

Project 1: Firewall and iptables

February 22, 2014

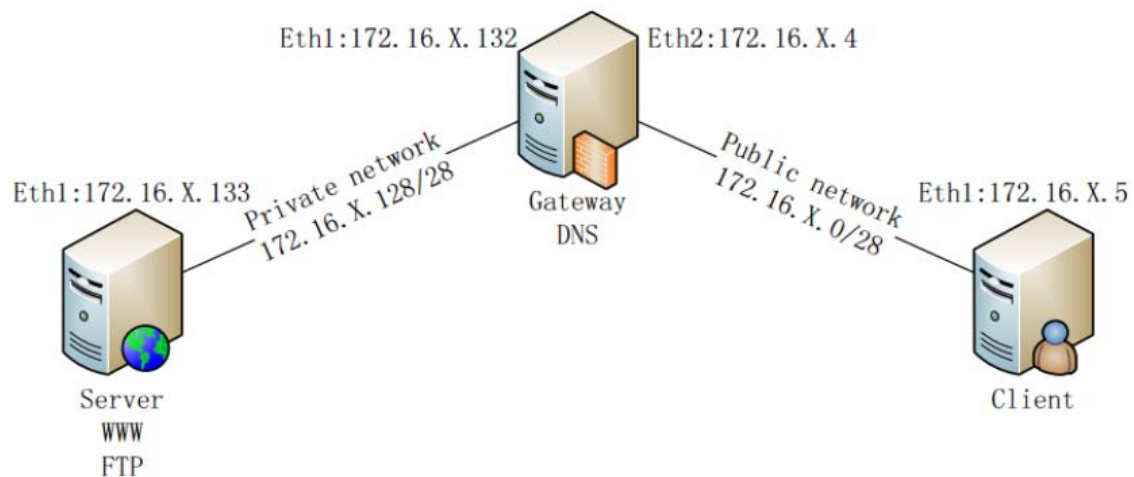
Bing Hao

Project description

The goal of this project is to gain hands-on experiences with the usage and functionality of iptables. The server student27vmg is supposed be configured as the gateway. The open source DNS server bind 9 and the sniffer tool Wireshark is installed on the gateway. Web server apache and FTP Server vsftpd is installed on the server student27vms. Gateway, Client, and Server simulate a typical network application scenario: the Server resides in a private network; the Client resides in a public network; the Gateway protects the Server from public access by using iptables.

Network set up of the project

The network topology is illustrated as follows:



(X represents your project number in vLab. Your current IP address should be 172.24.x.x/28)

For the client:

The client's IP address is 172.24.27.6 and its DNS is configured to 172.24.27.133.

For the Server:

The server's IP address is 172.24.27.134 and its DNS is configured to 8.8.8.8.

For the GW:

```
eth0    Link encap:Ethernet  HWaddr fa:16:3e:b6:bd:57
        inet addr:172.24.27.197  Bcast:172.24.27.207  Mask:255.255.255.240
        inet6 addr: fe80::f816:3eff:feb6:bd57/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:75664 errors:0 dropped:0 overruns:0 frame:0
        TX packets:49276 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:76827049 (76.8 MB)  TX bytes:5978729 (5.9 MB)

eth1    Link encap:Ethernet  HWaddr fa:16:3e:59:41:f7
        inet addr:172.24.27.5   Bcast:172.24.27.15  Mask:255.255.255.240
        inet6 addr: fe80::f816:3eff:fe59:41f7/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:60246 errors:0 dropped:0 overruns:0 frame:0
        TX packets:35256 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:5515111 (5.5 MB)  TX bytes:25314342 (25.3 MB)

eth2    Link encap:Ethernet  HWaddr fa:16:3e:99:72:a2
        inet addr:172.24.27.133 Bcast:172.24.27.143 Mask:255.255.255.240
        inet6 addr: fe80::f816:3eff:fe99:72a2/64 Scope:Link
        UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
        RX packets:90060 errors:0 dropped:0 overruns:0 frame:0
        TX packets:34212 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:1000
        RX bytes:6708065 (6.7 MB)  TX bytes:27100898 (27.1 MB)
```

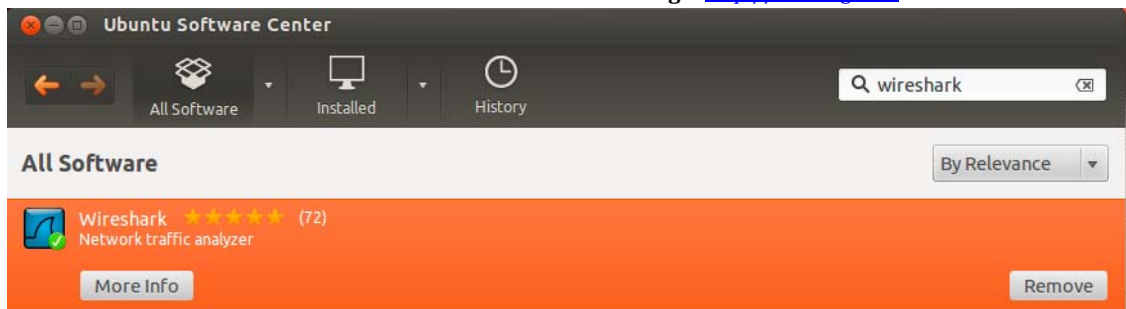
GW has 3 network cards, 172.24.27.133 will be used as the DNS server and the Gateway for other 2 machines.

Software packages used in the project

- Apache web server
- Bind9 DNS server
- VIM
- Iptables
- Wireshark
- Vsftpd
- Openssh-server

Step-by-step project description

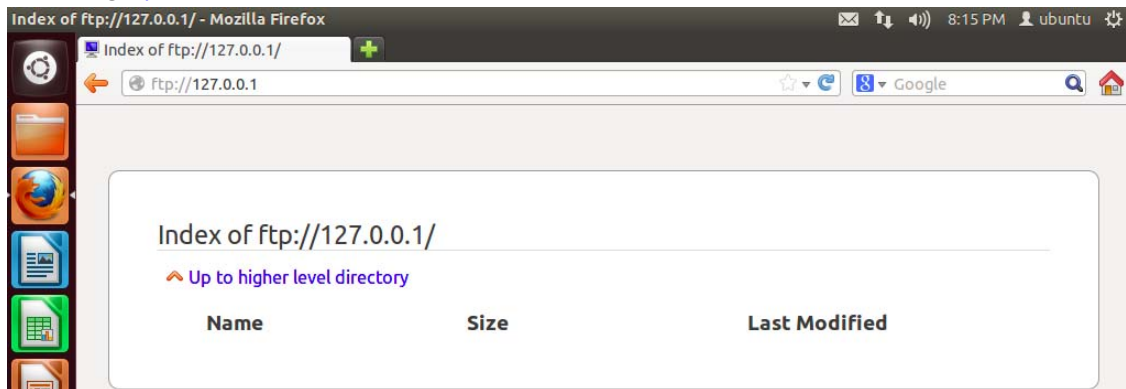
1. Install Wireshark on the server student27vmg

Home Page: <http://uniteng.com>

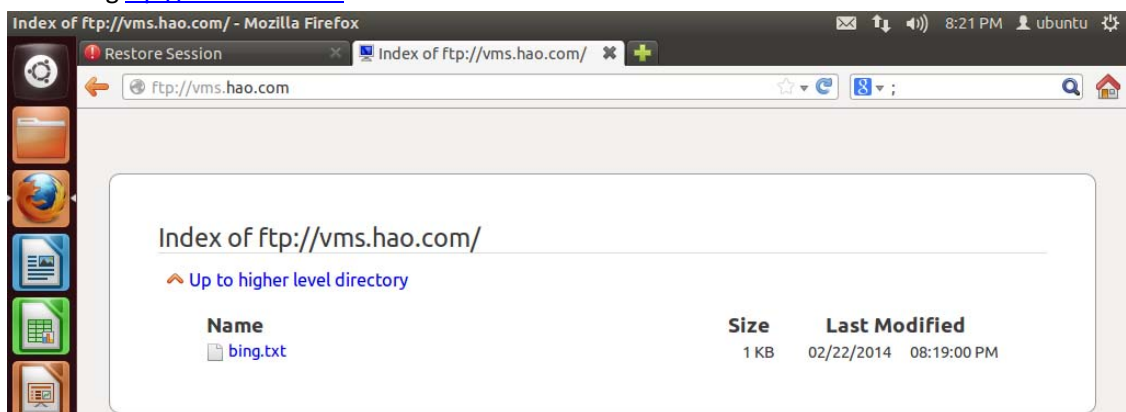
Wireshark could be installed using Ubuntu software center

2. Install vsftpd on the server student27vms
`sudo apt-get install vsftpd`
`sudo cp /etc/vsftpd.conf /etc/vsftpd.conf.original`

Accessing <ftp://127.0.0.1> in the firefox on student27vms:



Accessing <ftp://vms.hao.com> in the firefox on student27vmc:



3. Configure vsftpd to be passive mode
Add following contents to the end of the file /etc/vsftpd.conf:
`pasv_enable=YES`

Home Page: <http://uniteng.com>

```
pasv_min_port=40000
pasv_max_port=40080
pasv_promiscuous=YES
```

4. Use NAT to hide Server VM from Client VM on the gateway student27vmg
#Use NAT to hide Server VM from Client VM, change forward policy
\$IPTABLES -P FORWARD DROP
5. Install openssh-server on the gateway student27vmg
sudo apt-get install openssh-server

Accessing the gateway student27vmg from student27vms:

```
ubuntu@ubuntu-virtual-machine:/etc$ ssh vmg.hao.com
ubuntu@vmg.hao.com's password:
Welcome to Ubuntu 12.04.2 LTS (GNU/Linux 3.5.0-23-generic i686)

 * Documentation:  https://help.ubuntu.com/

Last login: Fri Feb 21 00:49:04 2014 from ubuntu-virtual-machine-2.local
ubuntu@ubuntu-virtual-machine:~$
```

6. Install openssh-server on the server student27vms:

On the student27vmg:
sudo iptables-P FORWARD ACCEPT

On the student27vms:
sudo apt-get install openssh-server

On the student27vmg:
sudo iptables-P FORWARD DROP

7. Execute following iptables rules on the gateway

```
#!/bin/sh
iptables -F
iptables -F -t nat

iptables -P FORWARD DROP
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#coming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
```

Home Page: <http://uniteng.com>Accessing <http://vmg.hao.com> (Gateway's IP) in the firefox on student27vmc:

It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Configured by Bing Hao @ ASU

No.	Time	Source	Destination	Protocol	Length	Info
3	0.927965	172.24.27.134	172.24.27.133	TCP	74	http > 43220 [SYN, ACK] Seq=0 Ack=1 Win=
4	0.929693	172.24.27.133	172.24.27.134	TCP	66	43220 > http [ACK] Seq=1 Ack=1 Win=14720
5	0.962182	172.24.27.133	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x89b2581
6	0.962404	172.24.27.133	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x89b2581
7	0.966464	fa:16:3e:6c:c6:9c	Broadcast	ARP	42	Who has 172.24.27.133? Tell 172.24.27.1
8	0.966485	fa:16:3e:99:72:a2	fa:16:3e:6c:c6:9c	ARP	42	172.24.27.133 is at fa:16:3e:99:72:a2
9	0.966814	fa:16:3e:6c:c6:9c	Broadcast	ARP	42	Who has 172.24.27.133? Tell 172.24.27.1
10	0.966823	fa:16:3e:99:72:a2	fa:16:3e:6c:c6:9c	ARP	42	172.24.27.133 is at fa:16:3e:99:72:a2
11	0.969427	172.24.27.130	172.24.27.133	DHCP	365	DHCP ACK - Transaction ID 0x89b2581
12	0.969469	172.24.27.130	172.24.27.133	DHCP	365	DHCP ACK - Transaction ID 0x89b2581
13	2.125610	172.24.27.134	172.24.27.133	TCP	74	http > 43220 [SYN, ACK] Seq=0 Ack=1 Win=
14	2.126550	172.24.27.133	172.24.27.134	TCP	78	[TCP Dup ACK 4#1] 43220 > http [ACK] Seq=
15	5.930941	fa:16:3e:99:72:a2	fa:16:3e:c5:0a:60	ARP	42	Who has 172.24.27.134? Tell 172.24.27.1
16	5.931320	172.24.27.133	172.24.27.134	TCP	66	43220 > http [FIN, ACK] Seq=1 Ack=1 Win=
17	5.932247	172.24.27.134	172.24.27.133	TCP	66	http > 43220 [FIN, ACK] Seq=1 Ack=2 Win=
18	5.932911	fa:16:3e:c5:0a:60	fa:16:3e:99:72:a2	ARP	42	172.24.27.134 is at fa:16:3e:c5:0a:60
19	5.932947	172.24.27.133	172.24.27.134	TCP	66	43220 > http [ACK] Seq=2 Ack=2 Win=14720

▶ Frame 4: 66 bytes on wire (528 bits), 66 bytes captured (528 bits)
 ▶ Ethernet II, Src: fa:16:3e:99:72:a2 (fa:16:3e:99:72:a2), Dst: fa:16:3e:c5:0a:60 (fa:16:3e:c5:0a:60)
 ▶ Internet Protocol Version 4, Src: 172.24.27.133 (172.24.27.133), Dst: 172.24.27.134 (172.24.27.134)
 ▶ Transmission Control Protocol, Src Port: 43220 (43220), Dst Port: http (80), Seq: 1, Ack: 1, Len: 0

```

0000  fa 16 3e c5 0a 60 fa 16 3e 99 72 a2 08 00 45 00  ..>... >.Γ...E.
0010  00 34 88 b8 40 00 3f 06 23 d0 ac 18 1b 85 ac 18  .4..@.?. #.....
0020  1b 86 a8 d4 00 50 6f 89 9a 01 59 58 ef 20 80 10  ....Po. .YX. ..
0030  00 73 bf b7 00 00 01 01 08 0a 1d ce 12 b8 1d cd  .S.....
  
```

File: "/tmp/wireshark_eth2_20140... Packets: 19 Displayed: 19 Marked: 0 Dropped: 0 Profile: Default

This means the forwarding is working

8. Modifying the iptables rules as following for FTP

Home Page: <http://uniteng.com>

```

# /bin/sh
iptables -F
iptables -F -t nat

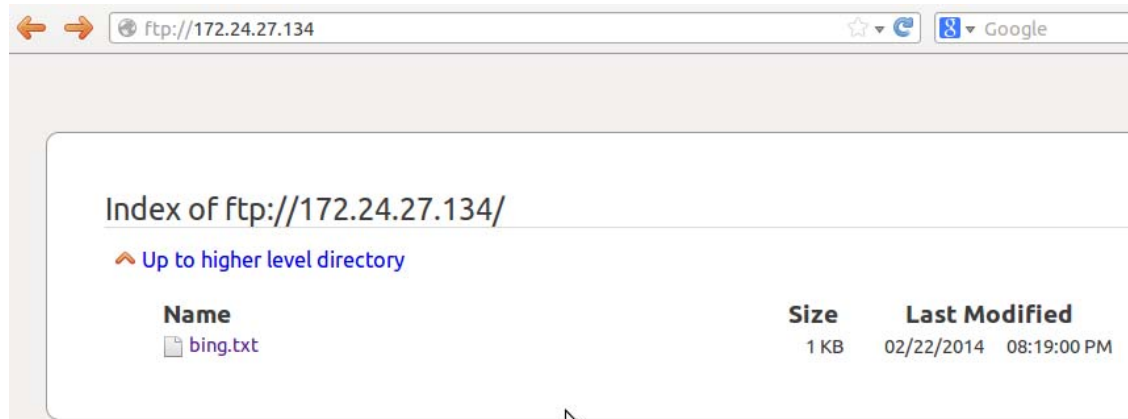
iptables -P FORWARD DROP
iptables -P INPUT ACCEPT
iptables -P OUTPUT ACCEPT

#For HTTP
#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#coming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT

#For FTP
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 21 -j DNAT --to 172.24.27.134:21
iptables -t nat -A POSTROUTING -p tcp --dport 21 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 21 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 21 -j ACCEPT
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 20 -j DNAT --to 172.24.27.134:20
iptables -t nat -A POSTROUTING -p tcp --dport 20 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 20 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 172.24.27.6 -j ACCEPT

```

Accessing <http://vms.hao.com> in the firefox on student27vmc:



9. Allowing DNS on Gateway

```

#DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT

```

10. Downloading a file from ftp from client

Home Page: <http://uniteng.com>

Filter: tcp Expression... Clear Apply

No.	Time	Source	Destination	Protocol	Length	Info
10	1.100314	172.24.27.134	172.24.27.133	FTP	117	Response: 227 Entering Passive Mode (17
11	1.102450	172.24.27.133	172.24.27.134	FTP	82	Request: SIZE /bing.txt
12	1.102827	172.24.27.6	172.24.27.134	TCP	74	59694 > 40009 [SYN] Seq=0 Win=14600 Len
13	1.103237	172.24.27.134	172.24.27.133	FTP	74	Response: 213 10
14	1.103964	172.24.27.133	172.24.27.134	FTP	82	Request: MDTM /bing.txt
15	1.104557	172.24.27.134	172.24.27.6	TCP	74	40009 > 59694 [SYN, ACK] Seq=0 Ack=1 Wi
16	1.104603	172.24.27.134	172.24.27.133	FTP	86	Response: 213 20140222201940
17	1.105542	172.24.27.133	172.24.27.134	FTP	82	Request: RETR /bing.txt
18	1.105751	172.24.27.6	172.24.27.134	TCP	66	59694 > 40009 [ACK] Seq=1 Ack=1 Win=147
19	1.106389	172.24.27.134	172.24.27.133	FTP	133	Response: 150 Opening BINARY mode data
20	1.106755	172.24.27.134	172.24.27.6	TCP	76	40009 > 59694 [PSH, ACK] Seq=1 Ack=1 Wi
21	1.106799	172.24.27.134	172.24.27.6	TCP	66	40009 > 59694 [FIN, ACK] Seq=11 Ack=1 W
22	1.107938	172.24.27.6	172.24.27.134	TCP	66	59694 > 40009 [ACK] Seq=1 Ack=11 Win=14
23	1.107973	172.24.27.6	172.24.27.134	TCP	66	59694 > 40009 [FIN, ACK] Seq=1 Ack=12 W
24	1.108566	172.24.27.134	172.24.27.6	TCP	66	40009 > 59694 [ACK] Seq=12 Ack=2 Win=14
25	1.108604	172.24.27.134	172.24.27.133	FTP	90	Response: 226 Transfer complete.
26	1.109212	172.24.27.133	172.24.27.134	TCP	66	59787 > ftp [ACK] Seq=55 Ack=171 Win=11

▶ Frame 9: 72 bytes on wire (576 bits), 72 bytes captured (576 bits)
 ▶ Ethernet II, Src: fa:16:3e:99:72:a2 (fa:16:3e:99:72:a2), Dst: fa:16:3e:c5:0a:60 (fa:16:3e:c5:0a:60)
 ▶ Internet Protocol Version 4, Src: 172.24.27.133 (172.24.27.133), Dst: 172.24.27.134 (172.24.27.134)
 ▶ Transmission Control Protocol, Src Port: 59787 (59787), Dst Port: ftp (21), Seq: 1, Ack: 1, Len: 6
 ▶ File Transfer Protocol (FTP)

```

0000  fa 16 3e c5 0a 60 fa 16 3e 99 72 a2 08 00 45 00  ..>... >.r...E.
0010  00 3a e4 ee 40 00 3f 06 c7 93 ac 18 1b 85 ac 18  ....@.?. .....
0020  1b 86 e9 8b 00 15 22 da ba c3 91 7b 4e ca 80 18  ....". ...{N...
0030  00 73 a8 88 00 00 01 01 08 0a 1d ce 80 da 1d ce  .s.....
  
```

File: "/tmp/wireshark_eth2_20140... Packets: 26 Displayed: 18 Marked: 0 Dropped: 0 Profile: Default

Conclusion

The project have been finished successfully. The client and server have been configured properly.

Attached files

File name: rc.firewall

Home Page: <http://uniteng.com>

```
#!/bin/sh
iptables -F
iptables -F -t nat

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP

#For HTTP
#iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
# iptables -t nat -A POSTROUTING -d 172.24.27.133 -p tcp --dport 80 -j SNAT --to 172.24.27.134:80
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 80 -j DNAT --to 172.24.27.134:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
#iptables -t nat -A POSTROUTING -d 172.24.27.134 -p tcp --dport 80 -j SNAT --to 172.24.27.133:80
iptables -t nat -A POSTROUTING -p tcp --dport 80 -j MASQUERADE
#iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 80 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 80 -j ACCEPT
#coming back
iptables -A FORWARD -m state --state ESTABLISHED -j ACCEPT
iptables -A FORWARD -s 172.24.27.134 -j ACCEPT
iptables -A FORWARD -s 172.24.27.133 -j ACCEPT
#iptables -A FORWARD -i eth2 -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT
#iptables -A FORWARD -s 172.24.27.6 -j ACCEPT
# iptables -A INPUT -i eth1 -s 172.24.27.134 -j DROP
# iptables -A FORWARD -s 172.24.27.6 -d 172.24.27.134 -p tcp --dport 80 -j DROP
iptables -A FORWARD -s 172.24.27.6 -p tcp --dport 80 -j ACCEPT

#For FTP
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 21 -j DNAT --to 172.24.27.134:21
iptables -t nat -A POSTROUTING -p tcp --dport 21 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 21 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 21 -j ACCEPT
iptables -t nat -A PREROUTING -d 172.24.27.133 -p tcp --dport 20 -j DNAT --to 172.24.27.134:20
iptables -t nat -A POSTROUTING -p tcp --dport 20 -j MASQUERADE
iptables -A FORWARD -i eth2 -s 172.24.27.134 -p tcp --sport 20 -j ACCEPT
iptables -A FORWARD -o eth2 -d 172.24.27.133 -p tcp --dport 20 -j ACCEPT
iptables -A FORWARD -s 172.24.27.6 -j ACCEPT

#DNS
```

```
#DNS
iptables -A OUTPUT -p udp --dport 53 -j ACCEPT
iptables -A INPUT -p udp --sport 53 -j ACCEPT
iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT
iptables -A INPUT -p tcp --sport 53 -j ACCEPT
```