Infoblox
CONTROL YOUR NETWORK

Talks about DNS: architectures & security

Agenda

- Increasing DNS availability using DNS Anycast
- “Opening” the internal DNS …
- Enhancing DNS security
  - DNS traffic monitoring & alerting
  - Leveraging DNS to protect against malwares
  - Securing your DNS infrastructure against attacks

Sounds 101 … ?

- DNS is part of the network plumbing ☺
- Still overlooked in many entreprises
  - Legacy infrastructure
  - Lack of monitoring
  - Patch management
  - Change management & traceability

- New IT infrastructure trends & apps are increasing pressure on the DNS infrastructure
  - Availability
  - Performance
  - Security
- … and might require some DNS redesign or new approach

Increasing DNS availability using Anycast

Customer use case – moving to Anycast

- Global WW press/media company headquartered in Europe

- Using legacy Solaris/Bind and Microsoft DNS infrastructure
- Lot of static laptop configuration ☹ long term change process

- Challenges:
  - Availability issues
  - Primary/secondary DNS usual setup is not efficient - issues with in-house applications

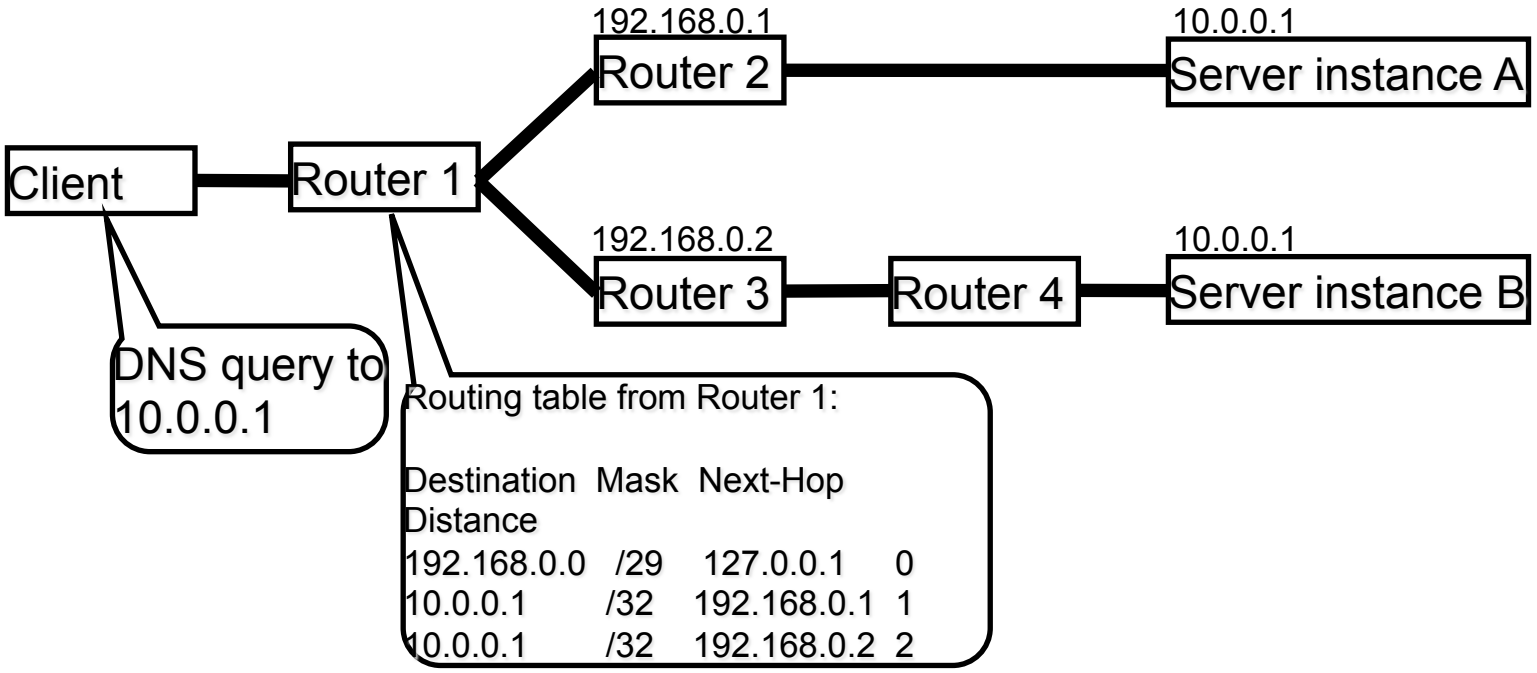
  - Lack of visibility – no traceability of DNS operations
  - Challenges with patching , esp. Solaris – lack of ressources/expertise

Anycast DNS – quick refresh

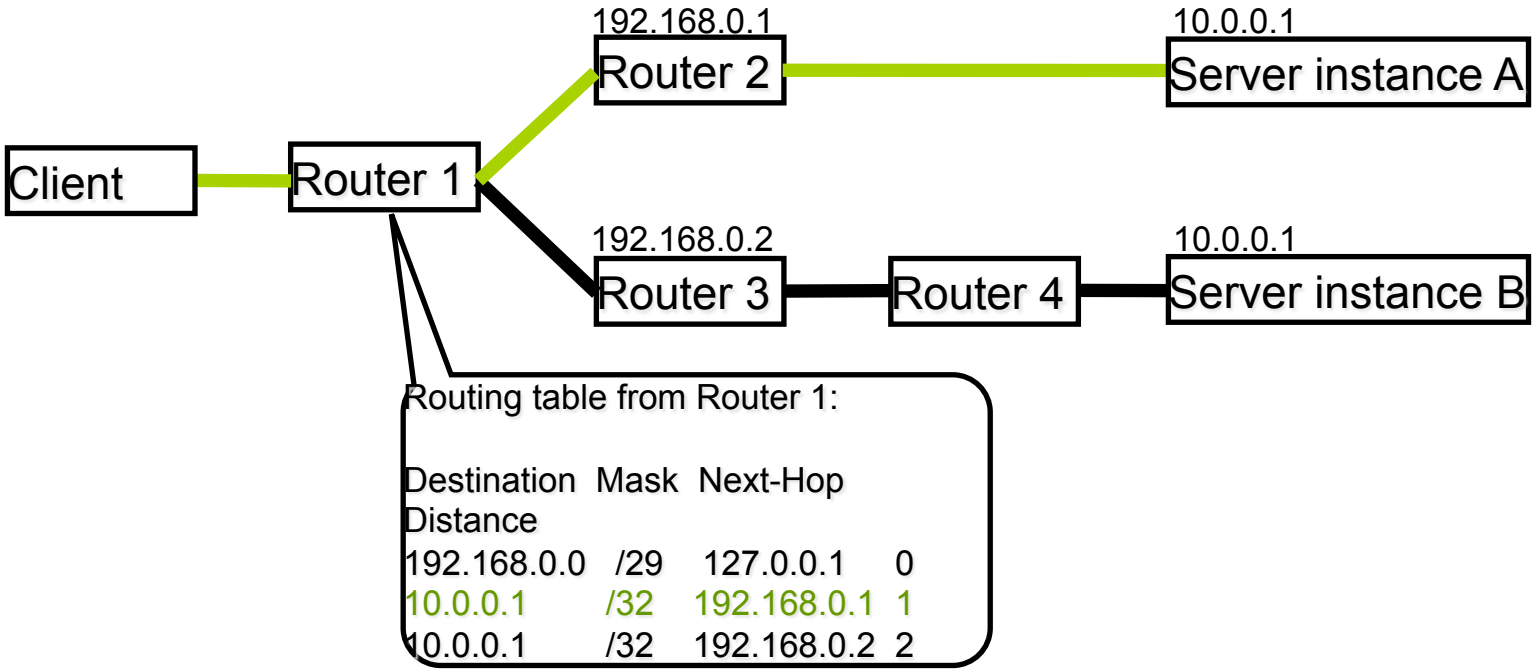
- Anycast DNS allows multiple, distributed name servers to share a single virtual IP address
- Each name server advertises a route to that address to its neighbors – typically using a routing protocol
- Queries sent to that address are routed to the closest name server instance

- From any one location on the Internet/Intranet, you can only see (and hence attack…) a single member of an anycast group at once

Anycast in Action



Anycast in Action



Infoblox

Customer use case – implementation highlights

- Customer choosed to deploy a unified infrastructure (based on Infoblox Grid)
- Anycast DNS is now running for a few years internally
- One high-availability pair per “geo” datacenter for internal DNS – using OSPF routing
- Key benefits
  - Easier setup (client side & mobility)
  - Increased SLA
  - Easy maintenance and patching
- Phased migration
  - Forward rules on legacy servers during transition/grace period (few months)
  - Traffic monitoring

Anycast DNS is a proven setup !

- Host anycasting service is not new (RFC1546 – 1993 ☺)

- Proven deployment in the Internet
  - C, F, I, J, K, L, M root-servers (hierarchical anycast)
  - .fr NS
  - Service providers for distributed DNS caching service

- Anycast is (and should be) more and more considered for internal DNS

“Opening” the internal DNS …

Customer use case - Need to open internal DNS

- European utility company
- Typical closed internal DNS infrastructure “company.local”
- No end-to-end resolution for external names
  “an internal laptop is not able to resolve www.google.com” using nslookup or dig”
- DNS resolvers for external resolutions used by proxy/selected DMZ servers
- Leveraging web proxys for external access

- Moving mail in the cloud, office 365 and other services
  - Office 365 requires some external name resolutions from laptop/desktop
  - Identified proxy challenges in terms of workload
    - SSL based connections
    - Long life connections

Customer use case - DNS implementation talks

- Decided to avoid proxy for office365
- More global thinking around internal DNS

- Selective DNS forward rules
  - Controlled DNS but …
  - … Maintenance / scalability
  - … Troubleshooting

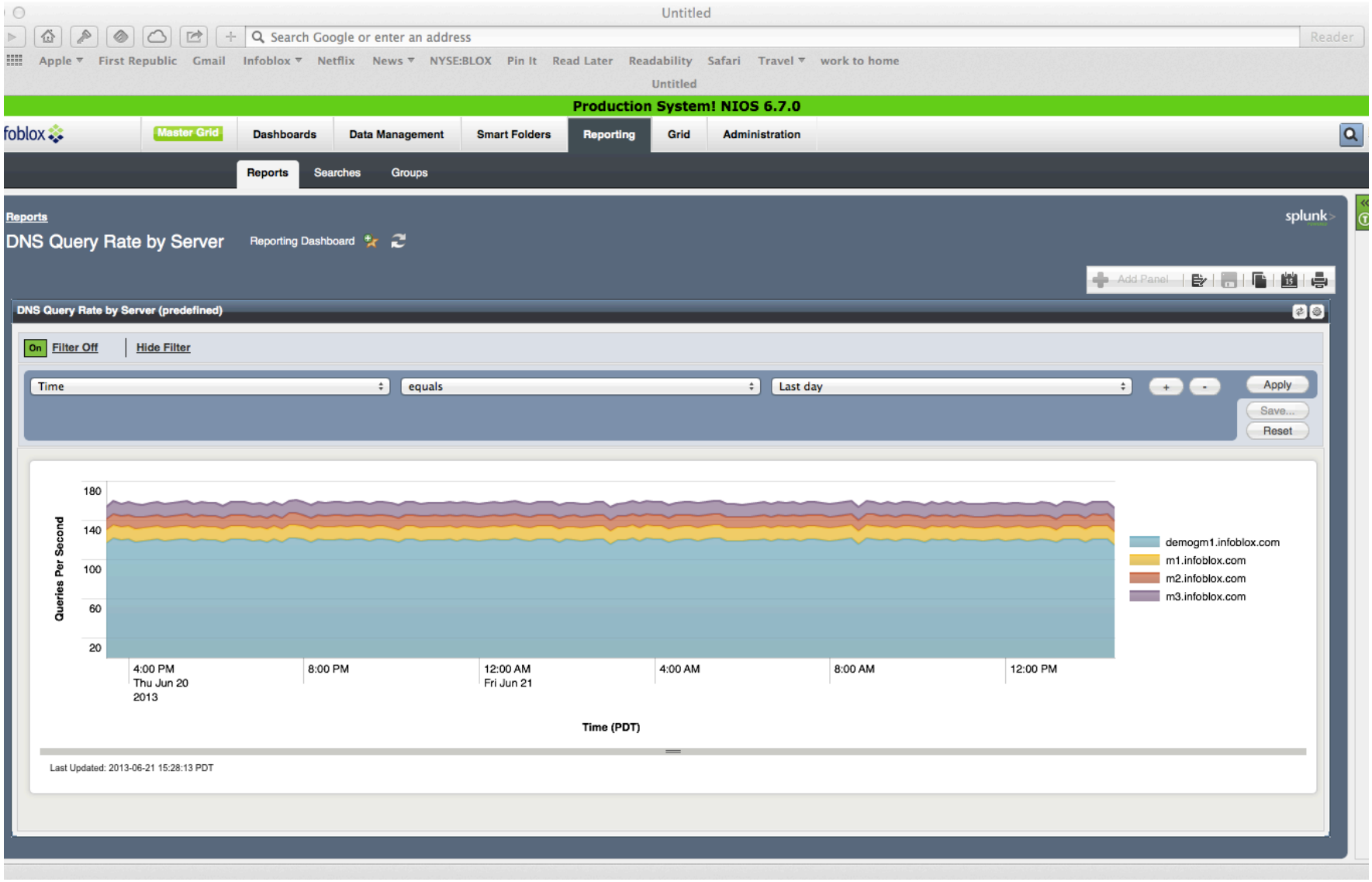
- “open” DNS resolution – easier / future proof but requires increased security
  - How can I improve my DNS monitoring?
  - How can I improve security around DNS?
    - Malware protection and mitigation
    - Advanced DNS protection

DNS traffic monitoring & alerting

Best practice: Monitoring DNS Traffic

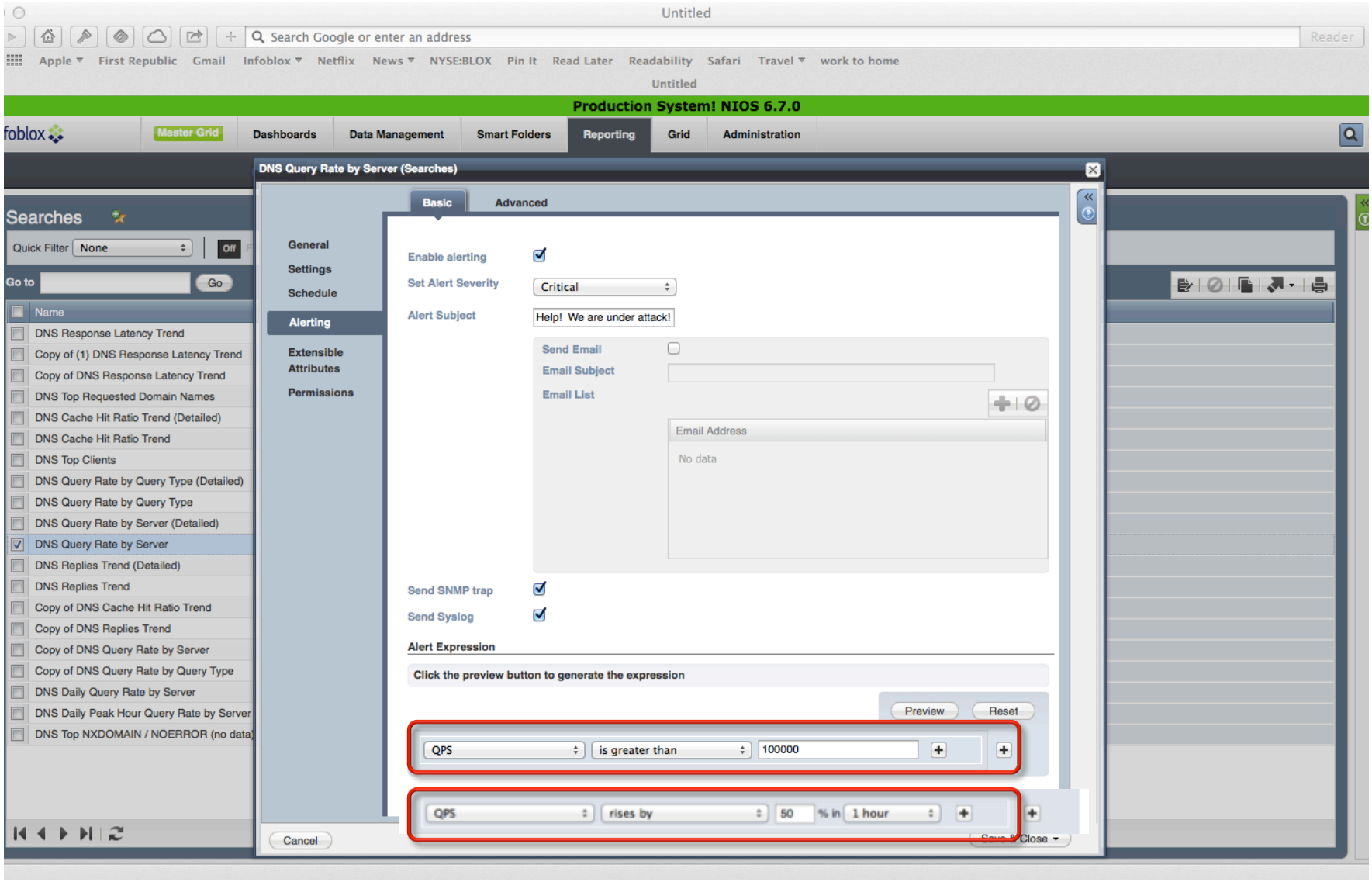
- Monitor traffic to your name servers:
  - Aggregated query rate
  - Top queriers
  - Top domains
  - Query types (with associated query rates)
  - Response latency trend
- Ability to set alert on traffic change (threshold, growth)
- Ability to analyze DNS traffic smoothly and selectively
  - DNS Queries AND Responses

Monitoring Aggregate Query Rate



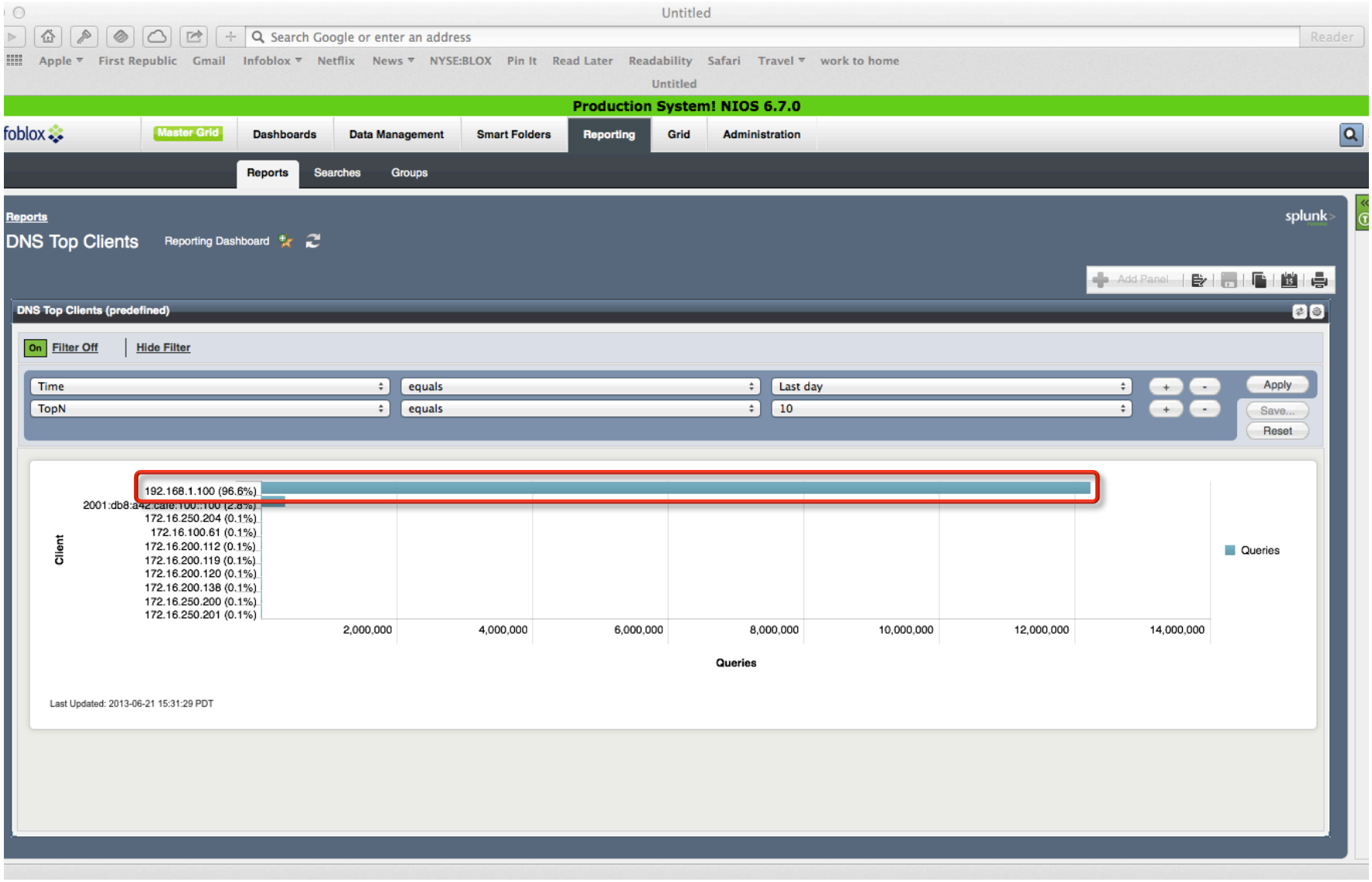
 |

Setting Alerts on Aggregate Query Rate



 |

Monitoring Top Clients



 |

Infoblox

Malware protection and mitigation using DNS ?

Malwares use DNS

- Malwares infects clients when they visit malicious web sites, whose names are resolved using DNS
- Malwares contact command-and-control channels using hardwired domain names and rapidly changing IP addresses (fast-flux, double fast-flux)
- Malwares can tunnel new malicious code through DNS

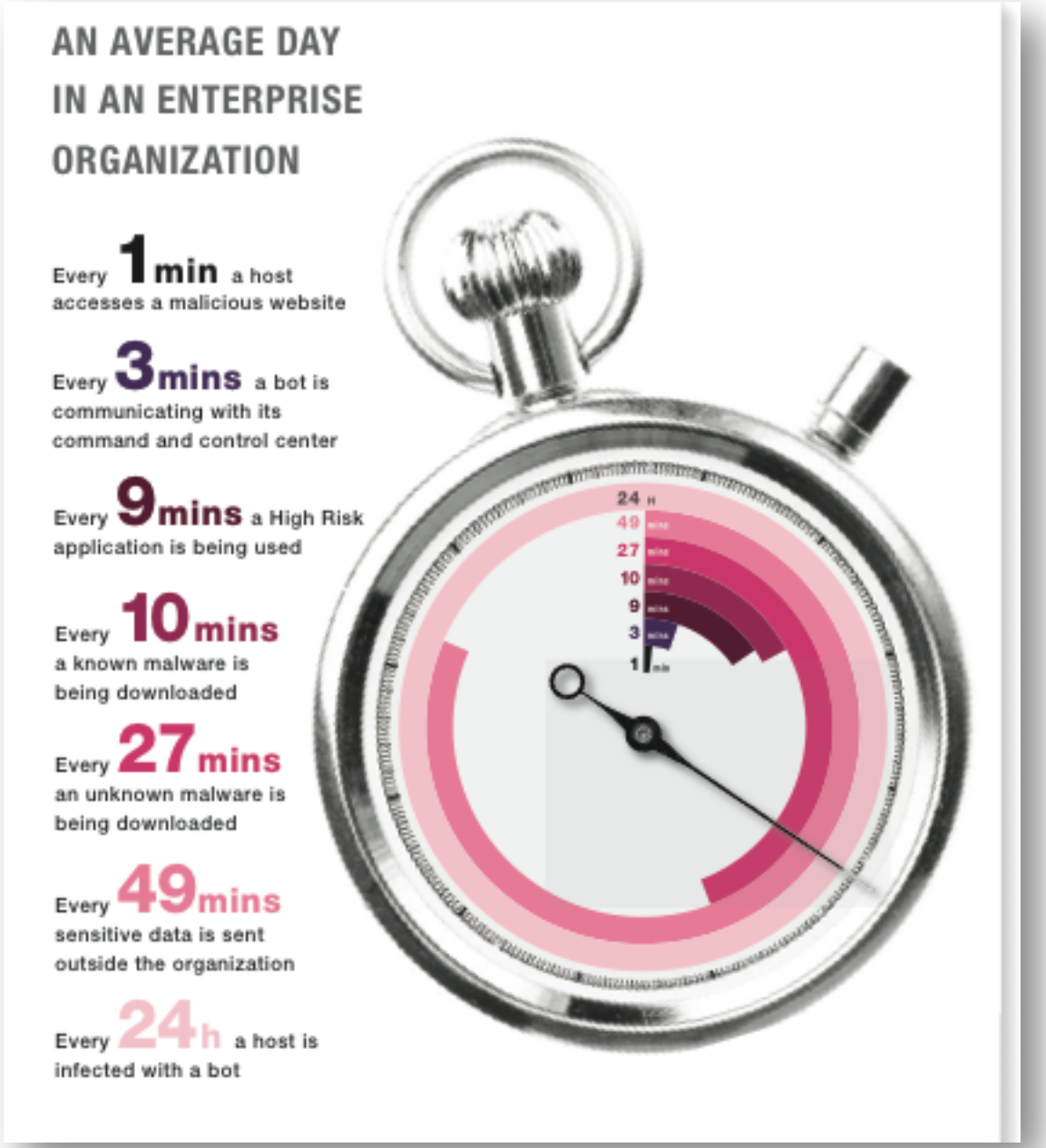
 |

Infoblox

Fast flux – *from Wikipedia*

- *“ The simplest type of fast flux, named "single-flux", is characterized by multiple individual nodes within the network registering and de-registering their addresses as part of the DNS A (address) record list for a single DNS name. This combines round robin DNS with very short TTL (…) values to create a constantly changing list of destination addresses for that single DNS name. “*

- *“A more sophisticated type of fast flux, referred to itself as "double-flux", is characterized by multiple nodes within the network registering and de-registering their addresses as part of the DNS **Name Server record list** for the DNS zone. This provides an additional layer of redundancy and survivability within the malware network.”*



Source: Checkpoint Security Report 2014

- **Almost all malware communications use DNS !!**
- Infoblox DNS Firewall makes it easy to detect this activity

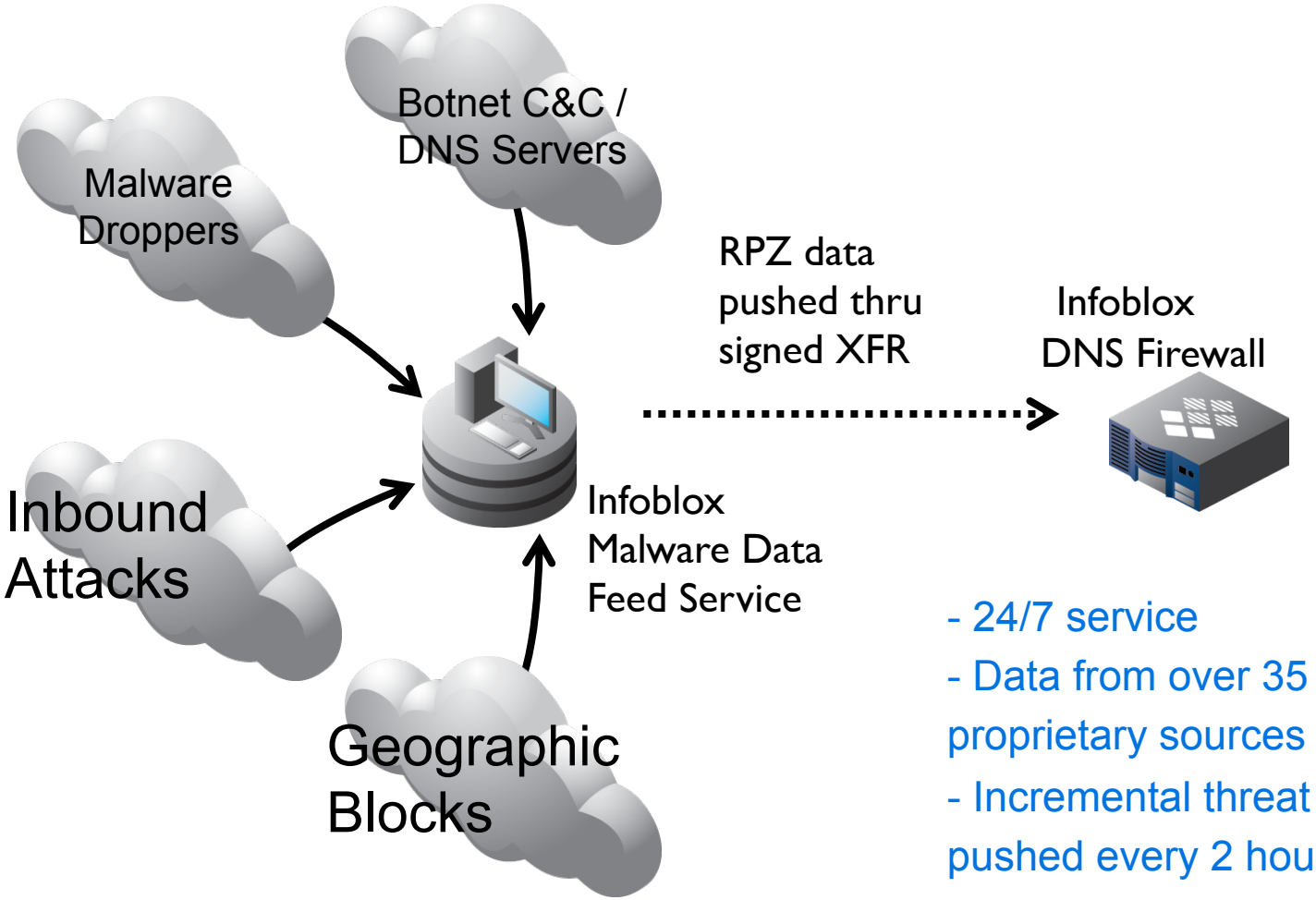
 |

Infoblox

Infoblox DNS Firewall- key concept

- Many organizations on the Internet track malicious activity
  - They know which web sites are malicious
  - They know which domain names malware look up to rendezvous with command-and-control servers
- Infoblox DNS Firewall leverages RPZ (Response Policy Zones)
- Response Policy Zones are funny-looking zones that embed rules instead of records
  - The rules say, “If someone looks up a record for this [malicious] domain name, or that points to this [malicious] IP address, do this.”
  - This is generally “return an error” or “return the address of this walled garden” instead

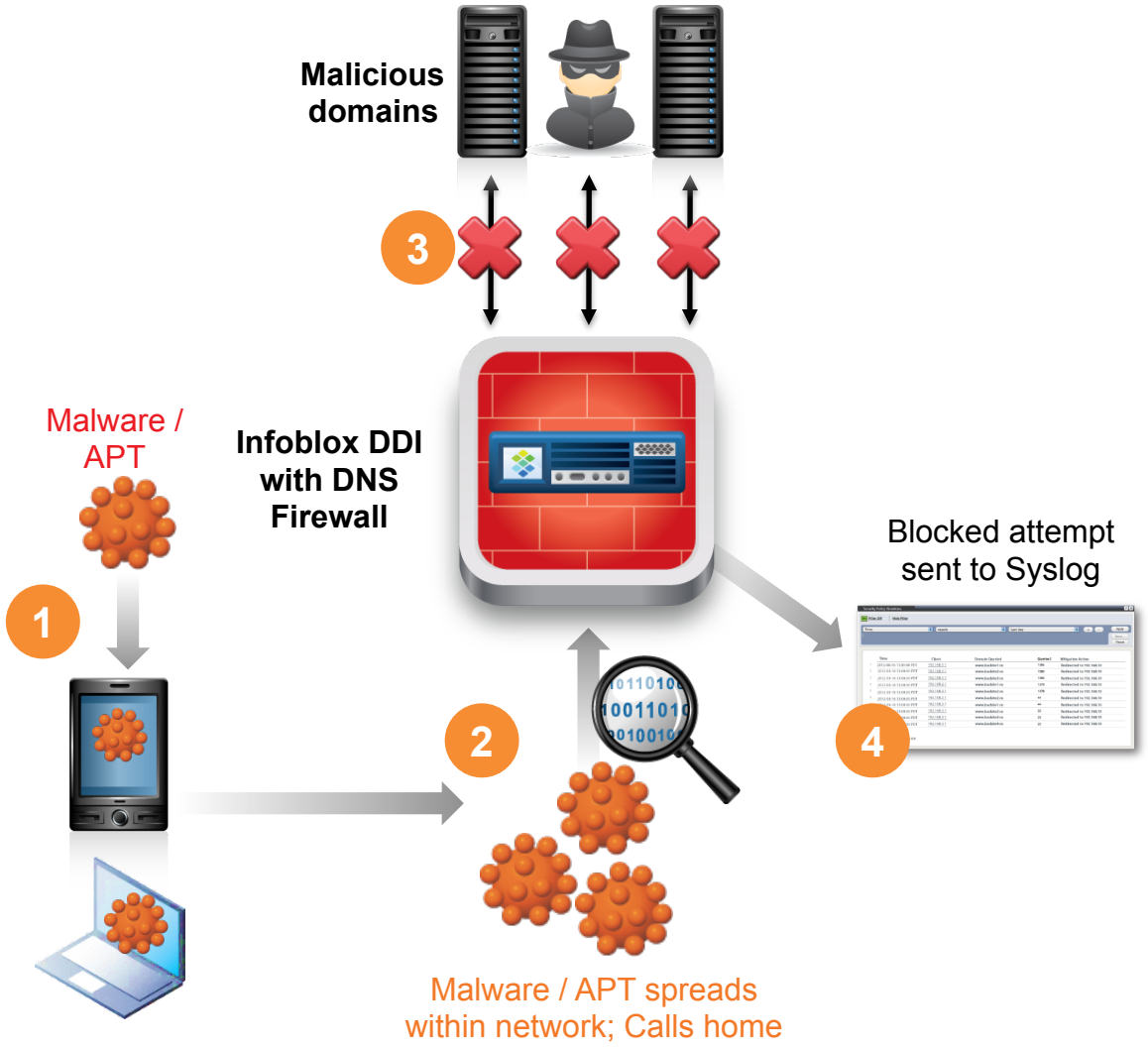
Infoblox Malware Data Feed Service



- 24/7 service
- Data from over 35 different public and proprietary sources – 7 feed types
- Incremental threat data changes are pushed every 2 hours
- Significant threats cause immediate updates (notify)

 |

Infoblox DNS Firewall in action



1. An infected device brought into the office. Malware spreads to other devices on network.

2. Malware makes a DNS query to find “home.” (botnet / C&C)

3. DNS Firewall blocks DNS query (by Domain name / IP Address)

4. Pinpoint any infected device:
   - IP address
   - MAC address
   - Device type (DHCP fingerprint)
   - Host name
   - DHCP lease history

Reputation data comes from:

- DNS Firewall Subscription Svc
- FireEye Adapter (NX Series)

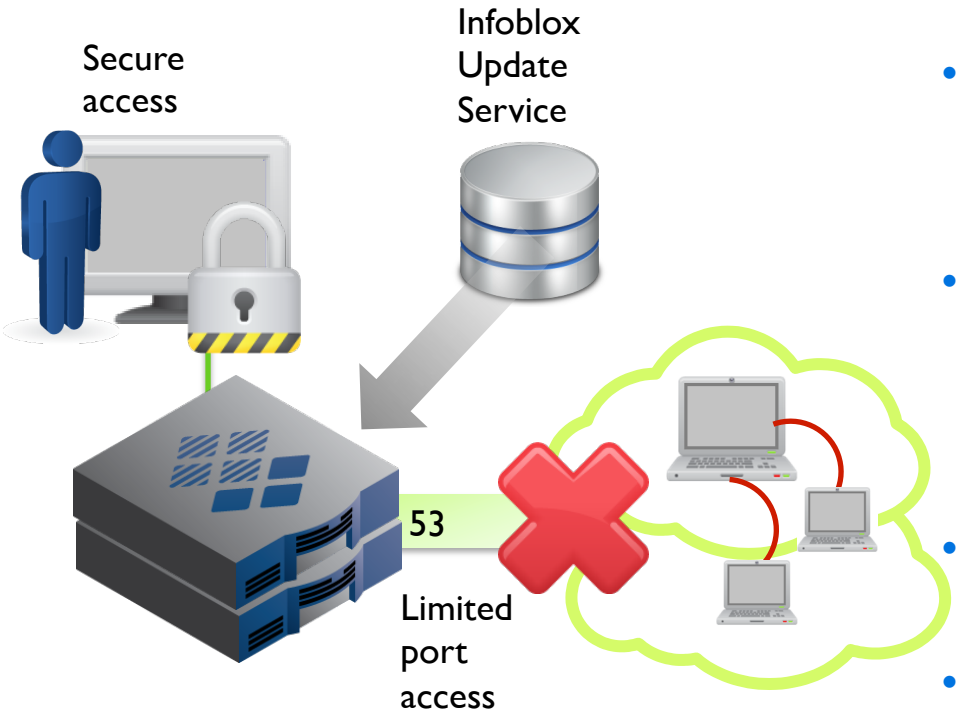
Advanced DNS Protection

Against DDoS and other funky stuff

How can I further secure my DNS servers?

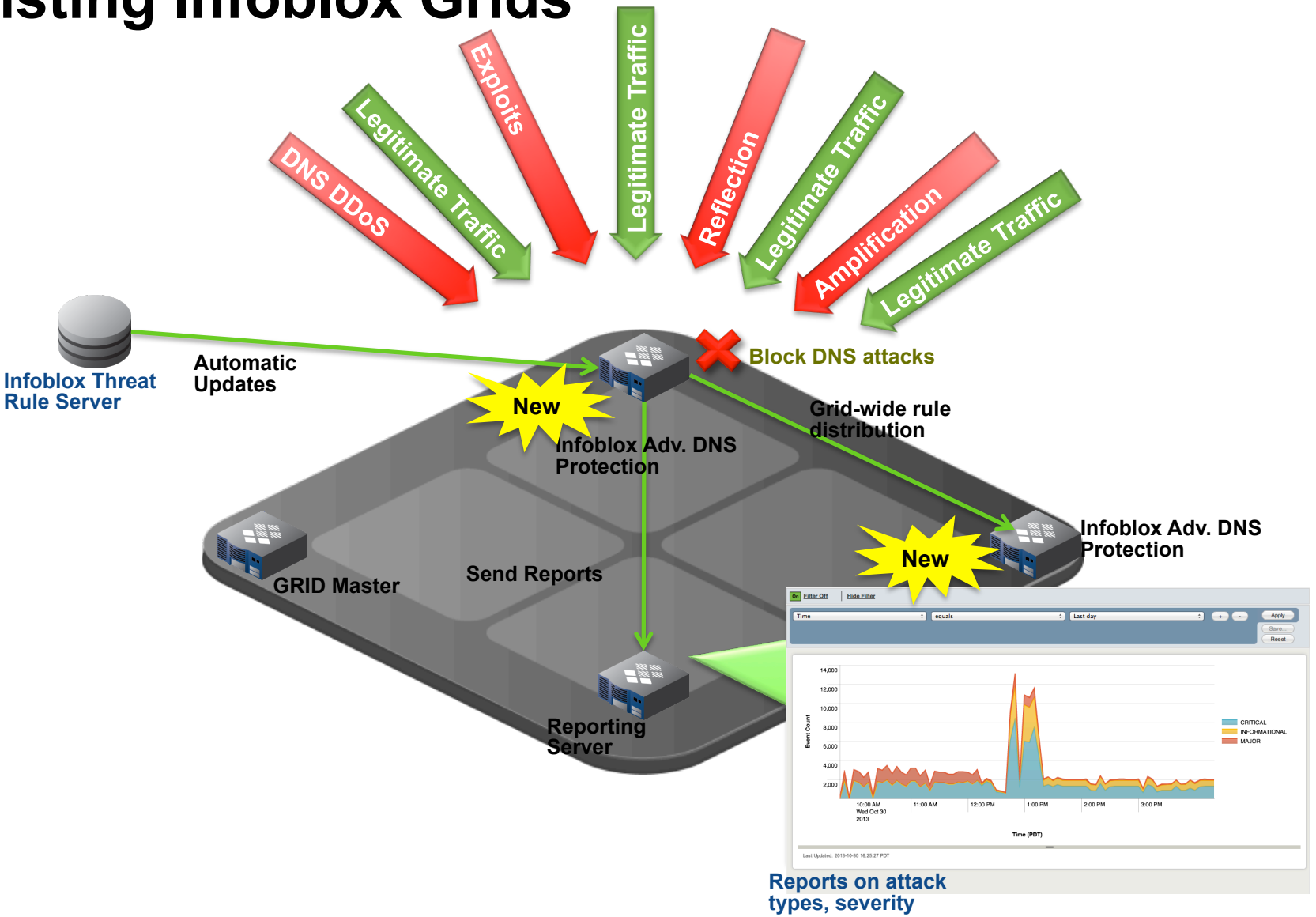
- Dedicated compute capacity to supervise DNS traffic with ability of early detection of attack symptoms
- Behavioral logic to mitigate flood based, DDOS reflection and amplification DNS attacks
- Fine-grain filters to allow/block specific DNS record types (DNS query using “ANY” type does not make sense from an application perspective …)
- Signature based attack detection for known vulnerabilities and exploits

Advanced DNS Protection from Infoblox



- Dedicated network processor card so the name server continues to serve “good” queries under attack
- Intelligently distinguishes legitimate traffic from attack traffic
- Protects the DNS infrastructure against incoming DNS-based attacks and floods
- Automated updates to protect against new threats
- Real-time centralized visibility via the Infoblox GUI and Reporting module

Advanced DNS Protection integrates into existing Infoblox Grids



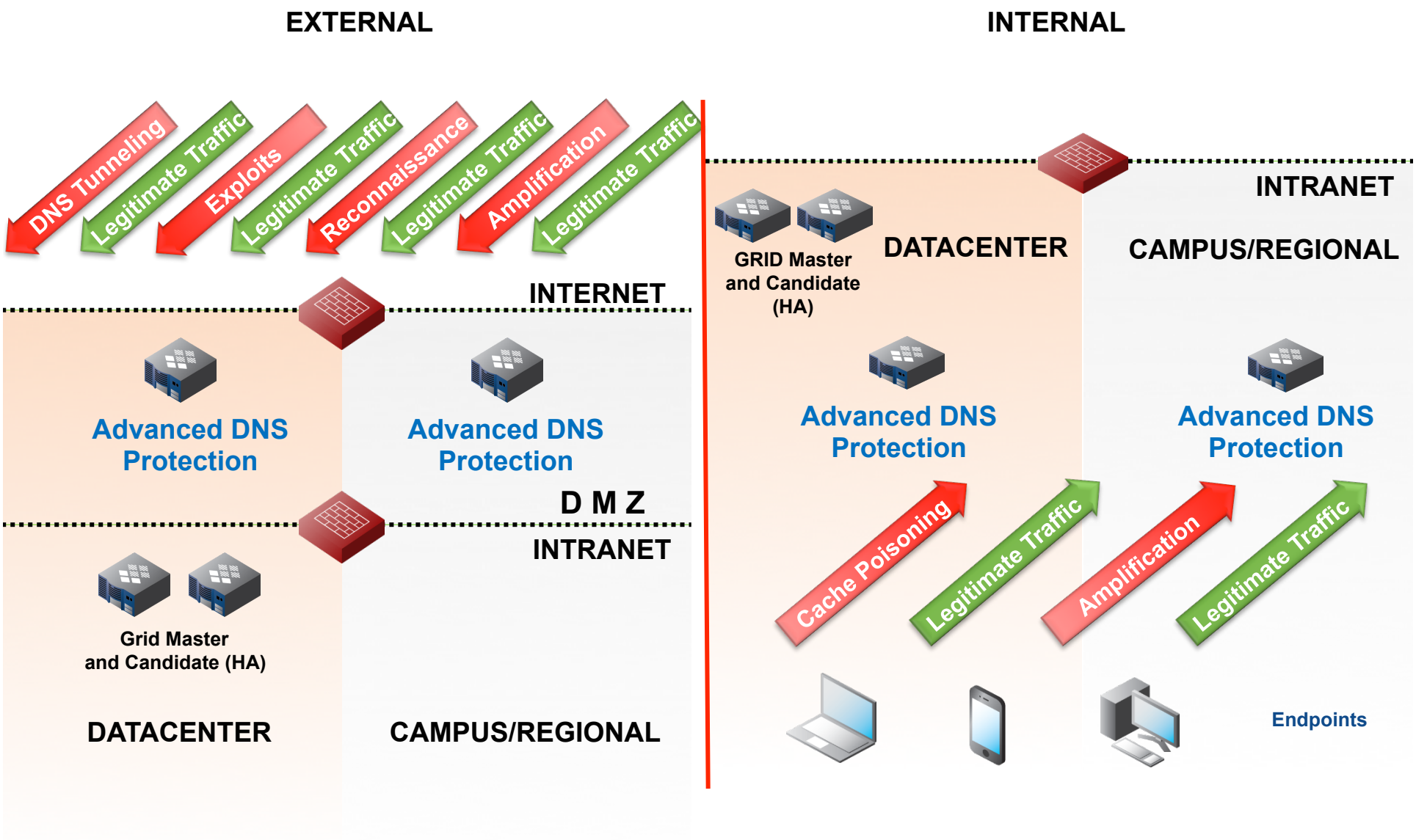
 |

DNS Protection is Not Just About DDoS

DNS reflection/DrDoS attacks	Using third-party DNS servers (mostly open resolvers) to propagate a DoS or DDoS attack
DNS amplification	Using a specially crafted query to create an amplified response to flood the victim with traffic
TCP/UDP/ICMP floods	Denial of service on layer 3 or 4 by bringing a network or service down by flooding it with large amounts of traffic
DNS-based exploits	Attacks that exploit bugs or vulnerabilities in the DNS software
DNS cache poisoning	Corruption of DNS server cache data with a rogue domain or IP
Protocol anomalies	Causing the server to crash by sending malformed DNS packets and queries
Reconnaissance	Attempts by hackers to get information on the network environment before launching a DDoS or other type of attack
DNS tunneling	Tunneling of another protocol through DNS port 53 for malware insertion and/or data exfiltration
DNS hijacking	Modifying the DNS record settings to point to a rogue DNS server or domain
NXDomain attack	Attacks that flood DNS server with requests for non-existent domains, causing it to send NXDomain (non-existent domain) responses
Phantom domain attack	Attacks where a DNS resolver is forced to resolve multiple non-existent domains, causing it to consume resources while waiting for responses

DNS-specific Exploits Volumetric/DDoS Attacks

Deployment Options



 |

Take aways

- New trends & applications are impacting the DNS service
- Emerging IT requirements can drive some DNS redesign on the internal side
- DNS monitoring and alerting is a must have
- Some advanced mechanisms can help protect the DNS infrastructure and its usage

… We can help ☺ – don't hesitate to contact us !

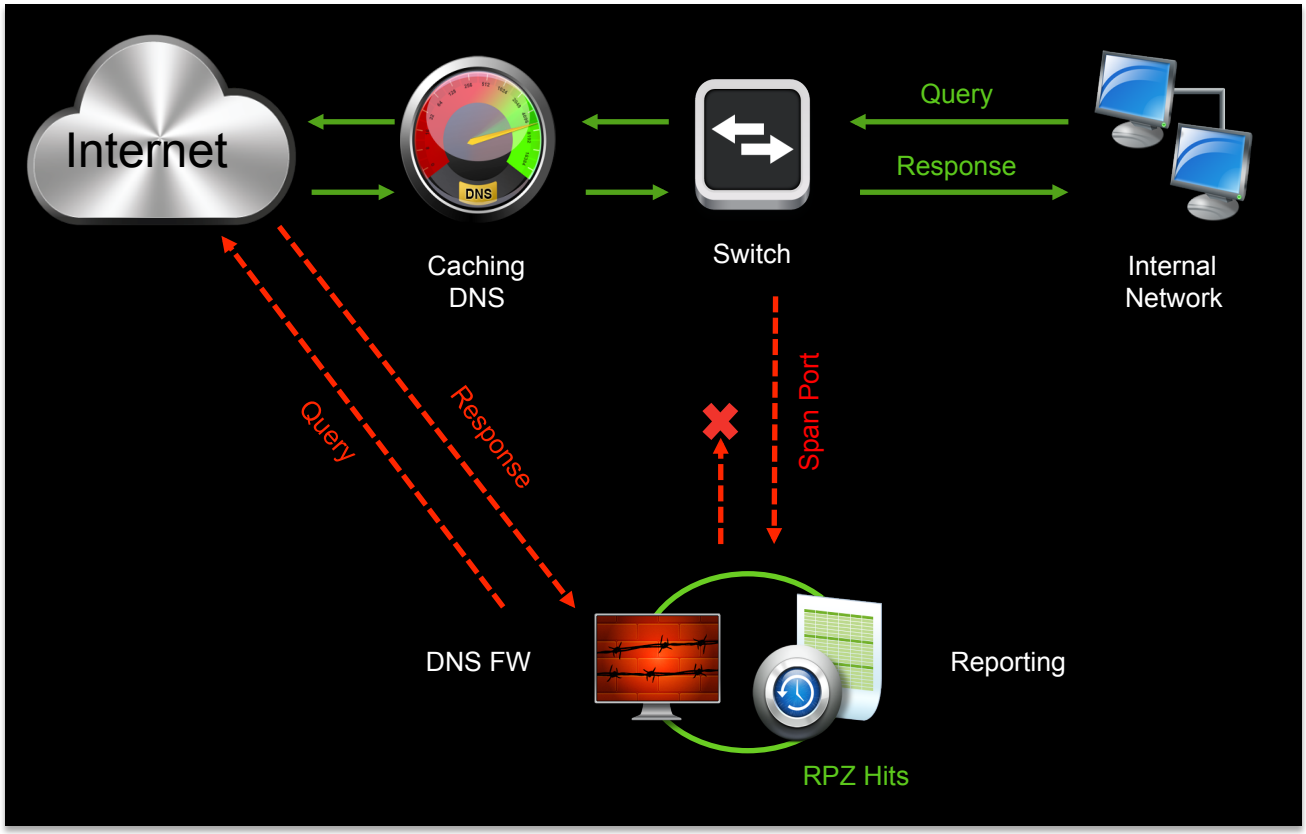
Questions ?

Muchas gracias por su atención!

Evaluate DNS Firewall now !

New!

Use DNS to Find Malware/APT Hiding in Your Network



- Shows malware activity
- No hardware (100% virtual)
- Non-disruptive to production network
- Fully automated with simple install
- 60-day trial

www.infoblox.com/catchmalware

 |

Infoblox