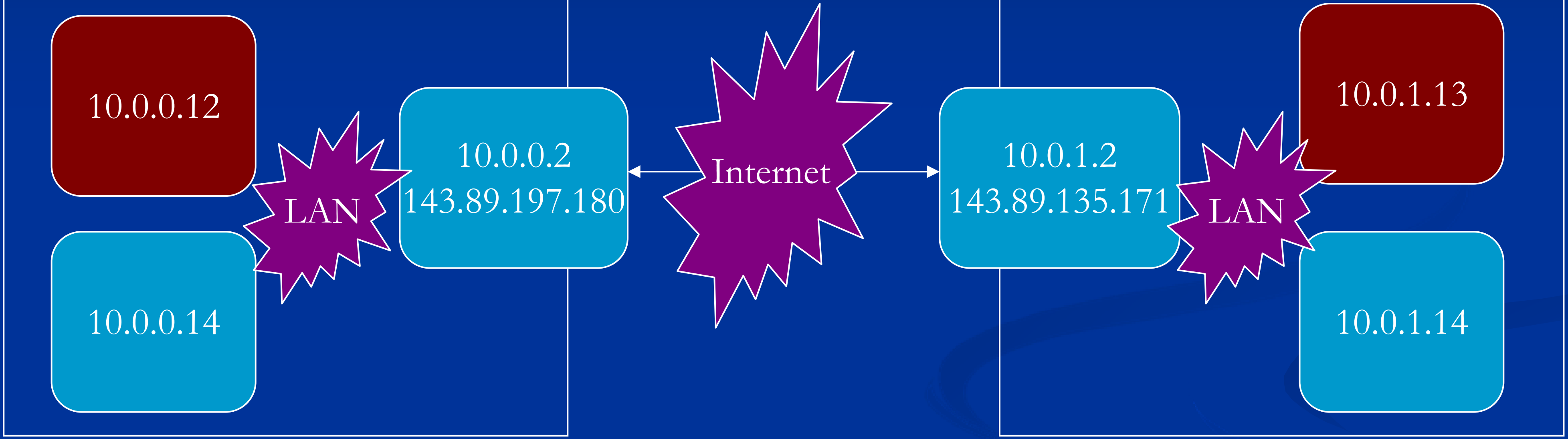
VPN using iptables

Zhiqiang Ma

VPN


10.0.0.12
10.0.0.14
LAN
10.0.0.2
143.89.197.180
Internet
10.0.1.2
143.89.135.171
LAN
10.0.1.13
10.0.1.14

iptables

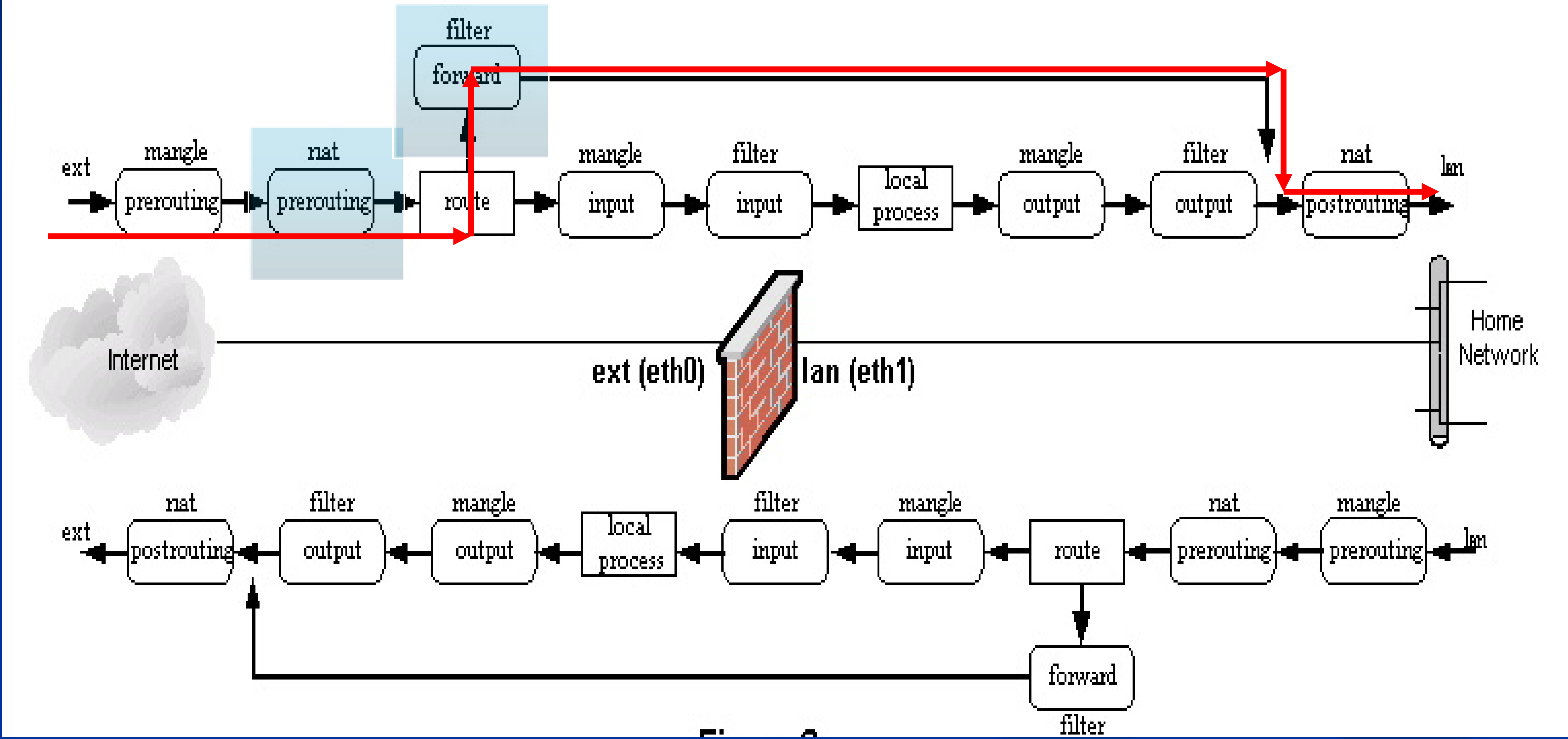


Image from: http://linuxnetmag.berlios.de/en/issue9/m9iptables1.html

iptables port forwarding

Type 1:

LAN -->
nat PREROUTING -->
route --> Internet

Type 2:

Internet -->
nat PREROUTING -->
route --> LAN

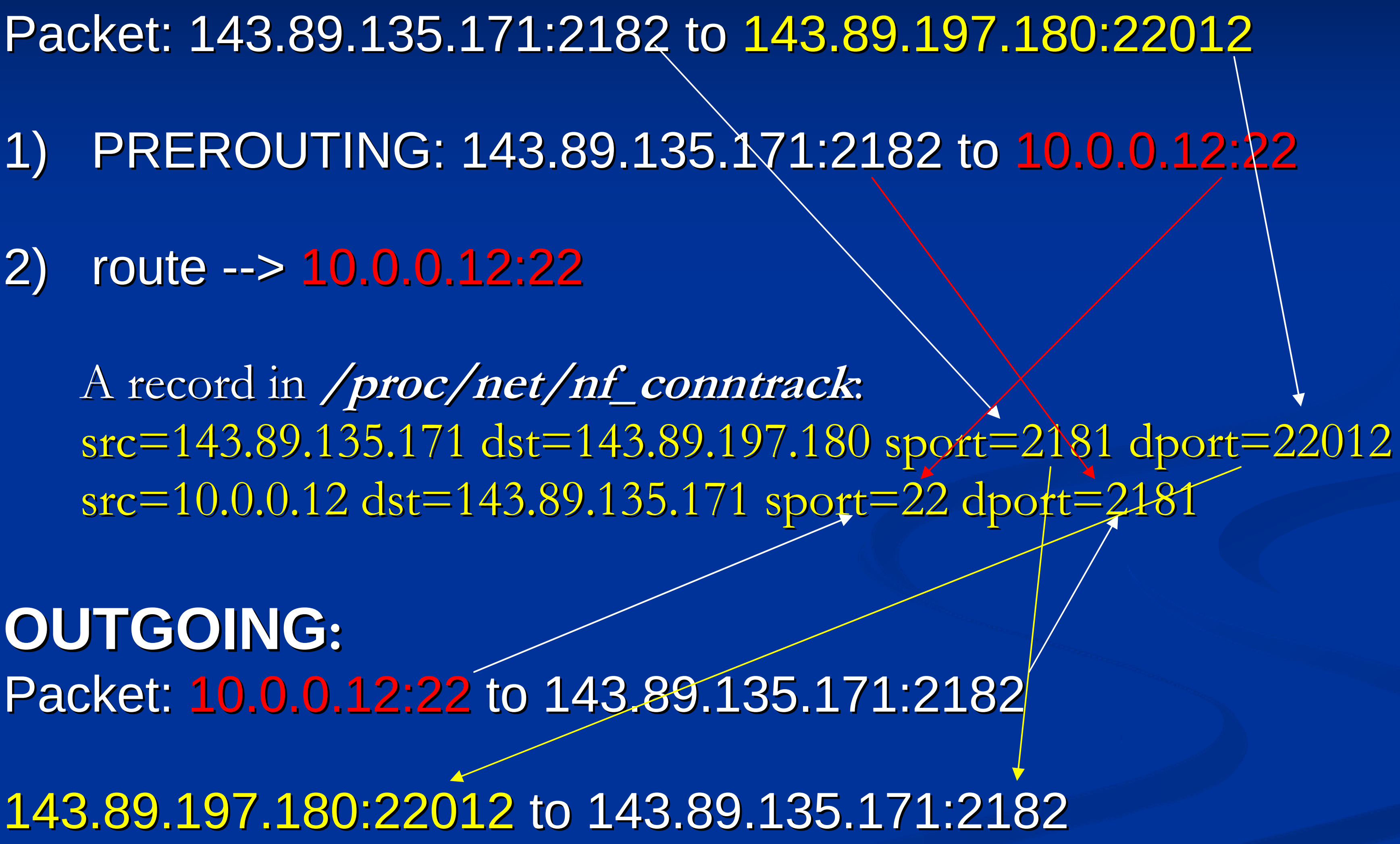
Example

On 143.89.197.180:

```
# iptables -t nat -A PREROUTING
  -d 143.89.197.180 -p tcp --
  dport 22012 -j DNAT --to-
  destination 10.0.0.12:22
```

Example

INCOMING:



Packet: 143.89.135.171:2182 to 143.89.197.180:22012

1) PREROUTING: 143.89.135.171:2182 to 10.0.0.12:22

2) route --> 10.0.0.12:22

A record in ***/proc/net/nf_conntrack***:
src=143.89.135.171 dst=143.89.197.180 sport=2181 dport=22012
src=10.0.0.12 dst=143.89.135.171 sport=22 dport=2181

OUTGOING:

Packet: 10.0.0.12:22 to 143.89.135.171:2182

143.89.197.180:22012 to 143.89.135.171:2182

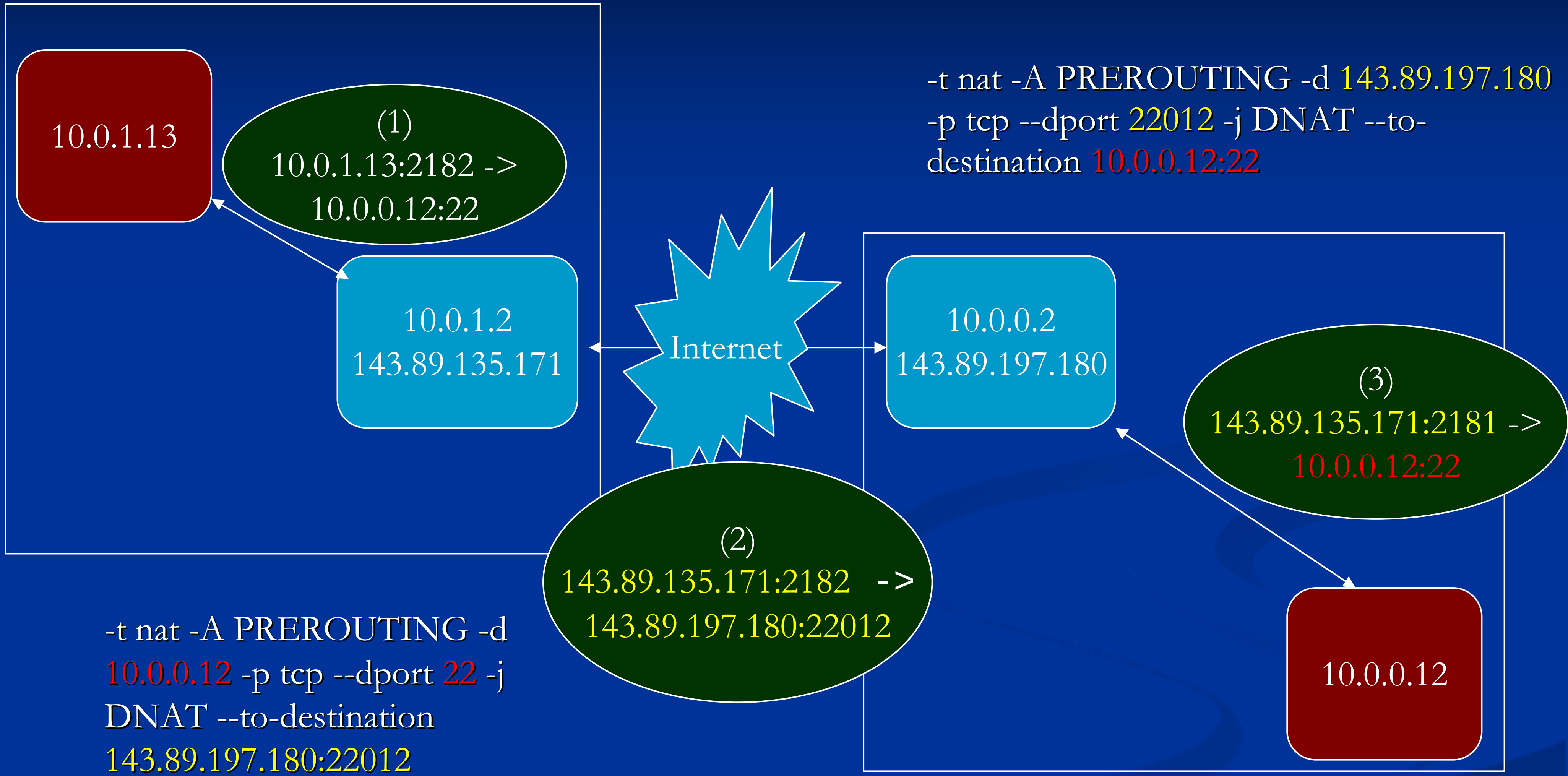
VPN

10.0.1.13 connects to 10.0.0.12:22

- On 143.89.135.171 (gateway of 10.0.1.0/24):
  - -t nat -A PREROUTING -d 10.0.0.12 -p tcp --dport 22 -j DNAT --to-destination 143.89.197.180:22012
  - -t nat ! -d 10.0.0.0/8 -o eth0 -A POSTROUTING -j SNAT --to-source 143.89.135.171

- On 143.89.197.180 (gateway of 10.0.0.0/24):
  - -t nat -A PREROUTING -d 143.89.197.180 -p tcp --dport 22012 -j DNAT --to-destination 10.0.0.12:22

VPN

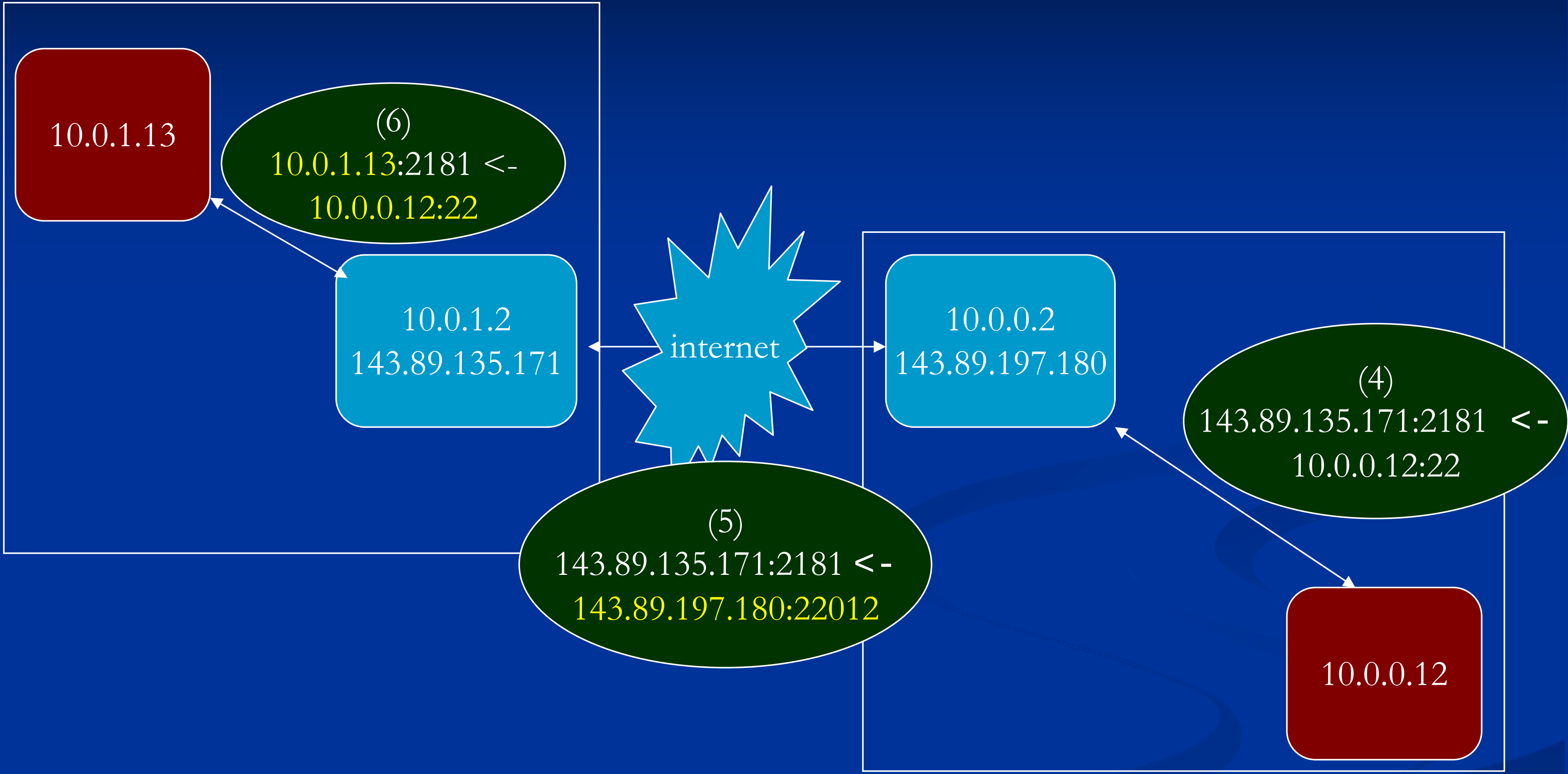


```
-t nat -A PREROUTING -d 143.89.197.180 -p tcp --dport 22012 -j DNAT --to-destination 10.0.0.12:22
```

```
-t nat -A PREROUTING -d 10.0.0.12 -p tcp --dport 22 -j DNAT --to-destination 143.89.197.180:22012
```

```
-t nat ! -d 10.0.0.0/8 -o eth0 -A POSTROUTING -j SNAT --to-source 143.89.135.171
```

VPN


10.0.1.13
(6)
10.0.1.13:2181 <-
10.0.0.12:22
10.0.1.2
143.89.135.171
internet
10.0.0.2
143.89.197.180
(4)
143.89.135.171:2181 <-
10.0.0.12:22
(5)
143.89.135.171:2181 <-
143.89.197.180:22012
10.0.0.12

Evaluation and Limitation

- Evaluation
  - Speed of NFS (10.0.0.2 to 10.0.1.12): 10~11MB/s
- Limitation
  - Only used for connecting to IP:port
  - Two rules on both gateways for one IP:port

Thank you!