

BAN CƠ YẾU CHÍNH PHỦ
HỌC VIỆN KỸ THUẬT MẬT MÃ



MODULE THỰC HÀNH
AN TOÀN MẠNG MÁY TÍNH

BÀI THỰC HÀNH SỐ 01

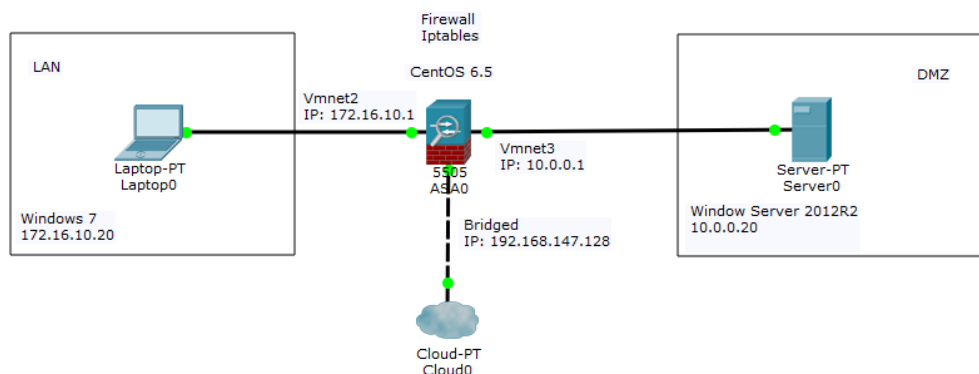
Thiết lập và cấu hình tường lửa Iptables

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.

```
root@kattt:~  
File Edit View Search Terminal Help  
TX packets:12 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:16406 (16.0 KiB) TX bytes:816 (816.0 b)  
Interrupt:16 Base address:0x2400  
  
lo  
Link encap:Local Loopback  
inet addr:127.0.0.1 Mask:255.0.0.0  
inet6 addr: ::1/128 Scope:Host  
UP LOOPBACK RUNNING MTU:16436 Metric:1  
RX packets:32 errors:0 dropped:0 overruns:0 frame:0  
TX packets:32 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:0  
RX bytes:2352 (2.2 KiB) TX bytes:2352 (2.2 KiB)  
  
[root@kattt ~]# service iptables status  
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  
  
Table: filter  
Chain INPUT (policy ACCEPT)  
num target prot opt source destination  
  
Chain FORWARD (policy ACCEPT)  
num target prot opt source destination  
1 ACCEPT icmp -- 172.16.10.0/24 0.0.0.0/0 icmp type 255  
2 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  
  
[root@kattt ~]#
```

The screenshot shows a Windows XP desktop environment. The taskbar at the top contains icons for 'Home', 'Windows 7', 'Control Panel', and 'Recycle Bin'. The 'Control Panel' window is open, displaying the 'Network and Sharing Center'. A command prompt window is open over the Control Panel, showing the results of a ping command to 8.8.8.8. The output indicates a 'General failure' and 'Packets: Sent = 3, Received = 0, Lost = 3 (100% loss)'. The Control Panel window also shows a 'Troubleshoot problems' link at the bottom.

Control Panel > Network and Internet > Network and Sharing Center

Search Control Panel

See full report

Connect or disconnect

Free Connection

is a router or access point.

Other

Sharing settings

Troubleshoot problems

Diagnose and repair network problems, or get troubleshooting information.

HomeGroup

Internet Options

Windows Firewall

```
C:\Windows\system32\cmd.exe
PING: transmit failed. General failure.
Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
    Control=C
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 0, Lost = 3 (100% loss),
    Control=C
C:\Users\admin>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=127
Reply from 8.8.8.8: bytes=32 time=25ms TTL=127
Reply from 8.8.8.8: bytes=32 time=25ms TTL=127

Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milliseconds:
    Minimum = 25ms, Maximum = 25ms, Average = 25ms
    Control=C
C:\Users\admin>
```

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

The screenshot shows a terminal window with the following commands and output:

```

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_forward
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

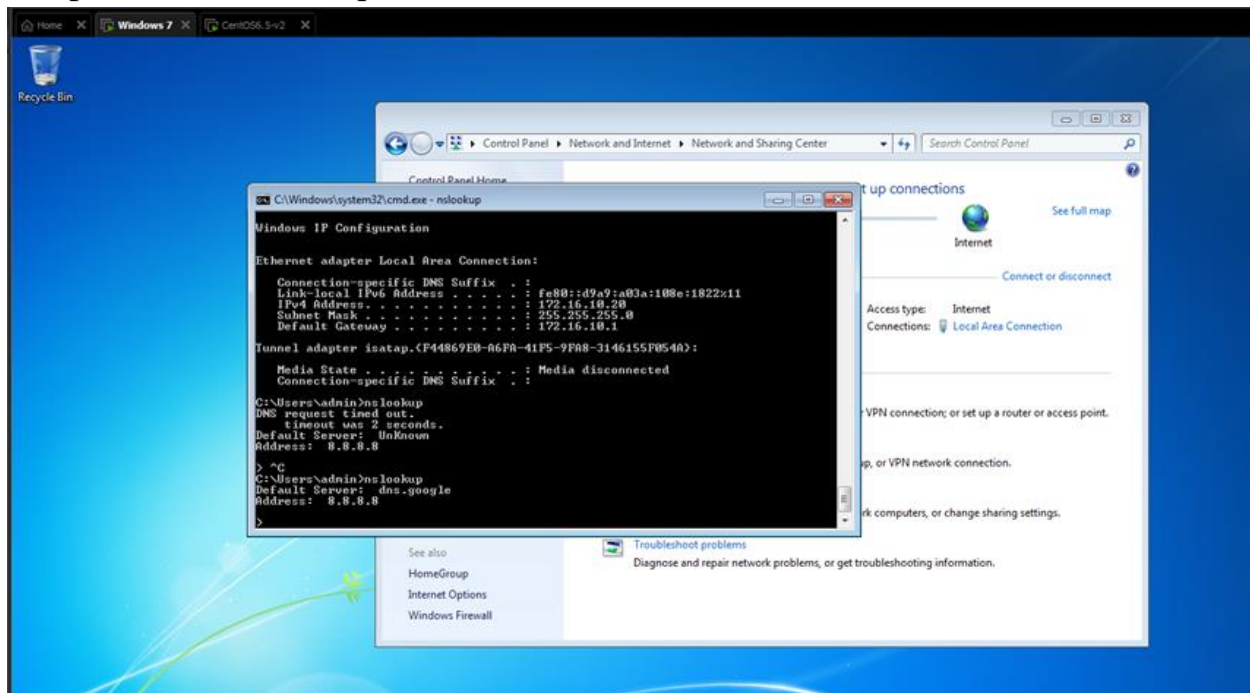
Table: nat
Chain PREROUTING (policy ACCEPT)
num target prot opt source destination

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

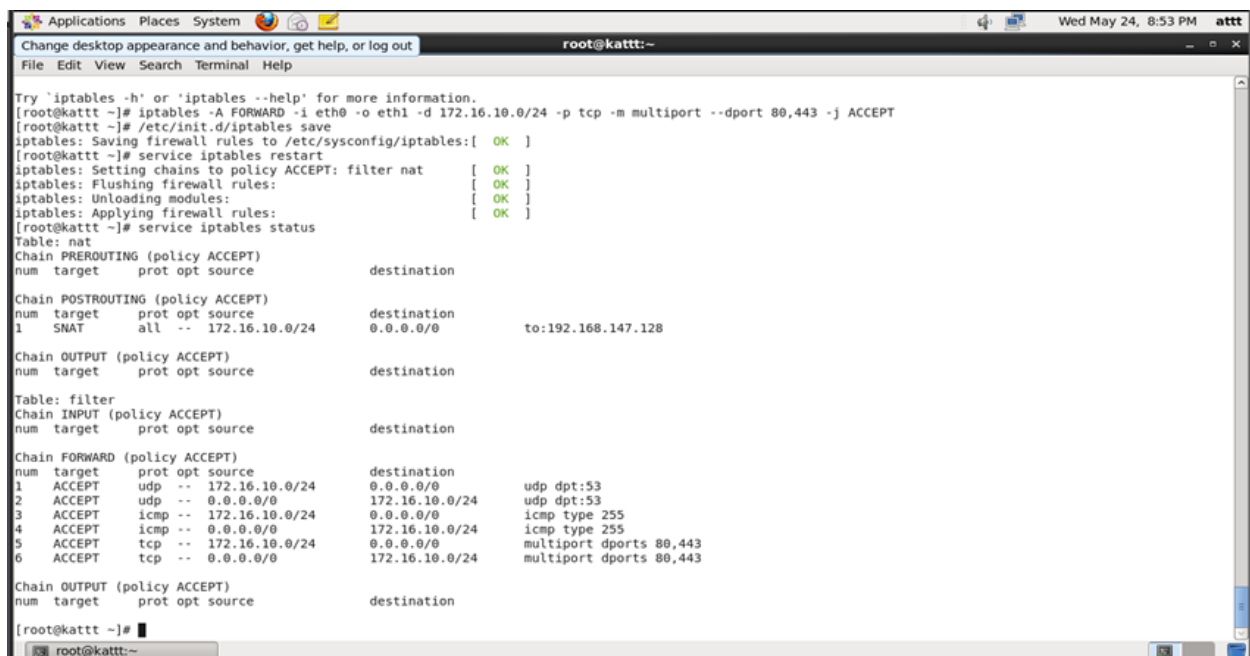
root@kattt ~#
  
```

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

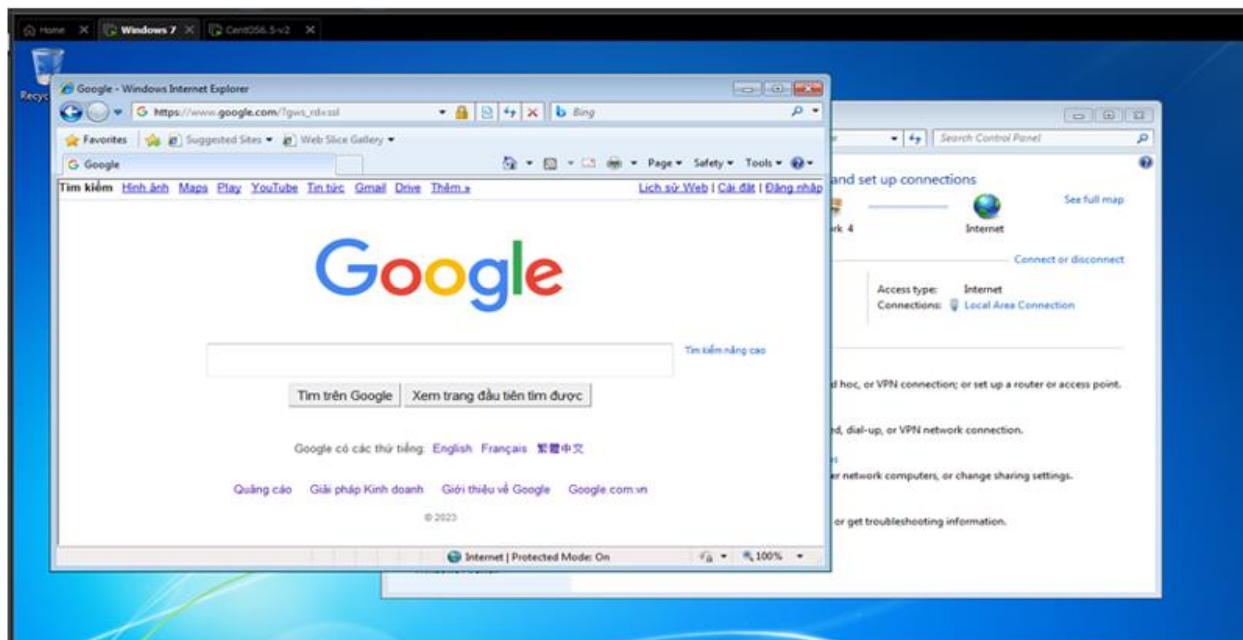


Kịch bản 3. Cho phép máy tính trong mạng LAN truy cập được các website từ mạng Internet

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.

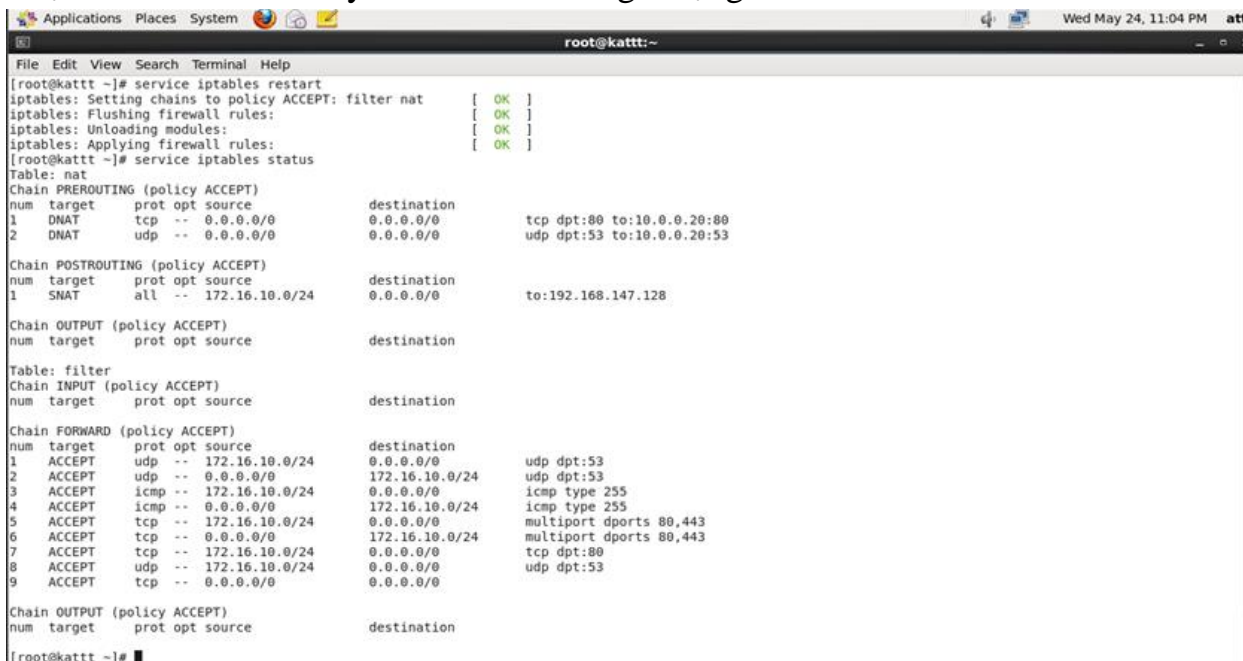


Chụp ảnh kiểm tra kết quả và dán vào bên dưới.



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.



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.

```
Applications Places System root@kattt:~ Wed May 24, 10:07 PM attt
File Edit View Search Terminal Help
[root@kattt ~]# iptables -t nat -A PREROUTING -i eth0 -p udp --dport 53 -j DNAT --to-destination 10.0.0.20:53
[root@kattt ~]# /etc/init.d/iptables save
iptables: Saving firewall rules to /etc/sysconfig/iptables:[ OK ]A
[root@kattt ~]# service iptables restart
iptables: Setting chains to policy ACCEPT: nat filter [ OK ]
iptables: Flushing firewall rules: [ OK ]
iptables: Unloading modules: ^[[A^[[A^[[A [ OK ]
iptables: Applying firewall rules: ^[[A [ 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
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
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
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
[root@kattt ~]#
```

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

