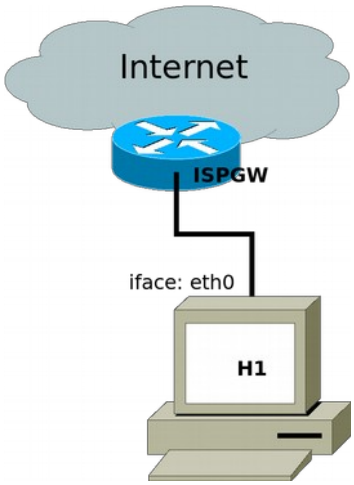
সমস্যা ১: ইন্টারনেটে সংযুক্ত একটি কম্পিউটারে (লিনাক্স চালিত) firewall configure করতে হবে।



নেটওয়ার্ক তথ্য: (হোস্ট H1)
নেটওয়ার্ক ইন্টারফেস: eth0
আইপি এড্রেস: 192.168.1.100/24

সমস্যার বর্ণনা:

- lo ইন্টারফেসের সাথে (যাওয়া ও আসা) সকল যোগযোগ বাধাহীন থাকবে।
- ব্যবহারকারীর সকল ইন্টারনেটগামী প্যাকেট (eth0 ইন্টারফেস দিয়ে বহির্গামী প্যাকেট) তাদের প্রতি উত্তরে ফেরত আসা সকল প্যাকেট বাধাহীন থাকবে।
- ইন্টারনেট থেকে আসা icmp প্যাকেট (সাইজ সর্বোচ্চ ২০০ বাইট) ও তার ফেরত উত্তর বাধাহীন থাকবে।

সমাধান ১: filter টেবিলের INPUT চেইনের ডিফল্ট পলিসি ACCEPT হলে

```
iptables  -P OUTPUT  ACCEPT

iptables  -P INPUT  ACCEPT
iptables  -A INPUT  -p ALL  -i lo  -j ACCEPT
iptables  -A INPUT  -p ALL  -m conntrack  --ctstate RELATED,ESTABLISHED  -j ACCEPT
iptables  -A INPUT  -p icmp  -m length  --length 1:200  -j ACCEPT
iptables  -A INPUT  -p ALL  -j DROP
```

সমাধান ২: filter টেবিলের INPUT চেইনের ডিফল্ট পলিসি DROP হলে

```
iptables  -P OUTPUT  ACCEPT

iptables  -P INPUT  DROP
iptables  -A INPUT  -p ALL  -i lo  -j ACCEPT
iptables  -A INPUT  -p ALL  -m conntrack  --ctstate RELATED,ESTABLISHED  -j ACCEPT
iptables  -A INPUT  -p icmp  -m length  --length 1:200  -j ACCEPT
```

দ্রষ্টব্য:

```
iptables  -A INPUT  -p ALL  -m conntrack  --ctstate RELATED,ESTABLISHED  -j ACCEPT
```

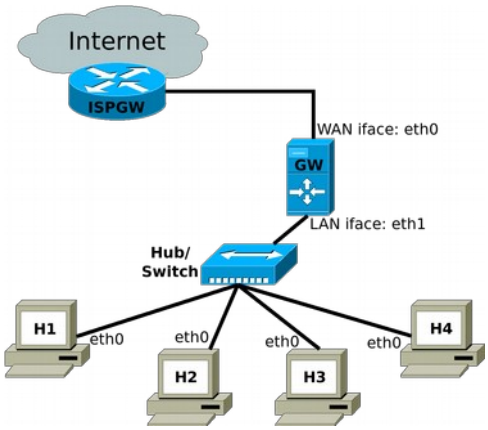
এর পরিবর্তে নিম্নলিখিত রুলও ব্যবহার করা যায়;

```
iptables  -A INPUT  -p ALL  -m state  --state ESTABLISHED,RELATED  -j ACCEPT
```

হোস্টের আইপি এড্রেস Fixed না হয়ে যদি DHCP থেকে নিয়ে থাকে সেক্ষেত্রে প্যাকেট DROP করার পূর্বে নিম্নলিখিত রুলটি ব্যবহার করতে হবে;

```
iptables  -A INPUT  -i eth0  -p udp  --dport 67:68  --sport 67:68  -j ACCEPT
```

সমস্যা ২: ইন্টারনেট গেটওয়েতে firewall configure করতে হবে।



নেটওয়ার্ক তথ্য: (গেটওয়ে GW)
WAN ইন্টারফেস: eth0
WAN ইন্টারফেস আইপি এড্রেস: 103.221.254.42/24
LAN ইন্টারফেস: eth1
LAN ইন্টারফেস আইপি এড্রেস: 192.168.1.254/24
DHCP সার্ভিস: eth1

সমাধান: filter টেবিলের INPUT ও FORWARD চেইনের ডিফল্ট পলিসি DROP হলে

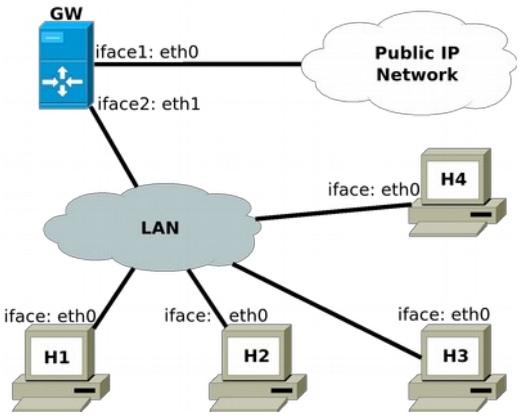
```
iptables  -P OUTPUT  ACCEPT

iptables  -P INPUT  DROP
iptables  -A INPUT  -p ALL  -i lo  -j ACCEPT
iptables  -A INPUT  -p ALL  -m conntrack  --ctstate RELATED,ESTABLISHED  -j ACCEPT
iptables  -A INPUT  -p icmp  -m length  --length 1:200  -j ACCEPT
iptables  -A INPUT  -i eth1  -p udp  --dport 67:68  --sport 67:68  -j ACCEPT

iptables  -P FORWARD  DROP
iptables  -A FORWARD  -p ALL  -i eth1  -j ACCEPT
iptables  -A FORWARD  -p ALL  -i eth0  -m conntrack  --ctstate RELATED,ESTABLISHED  -j ACCEPT
iptables  -A FORWARD  -p icmp  -m length  --length 1:200  -j ACCEPT

//SNAT
iptables  -t nat  -A POSTROUTING  -o eth0  -s 192.168.1.0/24  -j SNAT  --to-source  103.221.254.42
```

সমস্যা ৩: গেটওয়ের আড়ালে **private IP** তে সার্ভার পরিচালনা করতে হবে।



নেটওয়ার্ক তথ্য: (গেটওয়ে GW)

Public ইন্টারফেস: eth0

Public ইন্টারফেস আইপি এড্রেস: 103.221.254.42/24

LAN ইন্টারফেস: eth1

LAN ইন্টারফেস আইপি এড্রেস: 192.168.1.254/24

DNS তথ্য:

```
gw.example.com.      IN  A      103.221.254.42
www.example.com.     IN  CNAME  gw.example.com.
ssh.example.com.     IN  CNAME  gw.example.com.
smtp.example.com.    IN  CNAME  gw.example.com.
```

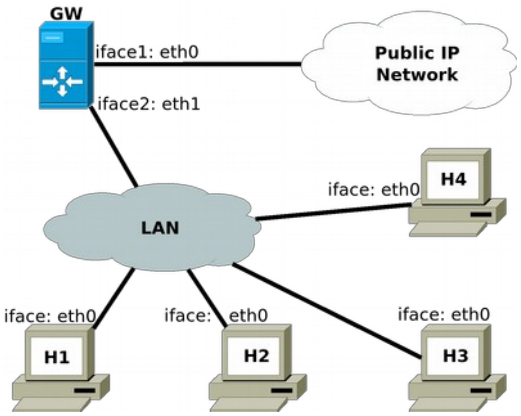
সমাধান:

গেটওয়ে GW:

```
// SNAT
iptables  -t nat  -A POSTROUTING  -o eth0  -s 192.168.1.0/24  -j SNAT  --to-source  103.221.254.42

// DNAT
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 80  -j DNAT --to-destination 192.168.1.1
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 25  -j DNAT --to-destination 192.168.1.2
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 22  -j DNAT --to-destination 192.168.1.3
```

সমস্যা ৪: একাধিক ওয়েব সার্ভারের মধ্যে লোড বন্টন করতে হবে।



নেটওয়ার্ক তথ্য: (গেটওয়ে GW)

Public ইন্টারফেস: eth0

Public ইন্টারফেস আইপি এড্রেস: 103.221.254.42/24

LAN ইন্টারফেস: eth1

LAN ইন্টারফেস আইপি এড্রেস: 192.168.1.254/24

DNS তথ্য:

```
gw.example.com.      IN   A   103.221.254.42
www.example.com.     IN   CNAME   gw.example.com.
```

সমাধান ১: Round Robin মোড ব্যবহার করে

গেটওয়ে GW:

```
// SNAT
iptables  -t nat  -A POSTROUTING  -o eth0  -s 192.168.1.0/24  -j SNAT  --to-source  103.221.254.42

// DNAT
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 80  -m statistic --mode nth --every 4 \
  --packet 0  -j DNAT --to-destination 192.168.1.1
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 80  -m statistic --mode nth --every 3 \
  --packet 0  -j DNAT --to-destination 192.168.1.2
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 80  -m statistic --mode nth --every 2 \
  --packet 0  -j DNAT --to-destination 192.168.1.3
iptables  -t nat  -A PREROUTING -d 103.221.254.42  -p tcp --dport 80  -j DNAT --to-destination 192.168.1.4
```

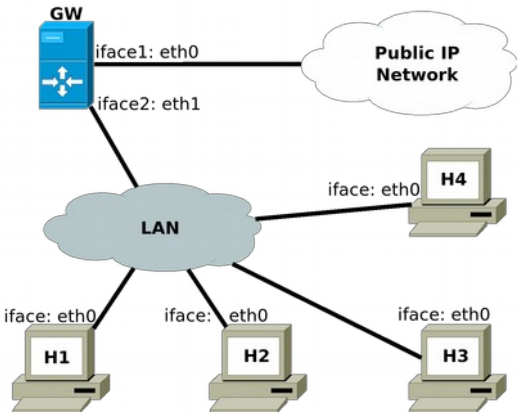
সমাধান ২: Random মোড ব্যবহার করে

গেটওয়ে GW:

```
// SNAT
iptables  -t nat  -A POSTROUTING  -o eth0  -s 192.168.1.0/24  -j SNAT  --to-source  103.221.254.42

// DNAT
iptables  -t nat  -A PREROUTING  -d 103.221.254.42  -p tcp  --dport 80  -m statistic  --mode random \
   --probability 0.25  -j DNAT  --to-destination 192.168.1.1
iptables  -t nat  -A PREROUTING  -d 103.221.254.42  -p tcp  --dport 80  -m statistic  --mode random \
   --probability 0.33  -j DNAT  --to-destination 192.168.1.2
iptables  -t nat  -A PREROUTING  -d 103.221.254.42  -p tcp  --dport 80  -m statistic  --mode random \
   --probability 0.5  -j DNAT  --to-destination 192.168.1.3
iptables -t nat -A PREROUTING  -d 103.221.254.42  -p tcp  --dport 80  -j DNAT --to-destination 192.168.1.4
```

সমস্যা ৫: একটি ওয়েব সার্ভারের ট্রাফিক অন্যান্য ওয়েব সার্ভারের মধ্যে বন্টন করতে হবে।



নেটওয়ার্ক তথ্য: (গেটওয়ে GW)

Public ইন্টারফেস: eth0

Public ইন্টারফেস আইপি এড্রেস: 103.221.254.42/24

LAN ইন্টারফেস: eth1

LAN ইন্টারফেস আইপি এড্রেস: 192.168.1.254/24

DNS তথ্য:

```
gw.example.com.      IN  A      103.221.254.42
www.example.com.     IN  CNAME  gw.example.com.
```

সমাধান ১: Round Robin মোড ব্যবহার করে

হোস্ট H1:

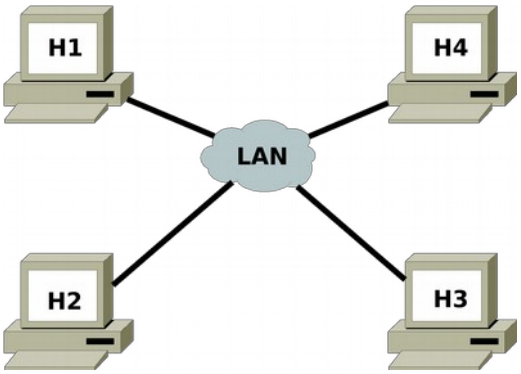
```
// DNAT
iptables  -t nat  -A PREROUTING -d 192.168.1.1  -p tcp --dport 80  -m statistic --mode nth --every 3 \
  --packet 0  -j DNAT --to-destination 192.168.1.2
iptables  -t nat  -A PREROUTING -d 192.168.1.1  -p tcp --dport 80  -m statistic --mode nth --every 2 \
  --packet 0  -j DNAT --to-destination 192.168.1.3
iptables  -t nat  -A PREROUTING -d 192.168.1.1  -p tcp --dport 80  -j DNAT --to-destination 192.168.1.4
// SNAT
iptables  -t nat  -A POSTROUTING  -d 192.168.1.2  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
iptables  -t nat  -A POSTROUTING  -d 192.168.1.3  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
iptables  -t nat  -A POSTROUTING  -d 192.168.1.4  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
```

সমাধান ২: Random মোড ব্যবহার করে

হোস্ট H1:

```
// DNAT
iptables  -t nat  -A PREROUTING  -d 192.168.1.1  -p tcp  --dport 80  -m statistic  --mode random \
   --probability 0.33  -j DNAT  --to-destination 192.168.1.2
iptables  -t nat  -A PREROUTING  -d 192.168.1.1  -p tcp  --dport 80  -m statistic  --mode random \
   --probability 0.5  -j DNAT  --to-destination 192.168.1.3
iptables -t nat -A PREROUTING  -d 192.168.1.1  -p tcp  --dport 80  -j DNAT --to-destination 192.168.1.4
// SNAT
iptables  -t nat  -A POSTROUTING  -d 192.168.1.2  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
iptables  -t nat  -A POSTROUTING  -d 192.168.1.3  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
iptables  -t nat  -A POSTROUTING  -d 192.168.1.4  -p tcp  --dport 80  -j SNAT  --to-source 192.168.1.1
```

সমস্যা ৬: mac spoof/man-in-the-middle এড়িয়ে দুটি হোস্টের মধ্যে যোগাযোগ করতে হবে।



নেটওয়ার্ক তথ্য: (হোস্ট H1)
নেটওয়ার্ক ইন্টারফেস: eth0
আইপি এড্রেস: 192.168.1.1/24
ম্যাক এড্রেস: 1:2:3:4:5:11

নেটওয়ার্ক তথ্য: (হোস্ট H2)
নেটওয়ার্ক ইন্টারফেস: eth0
আইপি এড্রেস: 192.168.1.2/24
ম্যাক এড্রেস: 1:2:3:4:5:22

সমস্যার বর্ণনা:

- H1 ও H2 এর মধ্যে যোগযোগের সময় হোস্টদ্বয়ের আইপি ও ম্যাক পরিবর্তন হওয়া যাবেনা।

হোস্ট H1:

```
ip neigh add 192.168.1.2 lladdr 1:2:3:4:5:22 dev eth0
iptables -A INPUT -s 192.168.1.2 -m mac ! --mac-source 1:2:3:4:5:22 -j DROP
. . .
. . .
. . .
```

হোস্ট H2:

```
ip neigh add 192.168.1.1 lladdr 1:2:3:4:5:11 dev eth0
iptables -A INPUT -s 192.168.1.1 -m mac ! --mac-source 1:2:3:4:5:11 -j DROP
. . .
. . .
. . .
```

বিবিধ:

উদাহরণ ১: filter টেবিলের চেইন সমূহে DROP কৃত প্যাকেটের তথ্য লগফাইলে লিপিবদ্ধ রাখতে নিম্নরূপ LOGDROP নামে user-define চেইন তৈরী করে উক্ত প্যাকেট সমূহকে তাতে পাঠিয়ে দিতে হবে।

```
iptables  -N LOGDROP
iptables  -A LOGDROP  -m limit  --limit 3/minute  --limit-burst 3  -j LOG \
          --log-level DEBUG  --log-prefix "IPT pkt: "
iptables  -A LOGDROP  -j DROP
```

উদাহরণ ২: ### Drop INVALID packets ###

```
iptables -t mangle  -A PREROUTING  -m conntrack --ctstate INVALID -j DROP
```

উদাহরণ ৩: ### Drop TCP packets that are NEW and are not SYN ###

```
iptables  -t mangle  -A PREROUTING  -p tcp  ! --syn  -m conntrack  --ctstate NEW  -j DROP
```

উদাহরণ ৪: ### Drop SYN packets with suspicious MSS value ###

```
iptables  -t mangle  -A PREROUTING  -p tcp -m conntrack --ctstate NEW -m tcpmss ! --mss 536:65535 -j DROP
```

উদাহরণ ৫: ### Block spoofed packets ###

```
iptables  -t mangle  -A PREROUTING  -s 224.0.0.0/3 -j DROP
iptables  -t mangle  -A PREROUTING  -s 169.254.0.0/16 -j DROP
iptables  -t mangle  -A PREROUTING  -s 172.16.0.0/12 -j DROP
iptables  -t mangle  -A PREROUTING  -s 192.168.0.0/16 -j DROP
iptables  -t mangle  -A PREROUTING  -s 10.0.0.0/8 -j DROP
iptables  -t mangle  -A PREROUTING  -s 0.0.0.0/8 -j DROP
iptables  -t mangle  -A PREROUTING  -s 240.0.0.0/5 -j DROP
iptables  -t mangle  -A PREROUTING  -s 127.0.0.0/8 ! -i lo -j DROP
```

উদাহরণ ৬: ### Drop ICMP (you usually don't need this protocol) ###

```
iptables  -t mangle  -A PREROUTING  -p icmp -j DROP
```

উদাহরণ ৭: ### Drop fragments in all chains ###

```
iptables  -t mangle  -A PREROUTING  -f  -j DROP
```

উদাহরণ ৮: ### Block packets with bogus TCP flags ###

```
iptables  -t mangle  -N BadTcp
iptables  -A BadTcp -p tcp --tcp-flags FIN,SYN,RST,PSH,ACK,URG NONE -j DROP
iptables  -A BadTcp -p tcp --tcp-flags FIN,SYN FIN,SYN -j DROP
iptables -A BadTcp -p tcp --tcp-flags SYN,RST SYN,RST -j DROP
iptables -A BadTcp -p tcp --tcp-flags SYN,FIN SYN,FIN -j DROP
iptables -A BadTcp -p tcp --tcp-flags FIN,RST FIN,RST -j DROP
iptables -A BadTcp -p tcp --tcp-flags FIN,ACK FIN -j DROP
iptables -A BadTcp -p tcp --tcp-flags ACK,URG URG -j DROP
iptables -A BadTcp -p tcp --tcp-flags ACK,FIN FIN -j DROP
iptables -A BadTcp -p tcp --tcp-flags ACK,PSH PSH -j DROP
iptables -A BadTcp -p tcp --tcp-flags ALL ALL -j DROP
iptables -A BadTcp -p tcp --tcp-flags ALL NONE -j DROP
iptables -A BadTcp -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
iptables -A BadTcp -p tcp --tcp-flags ALL SYN,FIN,PSH,URG -j DROP
iptables -A BadTcp -p tcp --tcp-flags ALL SYN,RST,ACK,FIN,URG -j DROP
iptables  -t mangle  -A PREROUTING -p tcp -j BadTcp
```

উদাহরণ ৯: ### Limit RST packets ###

```
iptables  -A INPUT -p tcp --tcp-flags RST RST -m limit --limit 2/s --limit-burst 2 -j ACCEPT
iptables  -A INPUT -p tcp --tcp-flags RST RST -j DROP
```

উদাহরণ ১০: ### Limit connections per source IP ###

```
iptables -A INPUT -p tcp --syn --dport 23 -m connlimit --connlimit-above 2 -j REJECT --reject-with tcp-reset
# or
iptables -A INPUT -p tcp --syn --dport 23 -m connlimit --connlimit-upto 2 -j ACCEPT
```

উদাহরণ ১১: ### Limit new TCP connections per second per source IP ###

```
iptables -A INPUT -p tcp -m conntrack --ctstate NEW -m limit --limit 60/s --limit-burst 20 -j ACCEPT
iptables -A INPUT -p tcp -m conntrack --ctstate NEW -j DROP
```

উদাহরণ ১২: ### SSH brute-force protection ###

```
iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --set
iptables -A INPUT -p tcp --dport ssh -m conntrack --ctstate NEW -m recent --update --seconds 60 --hitcount 10 -j
DROP
```

উদাহরণ ১৩: ### Protection against port scanning ###

```
iptables -N port-scanning
iptables -A port-scanning -p tcp --tcp-flags SYN,ACK,FIN,RST RST -m limit --limit 1/s --limit-burst 2 -j RETURN
iptables -A port-scanning -j DROP
```