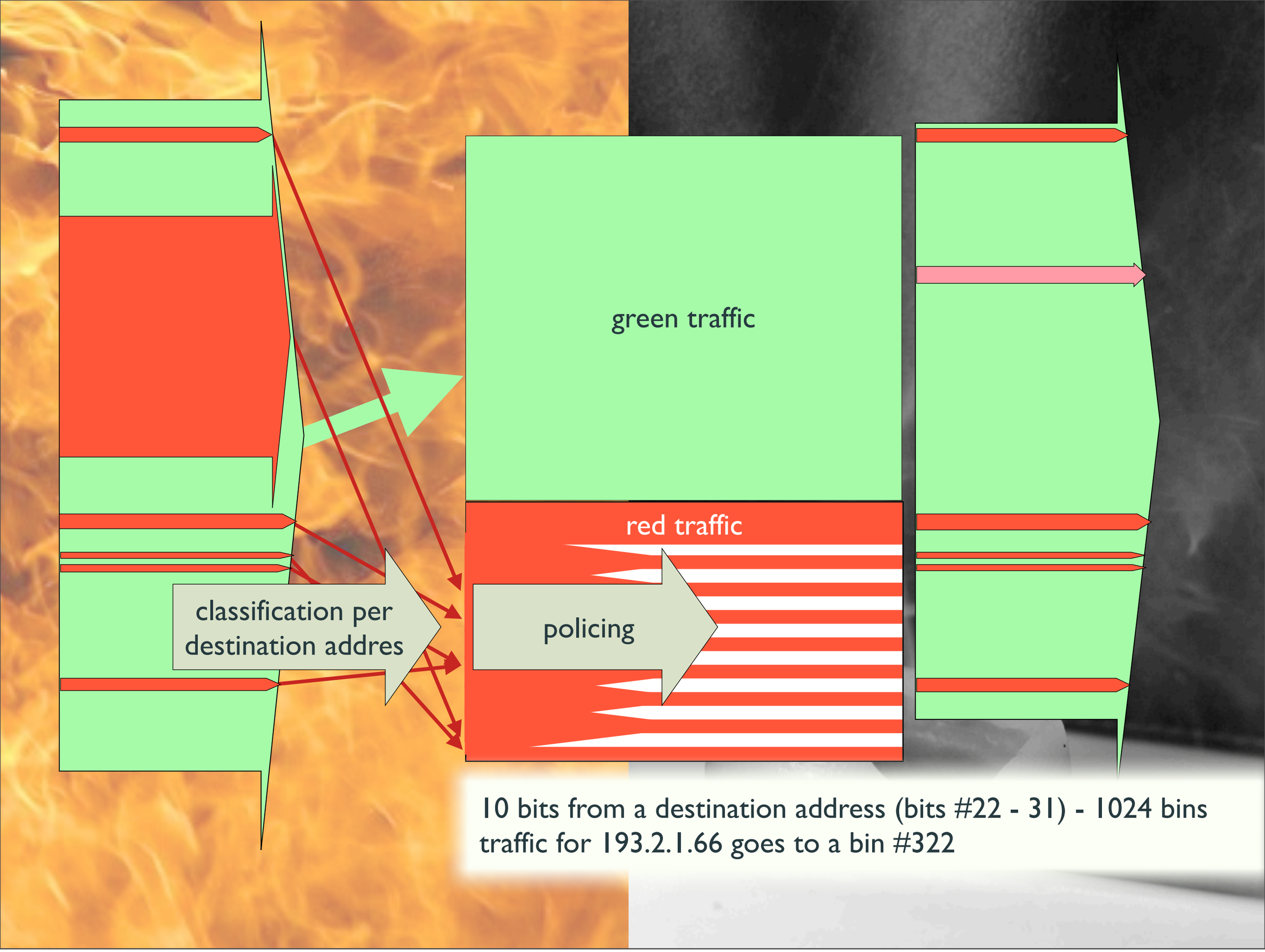
“Poor man’s DoS protection”, Matjaž Straus Istenič, ARNES (Slovenian National Research and Educational Network)
A lightning talk at RIPE 64, 17.4.2012.

You might have been DoSed recently. We were ...
And we don’t want to spend money on special and expensive DoS detection and mitigation systems.
But we have routers, don’t we? ;-). Some Cisper or Junico platforms support features which can be efficiently used to limit the impact of DoS attacks. Let’s take a brief look into one of these features.



torek, 17. april 12

How can we extinguish the fire or at least turn it to a smoking candle?
Let us assume that most of the internet traffic is green (TCP established sessions). But some is red. Red is important but much less in volume, like TCP/SYN, UDP etc.
It is reasonable to assume that DoS traffic is red in most cases. Actually it is.
First we separate the incoming traffic - green traffic is forwarded without interference, but red is classified into bins. The bin index is derived from some part of the destination IP address (this works for IPv4 only :-( ), say the last 10 bits -- this will give 2^10 = 1024 bins. For example, 193.2.1.66 maps to a bin #322.
Each bin serves multiple flows which have the same common 10 bits in the destination address.
Traffic in each of the bins is then policed. Committed rate for policers is set high enough not to impact the legitimate traffic, say 10-times the average.
Traffic combined and forwarded out. DoS traffic turns out pink ;-)

And the red traffic is...

TCP/SYN common ports	TCP/SYN	TCP/RST
UDP common ports	UDP tiny (plen = 28, 29)	UDP huge (plen = 1500)
other UDP	tunnels (proto 4, 41, 47, 50)	uncommon protocols
fragments	ICMP	IP toward campuses

A typical “red” traffic.
TCP/SYN and UDP can be further divided into several groups according to port number, packet length - most common ports like TCP/80, 443, UDP/53 etc can be put into a separate group than all other (rarely used) ports.
This technique may also be used to protect the end users, student campuses for example.

```
[edit firewall]
policer FlowPolicerUdpHuge {
    if-exceeding {
        bandwidth-limit 40m;
        burst-size-limit 4m;
    }
    then discard;
}

[edit firewall family inet]
prefix-action ActionUdpHuge {
    policer FlowPolicerUdpHuge;
    count;
    filter-specific;
    subnet-prefix-length 29;
    destination-prefix-length 32;
}
```

```
[edit firewall family inet filter ProtectMe]
term PoliceUdpHuge {
    from {
        destination-prefix-list {
            MyNetworks;
        }
        packet-length 1500;
        protocol udp;
    }
    then {
        accept;
        prefix-action ActionUdpHuge;
    }
}

[edit interfaces xe-0/0/0 unit 666 family inet]
filter {
    output ProtectMe;
}
```

torek, 17. april 12

Here is an example of prefix-specific policing actions configuration on Junipers (works on M, MX and T series).
- policer, - prefix-action policer with a counter (counts forwarded bytes/packets, dropped packets)
- used in the egress firewall filter on the LAN interface
A similar but somehow less powerful feature for Ciscos - microflow policing (User-Based Rate Limiting on Cat6500).

Routers can do many things besides routing :-)