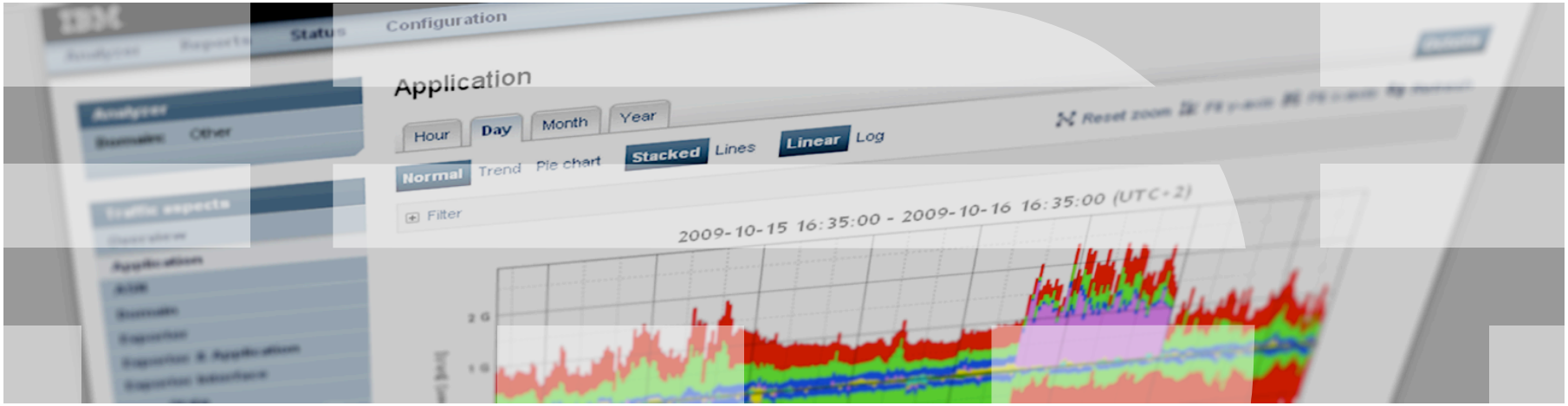
Security, DDoS and AntiSpam

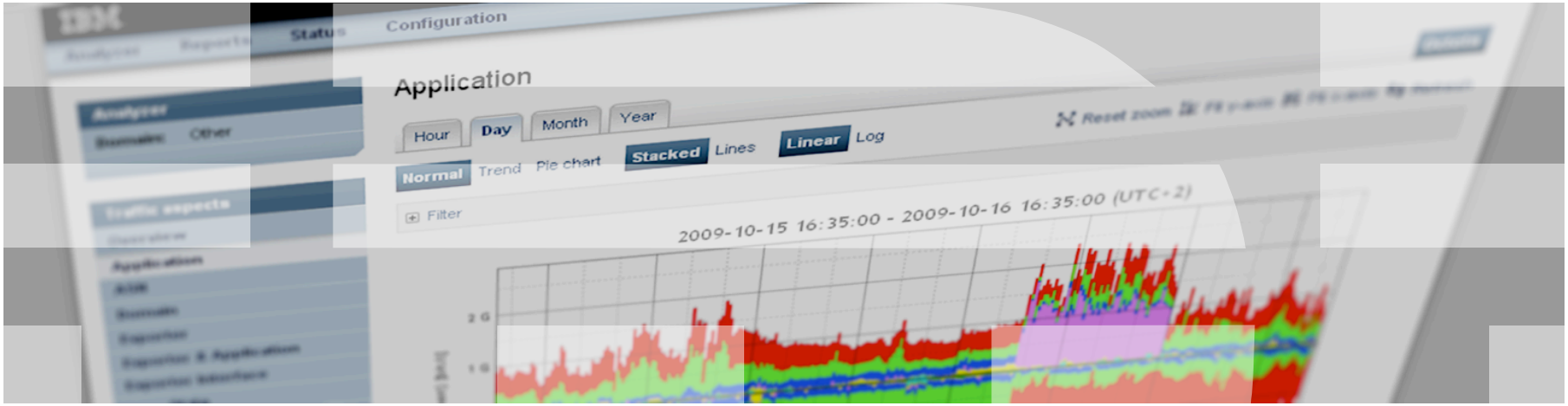
How to secure the Internet outside of the bunkers inside the Swiss Alps



Jeroen Massar <jma@zurich.ibm.com>

Contacts

Who you gonna call?



Jeroen Massar <jma@zurich.ibm.com>

Can somebody from company XYZ please contact me?

- Do you have proper working NOC/Security contacts for all your peers?
  - Email
  - Hard line phone
  - Cell phone
- Are you sure those numbers and addresses still work and that those people are still there?
- Looking it up in an external database somewhere on the Internet might work, but what if your connectivity is down or you can't reach that password list where the password for the database is down?
- Yelling on (Swi|NA|…)NOG for somebody to reach you might be too late, as your customers are affected and maybe you can't mail in the first place as your lines are clogged up
- Do keep your data upto date in RIPE db (IRT objects), NSP-SEC, at your local IX and of course peeringdb. Having roles for the contacts is a good idea.

Do you have IRT?

- An IRT object describes an “Incidence Response Team” and how to contact them
- IRT objects are referred to using mnt-irt in inetnum/inet6num and cover more specifics automatically.
- Retrieve the best IRT object: whois –h whois.ripe.net –c <ip-address/prefix>
- IRT objects are mandatory in the APNIC region, currently also a proposal in the RIPE region for requiring IRT objects to be present.
- And you are protecting your RIPE objects with a PGP key instead of a MD5 password we hope…. ;)

But do you actually read abuse@example.net? And do they?

- abuse@ should be non-spam/virus-checked, as you want to receive spam and virusses when people report them
- As such all spam will go through to it
- Need to filter out the cruft: the real spam, not the reports about spam
- There have been various attempts at coming up with a ‘reporting standard’, unfortunately there is not a generally accepted one

Security Communities

- NSP-SEC (+various sub-groups per region)
  - Trusted Community, need to be a ‘can type on routers’ person
  - Signup can be requested by joining the list and providing details, need to be vouched in
  - Meetings: NANOG, RIPE, APRICOT security BOF

- Ops-Trust
  - Highly vetted community, operators and people who can provide data/tools
  - Invite only

- ISC
- DSHIELD
- SANS

- FIRST/CERT (later slides)

- Government

CERT (Computer Emergency Response Team)

- See CERT (http://www.cert.org) and FIRST (http://www.first.org)
- Find your local CERTs and know who are there so you can contact them easily
- Generally PGP-signed & crypted email used as communication
  - Have your PGP key signed and properly published
- They will talk to other CERTs and ISPs, but they won't do your work

iNOC-DBA (Inter-NOC Dial-by-ASN)

- URL: http://www.pch.net/inoc-dba/
- Got an ASN? Then you can join the system
- Get a SIP phone or even a soft-phone
- Bind your FreeSWITCH/Asterisk box into the system

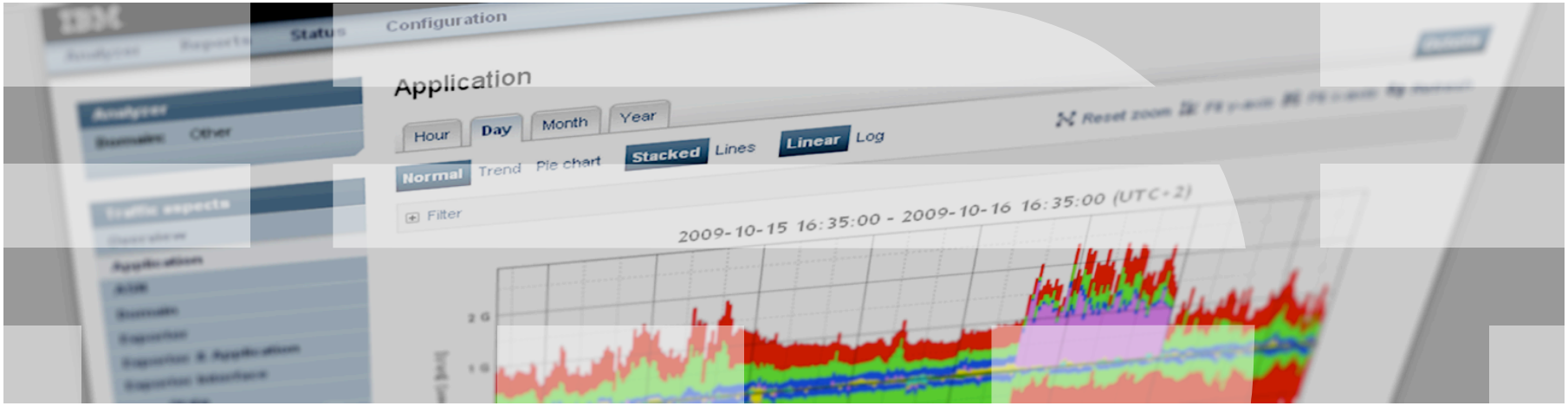
Voila:

- Direct contact to a large number of ISPs world wide
- Verified that you are at least in the ISP who runs that ASN
  - Avoids call-screening, as it is an iNOC-DBA call, they know it is not some random person just calling for pranks or because their latency is high in their game

For a couple of test numbers: http://unfix.org/projects/voip/

Precautions

How to avoid having to come out of bed



Jeroen Massar <jma@zurich.ibm.com>

Remote locations & Cheap survival

- Unless you are a very large ISP with several disjunct datacenters, consider setting up a DNS server, MX backup and various other such resources that are important to you as backups at a different ISP, under their prefix, managed by them

  When your network goes down, their network most likely keeps on working as they are disjunct from yours.

- A simple VM or just a 1U box at another ISP which acts as a tiny backup can save you

- Another approach: instead of hosting everything yourself, have the main version at your location under your full control, but be ready to trigger failover to a number of cheaply hosted VMs at various locations. These don't always have to carry the full version of the service you are providing, but might just enable you to keep on running and not be completely down

- Have a status URL so that if things break, that you can communicate to the Internet

- Being prepared to explain what is happening and thus informing customers earns a lot of kudo points from them and thus might save your face

Stepping on fibers, busting in doors

- Redundant paths are important, what if someone steps on one of your
  - Fibres
  - Electricity
  - Cooling

  somewhere in the middle of nowhere, or just right outside your bunker?

  Do you have a contingency plan, do you know how to detect and localize the problem?

- Is your datacenter secure?
  - Finger print scanner
  - Retina scanner
  - Access cards
  - Passport checks

  but the nice lady at the entrance can re-program the cards and even has a special key to open the door anyway…

Watch your network equipment

- Is the configuration really the configuration that you put on the box?
  - Store configurations in a central location, RCS them if possible
  - Verify regularly that the configuration you put on it is still there and not changed
  - RANCID is one of various tools for this purpose
- Do you have central control over your network equipment?
  - Make sure that you at least duplicate your centralization, thus distribute it
- Use TACACS+ with logging to verify what is happening to hosts and who is doing what
- Pushing configuration from a database is another good option, but make sure you have proper ACLs on the database and the tools to control them; and keep a backup of it
- Can the rest of the internet access your router console, or just your NOC?
  - Filter properly, use separate infrastructure
- Make sure that your equipment is properly NTP synced, otherwise logs don't make sense

Update and Access

- Do you have a proper security contact and contract with your vendors?
  - Generally only organizations with a contract will be warned in advance of nasty bugs
  - If some bug hits you, can you get them to fix it?
- Do you check and update your hardware/software regularly for security issues?
- Do you have Out-Of-Band (OOB) access to the device?
  - Drop a GPRS modem attached to a console server in the datacenter if possible
  - When using a network based AAA make sure the AAA backend can be reached OOB too otherwise you can't authenticate the moment you need to get in

BCP 38 (RFC 2827)

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

- In short: Do not send packets to the network that you should not be originating

- Do source-route filtering as close to the source as possible
  - Watch out for "multi-homed" customers

Techniques:

- Simple firewall rule blocking out the prefix
- Unicast RPF

  When there is no route towards that prefix it should not originate it
- Various device specific techniques eg in DSLAMs / Cable concentrators which also look at MAC addresses

Protect your routing

- Don't let anything else but the IX/peers talk to your BGP daemons
- BGP with TCP/MD5
- Generalized TTL Security Mechanism (GTSH)
  - Set TTL to 255 at sender and verify on receiver that the TTL is still 255
  - Packets then have to be from the same link and cannot have been routed
- Only accept packets from known MAC addresses
- Use arpwatch alike tools to make sure no new MACs are introduced on a switch, next to monitoring the switch that the cable was not unplugged

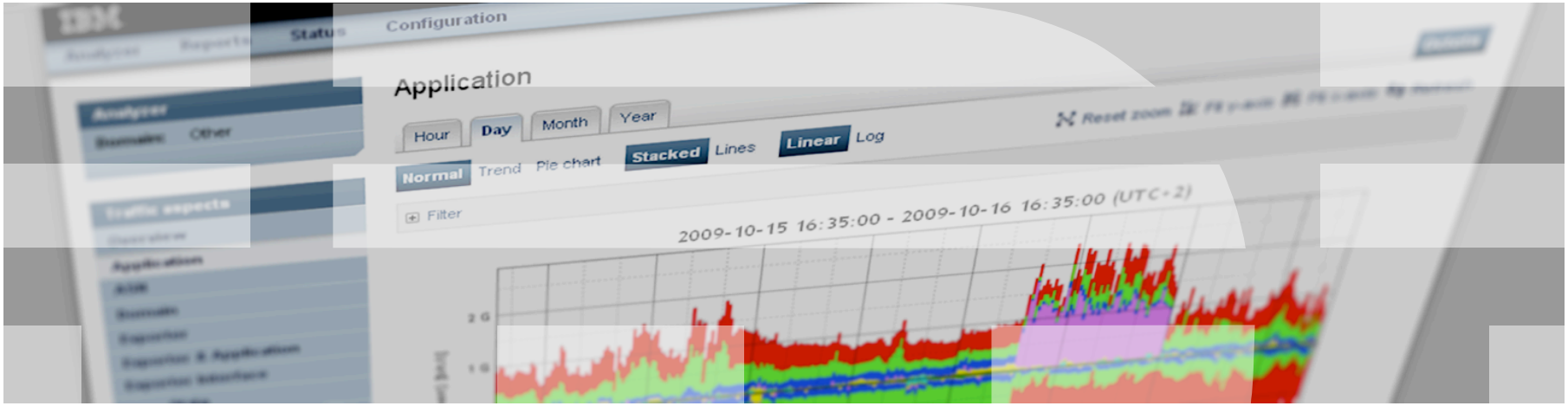
- Use RPSL
  - Put your route/route6 objects in the IRR
  - Generate prefix filters from it

- There are various secure routing proposals, unfortunately none in wide deployment

- Monitor your own prefix on the Internet so that you at least know that it is being used somewhere else by somebody else, of course inform folks of the hijack
- Using multiple prefixes can be useful because of that as they need to steel all your prefixes to be able to bring you down at ISPs that accept their advertisement

Knowledge is power

The use of Intelligence



Jeroen Massar <jma@zurich.ibm.com>

Monitoring

- NetFlow / IPFIX / sFlow
  - How many flows/sec can your routers meter, and how fast is your collector/analyzer?
  - What are you going to look at?
- SNMP
  - Are you looking at all the right values?
  - Are you polling 100.000 devices every second, every minute, every hour?
- Syslog
  - Need to set up proper rules to filter out the events you really want to see
- TACACS+ logging
  - Watch those authentication failures and changes to the nodes
- Packet Capturing?
  - Got Tap?

Passive DNS

- dnscap in front of recursive DNS servers, or even in line on the transit link
- Logs every DNS request made by clients on the network

- As such, if there is a virus, one can easily determine which clients made queries to the domains involved and then notify the clients

ISC SIE (Security Information Exchange) https://sie.isc.org/ provides several good feeds for this information; unfortunately mostly US based. Maybe time for a Swiss Edition?

Honeypots

- Honeypots can provide advance warning and trends
- Can detect that your own customers are running into it and get that problem resolved quickly
- Can also tell friendly peers about which customers are hitting your honeypot

- Do you operate your own Honeypot?

Walled Garden

- When you have detected that a customer is infected
  - Try to reach them, call them up (costly)
  - Walled Garden!

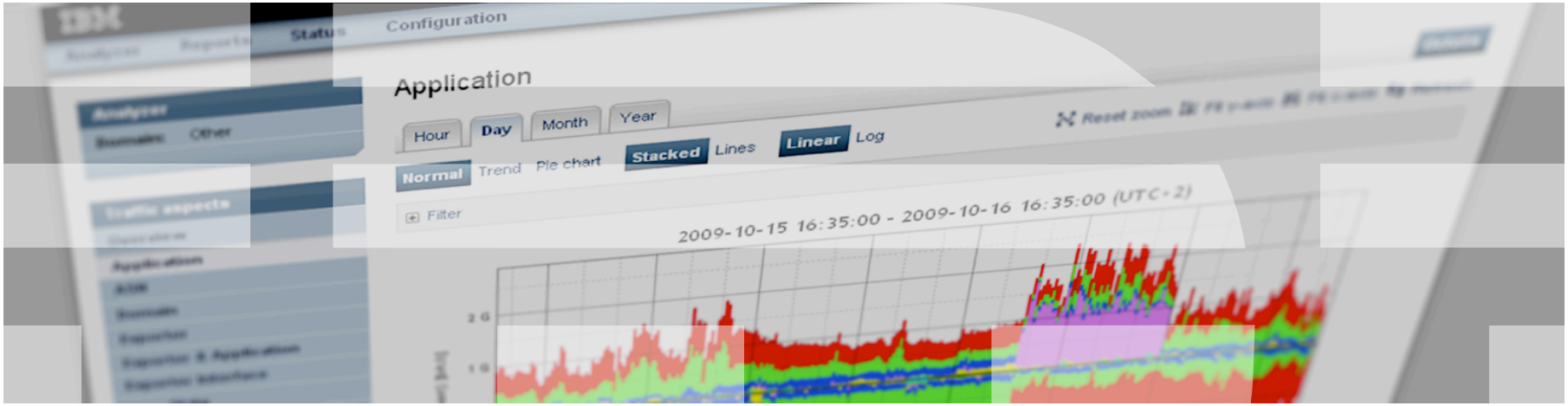
- Put customers and/or sources you do not trust in a special network
- Redirect all port 80/443 traffic to a website with a warning notice

- Always provide a “I need to use the Internet right now” button, but do give them a final warning

- Most likely need to allow VoIP traffic, thus at least SIP and Skype as they might have emergency calls going over it

Defend

Taking care of the nasties



Jeroen Massar <jma@zurich.ibm.com>

Remote Triggered Black Hole Filtering

You and your peers/transits/upstreams agree that if you announce a prefix to them with a certain BGP community set they will blackhole it at their borders.

- Can announce single /32's which are being targetted
- Avoids the traffic further entering their network and thus also yours
- Avoids you being billed for that traffic

See amongst others: http://www.nanog.org/mtg-0110/greene.html

PI space to the rescue: drop it when you don't want the traffic

Another trick employed generally for IRC servers is to put the IRC server in a /24 along with other resources that are DDoS sensitive/attractive.

When somebody is mad at it and starts DDoSing:

- Drop the announcement to your transits
  - Thus they won't route it and your pipe frees up, keeping traffic to your other customers flowing.
  - You don't pay for the DDoS bits

  Generally this means you have cut down on the DDoS heavily already as all the transited bots can't packet you anymore

- Drop the announcements to direct peers that are still involved

As you still announce to local peers they can still access the resource, useful if you generally only have local clients.

But:

- With IPv6 you have PA space and announce the full /32 or more, thus can't use this trick.
- DDoS kiddos wise up too and will start attacking other parts of your infrastructure.

BGP FlowSpec (RFC5575)

- Distributes a “Flow” inside BGP and marks that flow to be filtered by routers
- Requires cooperation of and implementation at upstreams

More information:

- http://www.terena.org/activities/tf-ngn/tf-ngn17/uze-flowspec.pdf

Open source (read: 3 clause BSD) tool that can do this:

- http://bgp.exa.org.uk/

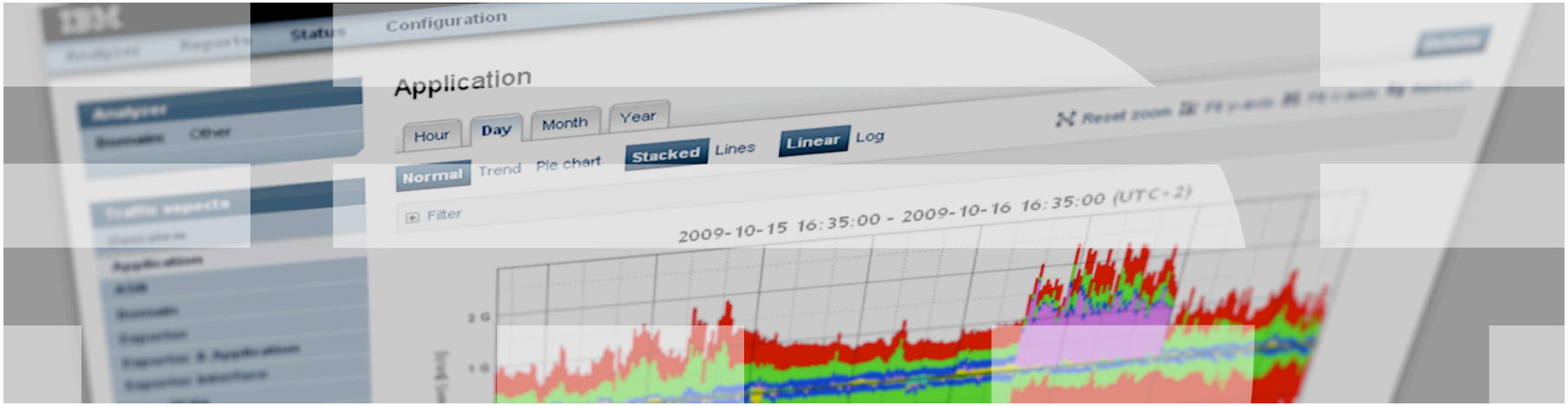
Implemented also on your favorite J and C boxes and a variety of other vendors

Scrubbers / Sinkholes

- A big big box that announce a specific prefix in iBGP for the host under attack
- Attack now goes to this big box
- The box either drops everything (sinkhole)
- Or it scrubs out the traffic it thinks is useful and routes it on to the host under attack
  - Using IDS, eg snort or similar tools
- Can be used also to route all un-allocated (darknet) space to, and it becomes a perfect IDS
- Anycast this service at the edge of your network to distribute the workload and to save the traffic from crossing your core

- If the customer was using BGP to announce the prefix to you, they will stop flapping and their connectivity restores

Questions?



Jeroen Massar <jma@zurich.ibm.com>