



pcextreme

DDoS detection & mitigation

Introduction

Name: Thomas de Looff

1 of 3 owners of PCextreme

- Management
- Datacenter
- Network
- Finance

Hobbies

- Programming
- Running
- Kitesurfing

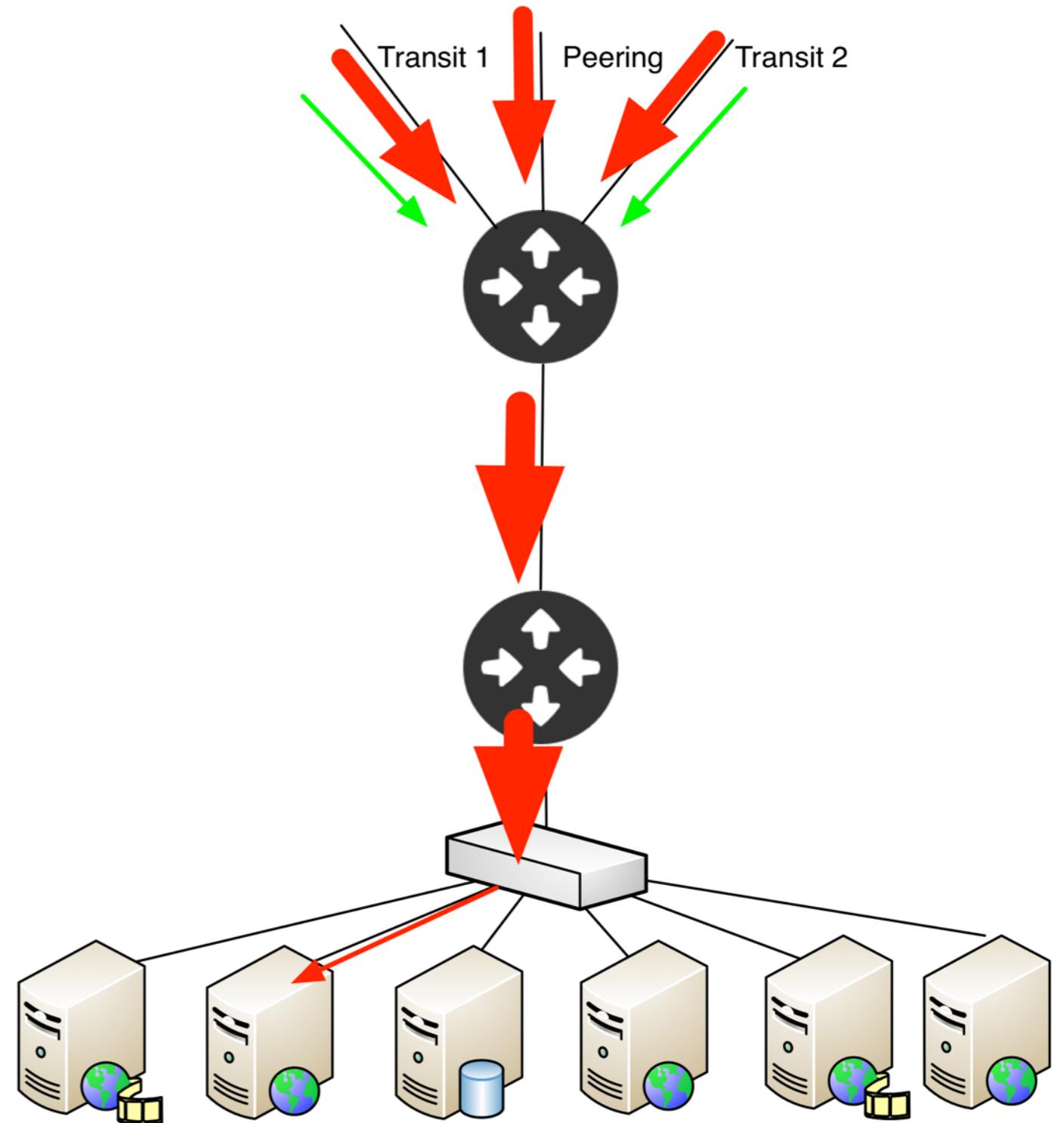
PCextreme

Services

- Cloud Compute & Objects
- Webhosting & Domain registration
- Dedicated Servers
- Colocation & Rackspace
- Managed Hosting

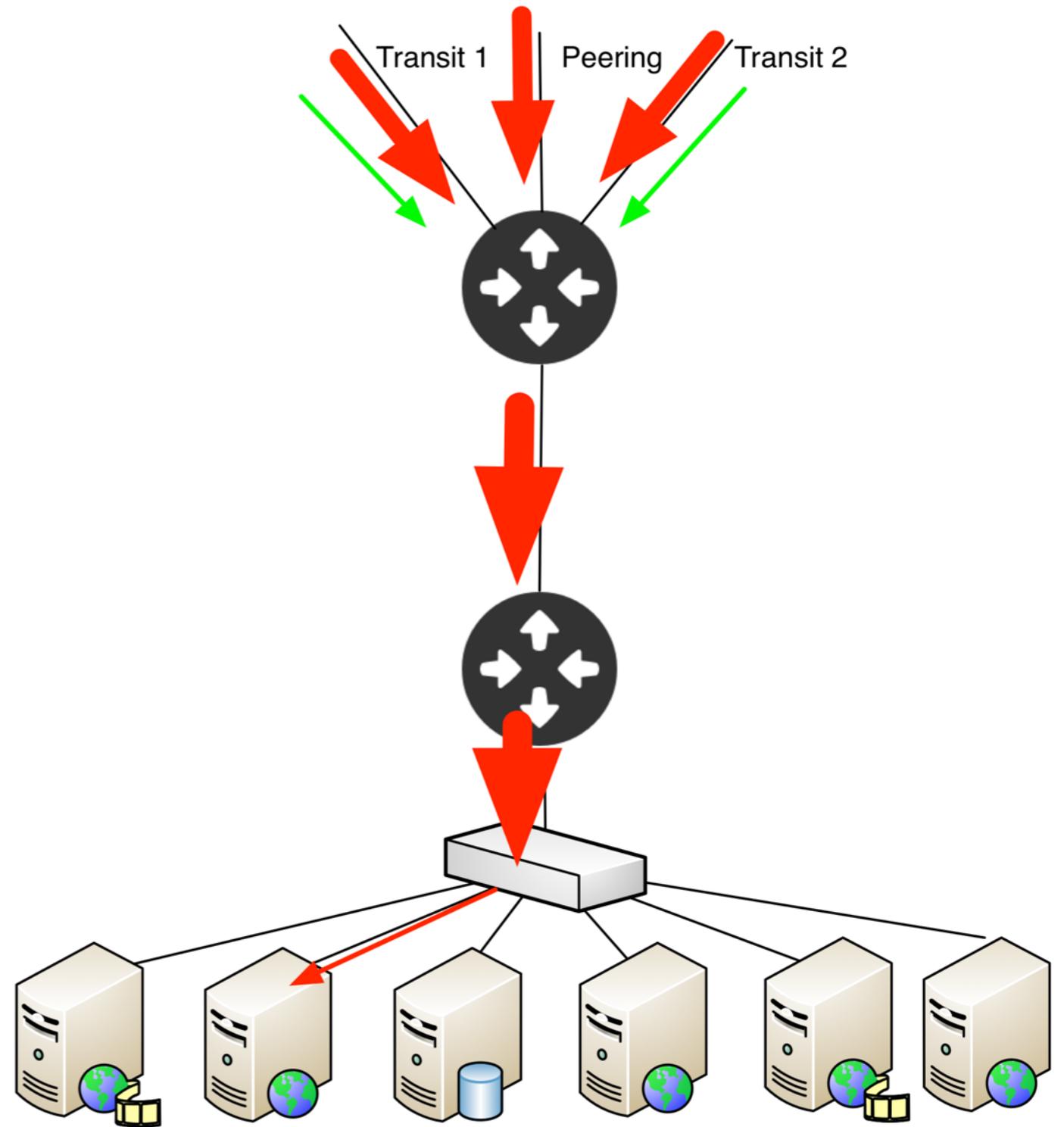
What is a DDoS attack?

- Making the host/network unreachable by sending a lot of traffic from different sources.



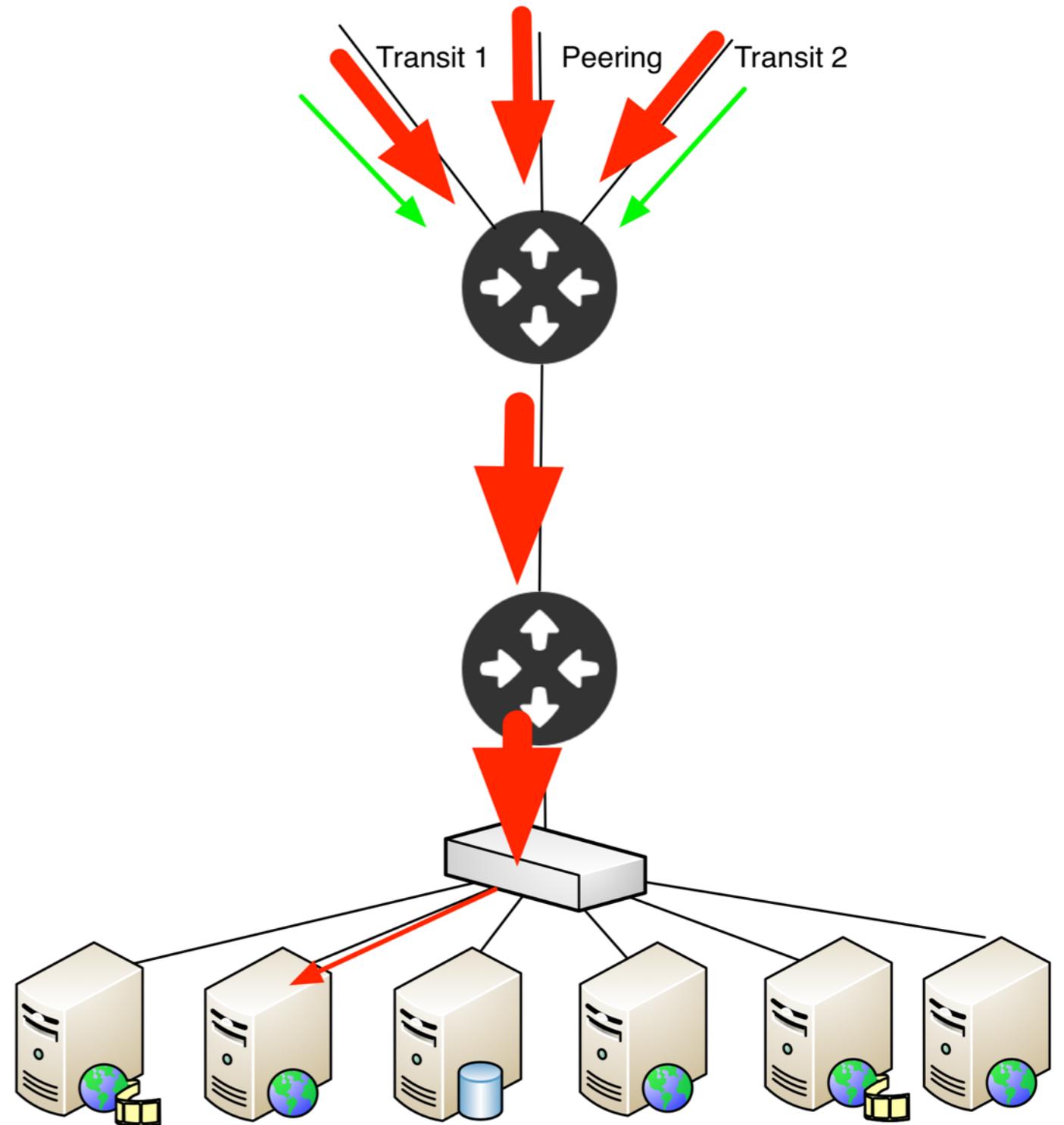
Mitigate a DDoS the old way

- Find the ip that is under attack
- Null route the ip address
- Attacker is happy

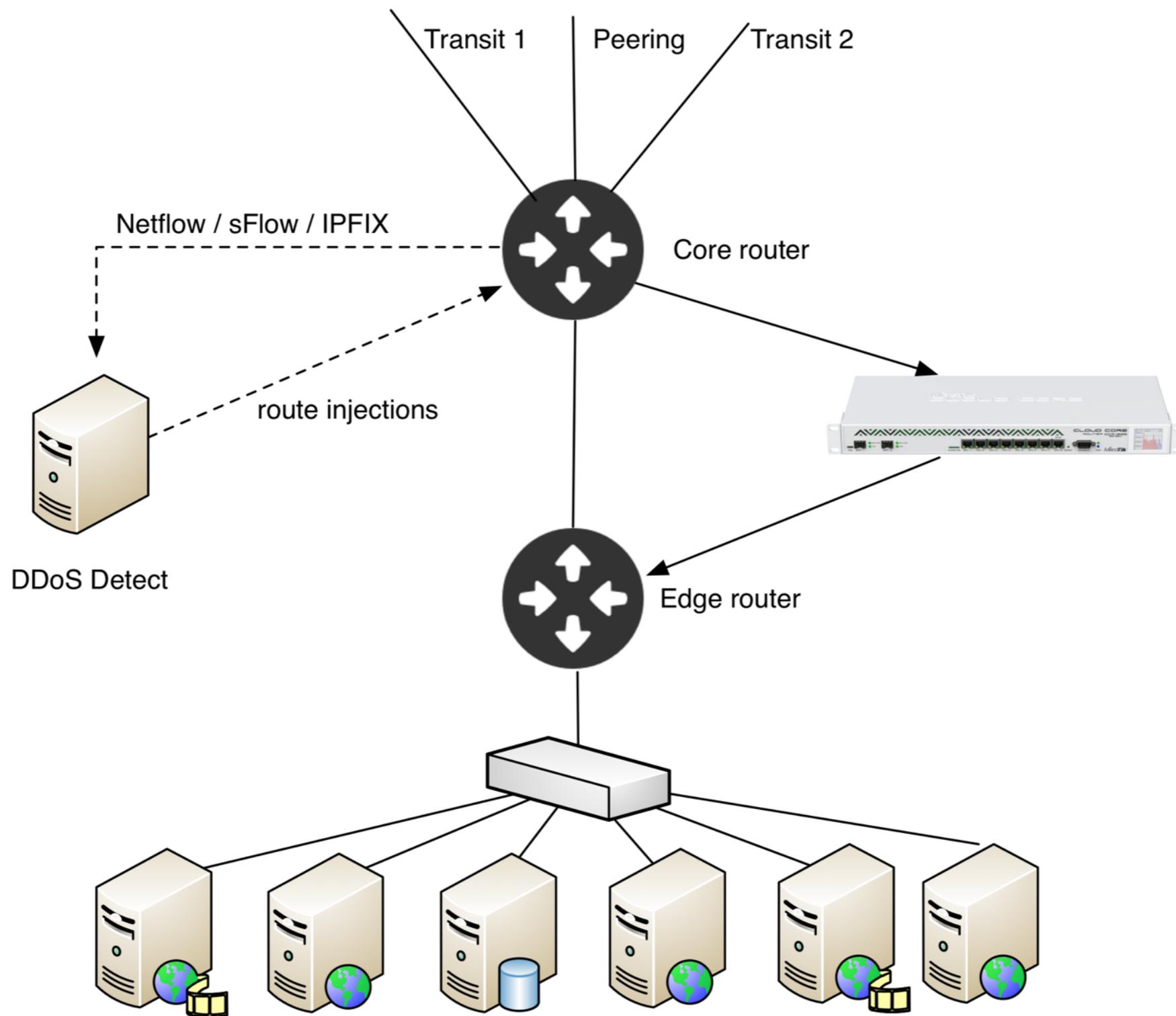


The Problem

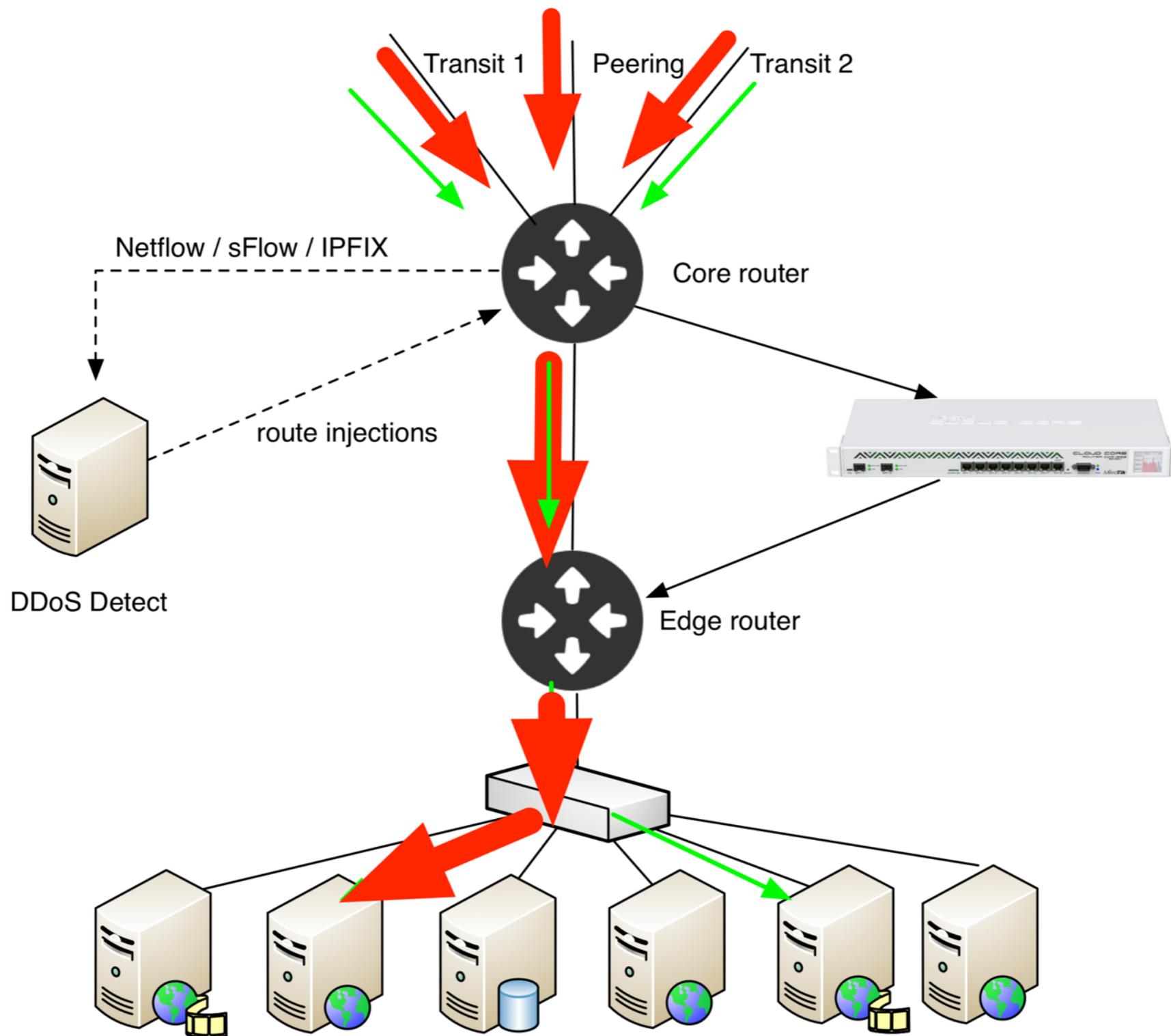
- Null route helps the attacker to reach his goal
- Human action is too slow
- (Stateful) firewall in between cause performance issues



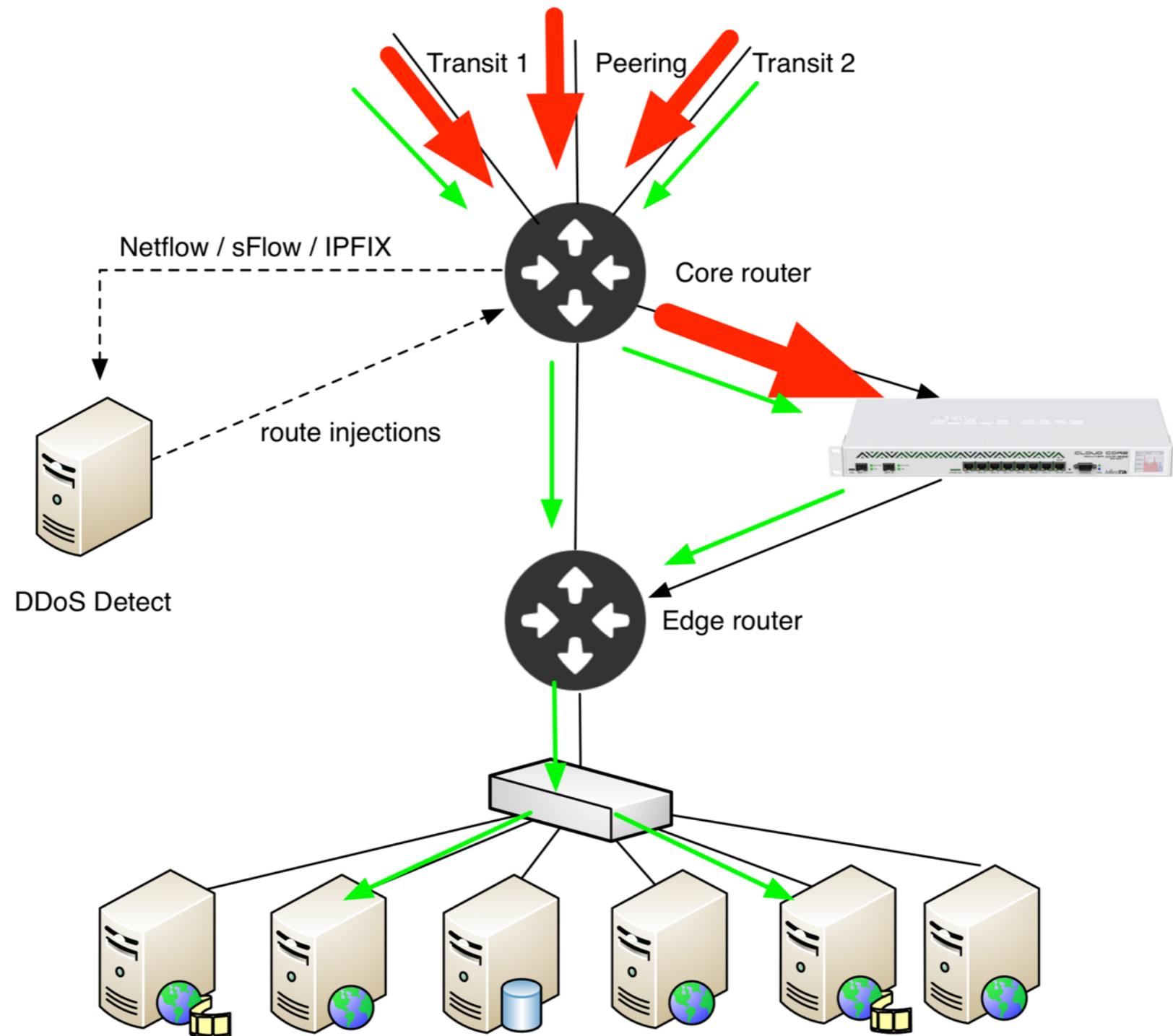
The solution



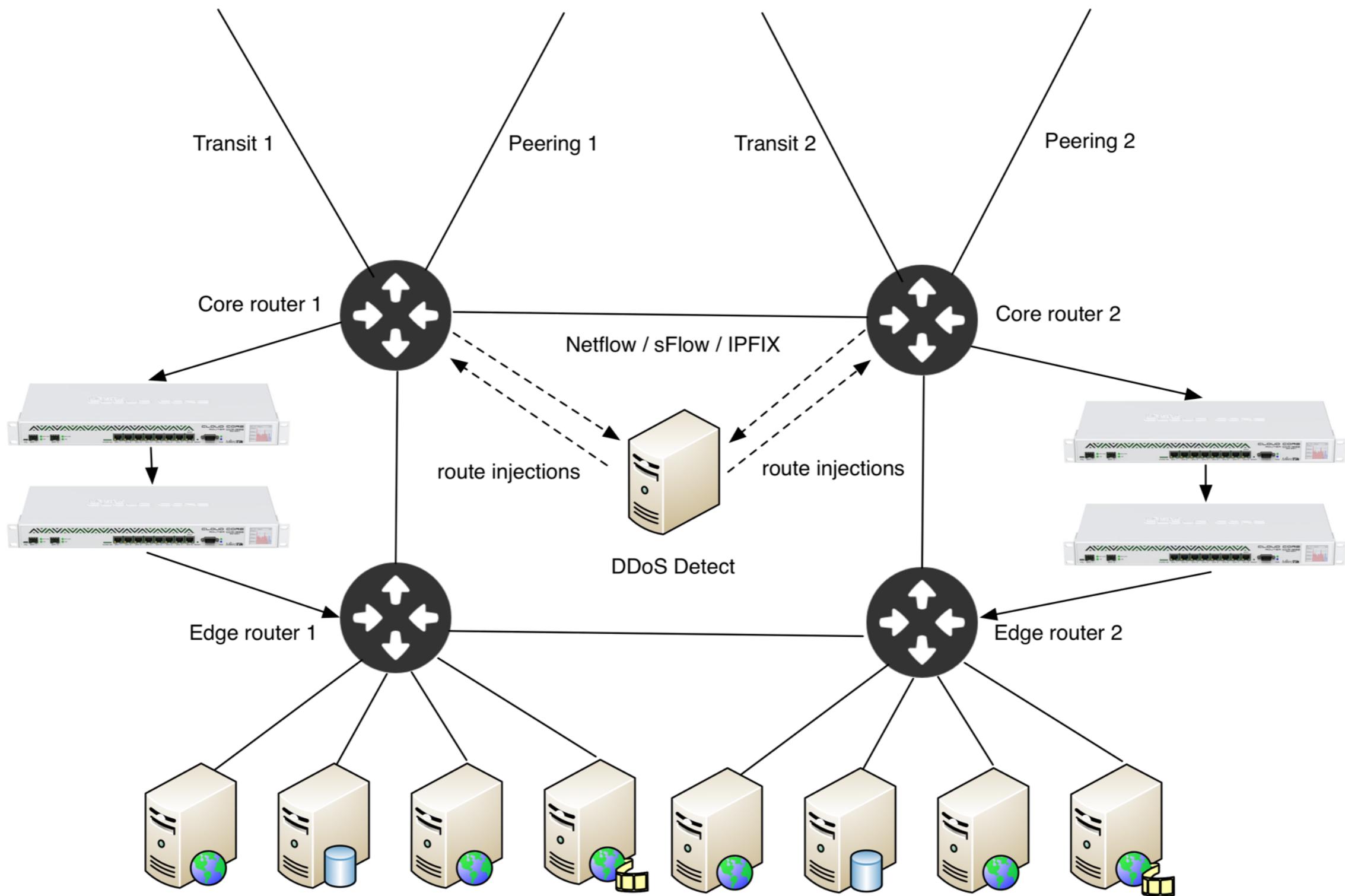
The solution



The solution



The solution



Collecting data with PMACT

```
:~# cat /etc/pmacct/sfacctd-1.conf
daemonize: true
sfacctd_port: 9997
aggregate[ddos]: dst_host, proto
plugins: memory[ddos]
imt_path[ddos]: /tmp/pmacct_ddos.pipe
```

```
:~# cat /etc/pmacct/sfacctd-1.conf
daemonize: true
sfacctd_port: 9998
aggregate[ddos]: dst_host, proto
plugins: memory[ddos]
imt_path[ddos]: /tmp/pmacct_ddos.pipe
```

```
:~# /usr/local/sbin/sfacctd -f /etc/pmacct/sfacctd-1.conf
```

```
:~# /usr/local/sbin/sfacctd -f /etc/pmacct/sfacctd-2.conf
```

DDoS Detect Configuration

```
:/opt/ddosdetect# cat ddosdetect.cfg
[ddosdetect]
interval = 0.5
log-cycle = 1
mitigate-back = 60
logfile = /var/log/ddosdetect.log
pmacct-pipe = /tmp/pmacct_ddos.pipe
blacklist = /opt/ddosdetect/blacklist.db
config-database = /opt/ddosdetect/config.db
```

Add range configuration

```
:/opt/ddosdetect# ./configadd.py -h
usage: configadd.py [-h] -r RANGE -n NETMASK [-pr PRIORITY] [-s SUBPRIORITY]
                  -p PROTOCOL -t TYPE -v VALUE -a
                  {log,firewall,pushover,nullroute} [-k {Y,N}]
```

Add config to database for DDoS Detect

optional arguments:

```
-h, --help            show this help message and exit
-r RANGE, --range RANGE
                       ip
-n NETMASK, --netmask NETMASK
                       range netmask
-pr PRIORITY, --priority PRIORITY
                       higher number is more important
-s SUBPRIORITY, --subpriority SUBPRIORITY
                       higher number is more important
-p PROTOCOL, --protocol PROTOCOL
                       tcp/udp
-t TYPE, --type TYPE  packets / bytes
-v VALUE, --value VALUE
                       trigger value packets/bytes per second
-a {log,firewall,pushover,nullroute}, --action {log,firewall,pushover,nullroute}
                       action to take
-k {Y,N}, --keepon {Y,N}
                       continue the process after triggering the trigger
```

Add range configuration

```
:/opt/ddosdetect# ./configadd.py -r 0.0.0.0 -n 0 -p tcp -t  
packet -v 0 -k Y -a log
```

```
:/opt/ddosdetect# ./configadd.py -r 0.0.0.0 -n 0 -p udp -t  
packet -v 0 -k Y -a log
```

```
:/opt/ddosdetect# ./configadd.py -r 66.66.66.0 -n 24 -p tcp -t  
packet -v 15 -pr 100 -k Y -a firewall
```

```
:/opt/ddosdetect# ./configadd.py -r 66.66.66.0 -n 24 -p udp -t  
packet -v 15 -pr 100 -k N -a firewall
```

```
:/opt/ddosdetect# ./configadd.py -r 66.66.66.0 -n 24 -p udp -t  
packet -v 100 -pr 666 -k N -a nullroute
```

Run DDoS Detect

```
root@pmacct:/opt/ddosdetect# ./ddosdetect.py
```

```
Config:
id: 1 keepon: Y priority: 0 range: 0.0.0.0/0 subpriority: 0 protocol: udp type: packets type_value:
10.0 action: log
id: 2 keepon: Y priority: 0 range: 0.0.0.0/0 subpriority: 0 protocol: tcp type: packets type_value:
10.0 action: log
id: 5 keepon: N priority: 666 range: 66.66.66.66/32 subpriority: 0 protocol: udp type: packets
type_value: 100.0 action: nullroute
id: 4 keepon: N priority: 100 range: 66.66.66.0/24 subpriority: 0 protocol: tcp type: packets
type_value: 15.0 action: firewall
id: 3 keepon: N priority: 100 range: 66.66.66.0/24 subpriority: 0 protocol: udp type: packets
type_value: 15.0 action: firewall
2015-09-15 09:51:03,142:INFO:Star Cycle
2015-09-15 09:51:05,189:INFO:Star Cycle
2015-09-15 09:51:07,226:INFO:Star Cycle
2015-09-15 09:51:09,248:INFO:Log:ip_dst: 66.66.66.66 ip_proto: udp packets p/s: 12.0 bytes p/s: 17748.0
Check protocol: udp type: packets value: 10.0
2015-09-15 09:51:09,255:INFO:Star Cycle
2015-09-15 09:51:11,293:INFO:Star Cycle
2015-09-15 09:51:13,329:INFO:Star Cycle
2015-09-15 09:51:15,349:INFO:Firewall:ip_dst: 66.66.66.66 ip_proto: udp packets p/s: 24.0 bytes p/s:
35496.0 Check protocol: udp type: packets value: 15.0
2015-09-15 09:51:15,358:INFO:Star Cycle
2015-09-15 09:51:17,391:INFO:Nullroute:ip_dst: 66.66.66.66 ip_proto: udp packets p/s: 184.0 bytes p/s:
266224.0 Check protocol: udp type: packets value: 100.0
2015-09-15 09:51:17,406:INFO:Star Cycle
```

Route injection with ExaBGP config

```
cat /etc/exabgp/exabgp1.conf
neighbor 92.63.170.217 {
    description "core01";
    router-id 1.1.1.1;
    local-address [router ip];
    local-as 65002;
    peer-as 65002;
    graceful-restart;

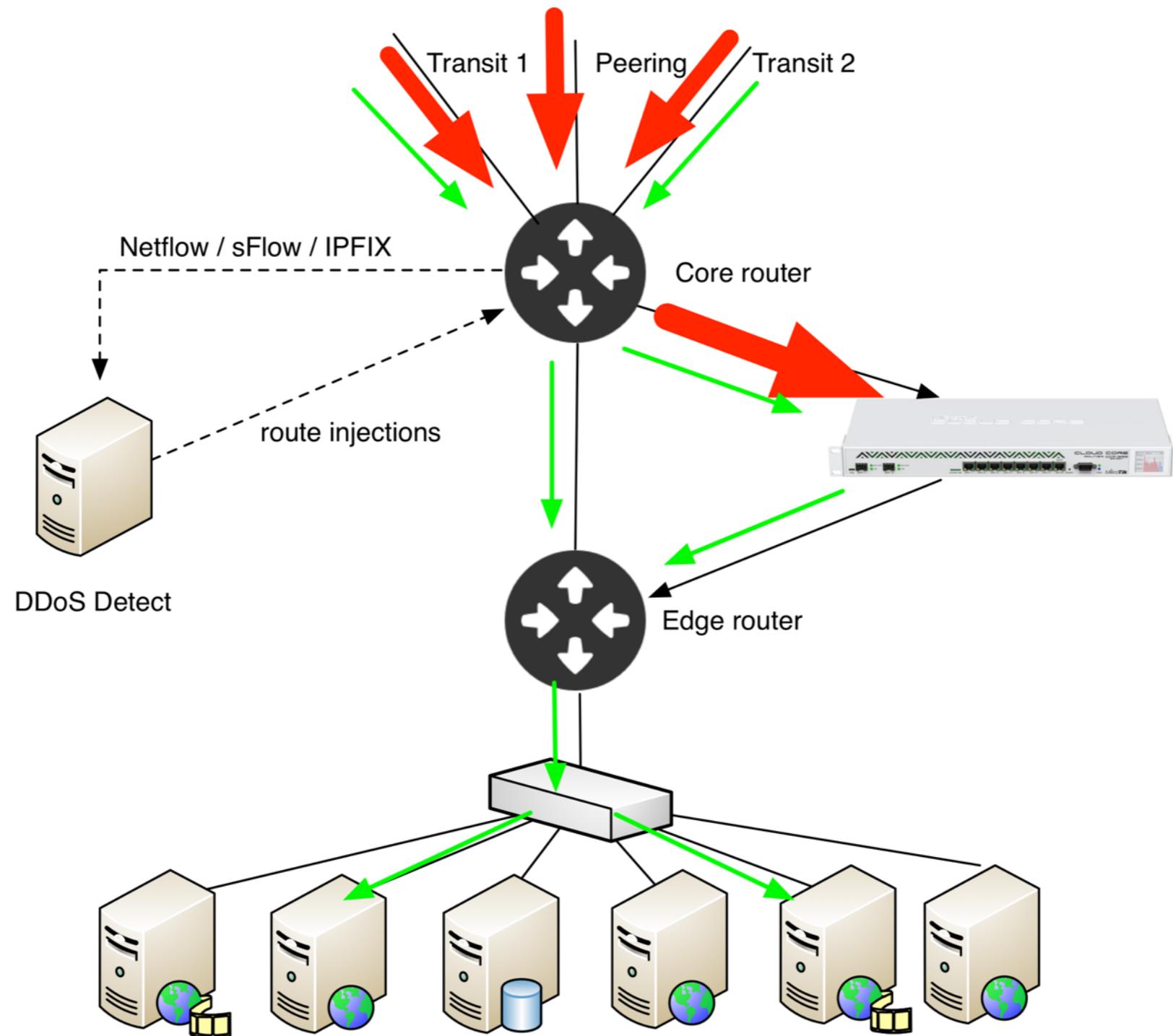
    static {
        route 88.88.88.0/24 next-hop [firewall ip] community [as]:[community];
    }

    process announce-routes {
        run /opt/ddosdetect/exabgproutes.py [router name] [firewall ip];
    }
}
```

Route injection with ExaBGP example

```
:/opt/ddosdetect# /opt/ddosdetect/exabgproutes.py  
announce route 92.63.168.230/32 next-hop [firewall ip]  
withdraw route 92.63.168.230/32 next-hop [firewall ip]
```

The solution



Thanks

Coming Soon

<https://github.com/thomasdelooff/>

Collaboration

- NBIP/ NaWas
- OSAS H2020

Interested?

thomas@pcextreme.nl