
BLOX FEST
Infoblox

Robert Nagy

CEO – DeepDive Networking

BLOX FEST

Topics Covered

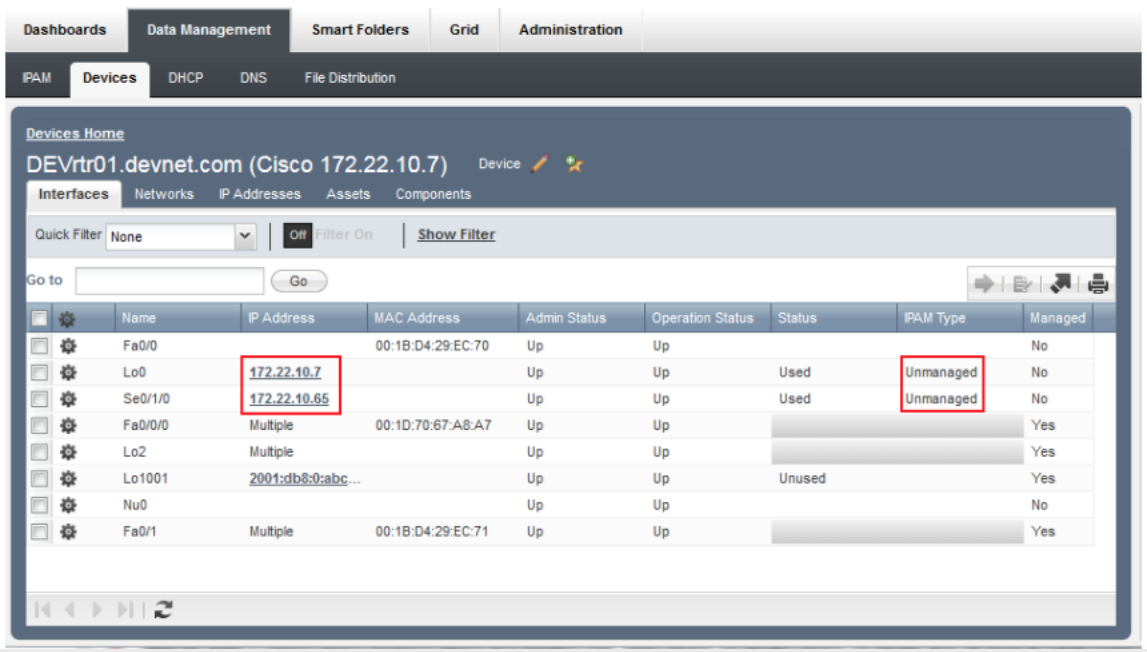
- Network Insight
- DNS Firewall (RPZ)
- Advanced DNS Protection (ADP)

Network Insight

Network Insight

Overview

- Enhance IPAM with Network Data for attached hosts
- Give single-pane visibility
- Give tools to take action

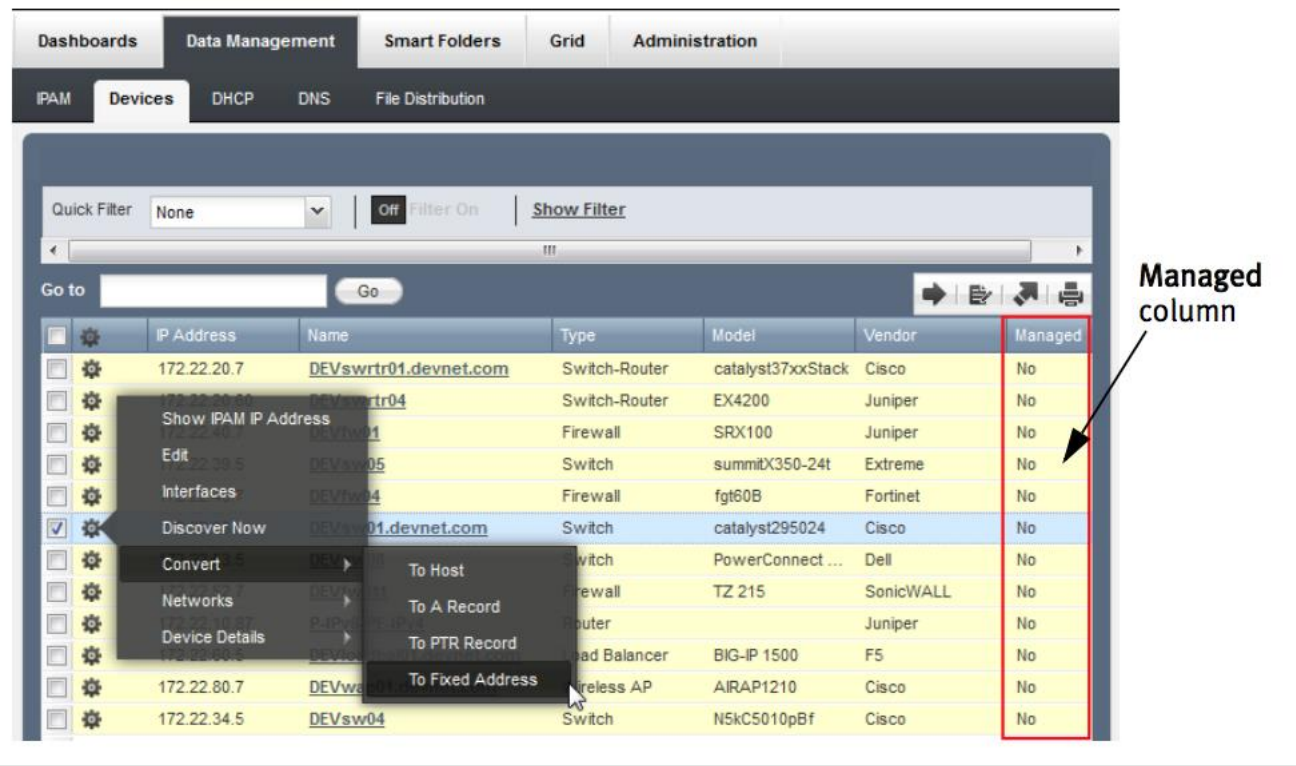


Network Insight

What do we get

Network Insight

Using Network insight Data as IPAM



Network Insight

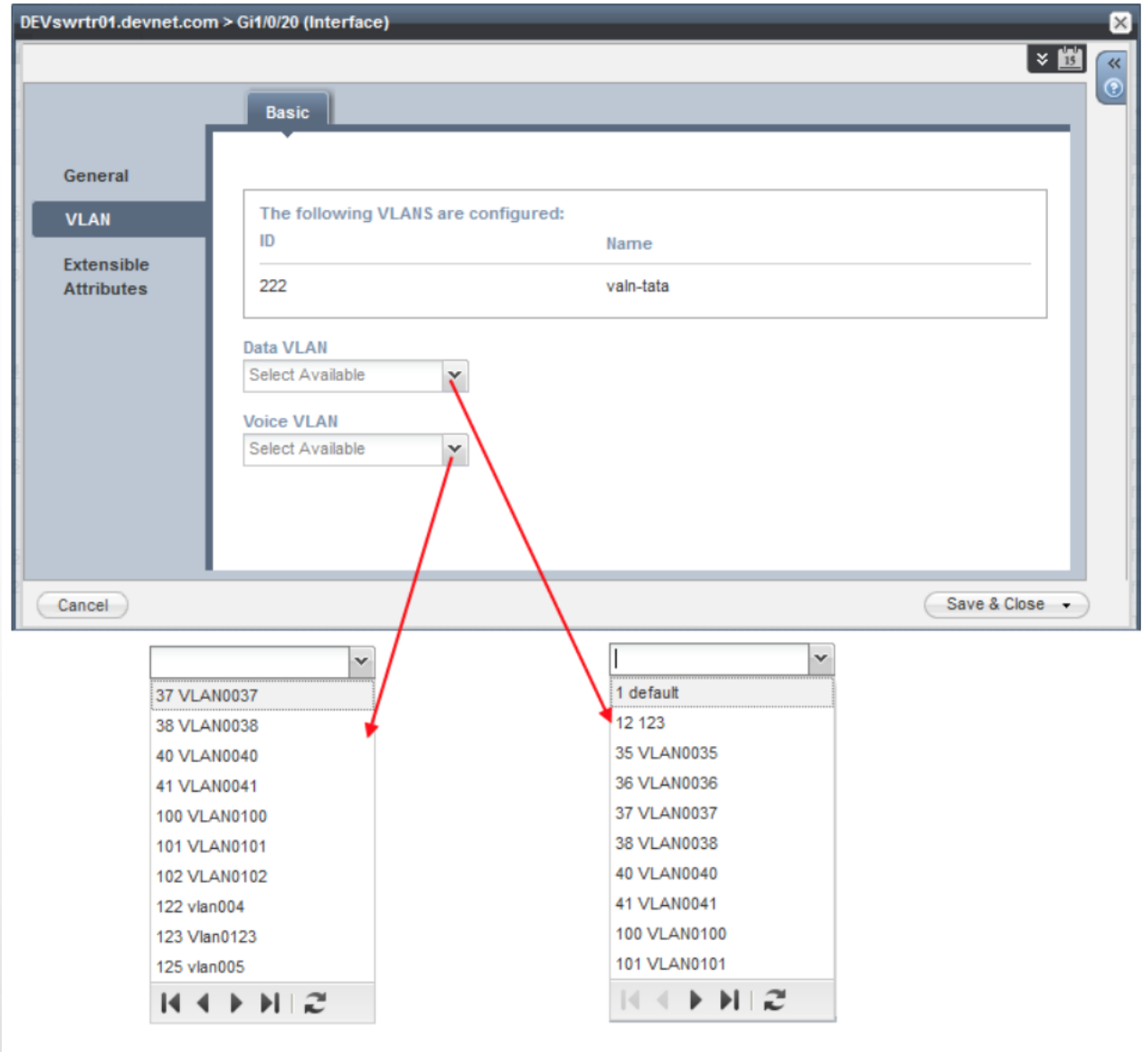
Taking Action

- What can we do with this information?
- If we find a bad host and know where it is patched in, let take action instead of logging into another device.
- Two tasks we most would need are;
  - Change VLAN – ie. Move to quarantine VLAN
  - Shut Port

Network Insight

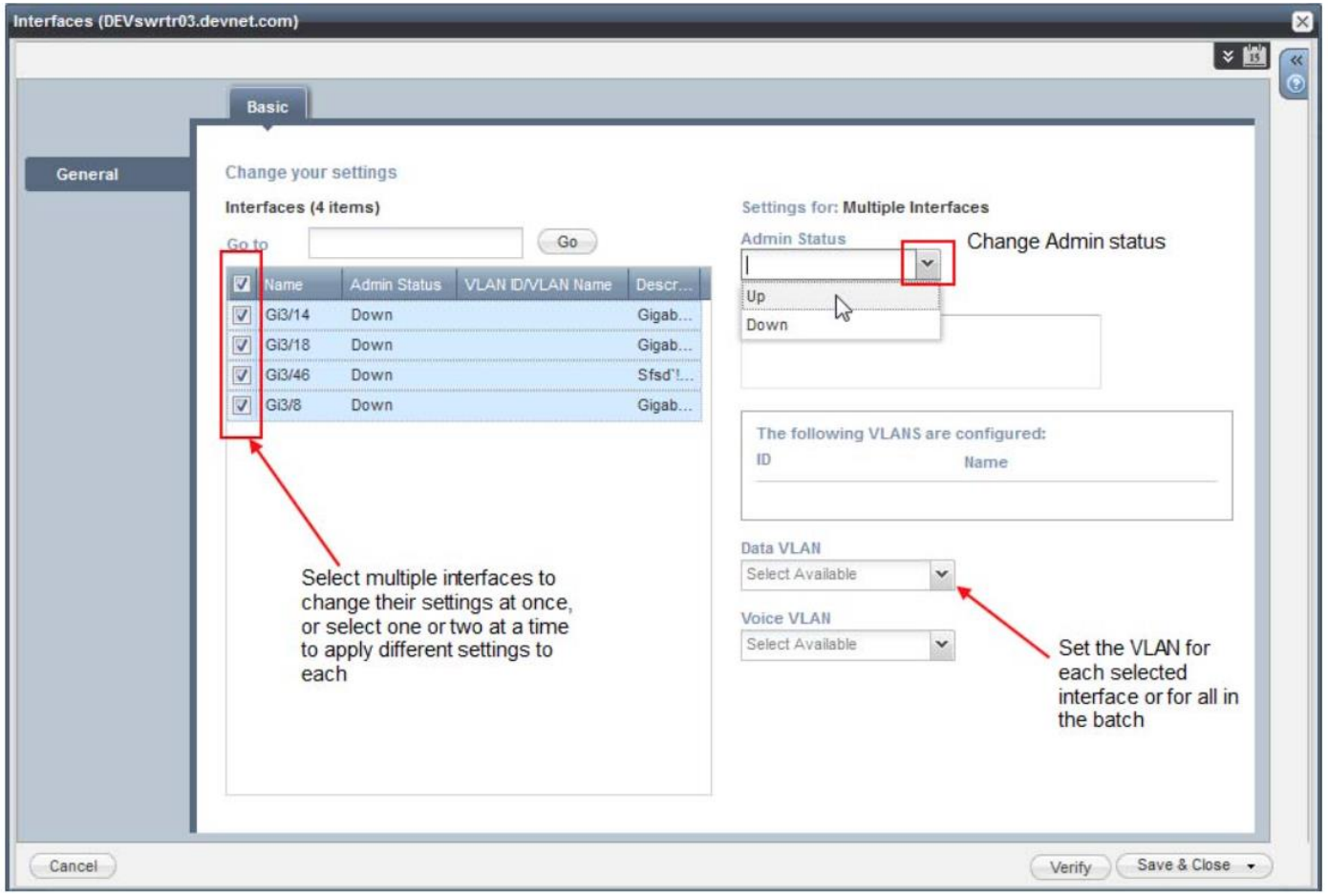
Taking Action

- Changing the VLAN



Network Insight

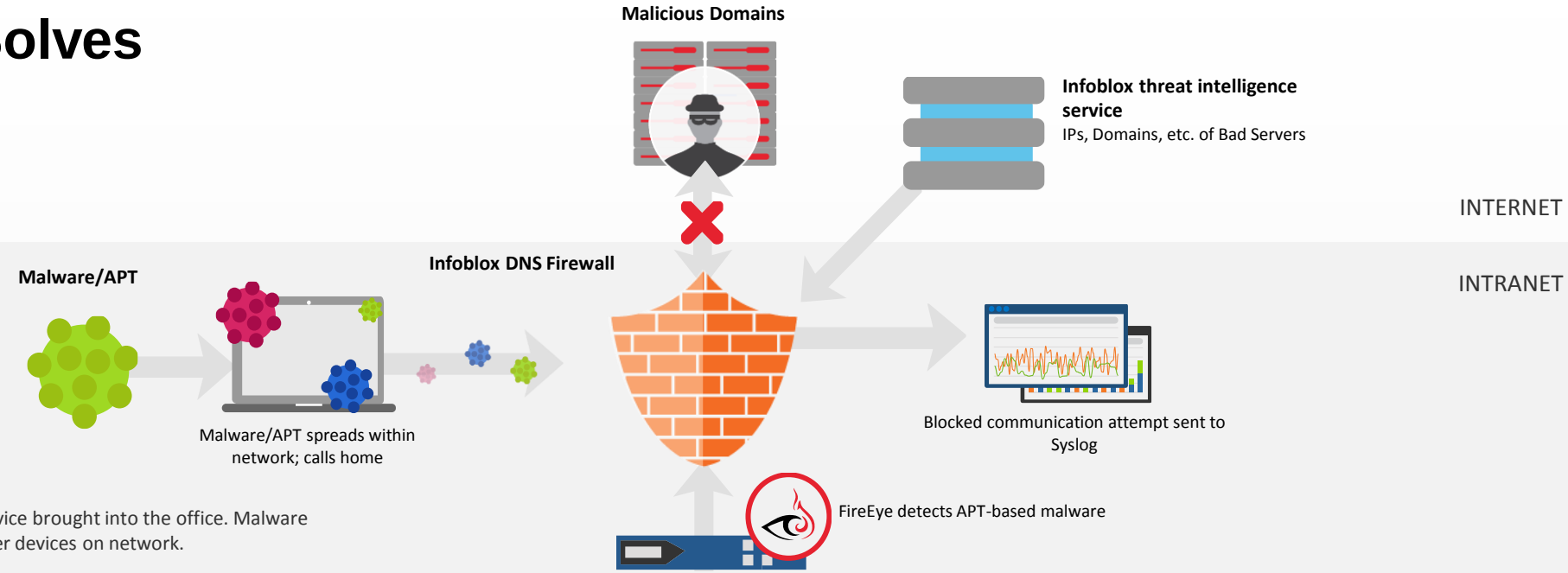
Taking Action – Manage Port



DNS Firewall

DNS Firewall - Response Policy Zones

What it Solves



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). DNS Firewall looks at the DNS response and takes admin-defined action (disallows communication to malware site or redirects traffic to a landing page or "walled garden" site).

3 **Pinpoint.** Infoblox Reporting lists DNS Firewall action as well as the:

- User name
- Device IP address
- Device MAC address
- Device type (DHCP fingerprint)
- Device host name
- Device lease history

4 An update will occur every 2 hours (or more often for significant threat).

5 Additional threat intelligence from sources outside Infoblox can also be used by DNS Firewall (e.g. FireEye)

DNS Firewall - Response Policy Zones

Overview

- DNS Firewall is built using Response Policy Zone (RPZ)
- RPZ is implemented in ISC BIND 9.8 and later
- DNS Firewall is one of several DNS security options available for Infoblox DNS appliances

Response Policy Zones

How it works

- Zone Transfer
- TSIG
- Triggers
- Logging
- Reputation Information

Response Policy Zones

How it works – Leverages Zones

- Both Local RPZ and RPZ Feeds are stored as DNS Zones
- To authenticate the source we use TSIG
- Standard Zone transfer is used, both AXFR and IXFR
- Requires Port 53 access

Response Policy Zones

Local versus Feed

- Local – whitelist, blacklist specific to your organization
- Feed – Someone else does the hard work

Response Policy Zones

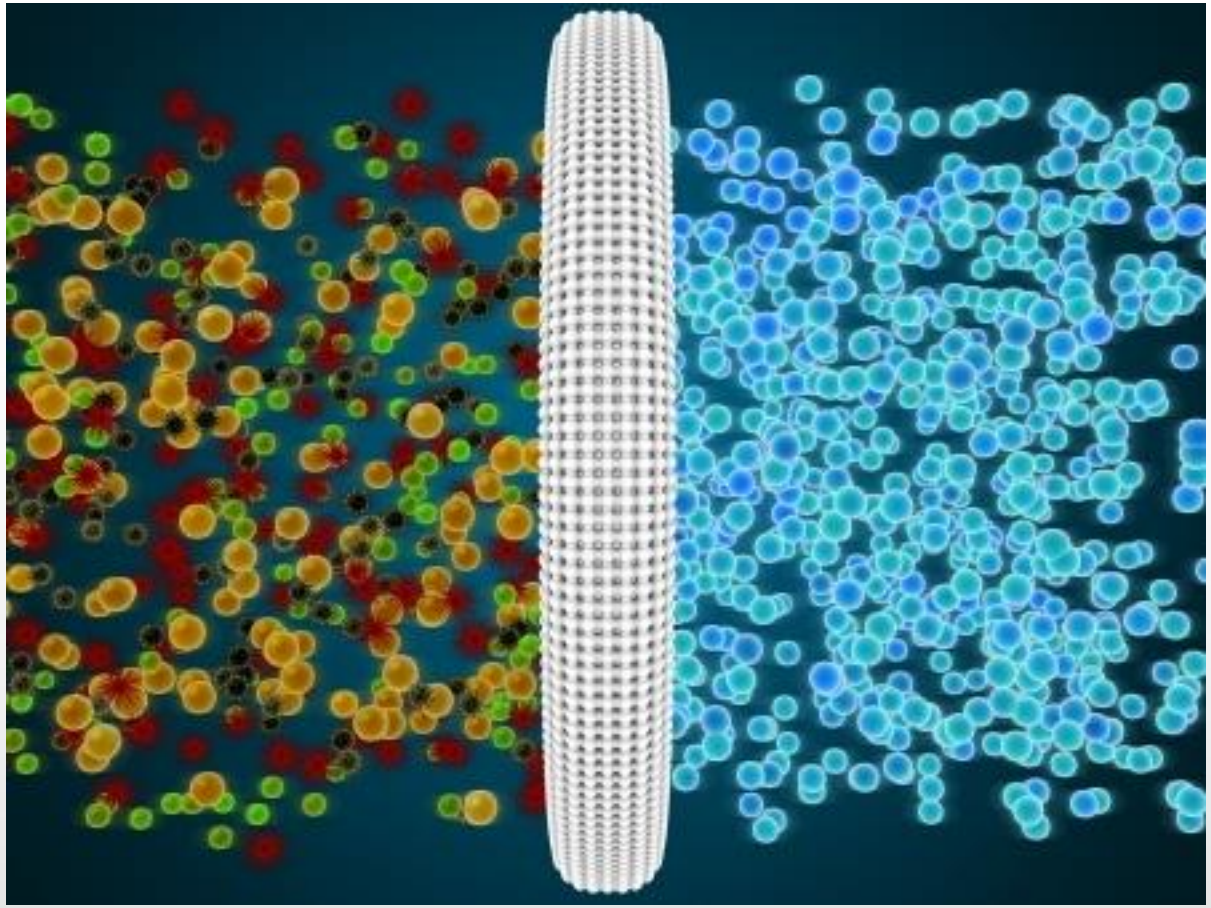
Triggers

- Triggers – when we see a match execute a policy
  - QNAME
  - IP
  - Client-IP
  - NSDNAME
  - NSIP

Response Policy Zones

Policies

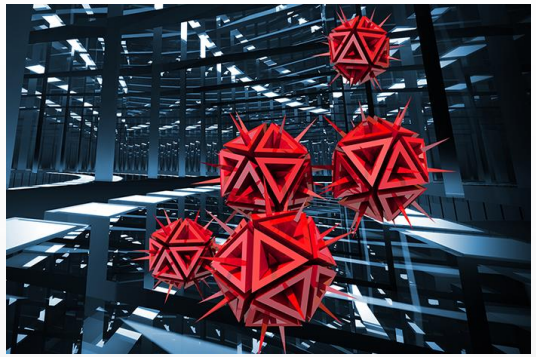
- Block – Two different ways
  - NXDOMAIN
  - NODATA
- Substitute
  - Use to redirect to a save haven
  - Substitute parts of the reply – depends on record type
- PassThru
  - Used to LOG queries when triggered



Insert Transition Slide – ADP

Advanced DNS Protection (ADP)

The Problem



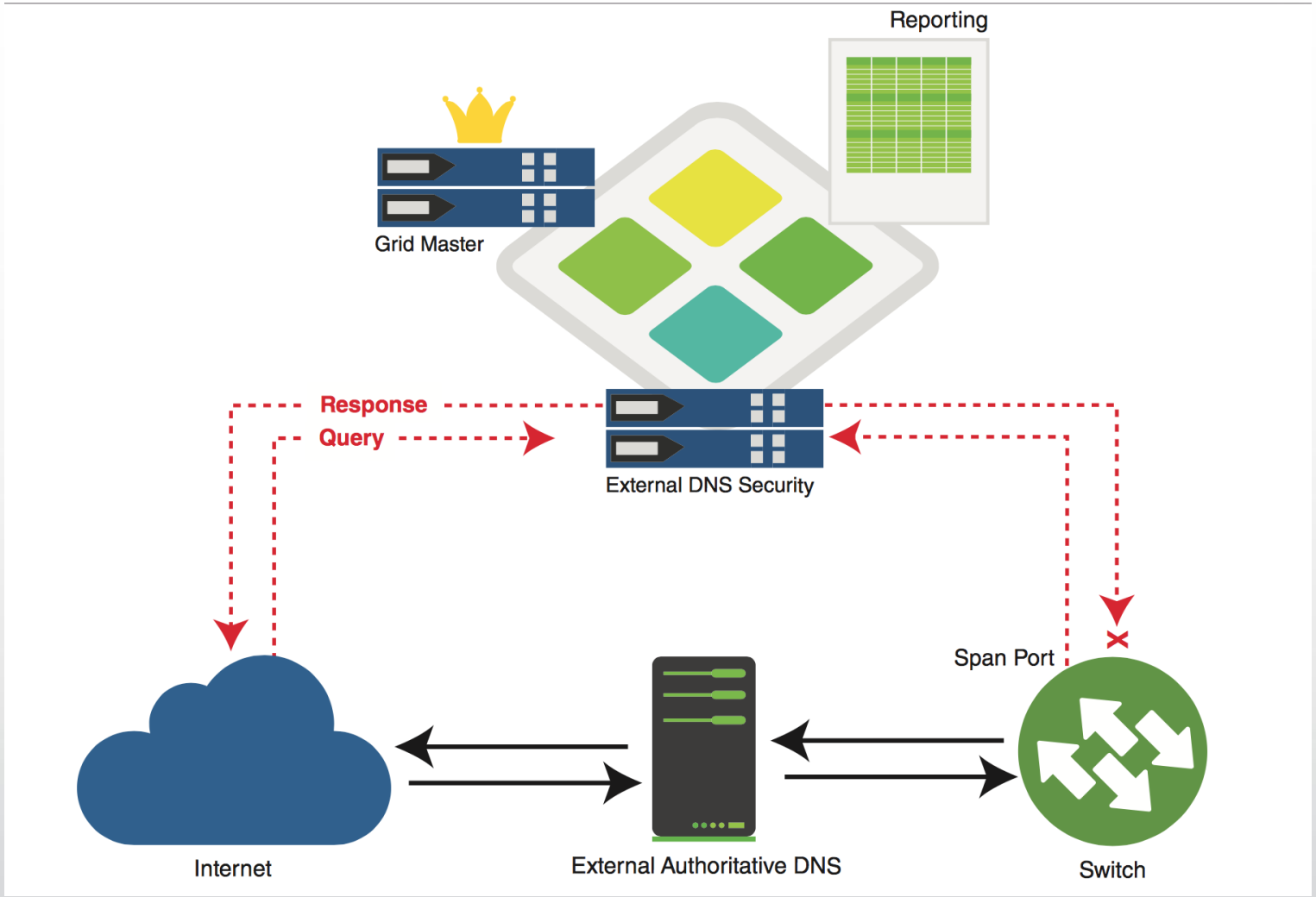
DNS-based attacks are on the rise

Traditional protection is ineffective against evolving threats

DNS cannot stop even under attack to avoid network downtime, loss of revenue, and negative brand impact

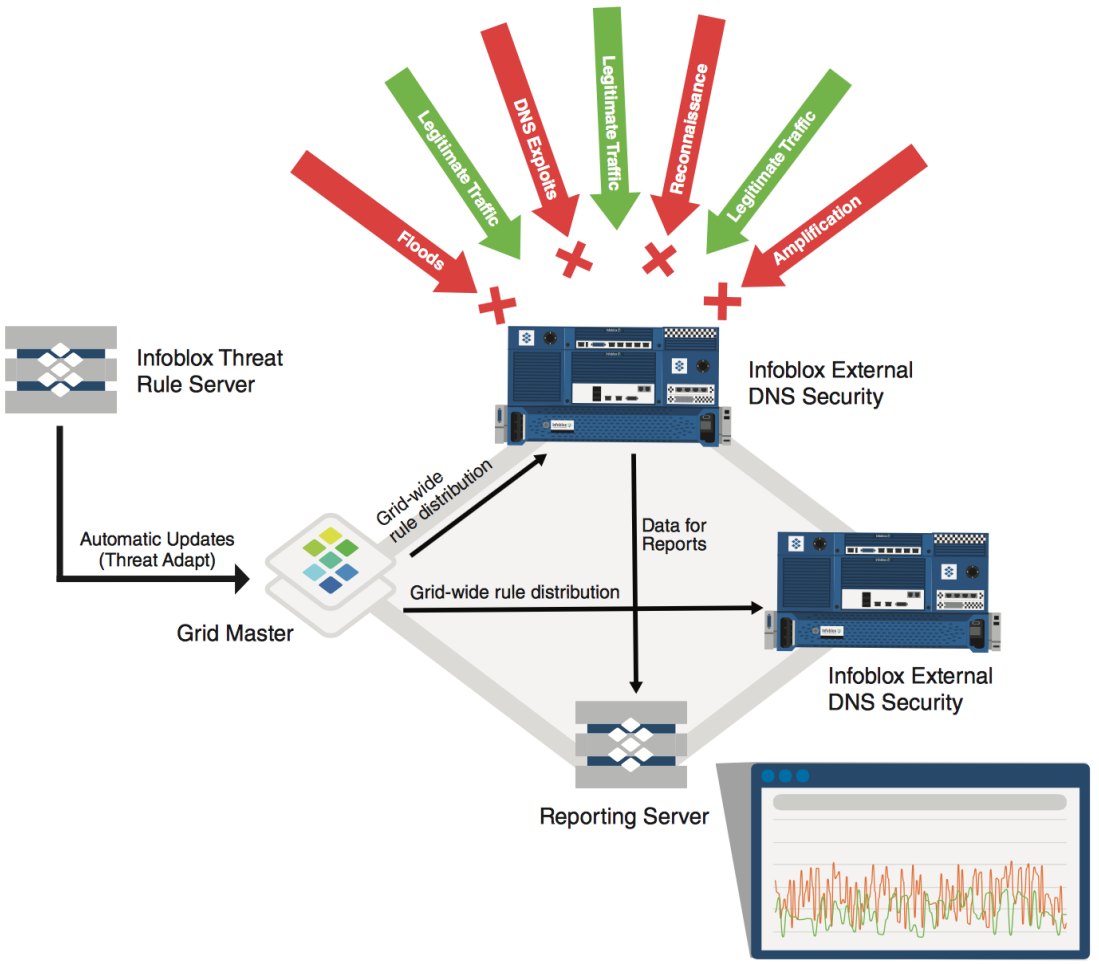
Advanced DNS Protection (ADP)

ADP Overview



Advanced DNS Protection (ADP)

The Threats



Advanced DNS Protection (ADP)

Threats ADP addresses

DNS Reflection/DrDoS attacks	Using third-party DNS servers(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
Protocol Anomalies	Causing the server to crash by sending malformed packets and queries
TCP/UDP/ICMP Floods	Denial of service on layer 3 by bringing a network or service down by flooding it with large amounts of traffic
DNS Cache Poisoning	Corruption of the DNS cache data with a rogue address
DNS-based exploits	Attacks that exploit vulnerabilities in the DNS software
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 for data exfiltration

Advanced DNS Protection (ADP)

The Rules

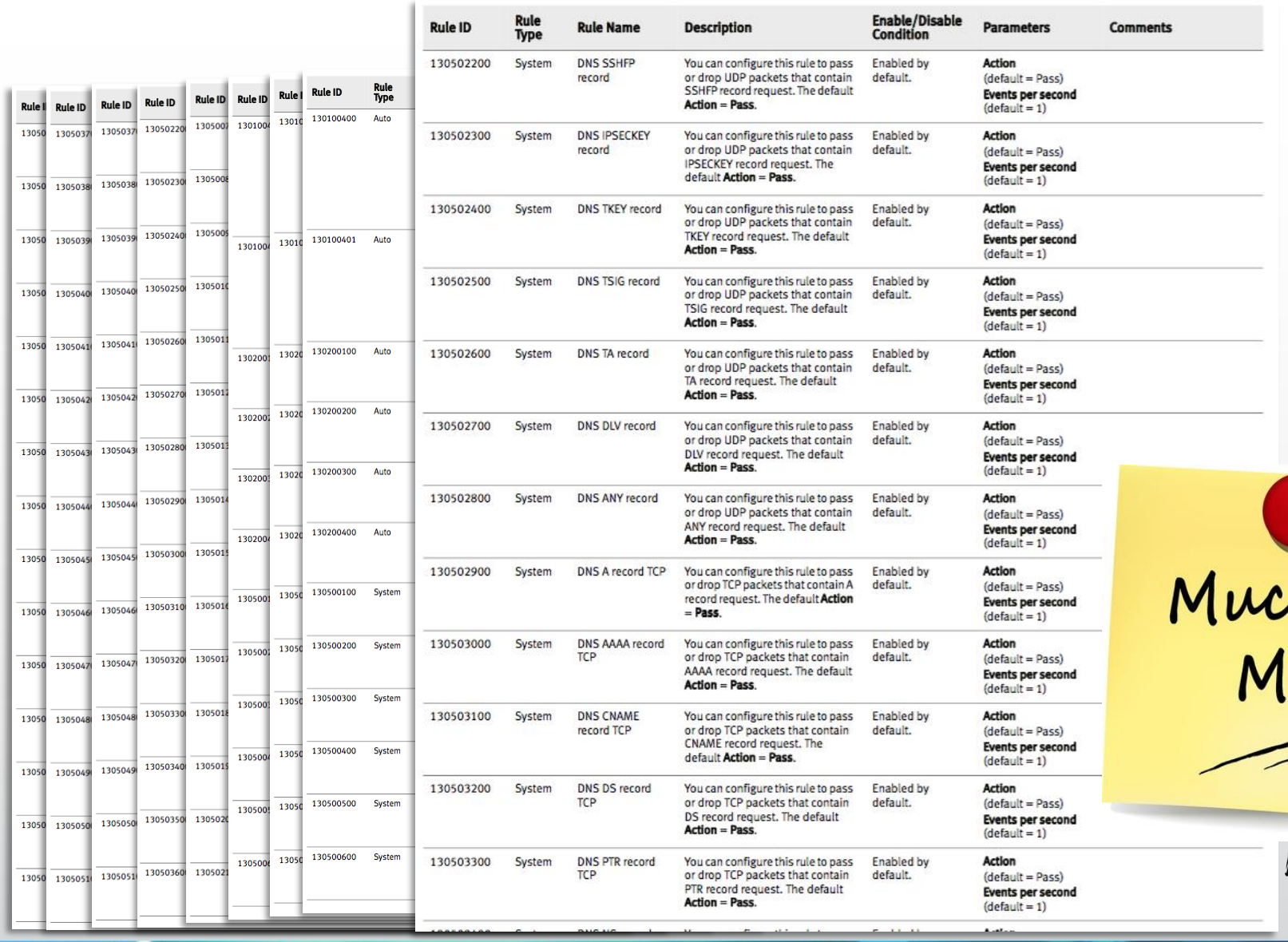
Advanced DNS Protection (ADP)

The Rules

You got a threat

We got a rule!

Lots of Rules



Rule ID	Rule Type	Rule Name	Description	Enable/Disable Condition	Parameters	Comments
130502200	System	DNS SSHFP record	You can configure this rule to pass or drop UDP packets that contain SSHFP record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502300	System	DNS IPSECKEY record	You can configure this rule to pass or drop UDP packets that contain IPSECKEY record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502400	System	DNS TKEY record	You can configure this rule to pass or drop UDP packets that contain TKEY record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502500	System	DNS TSIG record	You can configure this rule to pass or drop UDP packets that contain TSIG record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502600	System	DNS TA record	You can configure this rule to pass or drop UDP packets that contain TA record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502700	System	DNS DLV record	You can configure this rule to pass or drop UDP packets that contain DLV record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502800	System	DNS ANY record	You can configure this rule to pass or drop UDP packets that contain ANY record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130502900	System	DNS A record TCP	You can configure this rule to pass or drop TCP packets that contain A record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130503000	System	DNS AAAA record TCP	You can configure this rule to pass or drop TCP packets that contain AAAA record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130503100	System	DNS CNAME record TCP	You can configure this rule to pass or drop TCP packets that contain CNAME record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130503200	System	DNS DS record TCP	You can configure this rule to pass or drop TCP packets that contain DS record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	
130503300	System	DNS PTR record TCP	You can configure this rule to pass or drop TCP packets that contain PTR record request. The default **Action = Pass**.	Enabled by default.	**Action** (default = Pass) **Events per second** (default = 1)	

BLOX FEST

Advanced DNS Protection (ADP)

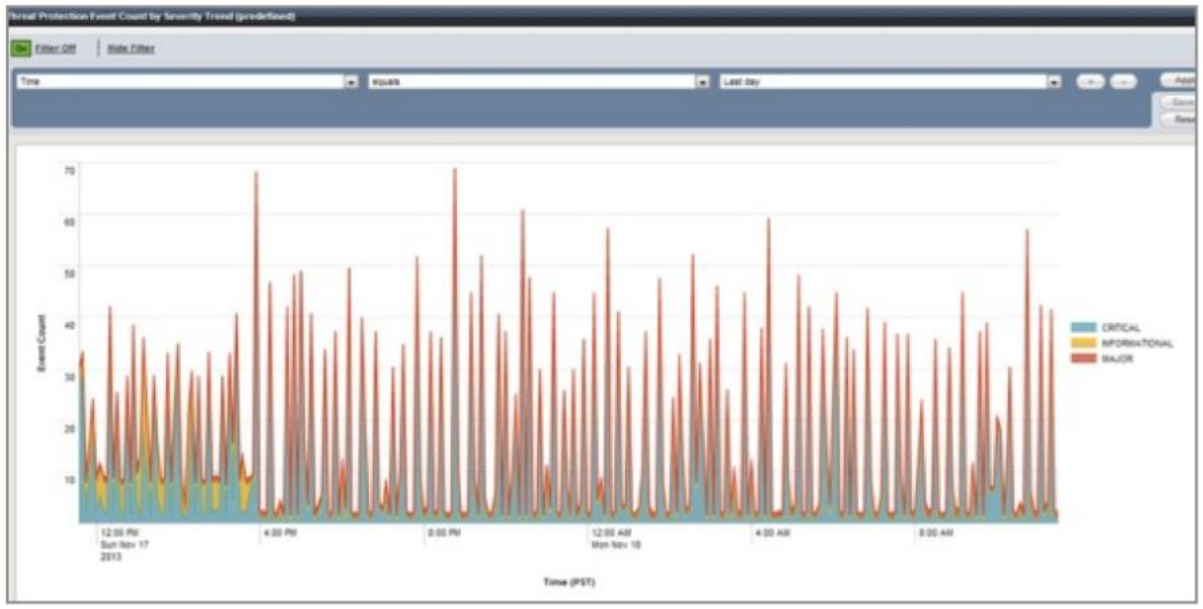
The Rules

Not Enough?

- Create up to 500 Custom Rules

Advanced DNS Protection (ADP)

Reporting



Threat Protection Event Count by Severity Trend Report

Threat Protection Statistics Widget

Questions?