DNS Security Filtering @ Chapel Hill

Will Whitaker, DDI Architect
Alex Everett, IT Security Architect
Oct 2018

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

What problems were we trying to solve?

+ **Address limitations of IP-based blacklisting**
+ **Provide blacklisting for roaming clients**
+ **Access curated list of malicious domains**

What option is best for me?

Solution Consideration

Define Solution Goals and Requirements

Threat Blocking Abilities

- Block logic independent of IP address
- Easy infrastructure integration
- Feedback to end user
- Metrics and reporting

Effective Coverage

- Maximize true readings
- Minimize false readings
- Stay within budget

True negative

True positive

False positive

False negative

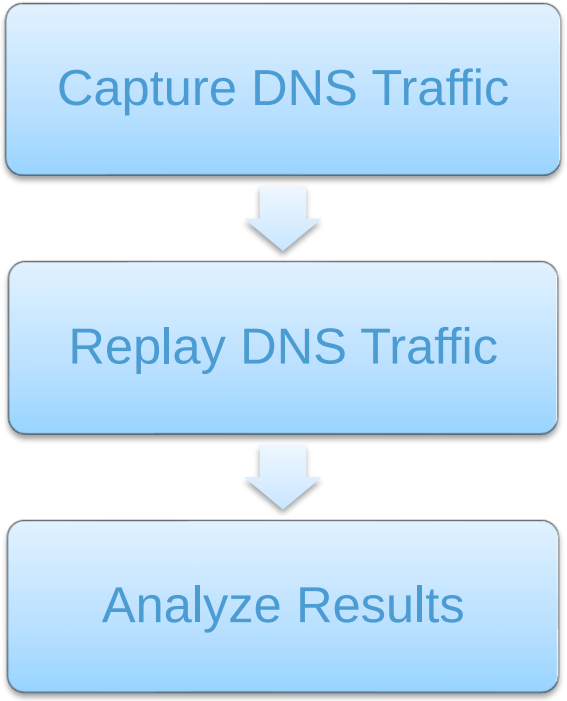
Compare Solution Options

Active Testing

- Production trials
- Leverage views

Passive Testing

- Custom scripts
- DNS Replay Tool (drool)



Decide Best Value

Cross Comparison Results

- Multiple solutions exist facilitating DNS firewalls
- Large diversity in our block results
- Cost and cost models vary significantly

Eventual Decision

- Akamai’s Enterprise Threat Protector via MCNC
- Akamai ETP is open to feedback and quickly evolving

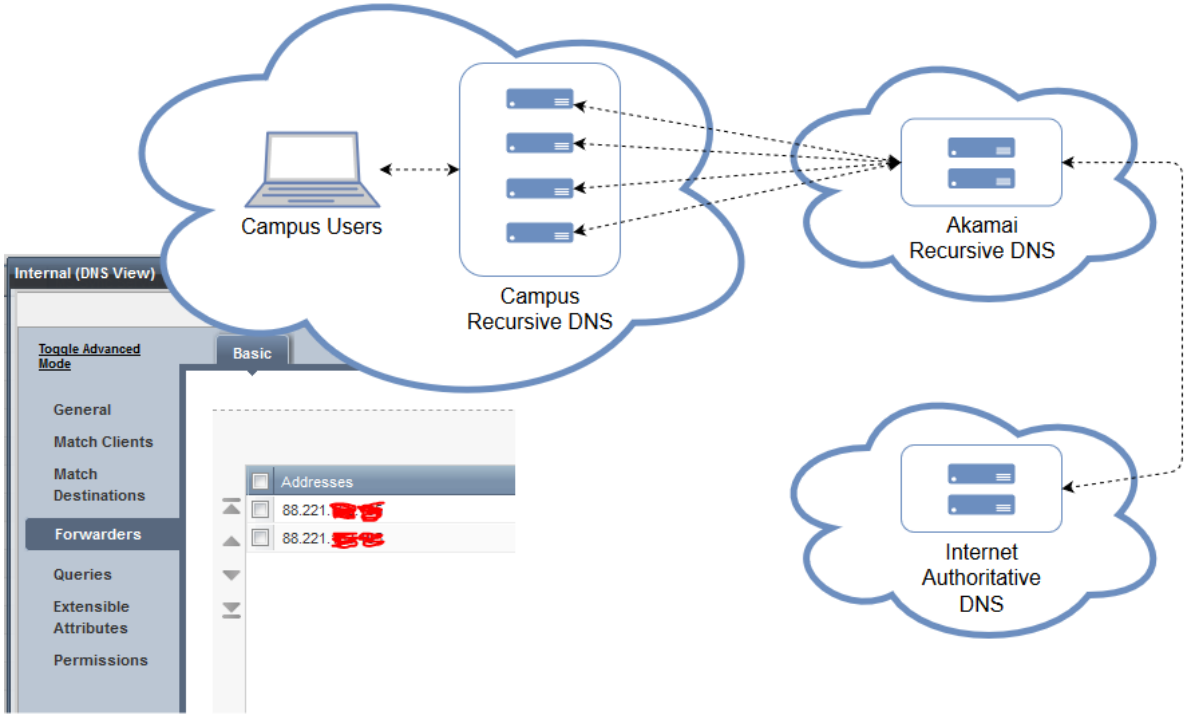
What does the service look like?

Enterprise Threat Protector Architecture

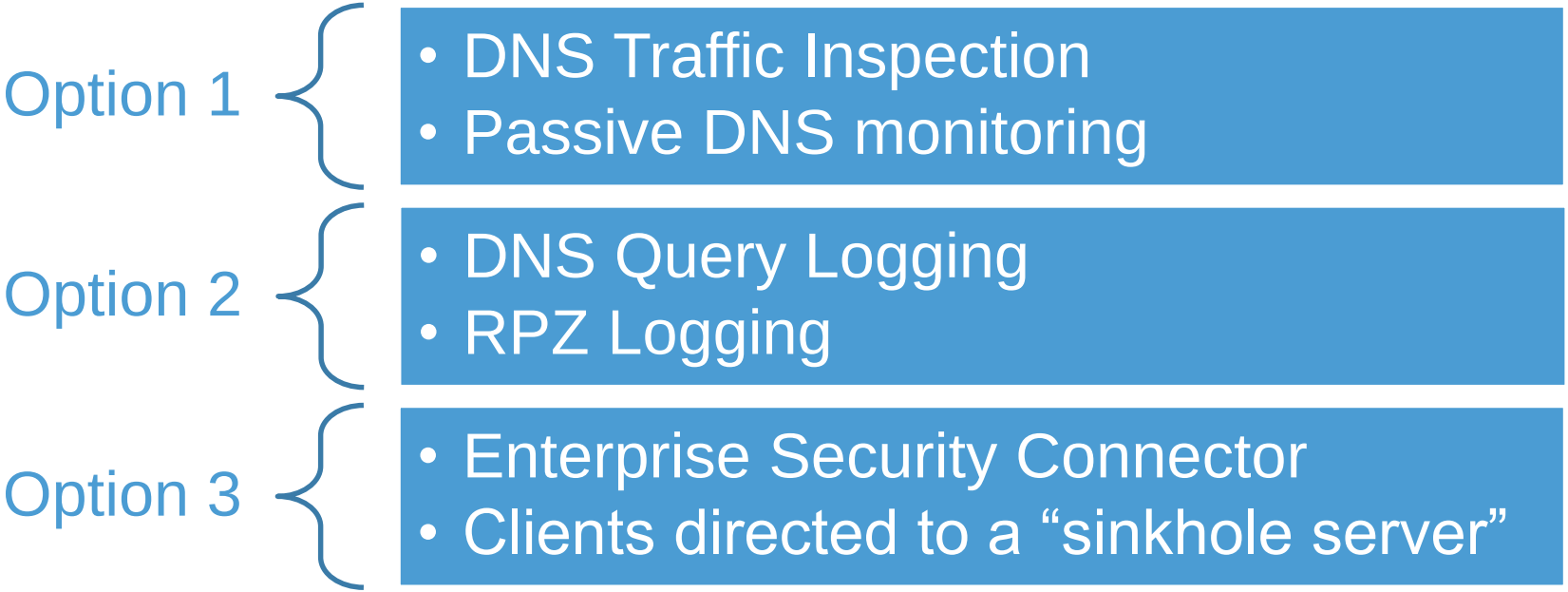
Enterprise Threat Protection Architecture

DNS Forwarders

- Pros
- Cons



Con: Difficult to Identify Client Source Addresses



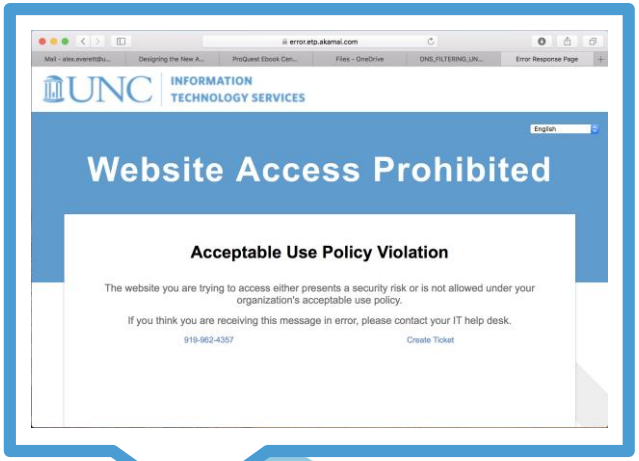
Agent or Client Connector

Benefits

- Protection for off-campus devices
- Easy to deploy

Limitations

- Beta
- No client yet for smartphones and tablets
- Fail closed issue



What can I make it do?

Policy Options

Policy Config

Security Lists

- Malware
- Phishing
- C&C/ botnets
- DNS Exfiltration
- Custom Lists

Acceptable Use Policies

- Dating
- Weapons
- Adult
- Illegal
- Anonymizers
- Drugs
- Games
- Social
- Suicide
- Pornography
- Tobacco
- Privacy
- Gambling
- Alcohol

Browsing

- Safe Search
- YouTube

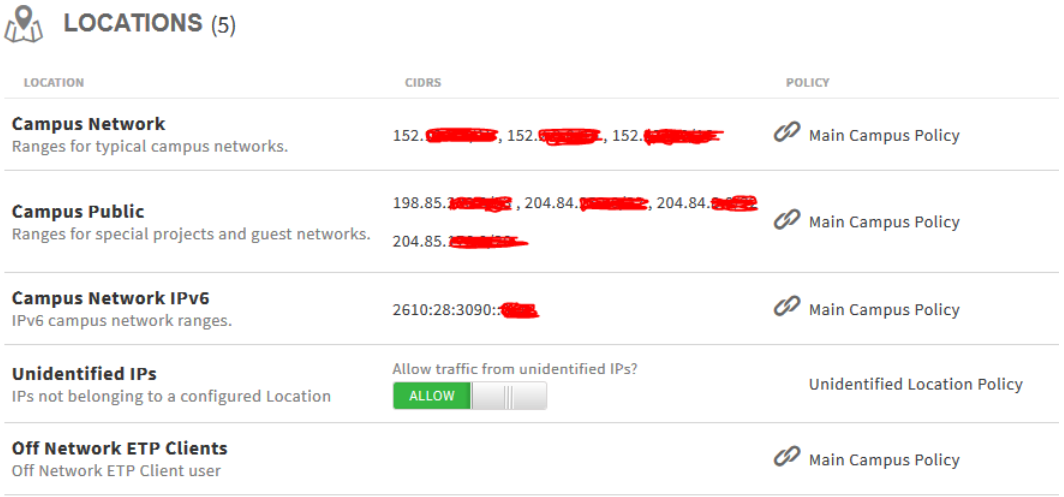
Location Config

Definitions

- Networks to policy map

Limitations

- Have max CIDR masks
- Are non-overlapping
- Affect deploy time



Now that I have it, how do I work with it?

Troubleshooting / Mitigation

Layered Security Factors

Host Specific

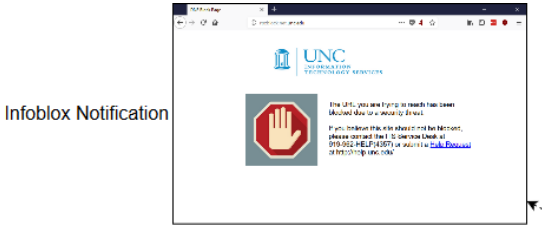
- Google Safe Browsing
- Microsoft SmartScreen URL
- Local plugins or agents

DNS Flow Specific

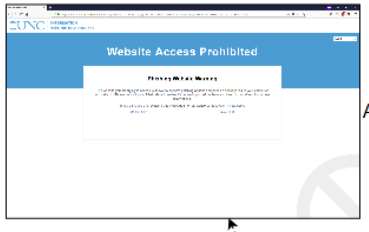
- Recursive DNS

Content Flow

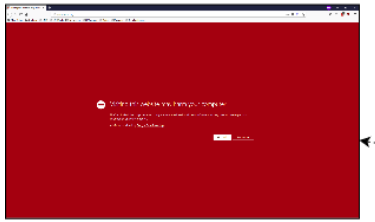
- URL filters



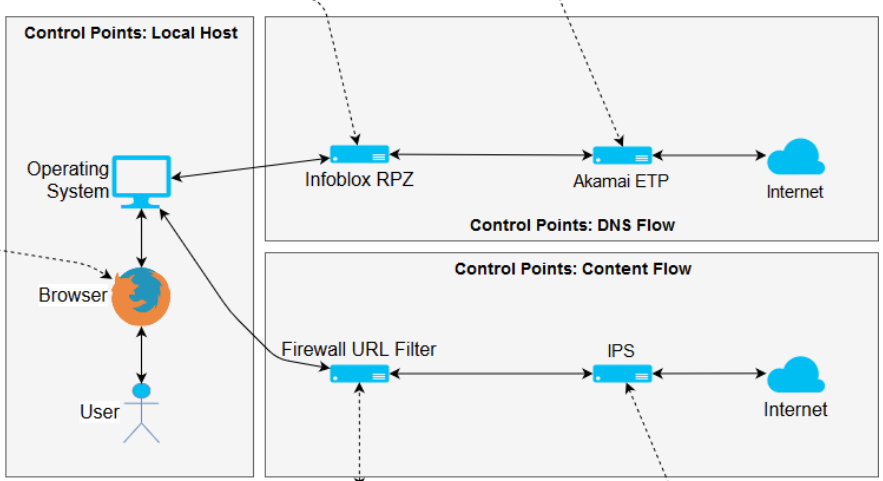
Infoblox Notification



Akamai Notification

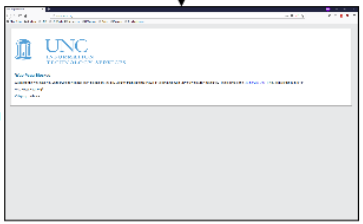


SafeBrowsing Notification



Notification Precedence
when accessing a bad site

1. Browser
2. Firewall URL Filter
3. Infoblox RPZ
4. Akamai ETP

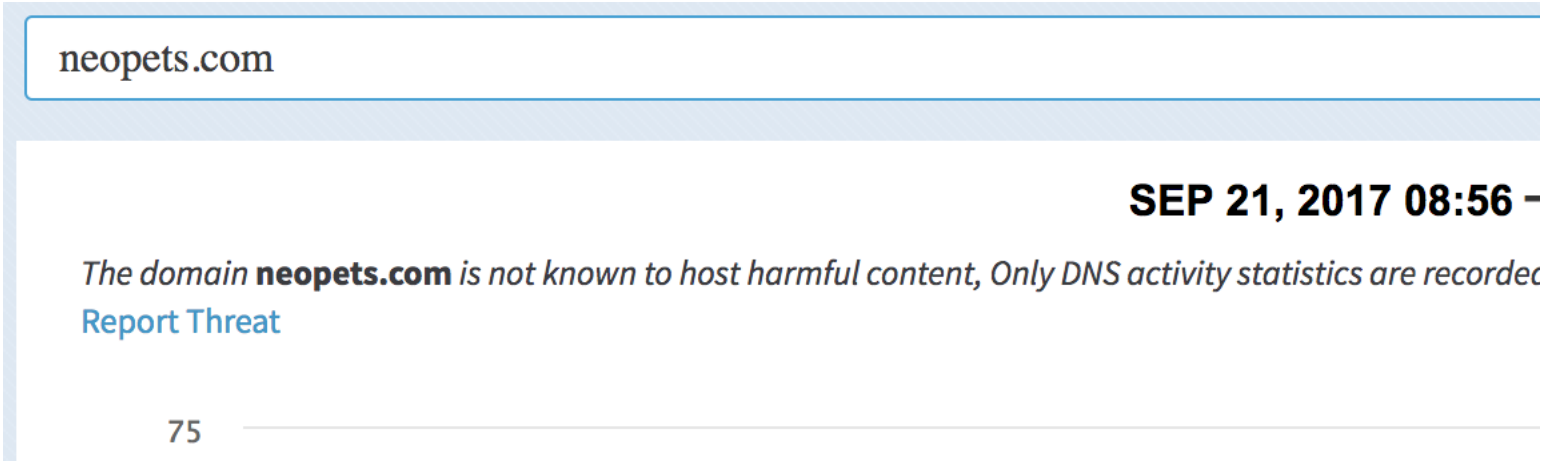


Firewall Notification

No Notification

Troubleshooting a false positive

- Customer calls in because neopets.com is blocked.
- You search for neopets.com in the Luna Control Center and find no results.

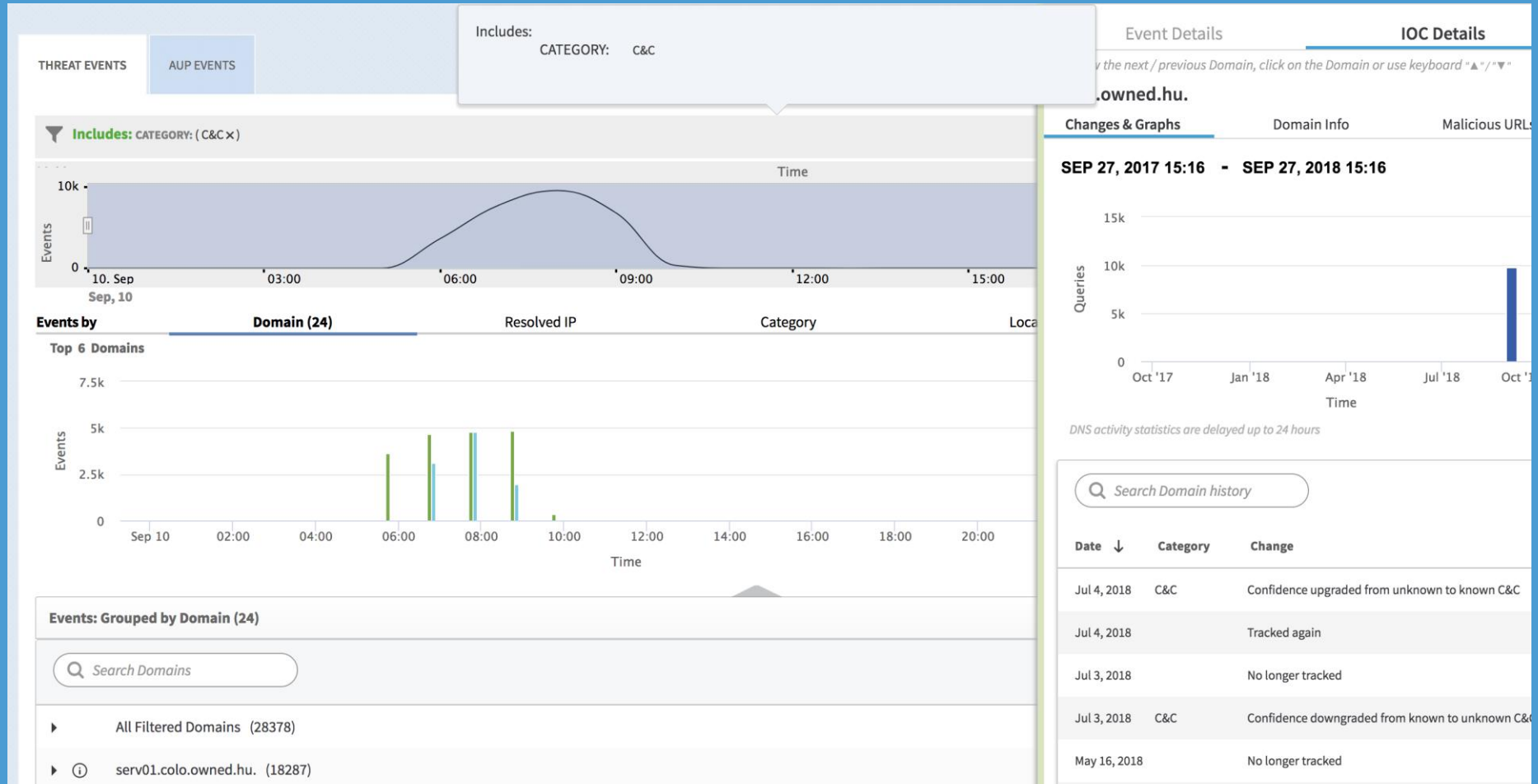


Troubleshooting Continued

neopets.com → www.neopets.com → webneocs.cloudapp.net

	Detected Time	Action	Location	Policy	Category	List	Confidence	Domain	Correlation
ⓘ	2018-09-21 08:53:58	⊖	Campus Network	Main Campus Policy	Phishing	Phishing	Known	webneocs.cloudapp.net.	None
ⓘ	2018-09-21 08:39:02	⊖	Campus Network	Main Campus Policy	Phishing	Phishing	Known	webneocs.cloudapp.net.	None
ⓘ	2018-09-21 08:39:02	⊖	Campus Network	Main Campus Policy	Phishing	Phishing	Known	webneocs.cloudapp.net.	None
ⓘ	2018-09-21 08:39:02	⊖	Campus Network	Main Campus Policy	Phishing	Phishing	Known	webneocs.cloudapp.net.	None

Identified multiple bots on campus on first day



10-15 minute Q & A

UNC Chapel Hill Information Technology Services

THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Thank you!