RELAX,
WE CARE

CISCO UMBRELLA

PROTECTION AND VISIBILITY FOR ENTERPRISE NETWORKS

03.10.2018 | Bolzano, Andrea Dainese

ABOUT

NTS

ANDREA DAINESE - SENIOR SYSTEMS ENGINEER

- Network and Security Architect (15+ years' exp.)
- Security Evangelist (Blue Team)
- Automation Addicted/Developer (UNetLab)
- Cisco CCIE #38620/VMware VCP/Red Hat RHCE


andrea.dainese@nts.eu


www.linkedin.com/in/adainese


@adainese

INTRODUCTION

INTRODUCTION

NTS

You cannot protect what you don't know

INTRODUCTION

NTS

WHAT ABOUT ENDPOINTS?

- Where users navigate?
- What they download?
- What they execute?
- What they attach to the computer/laptop?
- Where they are used to work?
- Are endpoints left unattended?

INTRODUCTION

NTS

Multi layered security approach

INTRODUCTION

NTS

PREREQUISITES FOR A WEB CONTENT FILTER

Must:

- Categorized web sites
- Set policies for user groups (AD integration)
- Protect on premises and mobile users

Should:

- Work for all protocols
- Easy to setup and maintain

INTRODUCTION

NTS

WEB CONTENT FILTER COMPARISON

	SWG	SIG
Protection	Enterprise Networks	Everywhere
Control	Granular web usage*	Any protocol
Setup Time	Days	Minutes
User experience	Can break some sites/apps**	No latency

*: Encrypted websites require a MITM approach
**: Some applications do not work behind a proxy server

CISCO UMBRELLA

CISCO UMBRELLA

NTS

BRIEF HISTORY

- 2006: OpenDNS Founded
- 2012: Umbrella enters the enterprise market
- 2015: Cisco squires OpenDNS/Umbrella

WHAT IS OPENDNS/UMBRELLA?

The largest cloud-based DNS service (and more)

TODAY

- 100B requests/day
- 85M daily users
- 12k Enterprise Customers

CISCO UMBRELLA

NTS

Threat prevention for:

- **Homes (OpenDNS)***
- **Enterprises (Umbrella)**

*: Dynamic IP Internet connection require to update the OpenDNS account using a DDNS protocol (link).

CISCO UMBRELLA

NTS

CISCO UMBRELLA PROTECT AGAINST:

- Unwanted Websites
- Suspicious Websites
- Advertising
- Malware
- Phishing Attacks
- Newly Seen Domains (and DGA*)
- Command and Control Callbacks
- DNS Tunnelling VPN**

*: www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com
**: A MRZGS3TLEBWW64TFEBXXMYLMOR.t.example.com
CNAME WW2IDPOZQWY5DJNZSQ.t.example.com

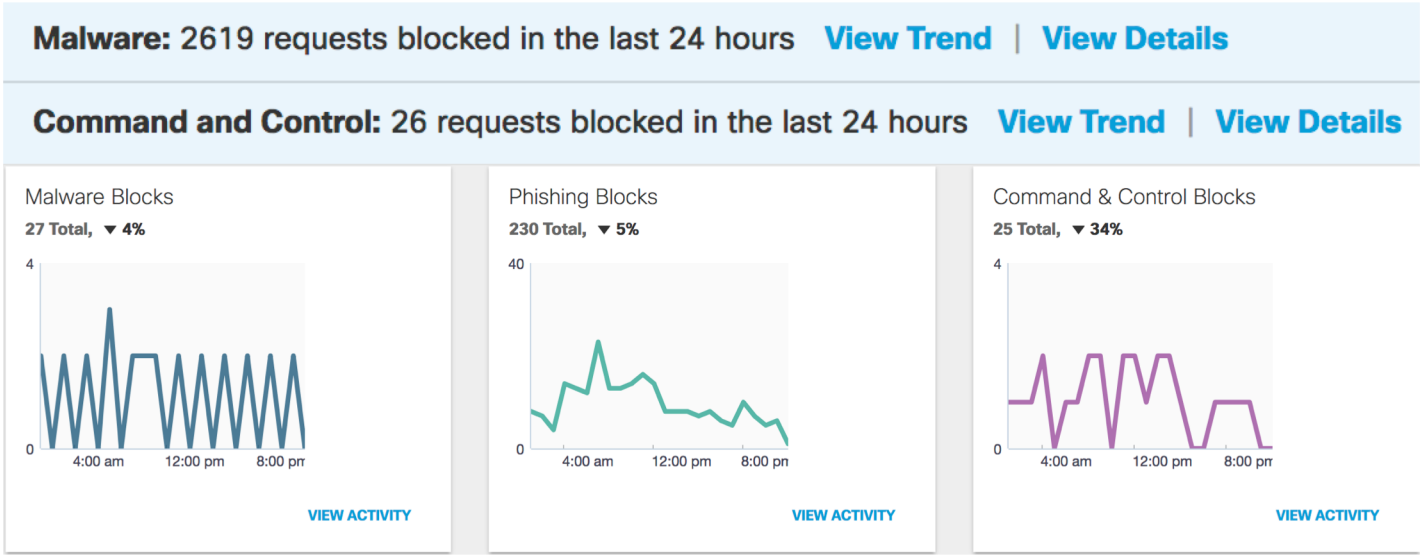
VISIBILITY

VISIBILITY

NTS

DASHBOARD

Cisco Umbrella v1 - Instant Demo @ Cisco dCloud



VISIBILITY

NTS

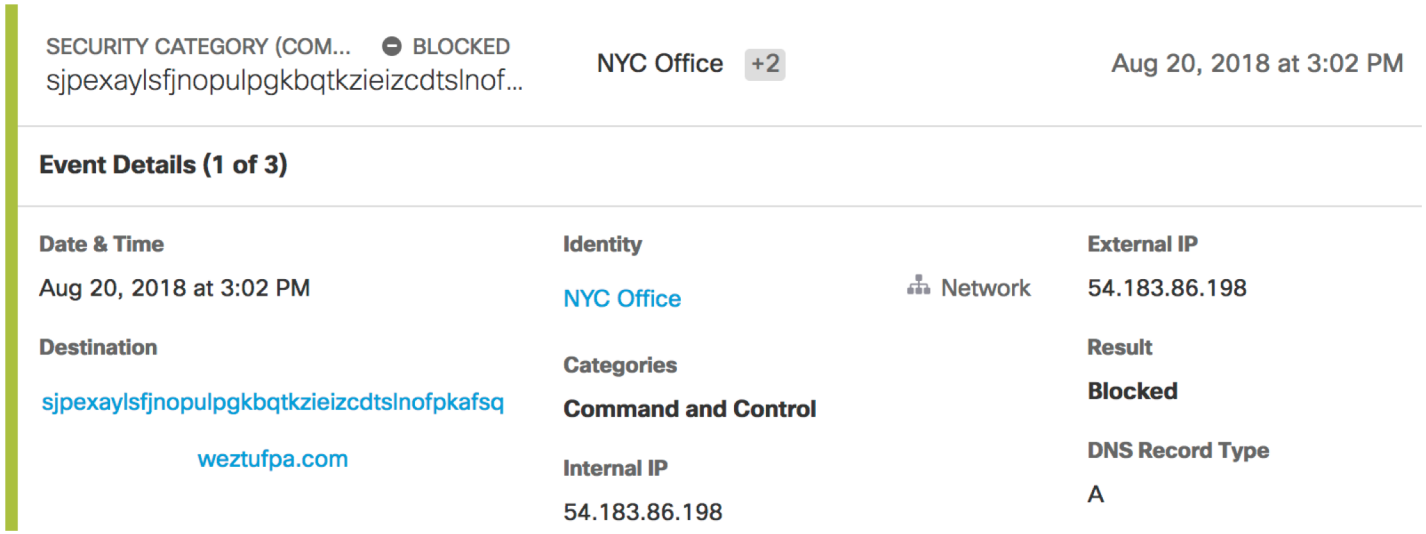
ACTIVITY SEARCH (C&C)

Identity	Identity Type	Destination
kayleighrogersgUs	Roaming Computers	so7bet7ob.net
William Neal	AD Users	syk3qe022.ru
William Neal	AD Users	so7bet7ob.net
johnathongravesXFu	Roaming Computers	hffmzplu.com
briannecomptonV2x	Roaming Computers	zjzhuji.com
NYC Office	Networks	t0pm0b1l3.com

VISIBILITY

NTS

ACTIVITY SEARCH (DETAIL)



VISIBILITY

NTS

ACTIVITY SEARCH (GENERIC)

Identity	Identity Type	Destination	Categories
keilarobertsu7c	Roaming Computers	binarycousins.com	**Malware**
keilarobertsu7c	Roaming Computers	binarycousins.com	**Malware**
keilarobertsu7c	Roaming Computers	chart.apis.google.com.ref.ualibrary.org	**Malware,** Research/Reference
keilarobertsu7c	Roaming Computers	binarycousins.com	**Malware**
Irvin McCarthy	AD Users	manualdohomemmoderno.com.br	**Nudity,** News/Media, Fashion
keilarobertsu7c	Roaming Computers	bookmyoffer.com	**Malware**
Marie Smith	AD Users	sexyteenboys.net	**Nudity, Pornography**

VISIBILITY

NTS

CLOUD SERVICES

Name	Classification	Identit...	Trend	Requ...	Blocked
QNAP	Cloud Data Services, B...	14	↑ 6	23	8%
Intermedia	Cloud Data Services, IT...	13	↑ 7	23	4%
Sina Weibo	Communication, Collab...	12	– 0	355	0%
BMC	IT Services	12	↑ 6	18	0%
Solidfiles	Cloud Data Services, St...	12	↑ 5	20	0%
GoToMeeting	Collaboration, Web Con...	11	↓ 8	28	3%
SaltStack	IaaS, IT Services	11	↑ 5	14	7%
Dropbox	File Sharing, Collaborati...	10	↑ 4	19	0%
Teamviewer	IT Services, Collaboration	10	– 0	17	11%

A FAMOUS CRYPTOLOCKER

#WANNACRY

NTS

A BRIEF STORY

- A Long Time Ago: EternalBlue by NSA
- March 14th, 2017: Microsoft Security Bulletin (MS17-010)
- April 15th, 2017: Shadow Brokers release

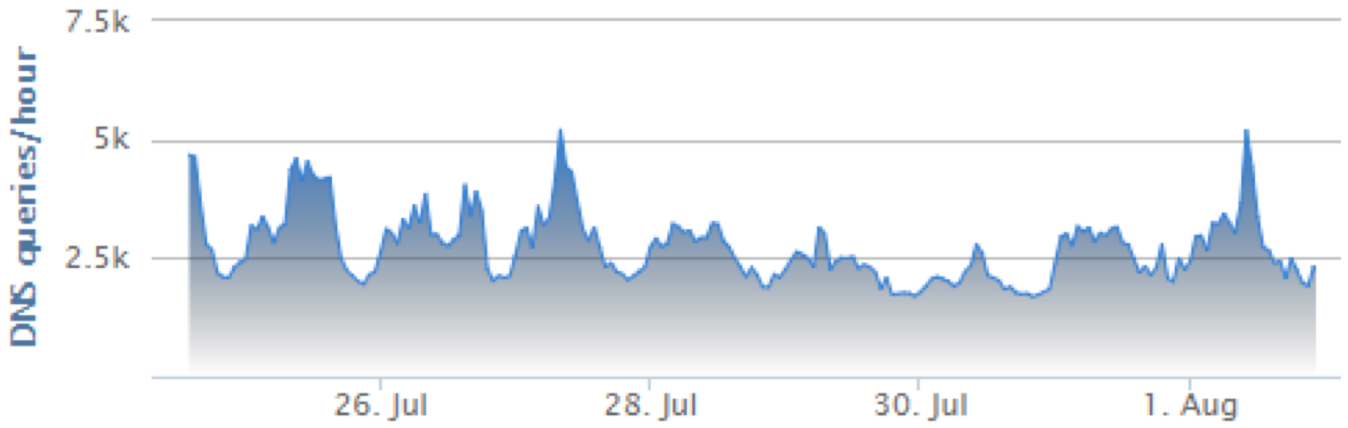
- May 12th, 2017 | 07:24 UTC: #WannaCry Patient Zero
- May 12th, 2017 | 07:30 UTC: @MalwareTechBlog Post
- May 12th, 2017 | 07:43 UTC: Kill Switch on Umbrella

UMBRELLA INVESTIGATE

INVESTIGATE

NTS

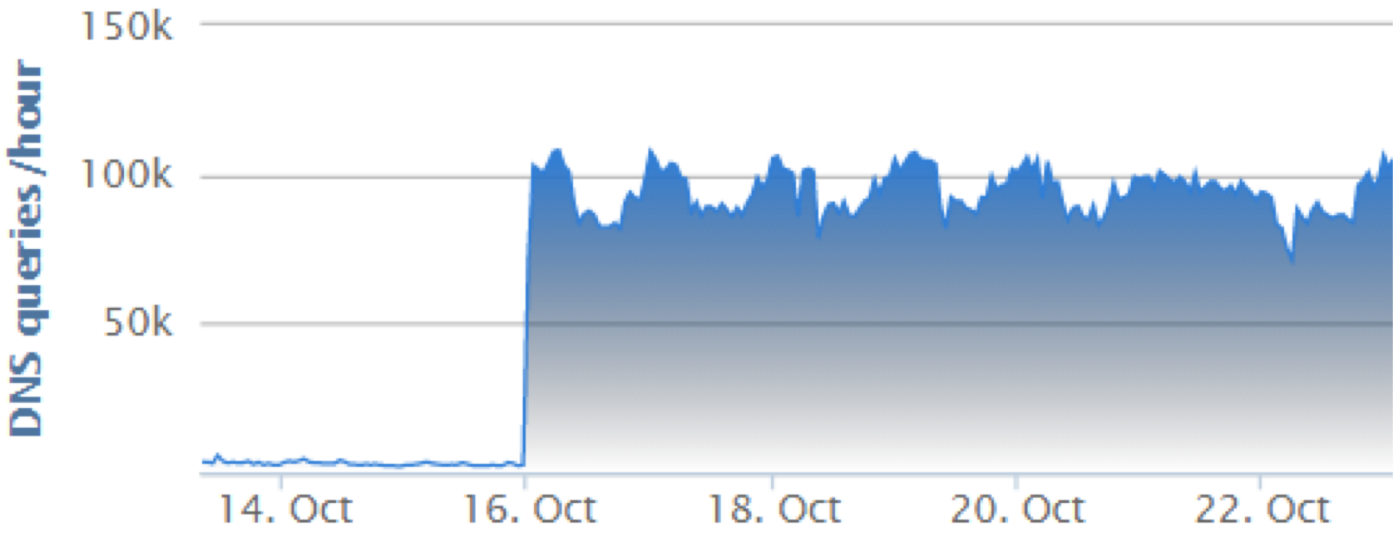
#WANNACRY (SUMMER 2017)



INVESTIGATE

NTS

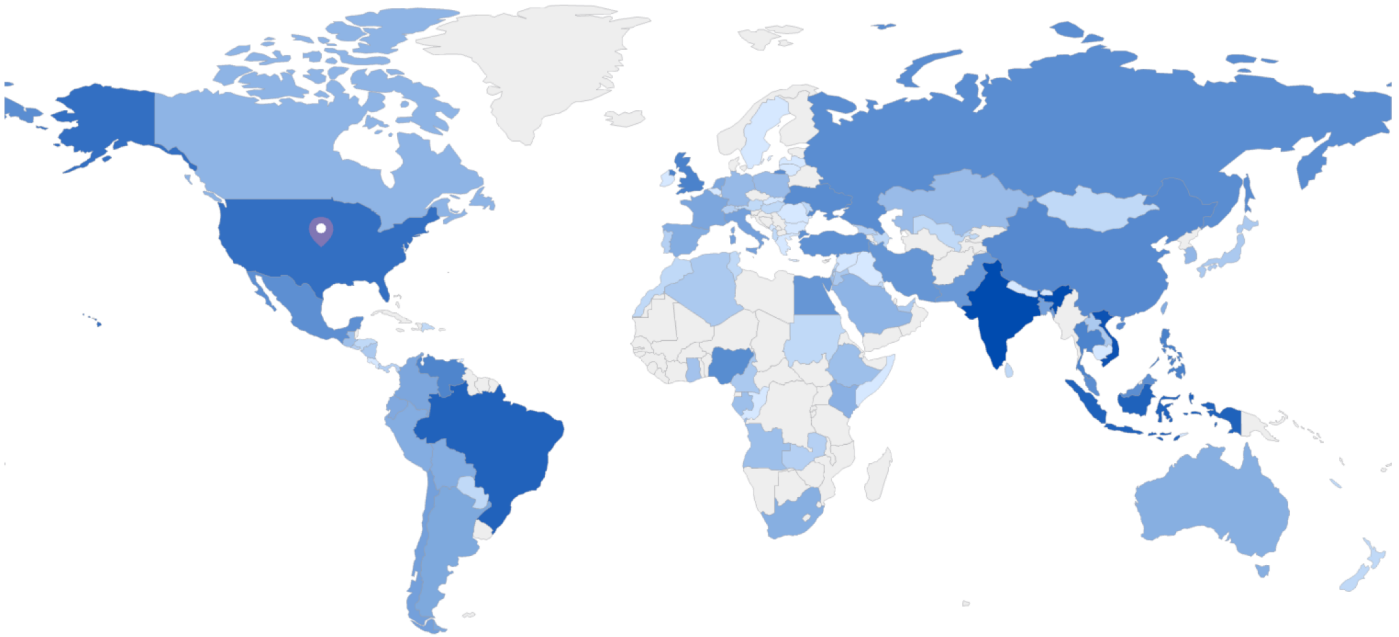
#WANNACRY (AUTUMN 2017)



INVESTIGATE

NTS

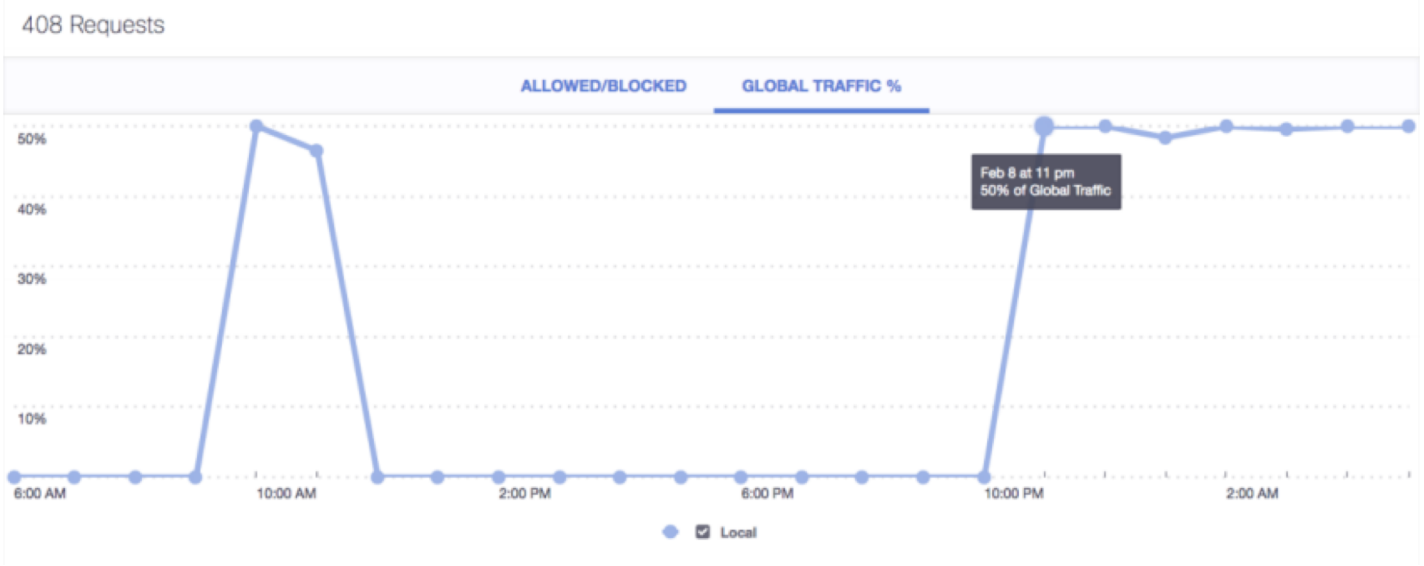
#WANNACRY (GEOGRAPHIC DISTRIBUTION)



INVESTIGATE

NTS

TARGETED MALWARE



ARCHITECTURE

ARCHITECTURE

NTS

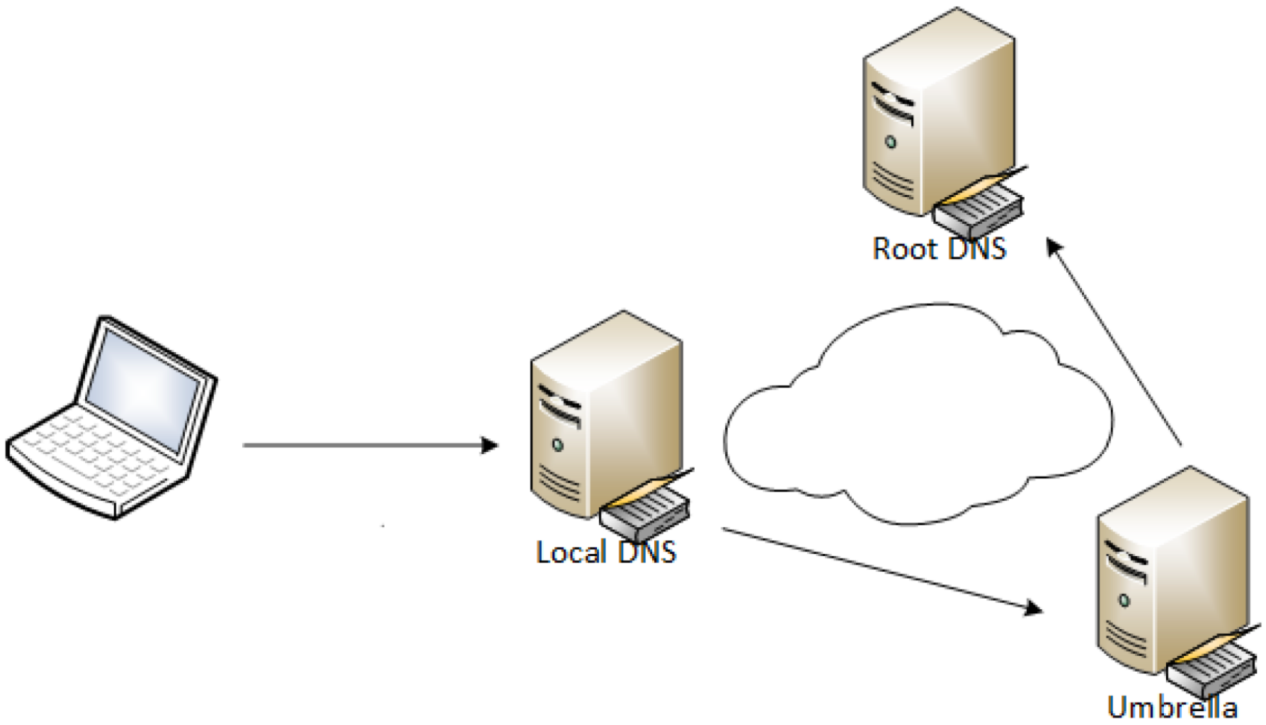
DEPLOYMENT MODES

- Networks
- Internal Networks (VA)
- Network Devices
  Roaming Computers
- Mobile Devices

ARCHITECTURE

NTS

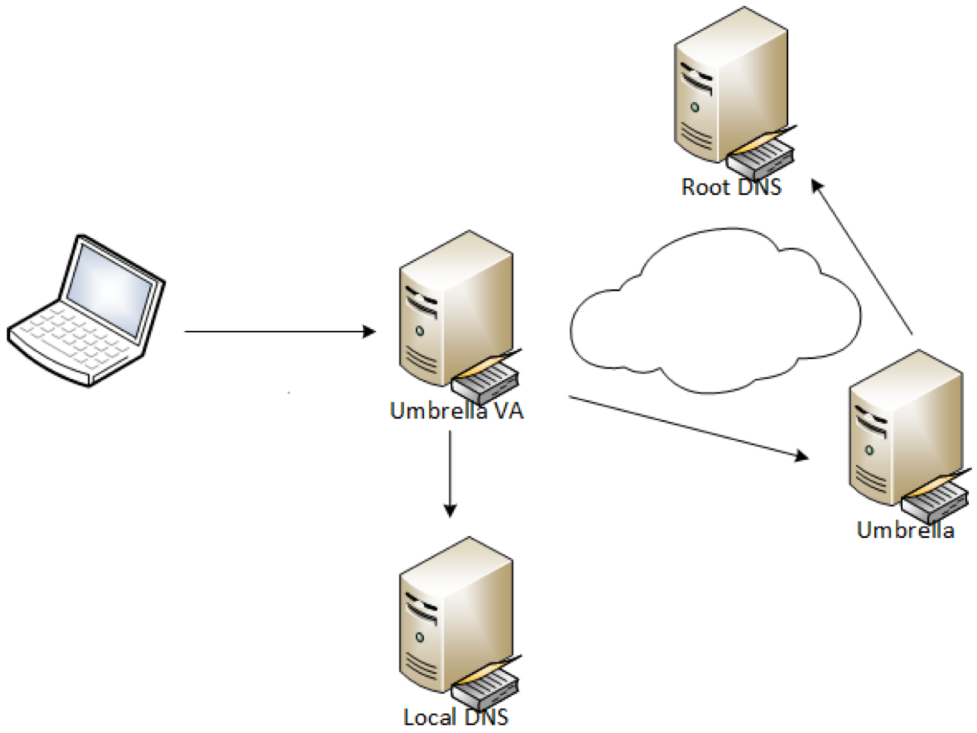
NETWORKS



ARCHITECTURE

NTS

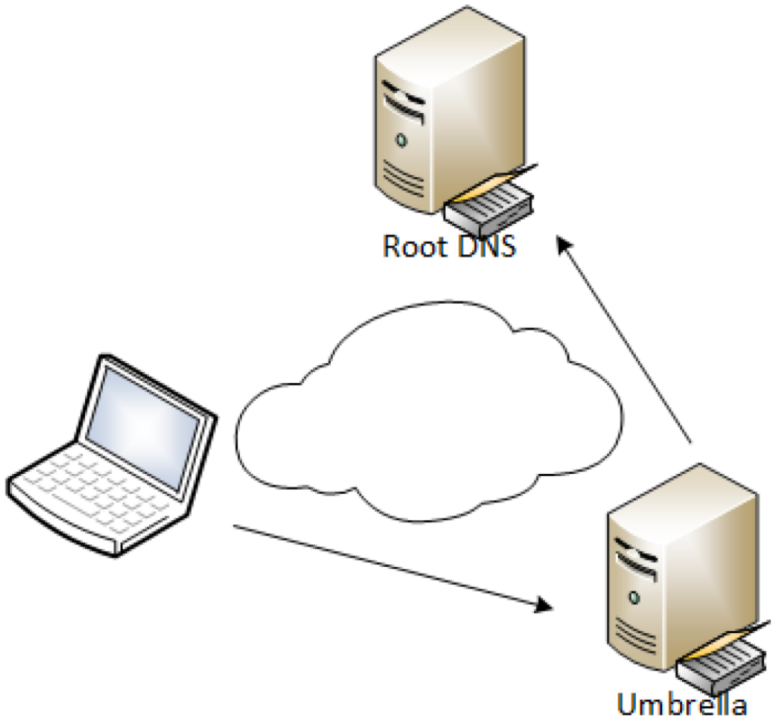
INTERNAL NETWORKS



ARCHITECTURE

NTS

ROAMING CLIENTS



ARCHITECTURE

NTS

HIGH AVAILABILITY (GLOBAL)

Anycast:

- 208.67.220.0/24 (.220 and .222)
- 298.67.222.0/24 (.220 and .222)

ARCHITECTURE

NTS

HIGH AVAILABILITY (LOCAL)

Windows:

- timeout 1s
- attempts 1
- use the last one for 15m

OS X:

- timeout 1s
- attempts 2
- use the last one for 10m

Linux:

- timeout 5s
- attempts 2
- use always the first one

ARCHITECTURE

NTS

~~Know your network~~

or

Start with non blocking policy

ARCHITECTURE

NTS

Multi-Layer Security

1. DNS: Cisco Umbrella
2. Url Filtering

DEMO


NTS
RELAX,
WE CARE