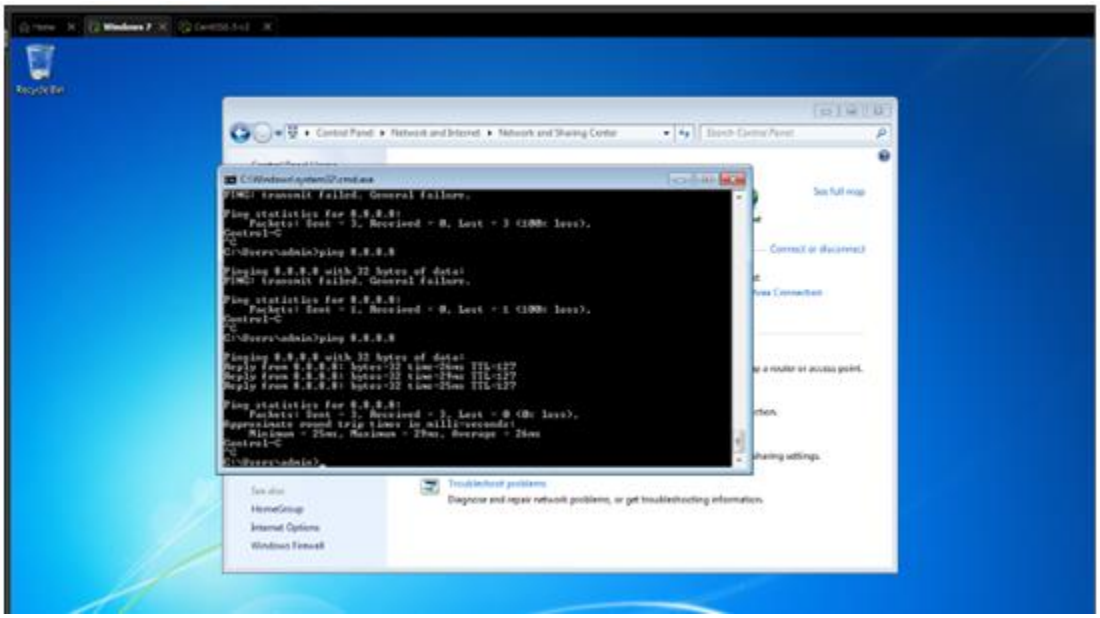
2. THỰC HÀNH

Kịch bản 1. Cho phép máy tính trong LAN Ping ra ngoài mạng Internet

Chụp ảnh luật trên tường lửa Iptables để cho phép máy trạm Ping ra bên ngoài và dán vào bên dưới.

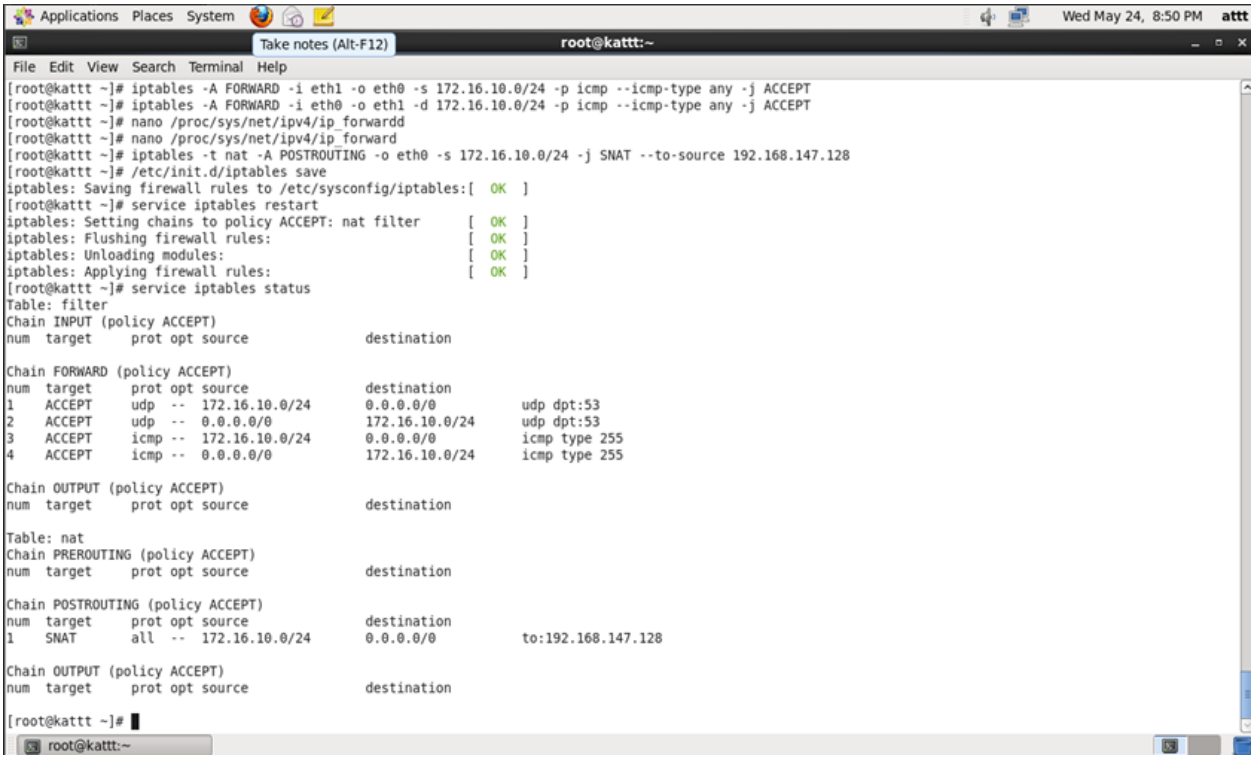


Chụp ảnh kiểm tra kết quả và dán vào bên dưới.



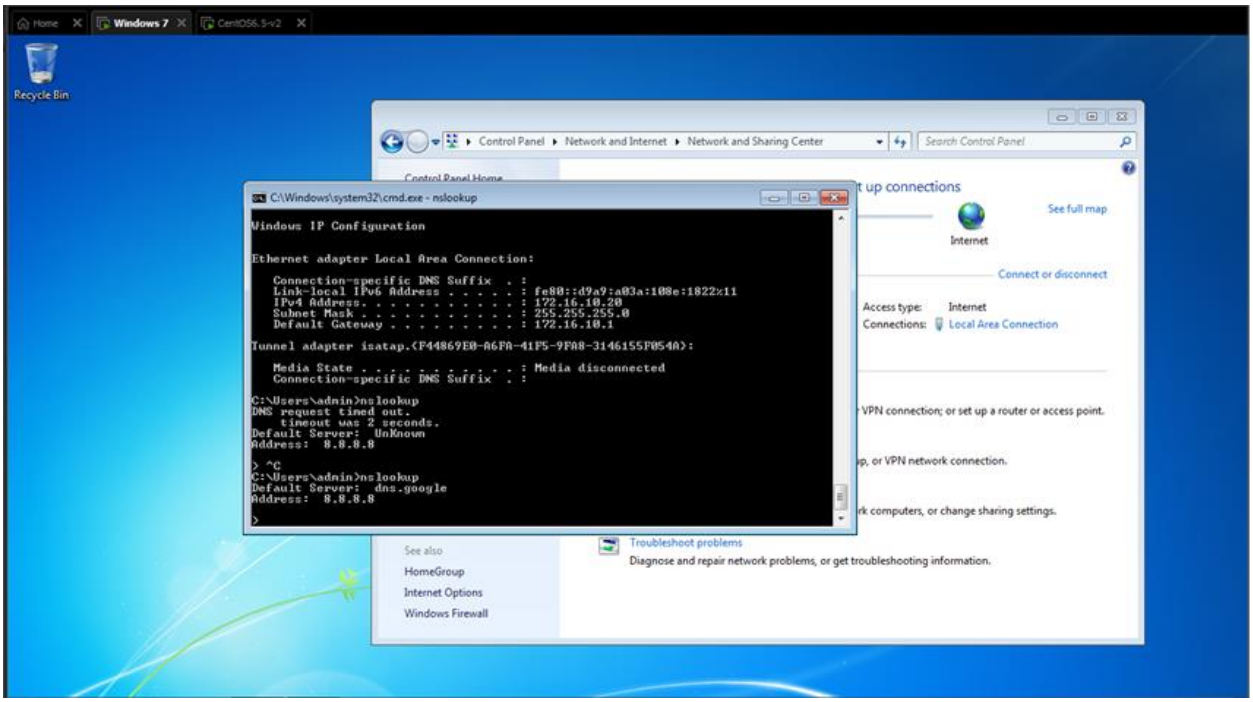
Kịch bản 2. Cho phép máy tính trong LAN truy vấn DNS ra Internet

Chụp ảnh cấu hình luật để cho phép truy vấn DNS tại tường lửa và dán vào bên dưới



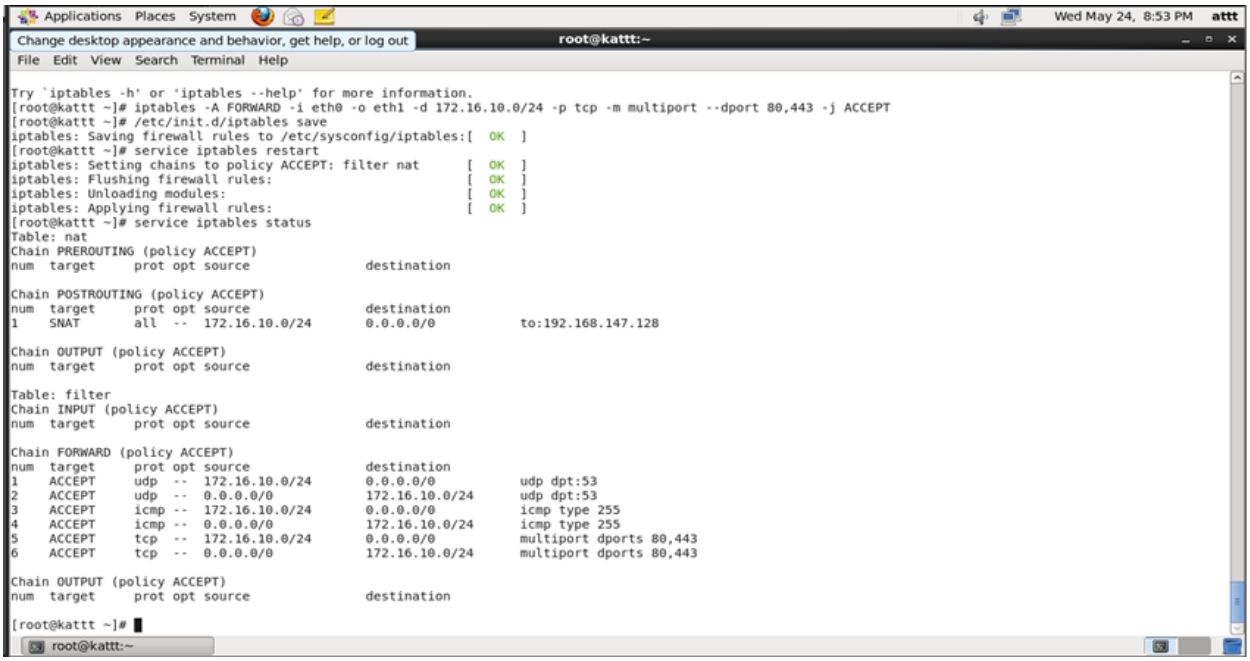
```
Applications  Places  System                                   Wed May 24, 8:50 PM  attt
Take notes (Alt-F12)                  root@kattt:~
File  Edit  View  Search  Terminal  Help
[root@kattt ~]# iptables -A FORWARD -i eth1 -o eth0 -s 172.16.10.0/24 -p icmp --icmp-type any -j ACCEPT
[root@kattt ~]# iptables -A FORWARD -i eth0 -o eth1 -d 172.16.10.0/24 -p icmp --icmp-type any -j ACCEPT
[root@kattt ~]# nano /proc/sys/net/ipv4/ip_forwardd
[root@kattt ~]# nano /proc/sys/net/ipv4/ip_forward
[root@kattt ~]# iptables -t nat -A POSTROUTING -o eth0 -s 172.16.10.0/24 -j SNAT --to-source 192.168.147.128
[root@kattt ~]# /etc/init.d/iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]
[root@kattt ~]# service iptables restart
iptables: Setting chains to policy ACCEPT: nat filter      [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
[root@kattt ~]# service iptables status
Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     udp  --  172.16.10.0/24       0.0.0.0/0           udp dpt:53
2    ACCEPT     udp  --  0.0.0.0/0            172.16.10.0/24      udp dpt:53
3    ACCEPT     icmp --  172.16.10.0/24       0.0.0.0/0           icmp type 255
4    ACCEPT     icmp --  0.0.0.0/0            172.16.10.0/24      icmp type 255

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Table: nat
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    SNAT       all  --  172.16.10.0/24       0.0.0.0/0           to:192.168.147.128

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

[root@kattt ~]#
root@kattt:~
```

Chụp ảnh kiểm tra kết quả và dán vào bên dưới.

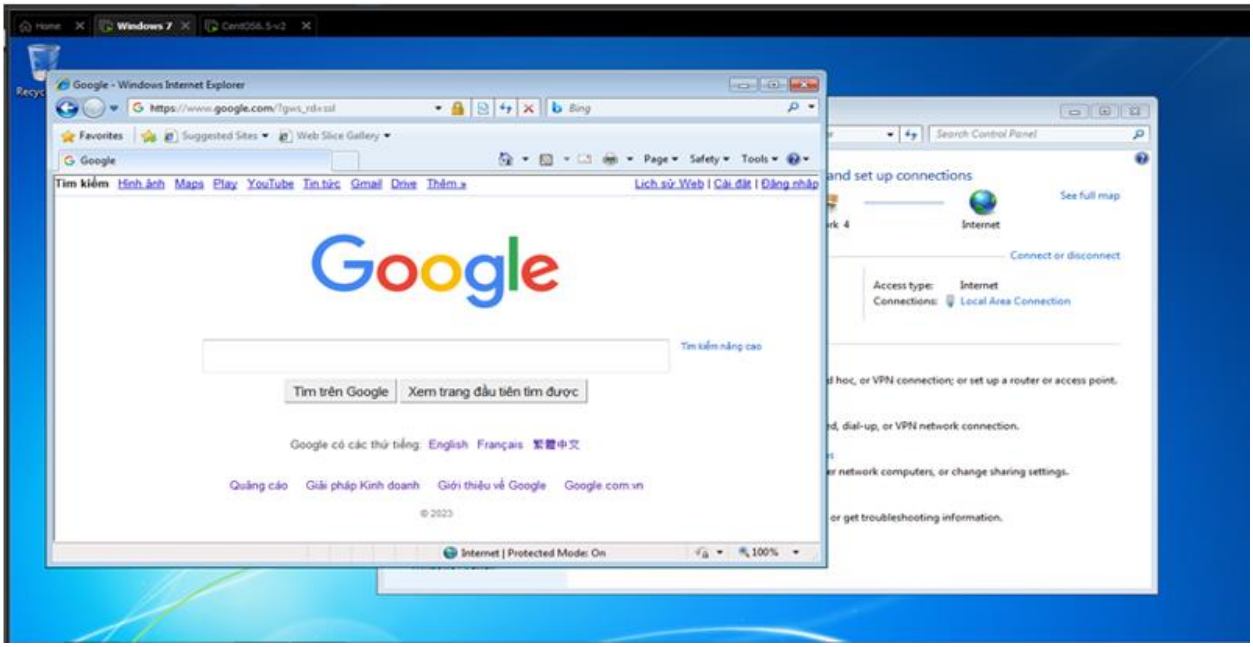


Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet

Chụp ảnh cấu hình luật để cho các máy tính trạng mạng nội bộ có thể truy cập được mạng Internet thông qua hai giao thức HTTP và HTTPS và dán vào bên dưới.



Chụp ảnh kiểm tra kết quả và dán vào bên dưới.

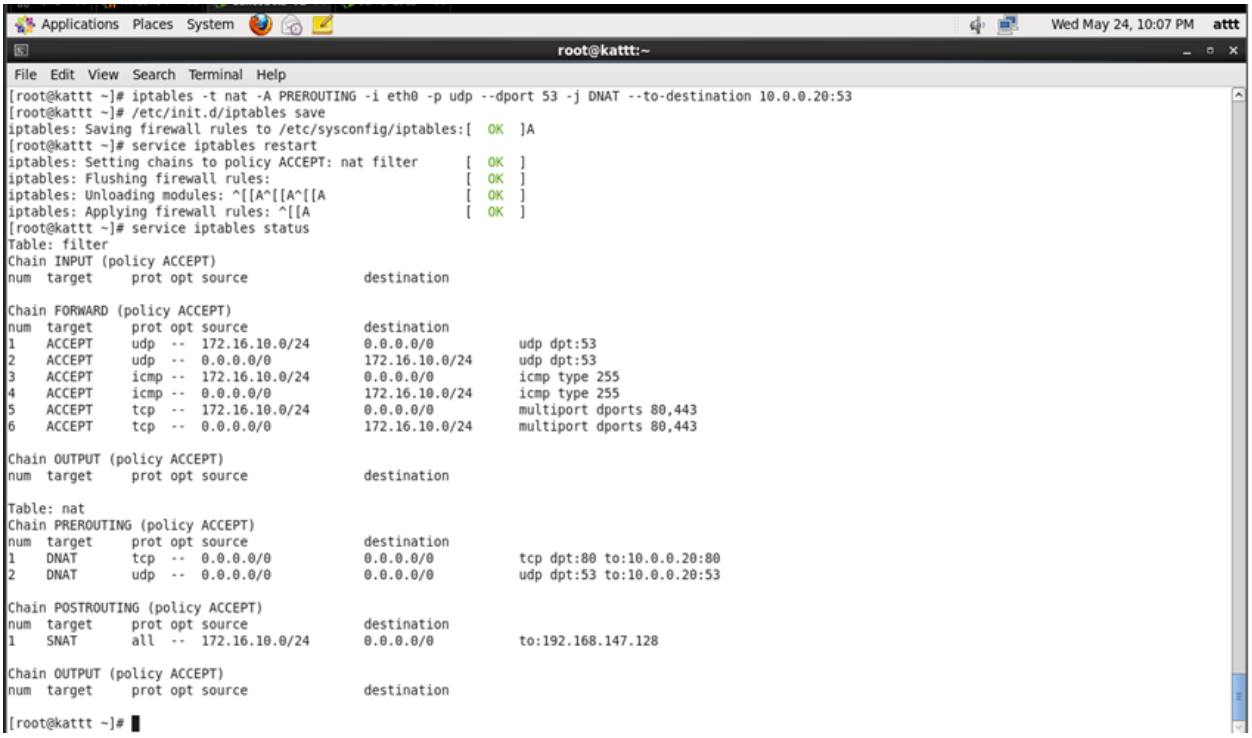


Kịch bản 4. Cho phép truy cập tới máy chủ web trong phân vùng mạng DMZ

Chụp ảnh cấu hình luật để cho các máy tính trong mạng nội bộ có thể truy cập được website từ máy chủ web trong mạng DMZ và dán vào bên dưới.

```
Applications  Places  System                                   Wed May 24, 11:04 PM  attt
root@kattt:~
File  Edit  View  Search  Terminal  Help
[root@kattt ~]# service iptables restart
iptables: Setting chains to policy ACCEPT: filter nat      [  OK  ]
iptables: Flushing firewall rules:                         [  OK  ]
iptables: Unloading modules:                               [  OK  ]
iptables: Applying firewall rules:                         [  OK  ]
[root@kattt ~]# service iptables status
Table: nat
Chain PREROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    DNAT       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 to:10.0.0.20:80
2    DNAT       udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53 to:10.0.0.20:53

Chain POSTROUTING (policy ACCEPT)
num  target     prot opt source               destination
1    SNAT       all  --  172.16.10.0/24       0.0.0.0/0           to:192.168.147.128

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

Table: filter
Chain INPUT (policy ACCEPT)
num  target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
num  target     prot opt source               destination
1    ACCEPT     udp  --  172.16.10.0/24       0.0.0.0/0           udp dpt:53
2    ACCEPT     udp  --  0.0.0.0/0            172.16.10.0/24      udp dpt:53
3    ACCEPT     icmp --  172.16.10.0/24       0.0.0.0/0           icmp type 255
4    ACCEPT     icmp --  0.0.0.0/0            172.16.10.0/24      icmp type 255
5    ACCEPT     tcp  --  172.16.10.0/24       0.0.0.0/0           multiport dports 80,443
6    ACCEPT     tcp  --  0.0.0.0/0            172.16.10.0/24      multiport dports 80,443
7    ACCEPT     tcp  --  172.16.10.0/24       0.0.0.0/0           tcp dpt:80
8    ACCEPT     udp  --  172.16.10.0/24       0.0.0.0/0           udp dpt:53
9    ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0

Chain OUTPUT (policy ACCEPT)
num  target     prot opt source               destination

[root@kattt ~]#
```

Chụp ảnh cấu hình luật để cho các máy tính từ mạng Internet có thể truy cập được website trong mạng DMZ và dán vào bên dưới.



Chụp ảnh kiểm tra kết quả và dán vào bên dưới.