

BLOX FEST

Infoblox 

Robert Nagy

CEO – DeepDive Networking



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

Devices Home
DEVrtr01.devnet.com (Cisco 172.22.10.7) Device

Interfaces Networks IP Addresses Assets Components

Quick Filter: None | Filter On | Show Filter

Go to: [] Go

	Name	IP Address	MAC Address	Admin Status	Operation Status	Status	IPAM Type	Managed
	Fa0/0		00:1B:D4:29:EC:70	Up	Up			No
	Lo0	172.22.10.7		Up	Up	Used	Unmanaged	No
	Se0/1/0	172.22.10.65		Up	Up	Used	Unmanaged	No
	Fa0/0/0	Multiple	00:1D:70:67:A8:A7	Up	Up			Yes
	Lo2	Multiple		Up	Up			Yes
	Lo1001	2001:db8:0:abc...		Up	Up	Unused		Yes
	Nu0			Up	Up			No
	Fa0/1	Multiple	00:1B:D4:29:EC:71	Up	Up			Yes

Network Insight

What do we get

Discovered Data	
NetBIOS Name:	OS: 6.10.2
Discovered MAC Address: 00:50:56:9e:4c:1c	Last Discovered: 2014-04-11 08:07:44 PDT
Device Type(s): vllb0s	Open port(s): TCP:53,443 UDP:67
Attached Device Address: 10.60.30.210	Discovered Name: infoblox.localdomain
First Discovered: 2014-03-13 16:54:00 PDT	Discoverer: ndp3.infoblox.com
Attached Device Description: Juniper Networks, Inc. ex4200-48t internet router, kernel JUNOS 10.2R1.8 #0: 2010-05-27 21:05:57 UTC builder@shoth.juniper.net:/volume/build/junos/10.2/release/10.2R1.8/obj-powerpcbsd/sys/compile/JUNIPER-EX Build date: 2010-05-27 20:46:44 UTC Copyri	Attached Device Model: EX4200
Attached Device Name: junos-rack2	Attached Device Port Description: ge-0/0/30.0
Attached Device Port Name: ge-0/0/30.0	Attached Device Vendor: Juniper
Attached Device Port: 543	Attached Device Type: Switch-Router
Device Vendor: Infoblox	Device Model: IB-VM-2220
Device Management IP: 10.60.30.10	Device Port Type: ethernet-csmacd
Device Port Name: eth1	Port Duplex: Full
Port Link: Not Connected	Port Speed: Unknown



Network Insight

Using Network insight Data as IPAM

The screenshot shows the Network Insight IPAM interface. The top navigation bar includes 'Dashboards', 'Data Management', 'Smart Folders', 'Grid', and 'Administration'. Below this, there are sub-tabs for 'IPAM', 'Devices', 'DHCP', 'DNS', and 'File Distribution'. The main area displays a table of devices with columns for IP Address, Name, Type, Model, Vendor, and Managed. A context menu is open over the row for 'DEVsw01.devnet.com', showing options like 'Show IPAM IP Address', 'Edit', 'Interfaces', 'Discover Now', 'Convert', 'Networks', and 'Device Details'. A red box highlights the 'Managed' column, and an arrow points to it with the text 'Managed column'.

IP Address	Name	Type	Model	Vendor	Managed
172.22.20.7	DEVswrtr01.devnet.com	Switch-Router	catalyst37xxStack	Cisco	No
172.22.20.7	DEVswrtr04	Switch-Router	EX4200	Juniper	No
172.22.20.5	DEVsw01	Firewall	SRX100	Juniper	No
172.22.20.5	DEVsw05	Switch	summitX350-24t	Extreme	No
172.22.20.4	DEVsw04	Firewall	fgt60B	Fortinet	No
172.22.20.1	DEVsw01.devnet.com	Switch	catalyst295024	Cisco	No
172.22.20.1	DEVsw01	Switch	PowerConnect ...	Dell	No
172.22.20.1	DEVsw01	Firewall	TZ 215	SonicWALL	No
172.22.20.1	DEVsw01	Router		Juniper	No
172.22.20.1	DEVsw01	Load Balancer	BIG-IP 1500	F5	No
172.22.80.7	DEVsw01	Wireless AP	AIRAP1210	Cisco	No
172.22.34.5	DEVsw04	Switch	N5kC5010pBf	Cisco	No

The screenshot shows the 'Smart Folders' window in Network Insight. It displays a hierarchical list of discovered devices. The 'Discovered Switches/Routers' folder is expanded, showing a list of device names and IP addresses. The list includes: DEVrtr01.devnet.com, DEVrtr02.devnet.com, DEVsw01.devnet.com, DEVsw02.devnet.com, DEVsw04, DEVsw05, DEVsw06, DEVsw08, DEVswrtr01.devnet.com, DEVswrtr02.devnet.com, DEVswrtr03.devnet.com, DEVswrtr04, DEVswrtr05, P-IPv6-PE-IPv4, and unknown.



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

DEVswrtr01.devnet.com > Gi1/0/20 (Interface)

Basic

The following VLANs are configured:

ID	Name
222	valn-tata

Data VLAN
Select Available

Voice VLAN
Select Available

Cancel Save & Close

37 VLAN0037
38 VLAN0038
40 VLAN0040
41 VLAN0041
100 VLAN0100
101 VLAN0101
102 VLAN0102
122 vlan004
123 Vlan0123
125 vlan005

1 default
12 123
35 VLAN0035
36 VLAN0036
37 VLAN0037
38 VLAN0038
40 VLAN0040
41 VLAN0041
100 VLAN0100
101 VLAN0101

Network Insight

Taking Action – Manage Port

Interfaces (DEVswrtr03.devnet.com)

Basic

General

Change your settings

Interfaces (4 items)

Go to Go

<input checked="" type="checkbox"/>	Name	Admin Status	VLAN ID/VLAN Name	Descr...
<input checked="" type="checkbox"/>	G/3/14	Down		Gigab...
<input checked="" type="checkbox"/>	G/3/18	Down		Gigab...
<input checked="" type="checkbox"/>	G/3/46	Down		Sfsd'l...
<input checked="" type="checkbox"/>	G/3/8	Down		Gigab...

Settings for: Multiple Interfaces

Admin Status Change Admin status

Up
Down

The following VLANS are configured:

ID	Name
----	------

Data VLAN
Select Available

Voice VLAN
Select Available

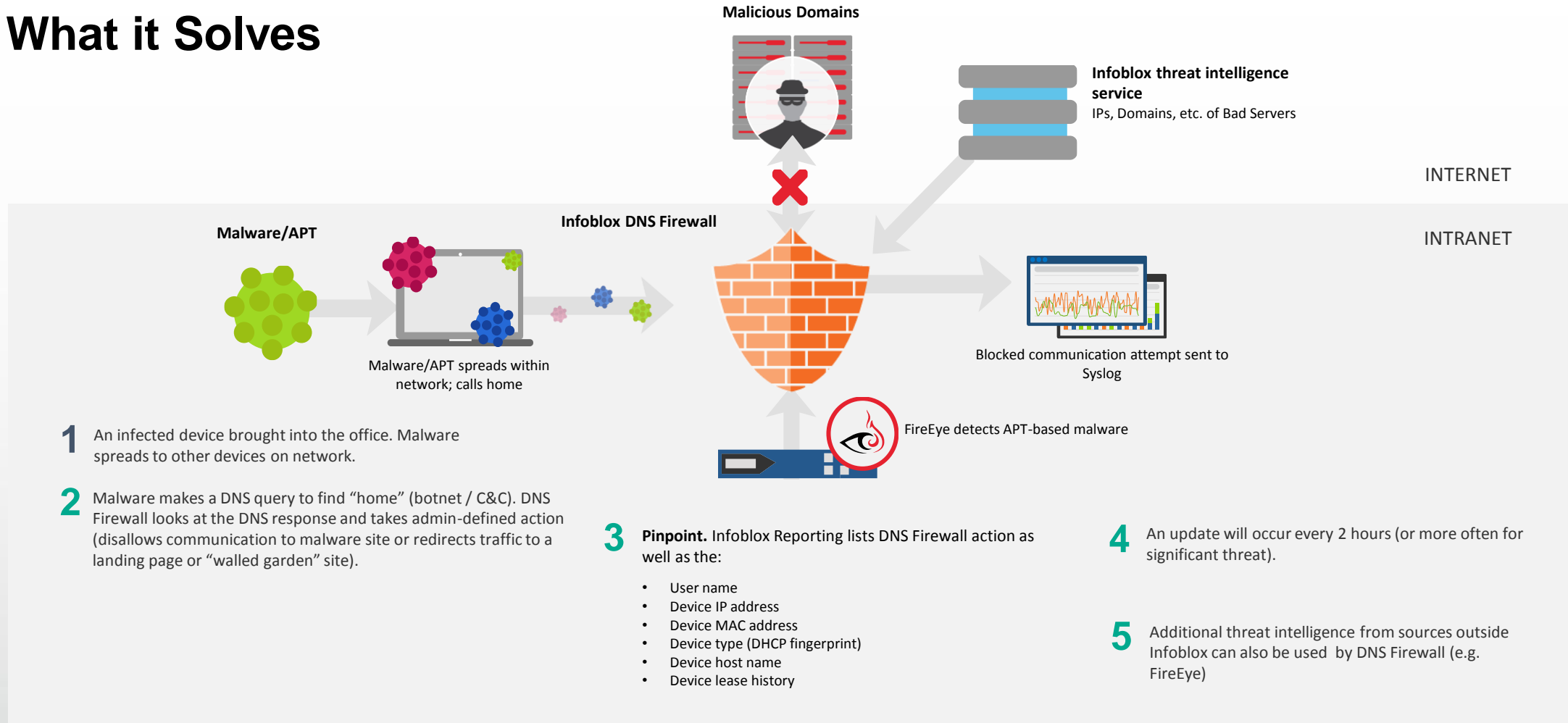
Set the VLAN for each selected interface or for all in the batch

Cancel Verify Save & Close

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

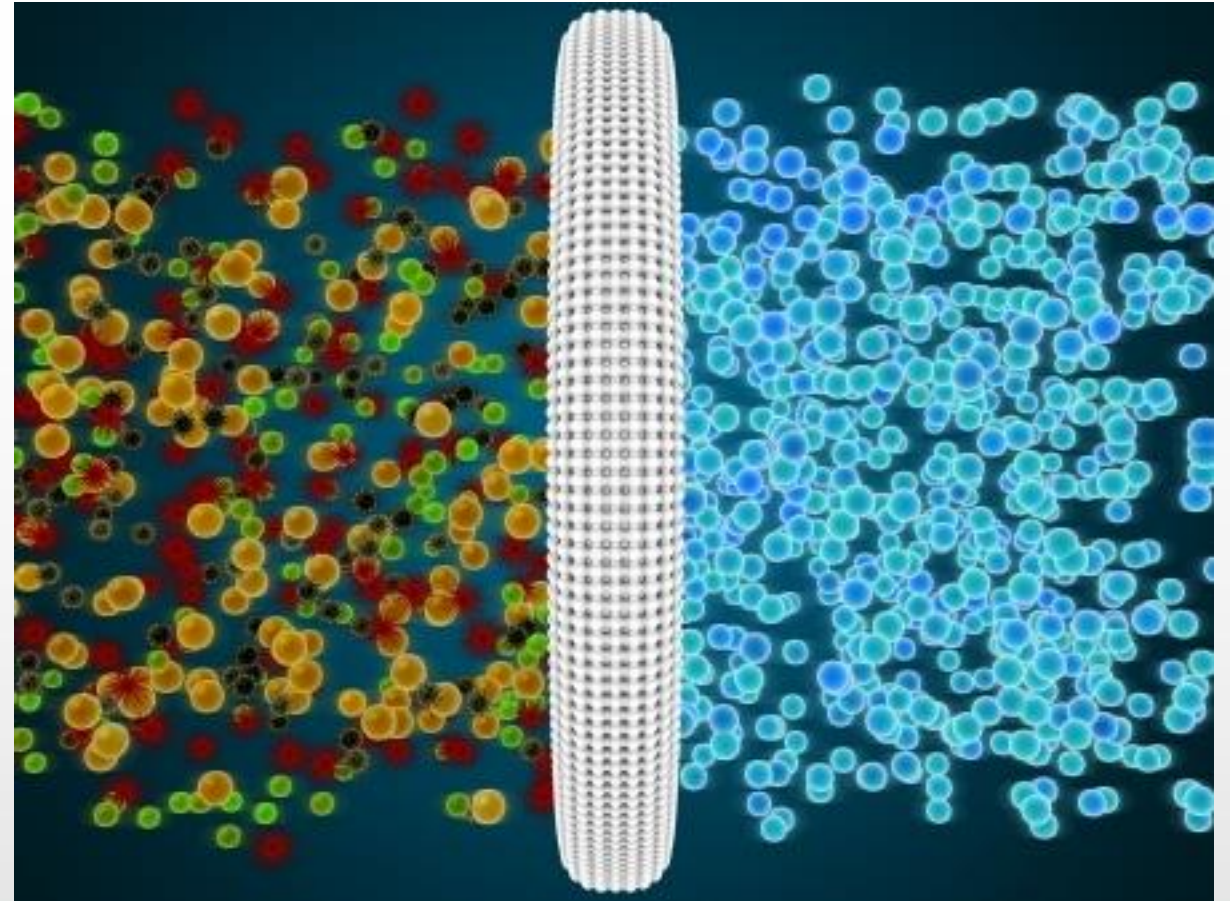
Triggers

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

Response Policy Zones

Policies

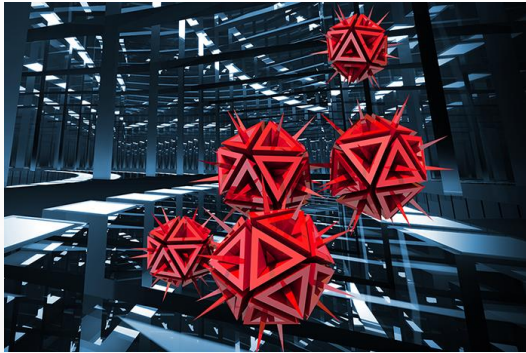
- Block – Two different ways
 - NXDOMAIN
 - NODATA
- Substitute
 - Use to redirect to a safe haven
 - Substitute parts of the reply – depends on record type
- PassThru
 - Used to LOG queries when triggered



Insert Transition Slide – ADP

Advanced DNS Protection (ADP)

The Problem



**DNS-based attacks are
on the rise**



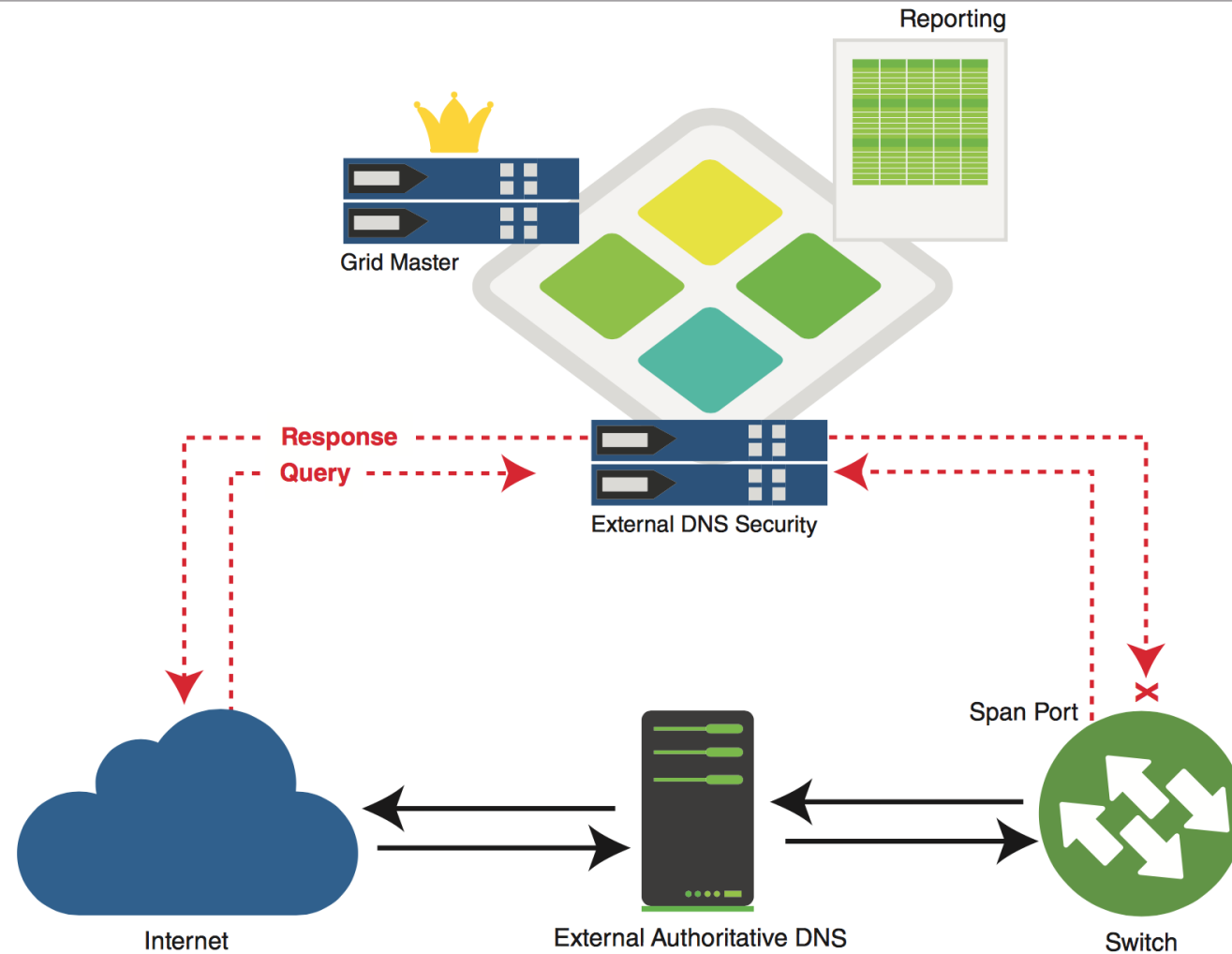
**Traditional
protection is ineffective
against evolving threats**



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

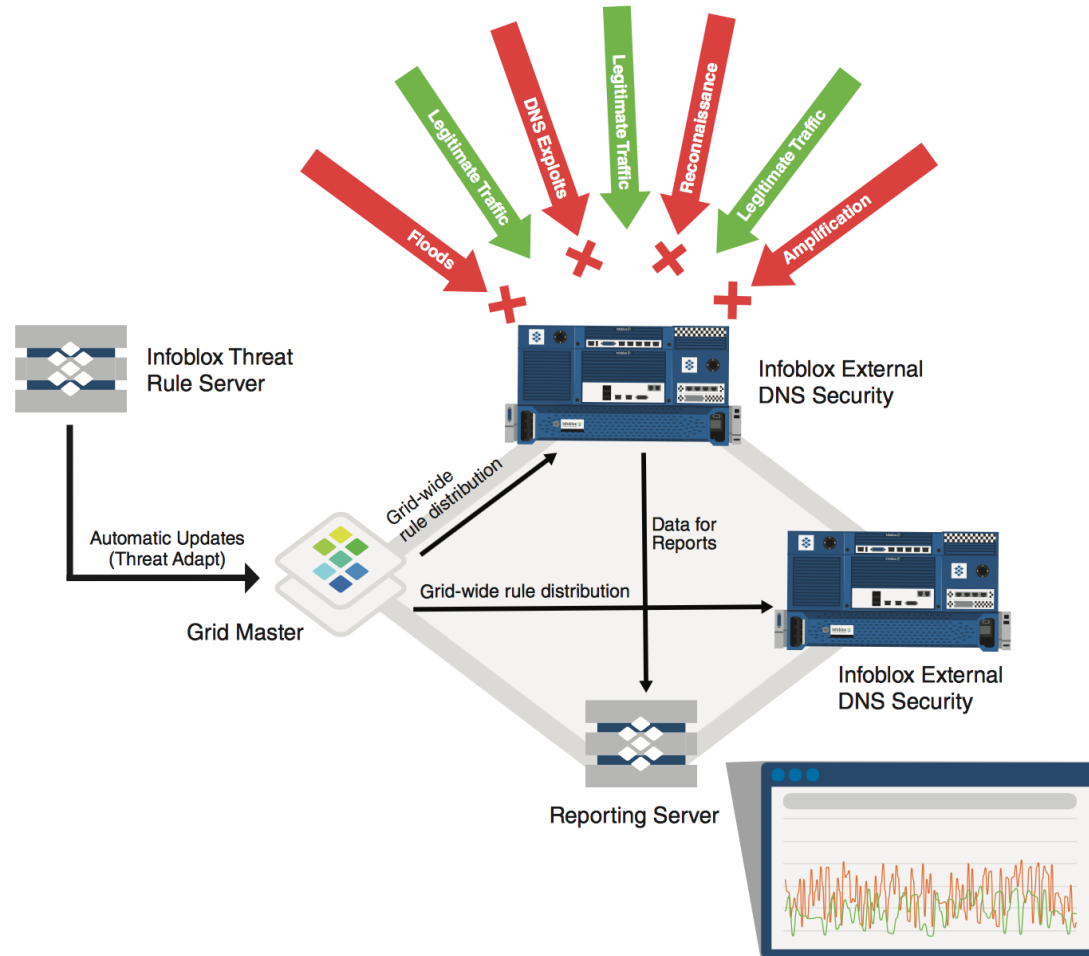
Advanced DNS Protection (ADP)

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 ID	Rule ID	Rule ID	Rule ID	Rule ID	Rule ID	Rule ID	Rule ID	Rule ID	Rule Type
13050	1305037	1305037	13050220	1305007	1301000	13010	130100400	13010	130100400	Auto
13050	1305038	1305038	13050230	1305008						
13050	1305039	1305039	13050240	1305009	1301000	13010	130100401	13010	130100401	Auto
13050	1305040	1305040	13050250	1305010						
13050	1305041	1305041	13050260	1305011	1302000	13020	130200100	13020	130200100	Auto
13050	1305042	1305042	13050270	1305012	1302000	13020	130200200	13020	130200200	Auto
13050	1305043	1305043	13050280	1305013	1302000	13020	130200300	13020	130200300	Auto
13050	1305044	1305044	13050290	1305014	1302000	13020	130200400	13020	130200400	Auto
13050	1305045	1305045	13050300	1305015						
13050	1305046	1305046	13050310	1305016	1305000	13050	130500100	13050	130500100	System
13050	1305047	1305047	13050320	1305017	1305000	13050	130500200	13050	130500200	System
13050	1305048	1305048	13050330	1305018	1305000	13050	130500300	13050	130500300	System
13050	1305049	1305049	13050340	1305019	1305000	13050	130500400	13050	130500400	System
13050	1305050	1305050	13050350	1305020	1305000	13050	130500500	13050	130500500	System
13050	1305051	1305051	13050360	1305021	1305000	13050	130500600	13050	130500600	System

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)	



Advanced DNS Protection (ADP)

The Rules

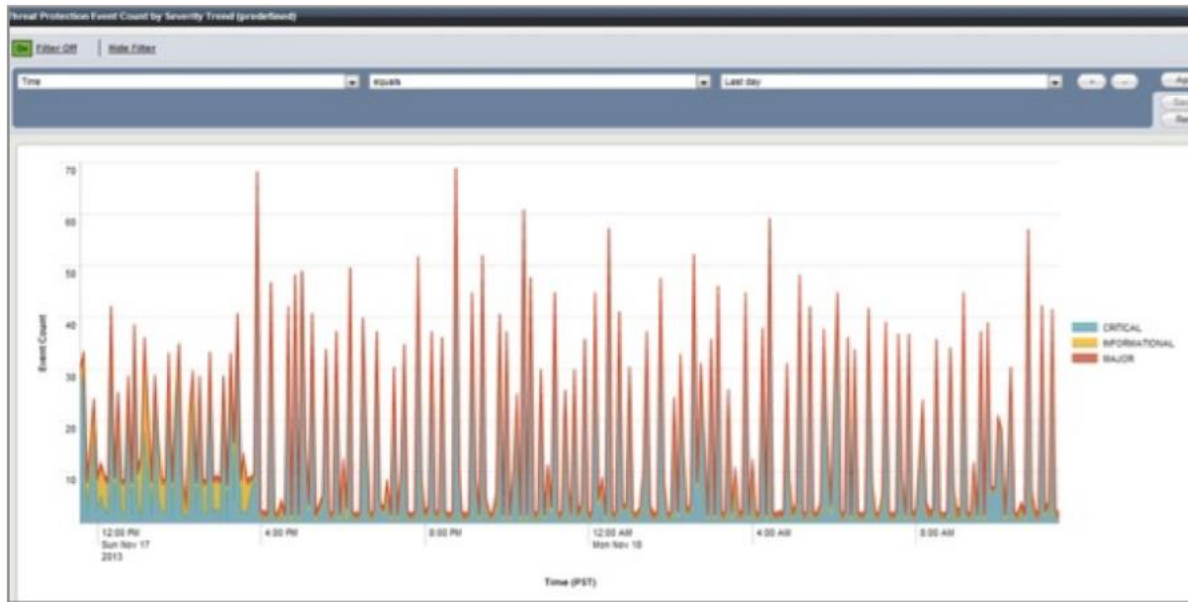
Not Enough?

- Create up to 500 Custom Rules

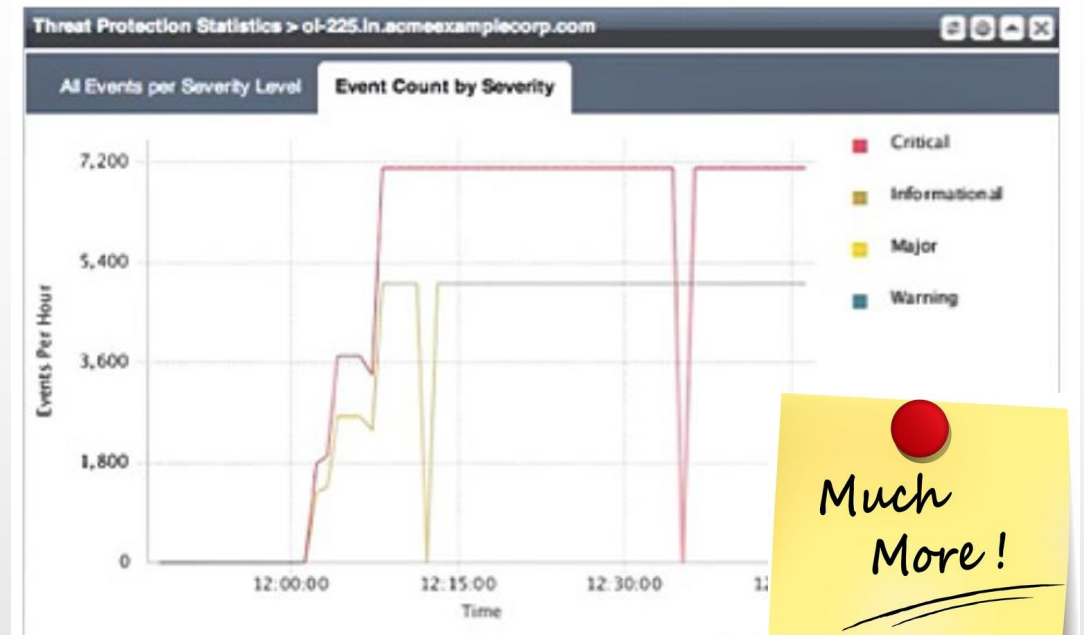


Advanced DNS Protection (ADP)

Reporting



Threat Protection Event Count by Severity Trend Report



Threat Protection Statistics Widget

Much More!



Questions?

