

```
global options: +cmd
Got answer:
->>HEADER<<- opcode: QUERY, status: NOERROR, id: 6339
flags: qr rd ra; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 1
```

DNS Security Filtering @ Chapel Hill

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

```
www.amazon.com. 1559 IN CNAME www.cdn.amazon.com.
www.cdn.amazon.com. 5 IN CNAME www.amazon.com.edgekey.net.
www.amazon.com.edgekey.net. 86 IN CNAME e15316.ci.akamaiedge.net.
e15316.ci.akamaiedge.net. 184.50.247.204 IN A
```



UNC Chapel Hill Information Technology Services



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](#))

Capture DNS Traffic



Replay DNS Traffic



Analyze Results

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

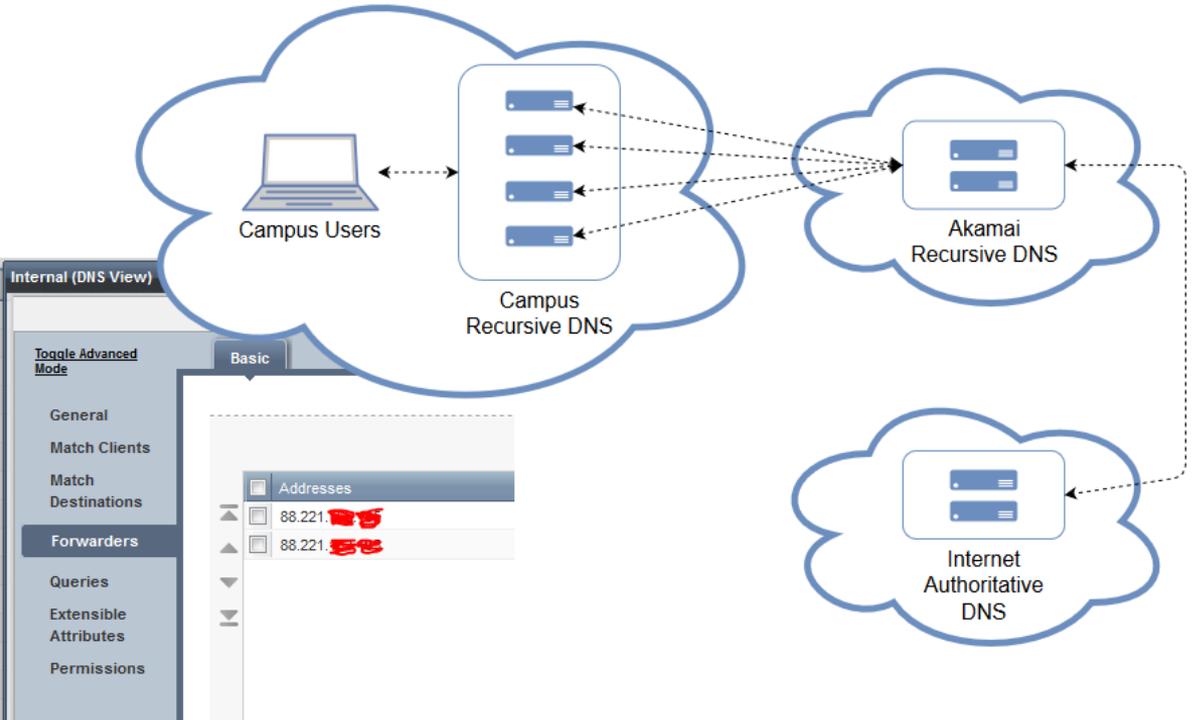
What does the service look like?

Enterprise Threat Protector Architecture

Enterprise Threat Protection Architecture

DNS Forwarders

- Pros
- Cons



Con: Difficult to Identify Client Source Addresses

- Option 1
 - DNS Traffic Inspection
 - Passive DNS monitoring
- Option 2
 - DNS Query Logging
 - RPZ Logging
- Option 3
 - Enterprise Security Connector
 - Clients directed to a “sinkhole server”



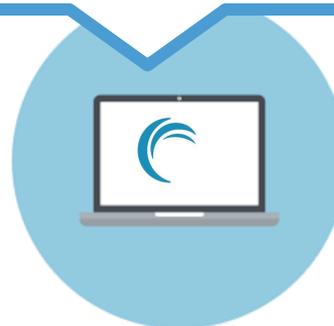
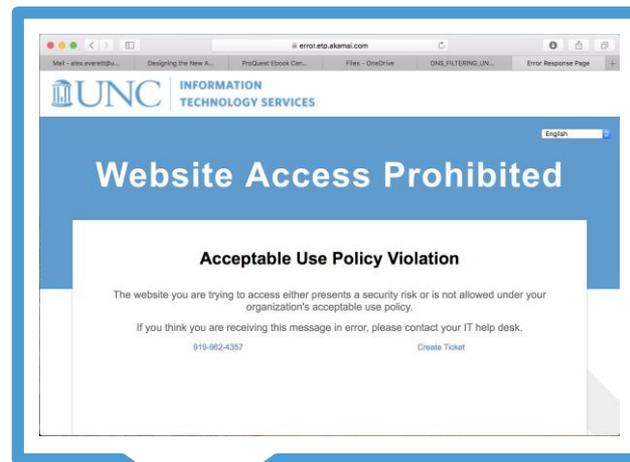
Agent or Client Connector

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 | Social |
| • Weapons | Suicide |
| • Adult | Pornography |
| • Illegal | Tobacco |
| • Anonymizers | Privacy |
| • Drugs | Gambling |
| • Games | Alcohol |

Browsing

- Safe Search
- YouTube

Location Config

Definitions

- Networks to policy map

Limitations

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



LOCATIONS (5)

LOCATION	CIDRS	POLICY
Campus Network Ranges for typical campus networks.	152.0.0.0/24, 152.0.0.0/24, 152.0.0.0/24	🔗 Main Campus Policy
Campus Public Ranges for special projects and guest networks.	198.85.0.0/24, 204.84.0.0/24, 204.84.0.0/24 204.85.0.0/24	🔗 Main Campus Policy
Campus Network IPv6 IPv6 campus network ranges.	2610:28:3090::/48	🔗 Main Campus Policy
Unidentified IPs IPs not belonging to a configured Location	Allow traffic from unidentified IPs? <input checked="" type="checkbox"/> ALLOW <input type="checkbox"/>	Unidentified Location Policy
Off Network ETP Clients Off Network ETP Client user		🔗 Main Campus Policy

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

Troubleshooting / Mitigation

Layered Security Factors

Host Specific

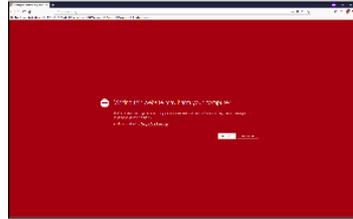
- Google Safe Browsing
- Microsoft SmartScreen URL
- Local plugins or agents

DNS Flow Specific

- Recursive DNS

Content Flow

- URL filters

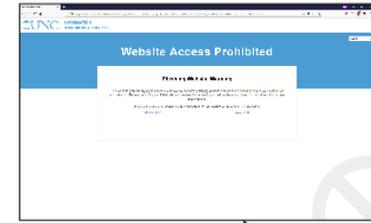


SafeBrowsing Notification

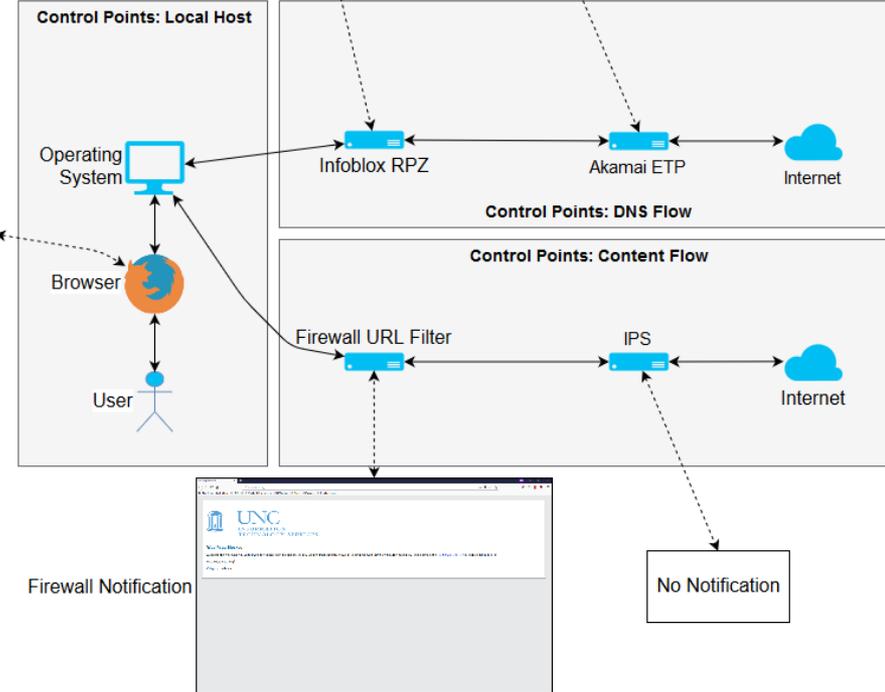
- Notification Precedence when accessing a bad site**
1. Browser
 2. Firewall URL Filter
 3. Infoblox RPZ
 4. Akamai ETP



Infoblox Notification



Akamai 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.

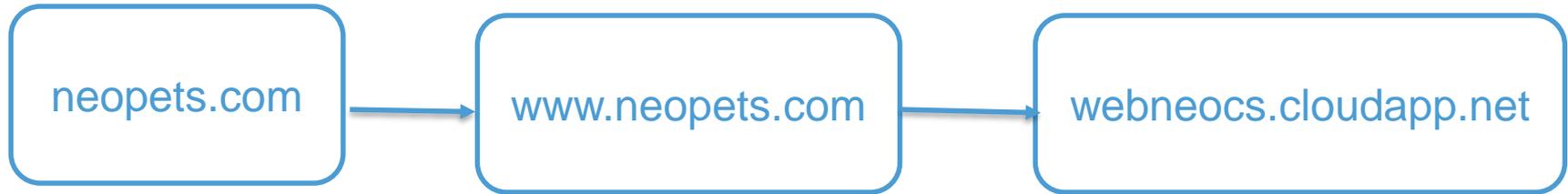
neopets.com

SEP 21, 2017 08:56 -

*The domain **neopets.com** is not known to host harmful content, Only DNS activity statistics are recorded*
Report Threat

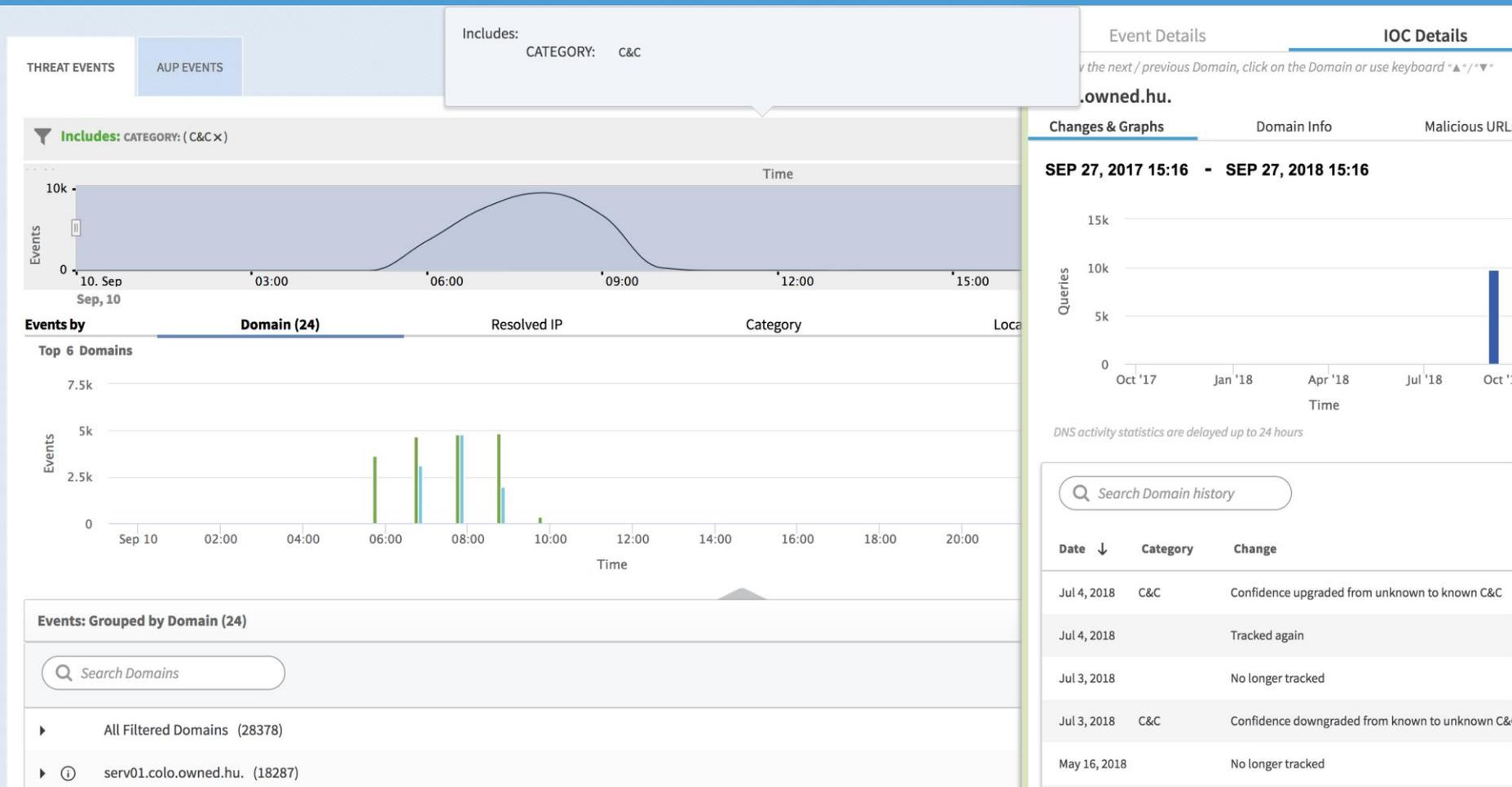
75

Troubleshooting Continued



	Detected Time	Action	Location	Policy	Category	List	Confidence	Domain	Correlation
①	2018-09-21 08:53:58	⊖	Campus Network	Main Campus Policy	Phishing	☾ Phishing	⊕ Known	webneocs.cloudapp.net.	None
①	2018-09-21 08:39:02	⊖	Campus Network	Main Campus Policy	Phishing	☾ Phishing	⊕ Known	webneocs.cloudapp.net.	None
①	2018-09-21 08:39:02	⊖	Campus Network	Main Campus Policy	Phishing	☾ Phishing	⊕ Known	webneocs.cloudapp.net.	None
①	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



MCNC

UNC Chapel Hill

Information Technology Services



THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL



THE UNIVERSITY
of NORTH CAROLINA
at CHAPEL HILL

Thank you!