cisco Live!

#CiscoLive

The bridge to possible

DNS and BGP Exposed

How to Monitor and Mitigate Two Notorious “Uptime Killers”

Tim Hale – Technical Solutions Architect
LinkedIn: timlhale

BRKAPP-1006

Cisco Webex App

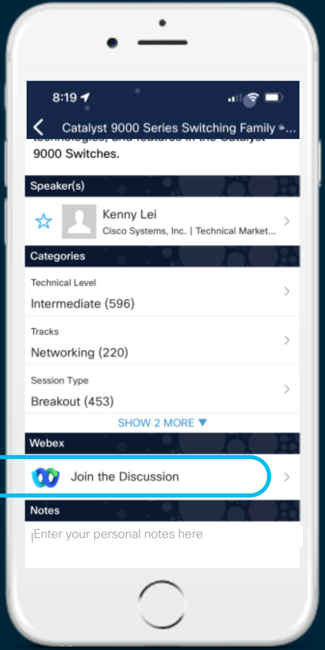
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated
by the speaker until June 17, 2022.



8:19

Catalyst 9000 Series Switching Family ...

9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKAPP-1006

Meet your speaker

Name: Tim Hale
Role: Technical Solutions Architect
Company: Cisco ThousandEyes
Location: Brighton, UK

Eight years working with DNS and internet monitoring solutions.

Agenda

- DNS 101
- Interesting DNS outages
- Monitoring best practices
- BGP 101
- Interesting BGP outages
- Monitoring best practices

Agenda

ThousandEyes

ThousandEyes monitors network infrastructure, troubleshoots application delivery and maps Internet performance, all from a SaaS-based platform.

DNS

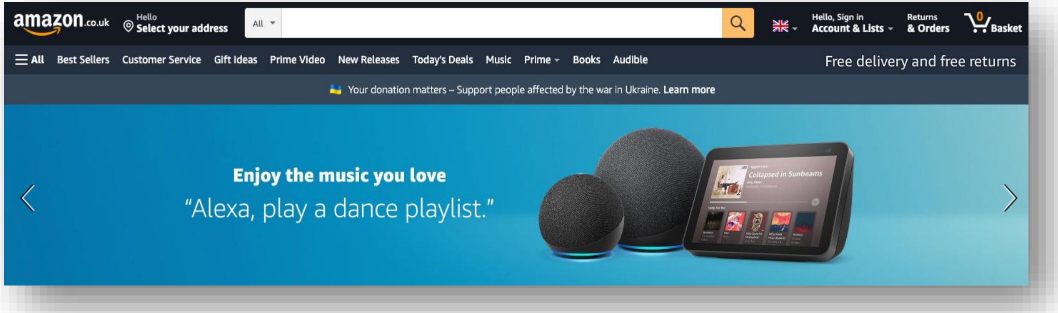
"It's always DNS!”

Why?

What is the IP address for www.amazon.com?

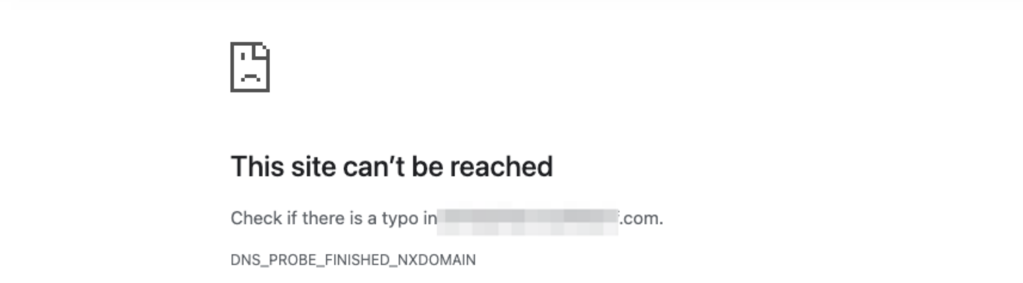
DNS ✓

205.251.242.103



DNS ✗

?

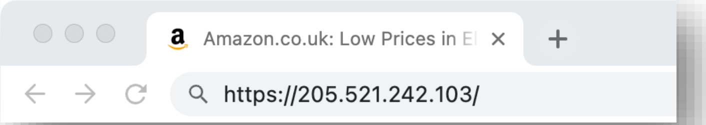


This site can't be reached

Check if there is a typo in [redacted].com.

DNS_PROBE_FINISHED_NXDOMAIN

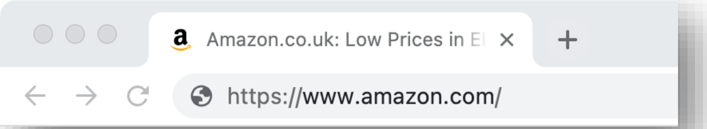
Why not use IPs For websites?



Amazon.co.uk: Low Prices in El

https://205.521.242.103/

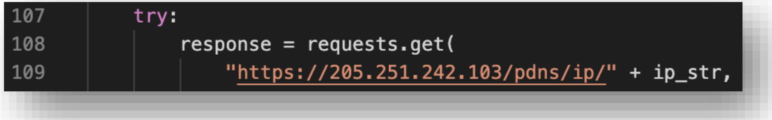
VS



Amazon.co.uk: Low Prices in El

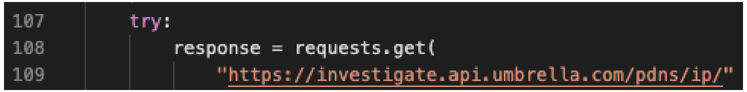
https://www.amazon.com/

Why not use IPs in application code?



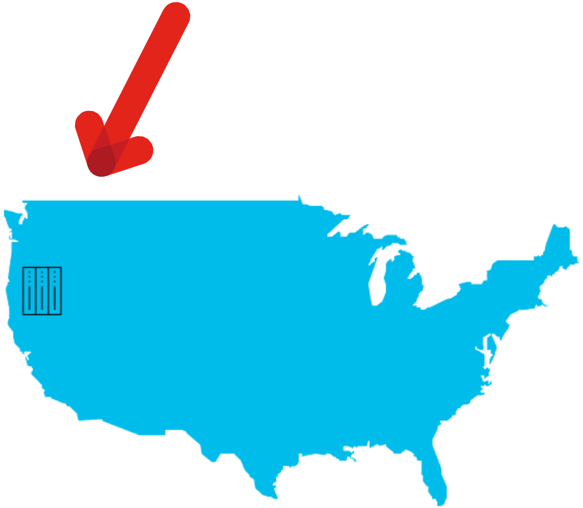
```
    try:
        response = requests.get(
            "https://205.251.242.103/pdns/ip/" + ip_str,
```

VS

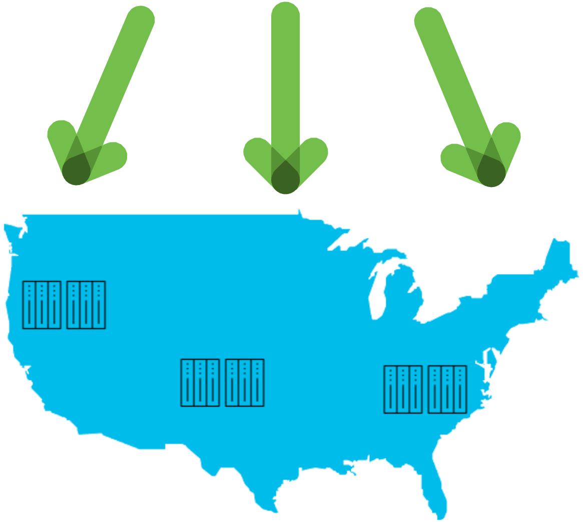


```
    try:
        response = requests.get(
            "https://investigate.api.umbrella.com/pdns/ip/"
```

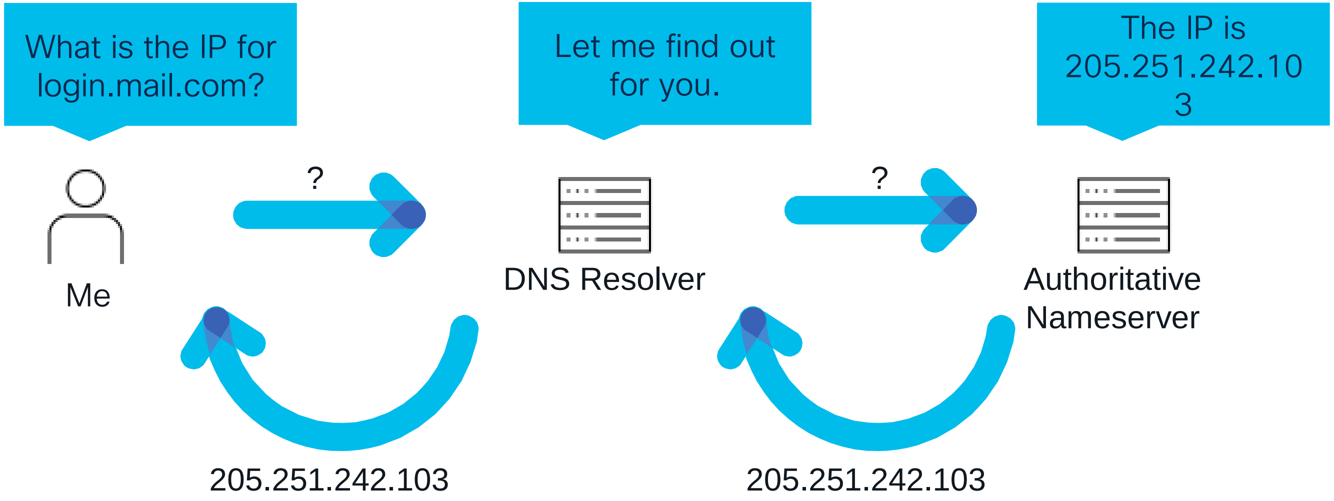
Unicast IP Address



Load Balanced Hostname



DNS Resolvers and Authoritative DNS



What is the IP for login.mail.com?

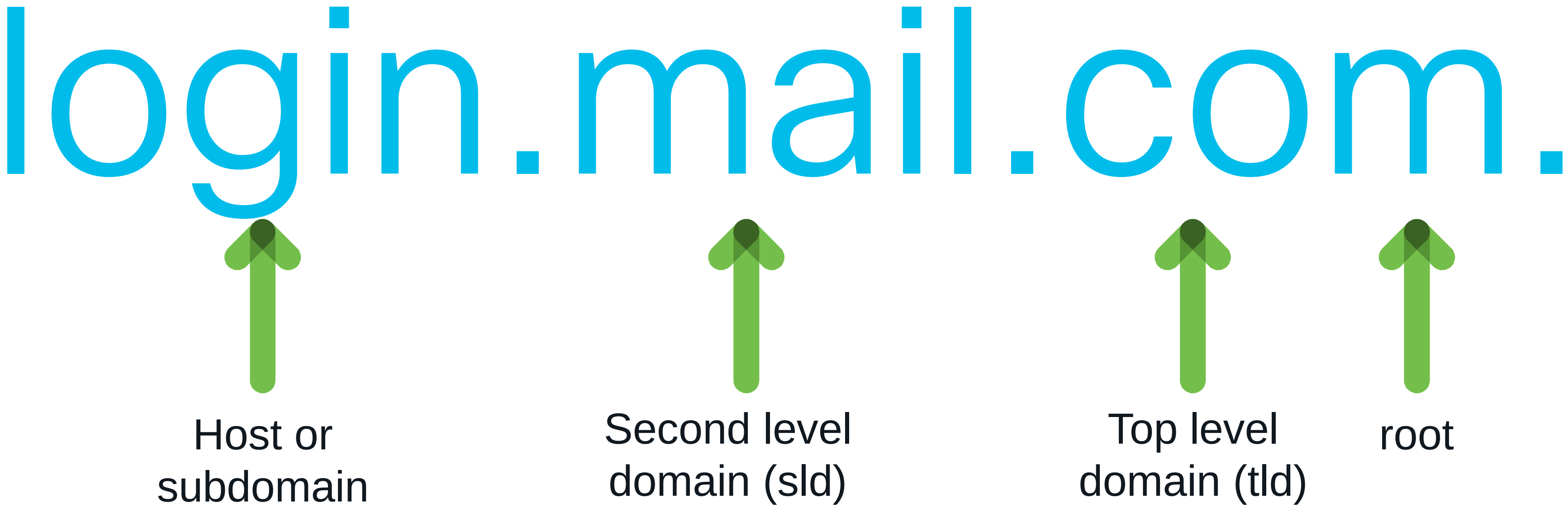
Let me find out for you.

The IP is 205.251.242.10 3

Is it that simple?

No!

Anatomy of a domain



login.mail.com.

Host or subdomain

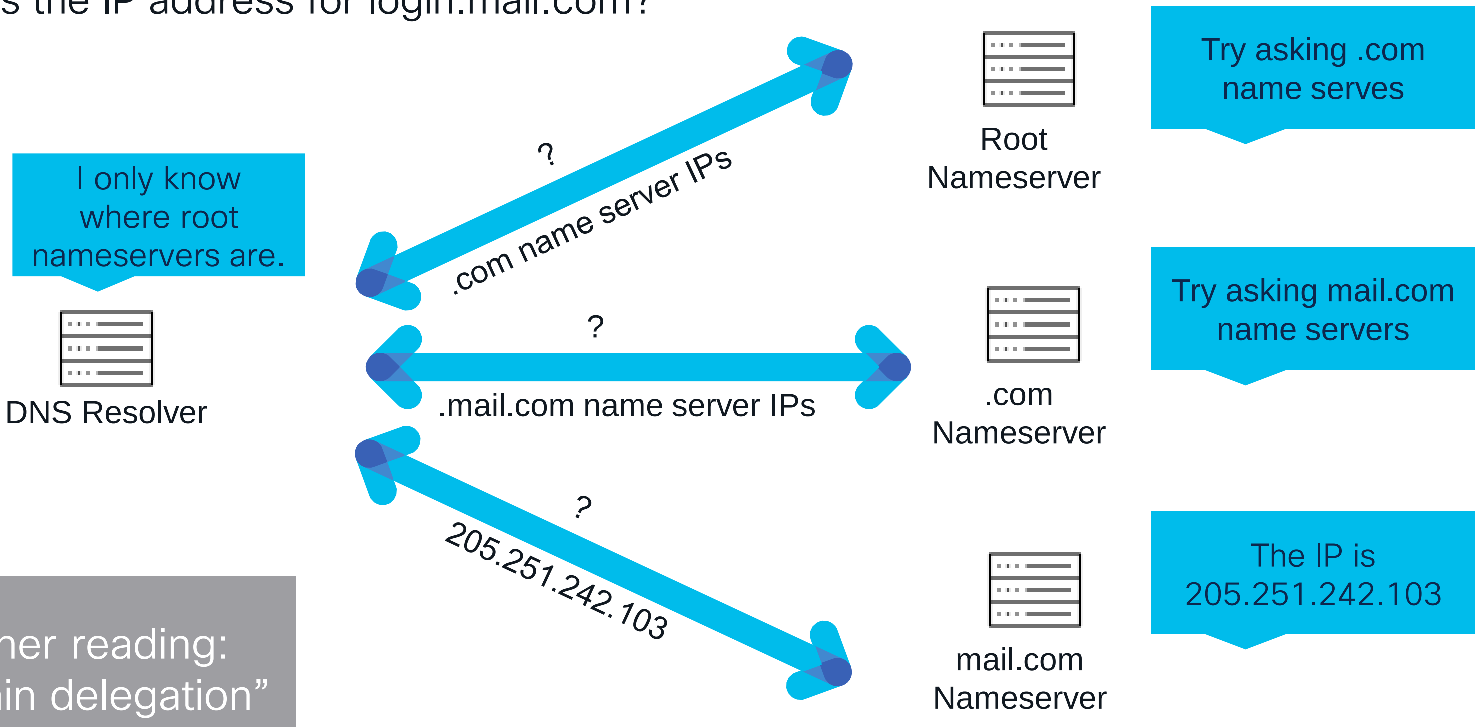
Second level domain (sld)

Top level domain (tld)

root

Recursion: Root, TLD and customer authoritative

What is the IP address for login.mail.com?



I only know where root nameservers are.

DNS Resolver

?

.com name server IPs

Root Nameserver

Try asking .com name serves

?

.mail.com name server IPs

.com Nameserver

Try asking mail.com name servers

?

205.251.242.103

mail.com Nameserver

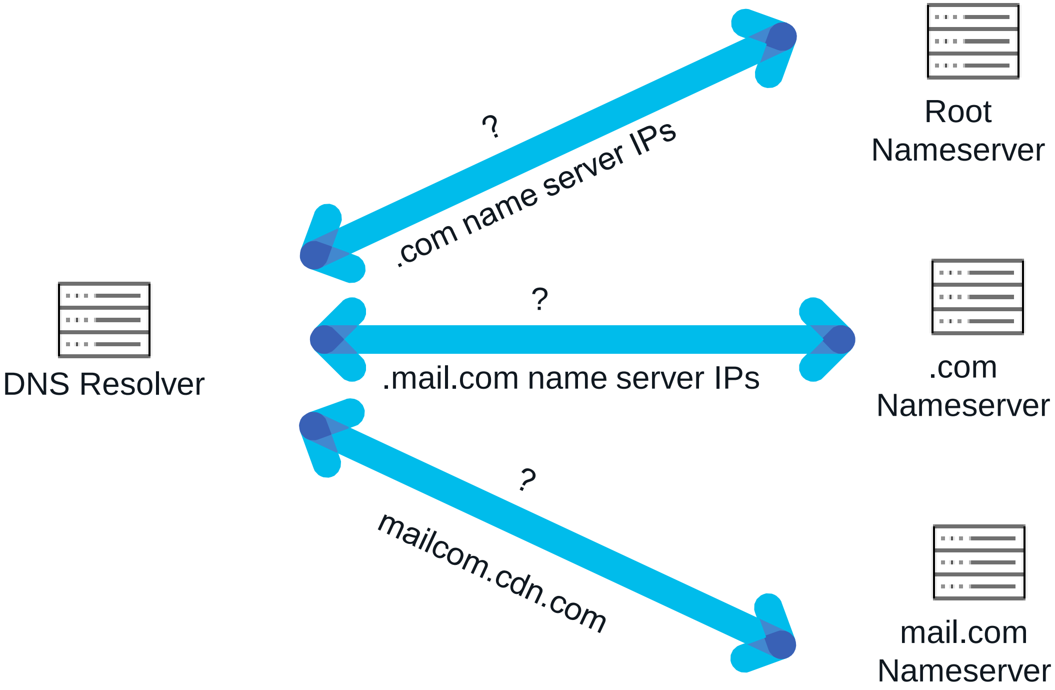
The IP is 205.251.242.103

Further reading: “domain delegation”

How do CDNs add extra DNS complexity?

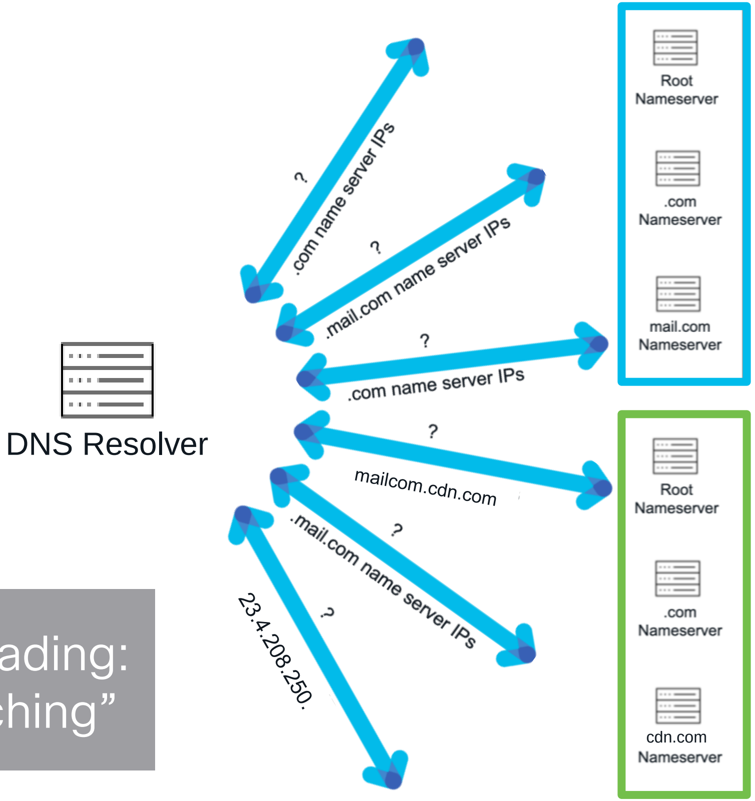
Recursion: CDNs

What is the IP address for login.mail.com?



I don’t have the IP! Ask the CDN’s DNS servers.

Recursion: CDNs

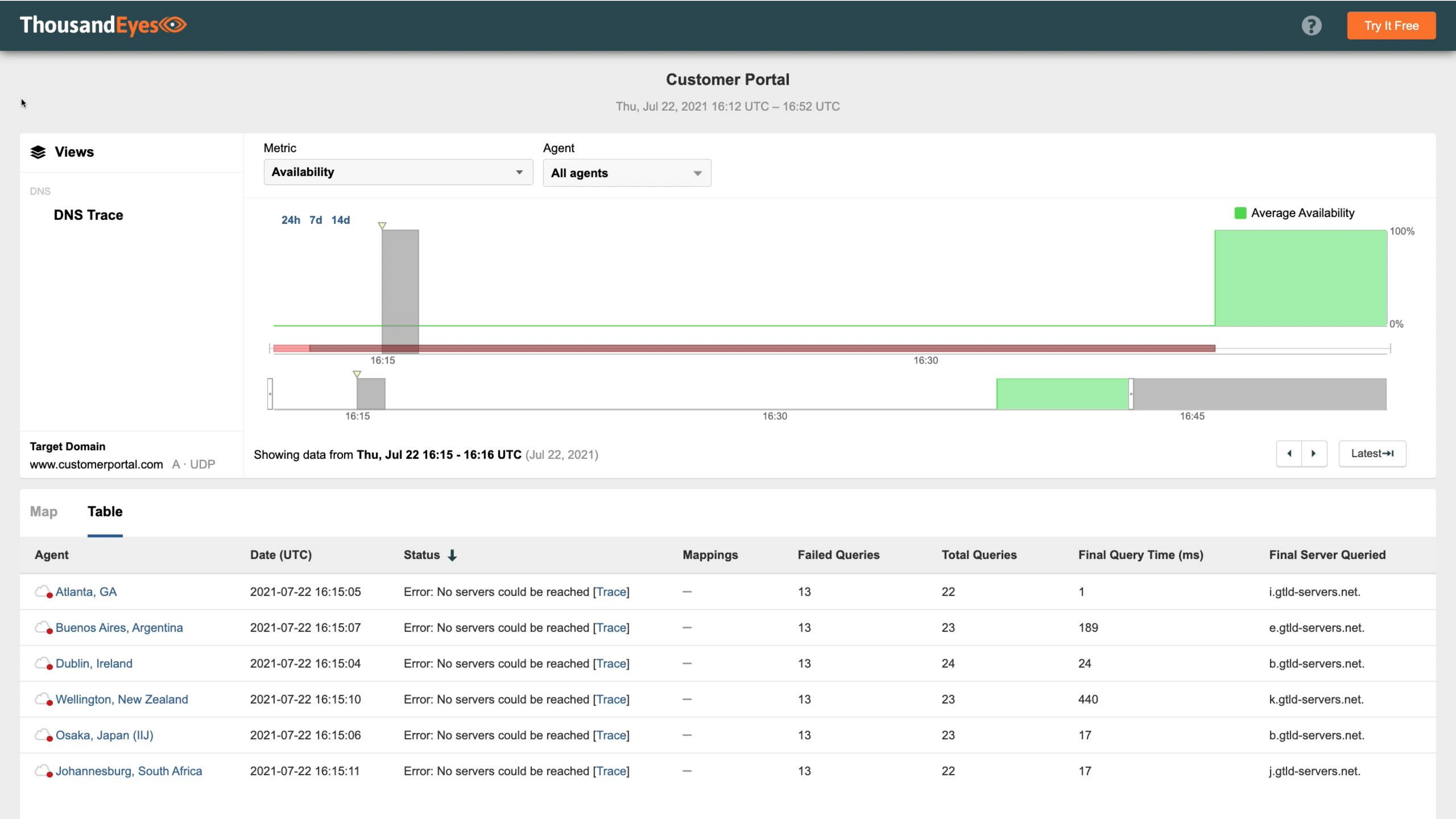


Recursion for login.mail.com

Recursion for mailcom.cdn.com

Further reading: “DNS caching”

Akamai DNS Outage Analysis



Customer Portal

Thu, Jul 22, 2021 16:12 UTC – 16:52 UTC

DNS

DNS Trace

Metric: Availability

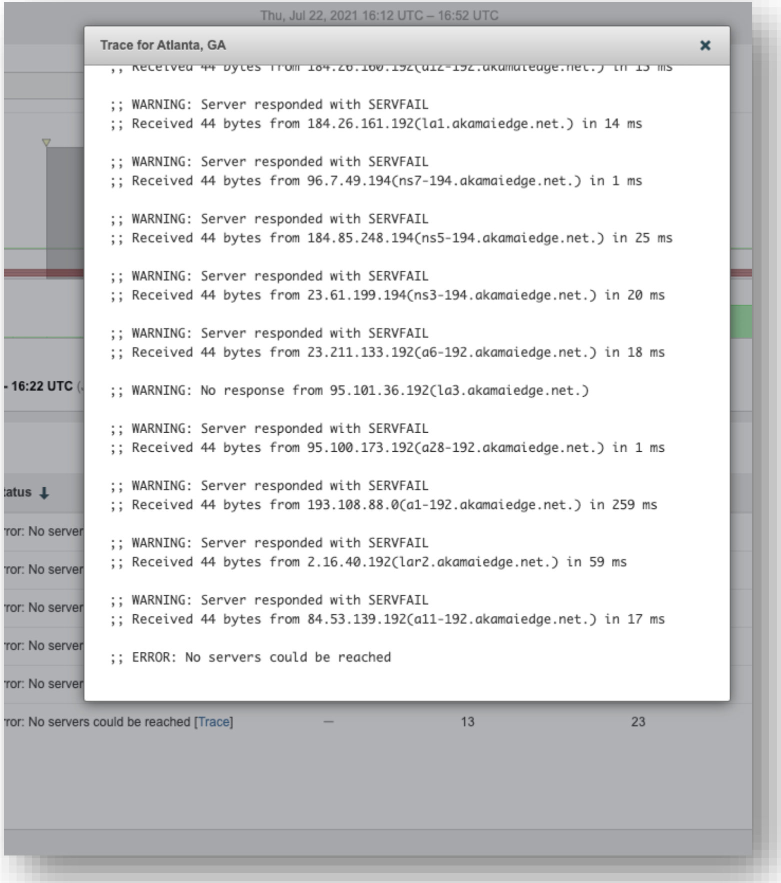
Agent: All agents

Target Domain
www.customerportal.com A · UDP

Showing data from **Thu, Jul 22 16:15 - 16:16 UTC** (Jul 22, 2021)

Agent	Date (UTC)	Status	Mappings	Failed Queries	Total Queries	Final Query Time (ms)	Final Server Queried
Atlanta, GA	2021-07-22 16:15:05	Error: No servers could be reached [Trace]	—	13	22	1	i.gtld-servers.net.
Buenos Aires, Argentina	2021-07-22 16:15:07	Error: No servers could be reached [Trace]	—	13	23	189	e.gtld-servers.net.
Dublin, Ireland	2021-07-22 16:15:04	Error: No servers could be reached [Trace]	—	13	24	24	b.gtld-servers.net.
Wellington, New Zealand	2021-07-22 16:15:10	Error: No servers could be reached [Trace]	—	13	23	440	k.gtld-servers.net.
Osaka, Japan (IIJ)	2021-07-22 16:15:06	Error: No servers could be reached [Trace]	—	13	23	17	b.gtld-servers.net.
Johannesburg, South Africa	2021-07-22 16:15:11	Error: No servers could be reached [Trace]	—	13	22	17	j.gtld-servers.net.

Proactive monitoring and actionable visibility across all authoritative DNS dependencies.



Thu, Jul 22, 2021 16:12 UTC – 16:52 UTC

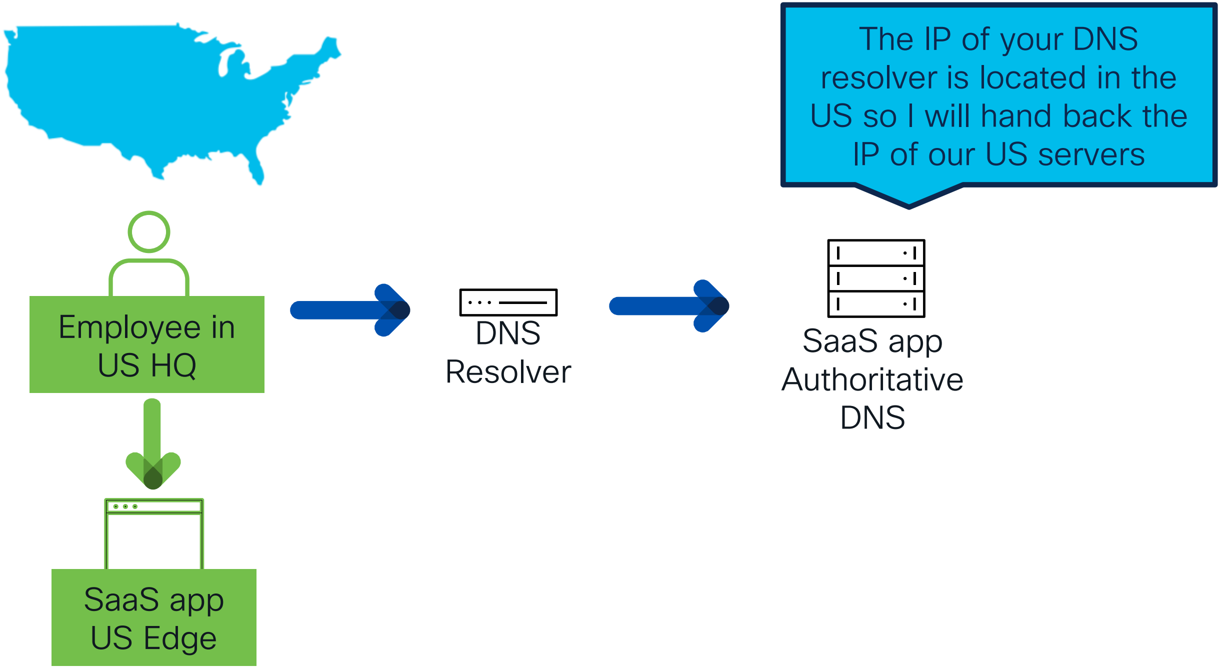
Trace for Atlanta, GA

```
;; Received 44 bytes from 184.26.160.192(a12-192.akamaiedge.net.) in 13 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 184.26.161.192(la1.akamaiedge.net.) in 14 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 96.7.49.194(ns7-194.akamaiedge.net.) in 1 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 184.85.248.194(ns5-194.akamaiedge.net.) in 25 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 23.61.199.194(ns3-194.akamaiedge.net.) in 20 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 23.211.133.192(a6-192.akamaiedge.net.) in 18 ms

;; WARNING: No response from 95.101.36.192(la3.akamaiedge.net.)

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 95.100.173.192(a28-192.akamaiedge.net.) in 1 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 193.108.88.0(a1-192.akamaiedge.net.) in 259 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 2.16.40.192(lar2.akamaiedge.net.) in 59 ms

;; WARNING: Server responded with SERVFAIL
;; Received 44 bytes from 84.53.139.192(a11-192.akamaiedge.net.) in 17 ms

;; ERROR: No servers could be reached
```

Root cause identified in secondary Akamai DNS platform

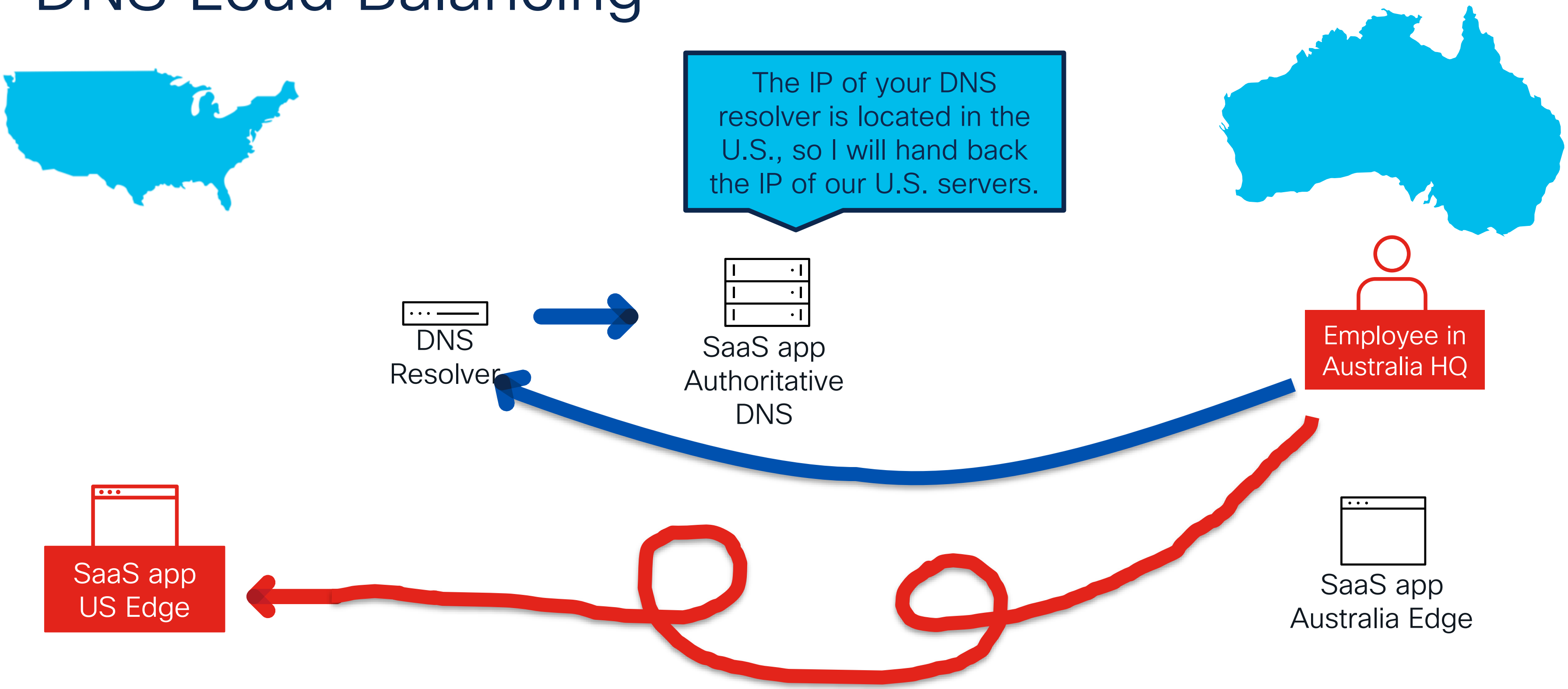
Why should you keep your DNS resolvers close?

DNS Load Balancing



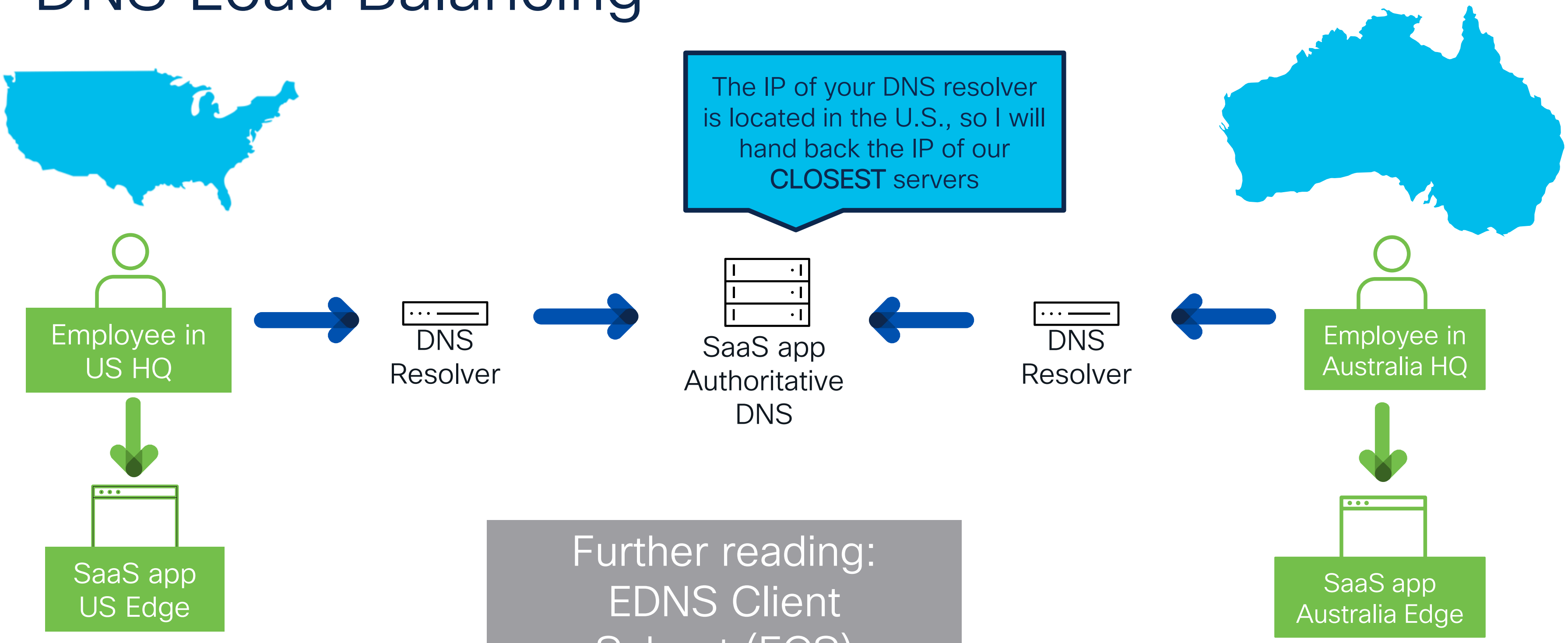
The IP of your DNS resolver is located in the US so I will hand back the IP of our US servers

DNS Load Balancing



The IP of your DNS resolver is located in the U.S., so I will hand back the IP of our U.S. servers.

DNS Load Balancing

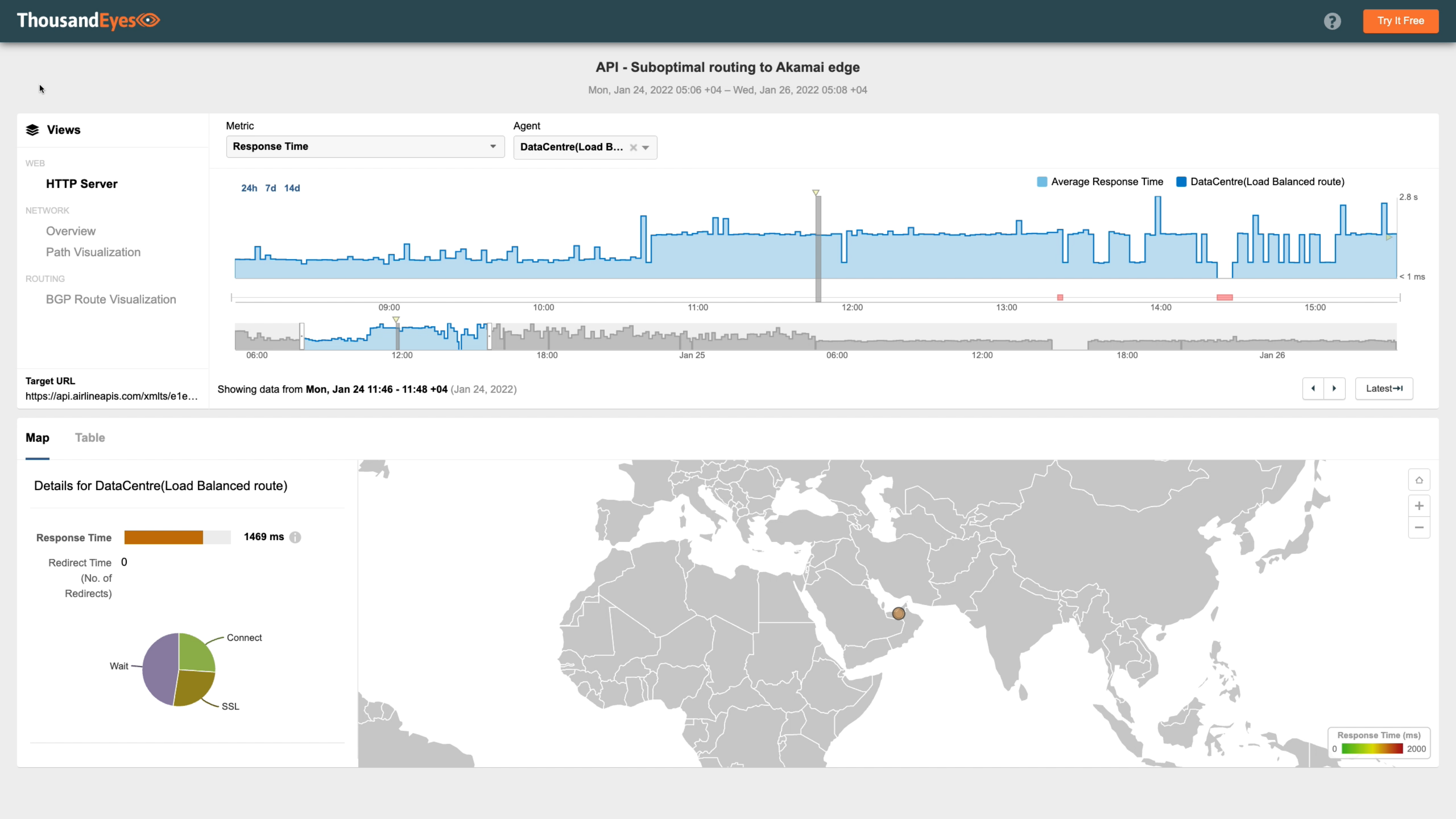


The IP of your DNS resolver is located in the U.S., so I will hand back the IP of our **CLOSEST** servers

Further reading: EDNS Client Subnet (ECS)

How can DNS can be your best weapon against lazy load balancers?

Intentional DNS hijacking example



API - Suboptimal routing to Akamai edge

Mon, Jan 24, 2022 05:06 +04 – Wed, Jan 26, 2022 05:08 +04

Target URL
https://api.airlineapis.com/xmlts/e1e...

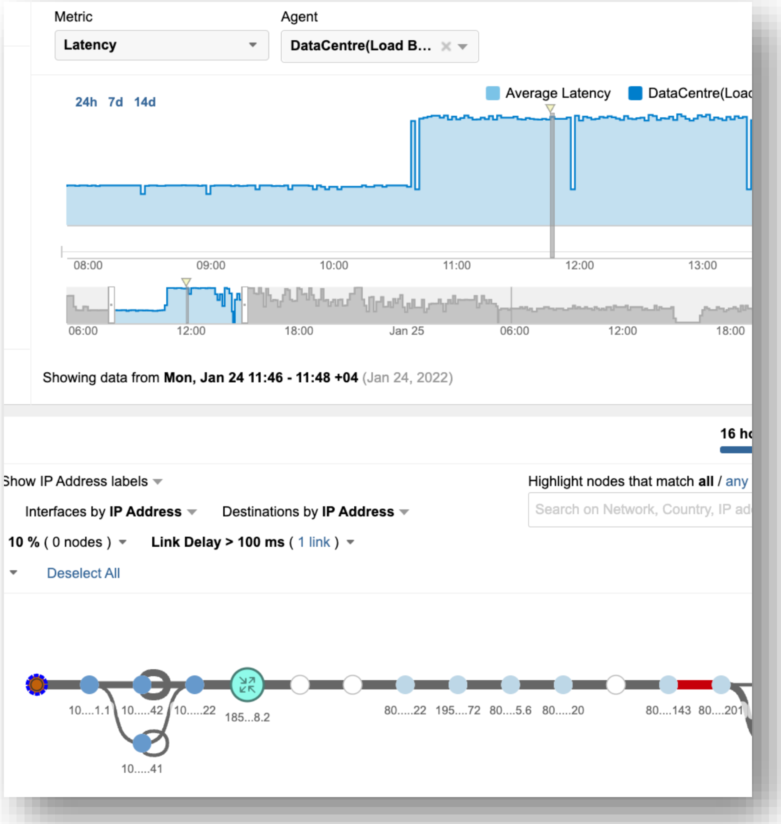
Showing data from **Mon, Jan 24 11:46 - 11:48 +04** (Jan 24, 2022)

Details for DataCentre(Load Balanced route)

Response Time **1469 ms**

Redirect Time (No. of Redirects) 0

Correlate application performance with network visibility for actionable insights.



Metric: Latency

Agent: DataCentre(Load B...

Showing data from **Mon, Jan 24 11:46 - 11:48 +04** (Jan 24, 2022)

Show IP Address labels

Interfaces by **IP Address**

Destinations by **IP Address**

10 % (0 nodes)

Link Delay > 100 ms (1 link)

Deselect All

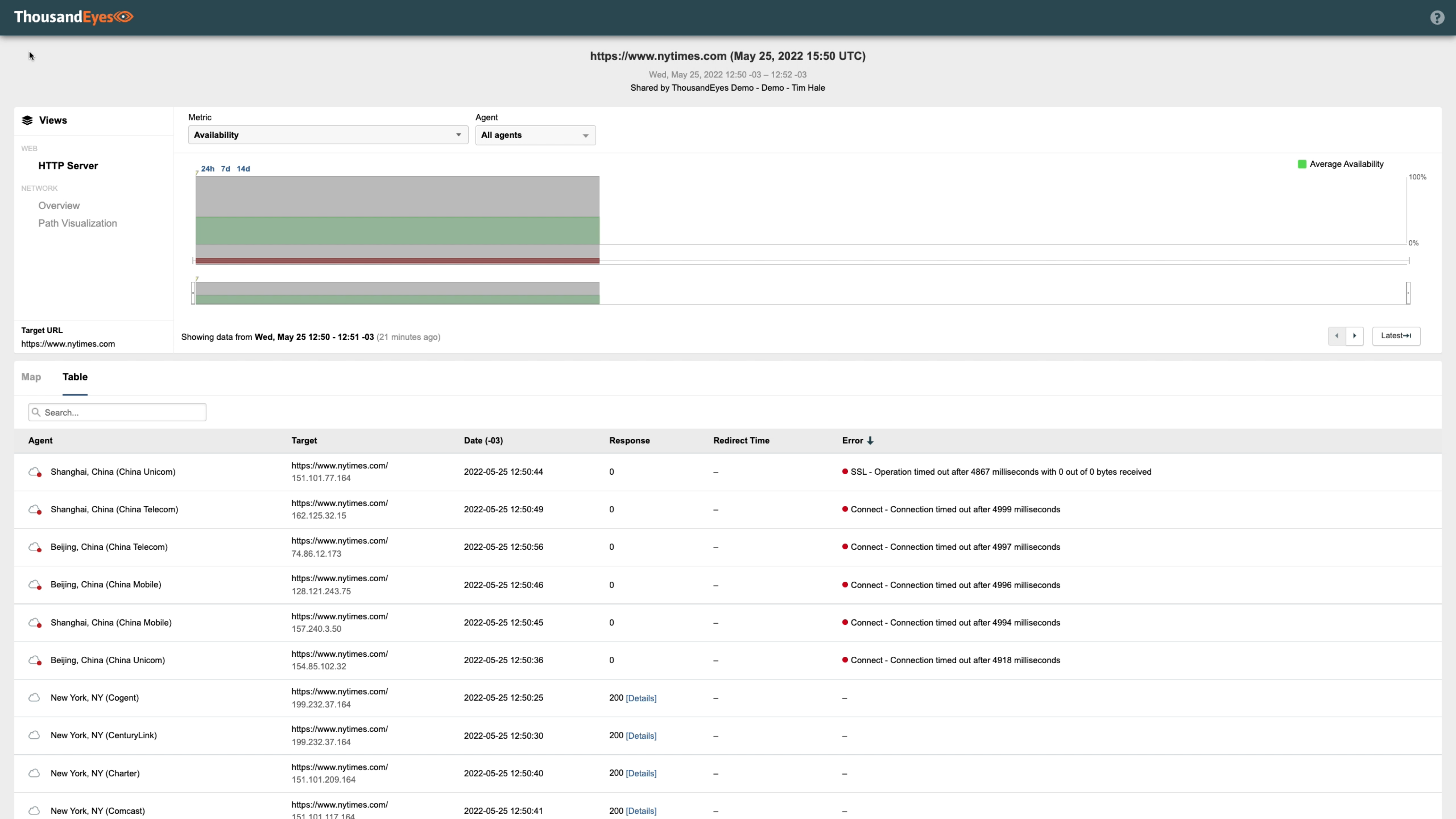
Highlight nodes that match **all** / any

Search on Network, Country, IP ad

API response time increased due to CDN routing traffic sub-optimally

What's up with China and DNS?

China DNS hijacking example



https://www.nytimes.com (May 25, 2022 15:50 UTC)

Wed, May 25, 2022 12:50 -03 – 12:52 -03

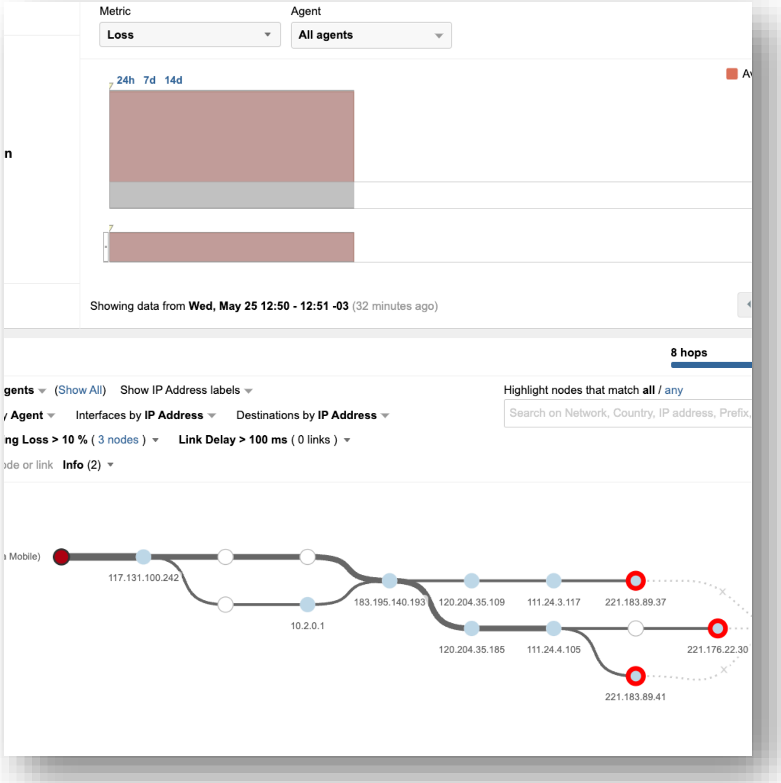
Shared by ThousandEyes Demo - Demo - Tim Hale

Target URL
https://www.nytimes.com

Showing data from **Wed, May 25 12:50 - 12:51 -03** (21 minutes ago)

Agent	Target	Date (-03)	Response	Redirect Time	Error ↓
Shanghai, China (China Unicom)	https://www.nytimes.com/ 151.101.77.164	2022-05-25 12:50:44	0	–	● SSL - Operation timed out after 4867 milliseconds with 0 out of 0 bytes received
Shanghai, China (China Telecom)	https://www.nytimes.com/ 162.125.32.15	2022-05-25 12:50:49	0	–	● Connect - Connection timed out after 4999 milliseconds
Beijing, China (China Telecom)	https://www.nytimes.com/ 74.86.12.173	2022-05-25 12:50:56	0	–	● Connect - Connection timed out after 4997 milliseconds
Beijing, China (China Mobile)	https://www.nytimes.com/ 128.121.243.75	2022-05-25 12:50:46	0	–	● Connect - Connection timed out after 4996 milliseconds
Shanghai, China (China Mobile)	https://www.nytimes.com/ 157.240.3.50	2022-05-25 12:50:45	0	–	● Connect - Connection timed out after 4994 milliseconds
Beijing, China (China Unicom)	https://www.nytimes.com/ 154.85.102.32	2022-05-25 12:50:36	0	–	● Connect - Connection timed out after 4918 milliseconds
New York, NY (Cogent)	https://www.nytimes.com/ 199.232.37.164	2022-05-25 12:50:25	200 [Details]	–	–
New York, NY (CenturyLink)	https://www.nytimes.com/ 199.232.37.164	2022-05-25 12:50:30	200 [Details]	–	–
New York, NY (Charter)	https://www.nytimes.com/ 151.101.209.164	2022-05-25 12:50:40	200 [Details]	–	–
New York, NY (Comcast)	https://www.nytimes.com/ 151.101.117.164	2022-05-25 12:50:41	200 [Details]	–	–

Understand global connectivity and catch issues issues with application dependencies



Metric: Loss

Agent: All agents

24h 7d 14d

Showing data from **Wed, May 25 12:50 - 12:51 -03** (32 minutes ago)

8 hops

gents (Show All) Show IP Address labels

Highlight nodes that match **all** / any

Search on Network, Country, IP address, Prefix,

Agent Interfaces by **IP Address** Destinations by **IP Address**

ng Loss > 10 % (3 nodes) **Link Delay > 100 ms** (0 links)

de or link **Info** (2)

New York Times DNS queries from inside China are hijacked and IPs of SaaS platforms are handed back. Traffic to these IPs is blocked at the network layer.

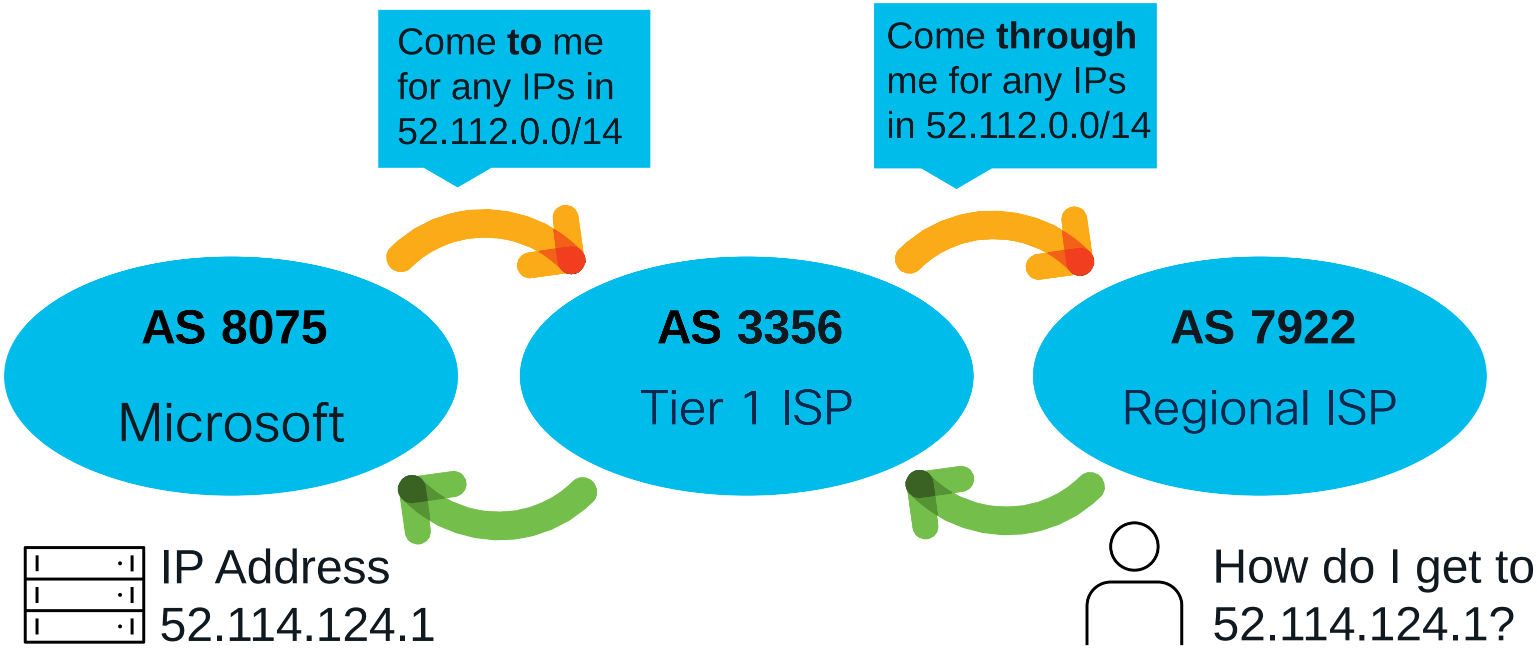
Requirements for successful DNS monitoring

- Test full delegation chain from root all the way to an IP
- Correlate application with DNS health to make monitoring data more business relevant
- Use in protocol DNS tests, just checking port 53 is open or pinging a DNS server is no good
- Correlate DNS with other dependencies such as the network

BGP

Do I need BGP monitoring? For those who have an ASN and those who don’t.

What is BGP?



Come **to** me for any IPs in 52.112.0.0/14

Come **through** me for any IPs in 52.112.0.0/14

AS 8075

Microsoft

AS 3356

Tier 1 ISP

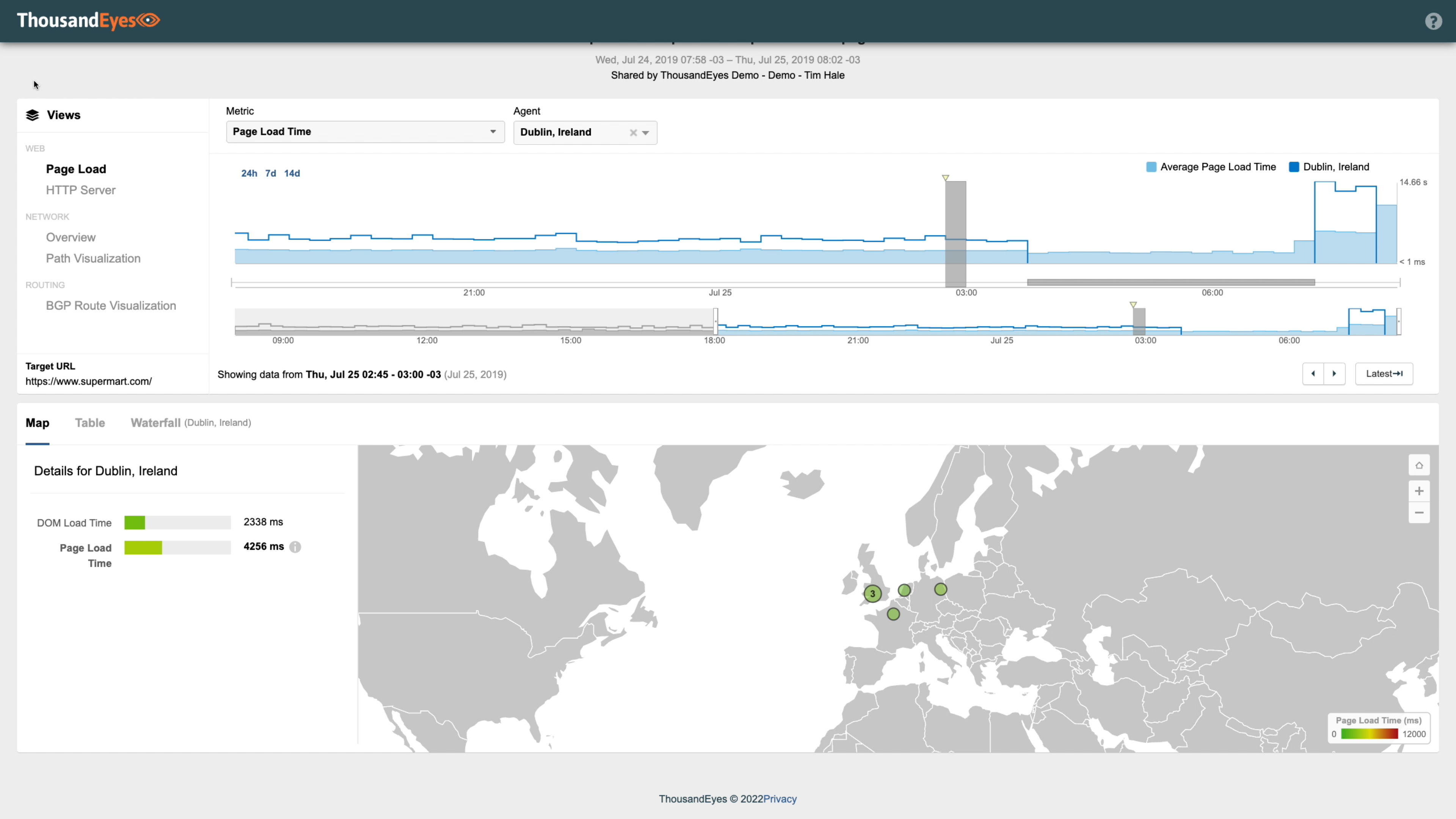
AS 7922

Regional ISP

IP Address 52.114.124.1

How do I get to 52.114.124.1?

CDN Suboptimal routing example



ThousandEyes

Wed, Jul 24, 2019 07:58 -03 – Thu, Jul 25, 2019 08:02 -03

Shared by ThousandEyes Demo - Demo - Tim Hale

Target URL
https://www.supermart.com/

Metric: Page Load Time

Agent: Dublin, Ireland

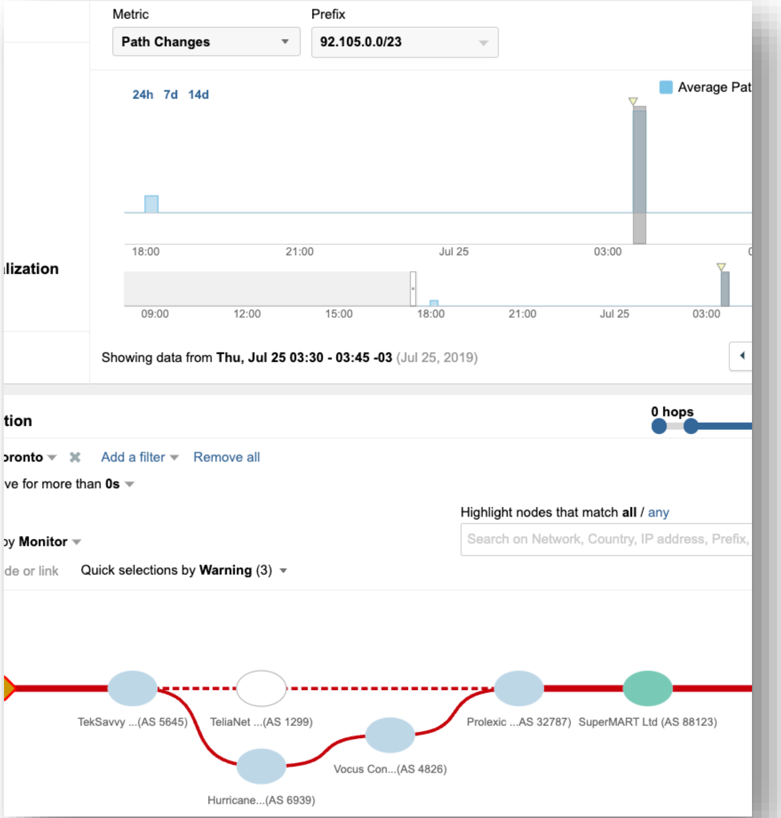
Showing data from **Thu, Jul 25 02:45 - 03:00 -03** (Jul 25, 2019)

Details for Dublin, Ireland

DOM Load Time		2338 ms
Page Load Time		**4256 ms**

ThousandEyes © 2022Privacy

See how third party / your own BGP announcements impact application performance. Use these insights to escalate issues and lower MTTR.



Metric: Path Changes

Prefix: 92.105.0.0/23

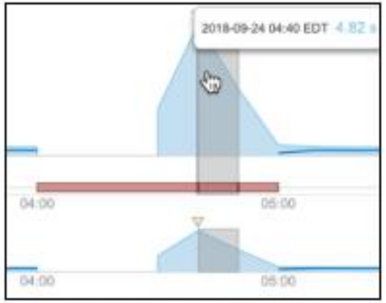
Showing data from Thu, Jul 25 03:30 - 03:45 -03 (Jul 25, 2019)

A BGP change introduced sub optimal routing and pulled traffic originating in Europe into Japan.

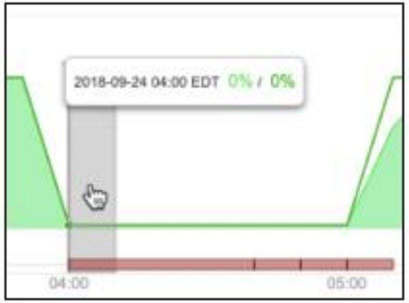
How to turn interesting BGP data into critical visibility

Cross Layer Correlation

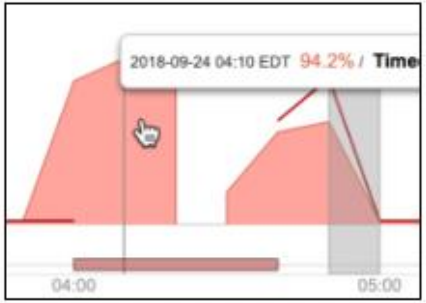
Correlate across multiple layers to show business impact and escalate to correct resolver group



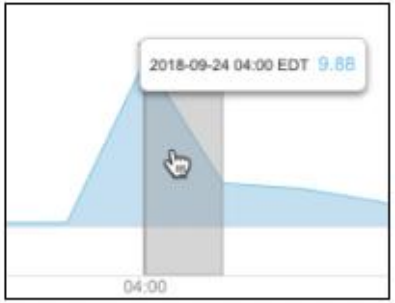
High Page Load



HTTP Availability

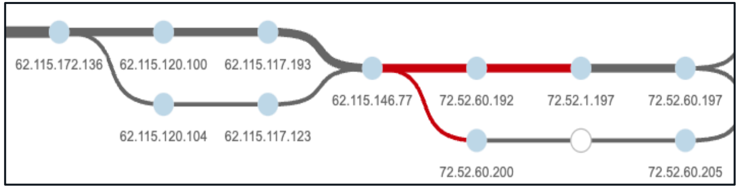


Packet Loss

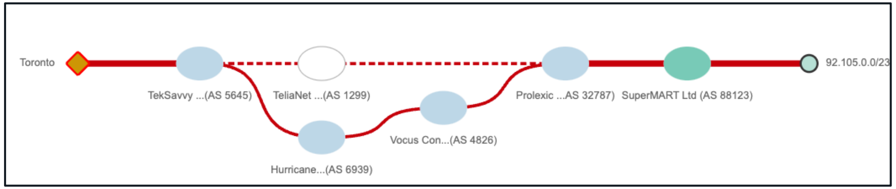


BGP Changes

Visualize network paths and BGP for effective root cause analysis and third-party escalations

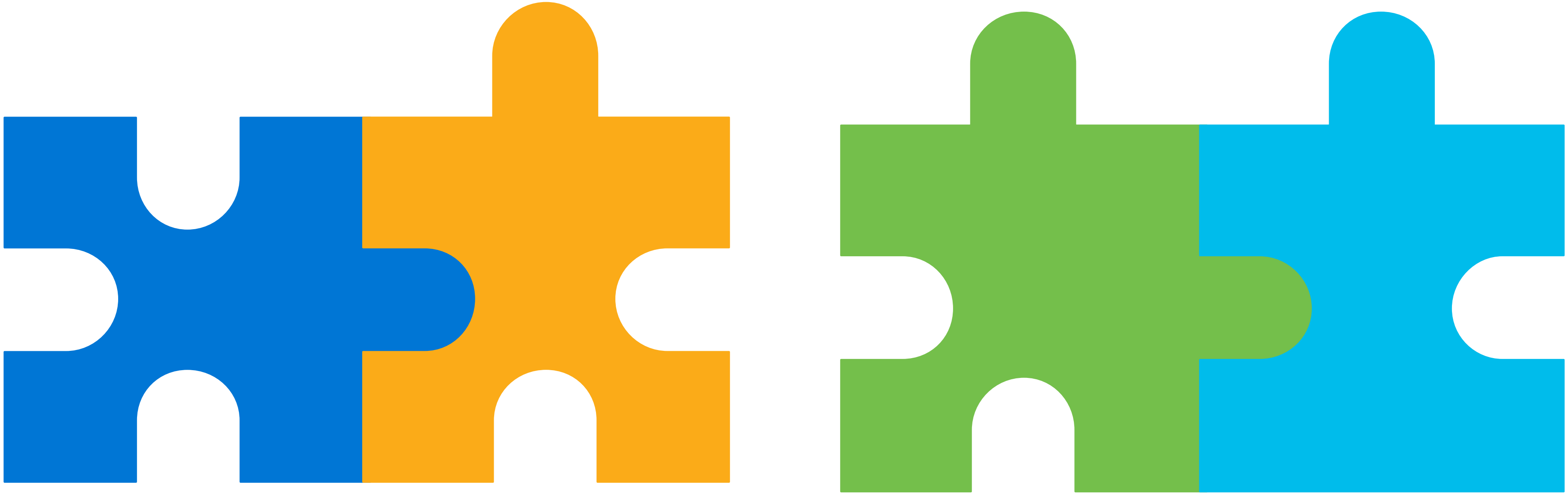


Network Path Visualization



BGP Route Visualization

Don’t leave a missing piece of the puzzle



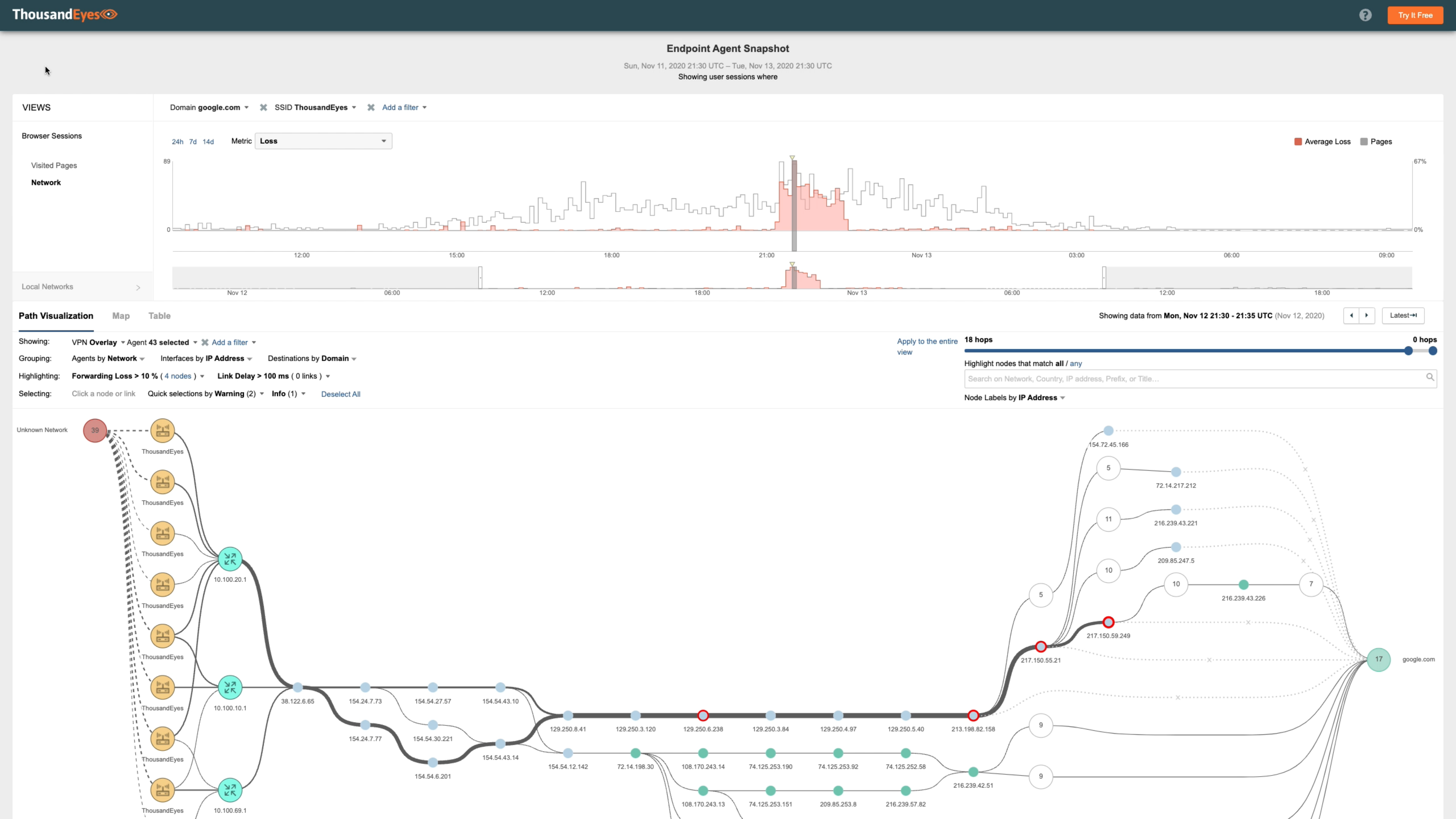
I can see packet loss but why?

BGP Outage!

Why is US traffic being routed via APAC?

BGP Hijack!

Why is my traffic suddenly being routed through country XYZ?



ThousandEyes

Try It Free

Endpoint Agent Snapshot

Sun, Nov 11, 2020 21:30 UTC – Tue, Nov 13, 2020 21:30 UTC
Showing user sessions where

VIEWS

Domain **google.com** ✖ SSID **ThousandEyes** ✖ Add a filter

Browser Sessions

Visited Pages

Network

Local Networks

24h 7d 14d

Metric **Loss**

🟥 Average Loss ▨ Pages

Path Visualization Map Table

Showing data from **Mon, Nov 12 21:30 - 21:35 UTC** (Nov 12, 2020)

Latest

Showing: VPN **Overlay** Agent **43 selected** ✖ Add a filter

Grouping: Agents by **Network** Interfaces by **IP Address** Destinations by **Domain**

Highlighting: **Forwarding Loss > 10 %** (4 nodes) **Link Delay > 100 ms** (0 links)

Selecting: Click a node or link Quick selections by **Warning** (2) **Info** (1) Deselect All

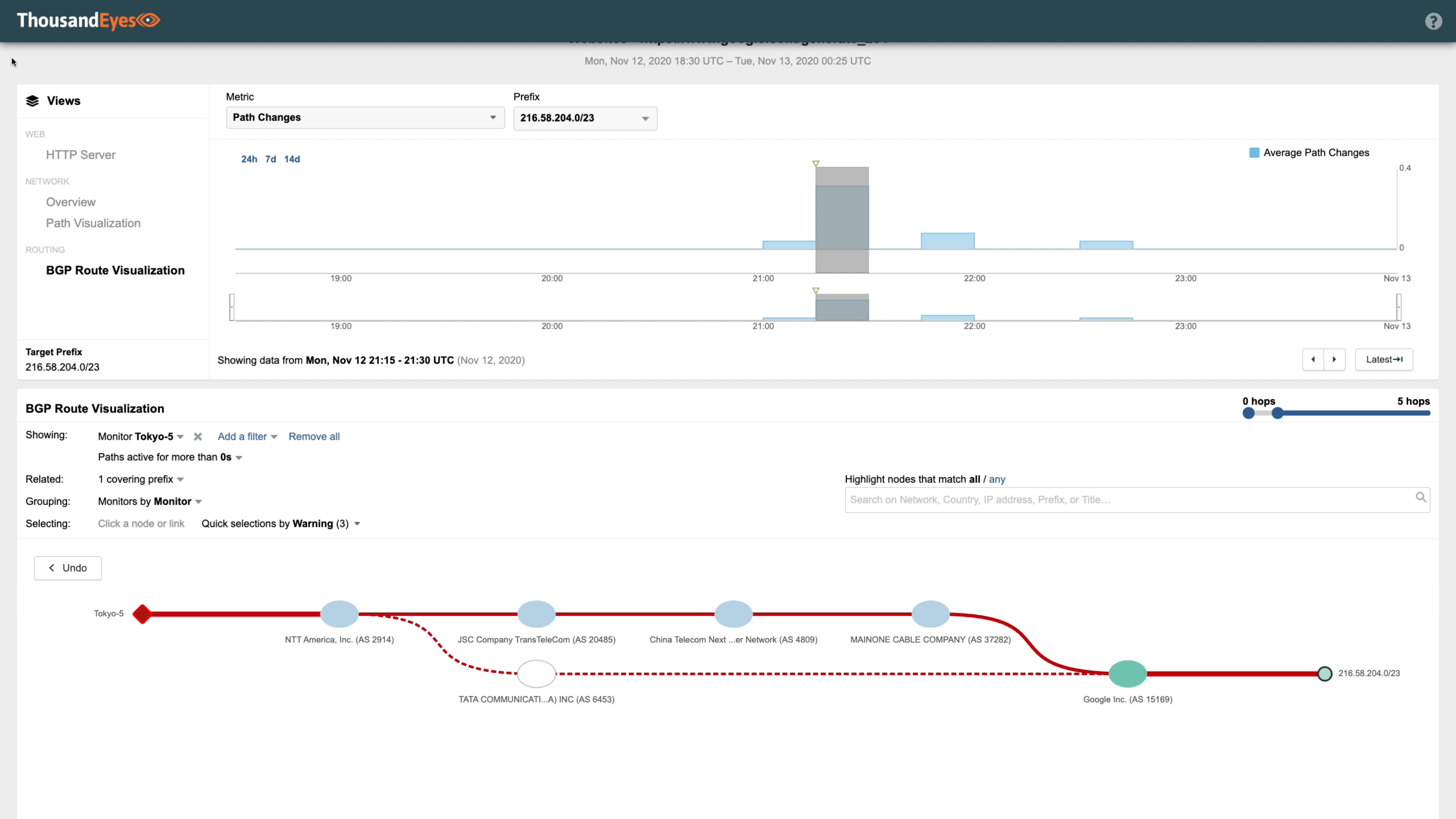
Apply to the entire view

18 hops **0 hops**

Highlight nodes that match **all** / any

Search on Network, Country, IP address, Prefix, or Title...

Node Labels by **IP Address**



Mon, Nov 12, 2020 18:30 UTC – Tue, Nov 13, 2020 00:25 UTC

Target Prefix
216.58.204.0/23

Metric: Path Changes

Prefix: 216.58.204.0/23

Showing data from **Mon, Nov 12 21:15 - 21:30 UTC** (Nov 12, 2020)

BGP Route Visualization

Showing: Monitor **Tokyo-5**

Paths active for more than **0s**

Related: 1 covering prefix

Grouping: Monitors by **Monitor**

Selecting: Click a node or link

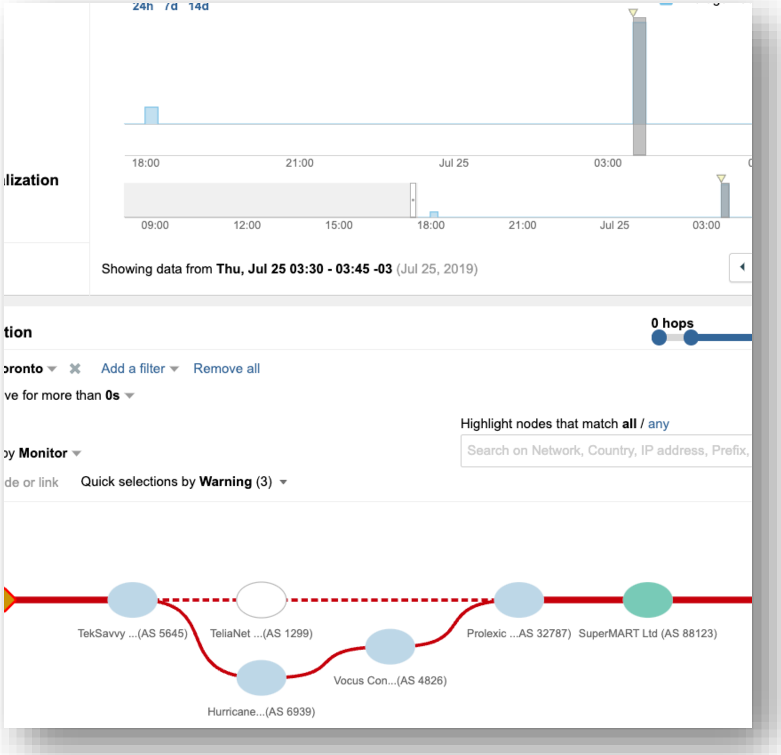
Quick selections by **Warning** (3)

Highlight nodes that match **all** / any

Search on Network, Country, IP address, Prefix, or Title…

Undo
Tokyo-5
NTT America, Inc. (AS 2914)
JSC Company TransTeleCom (AS 20485)
China Telecom Next ...er Network (AS 4809)
MAINONE CABLE COMPANY (AS 37282)
TATA COMMUNICATI...A) INC (AS 6453)
Google Inc. (AS 15169)
216.58.204.0/23

Proactive visibility into large scale internet events and how they impact your business.

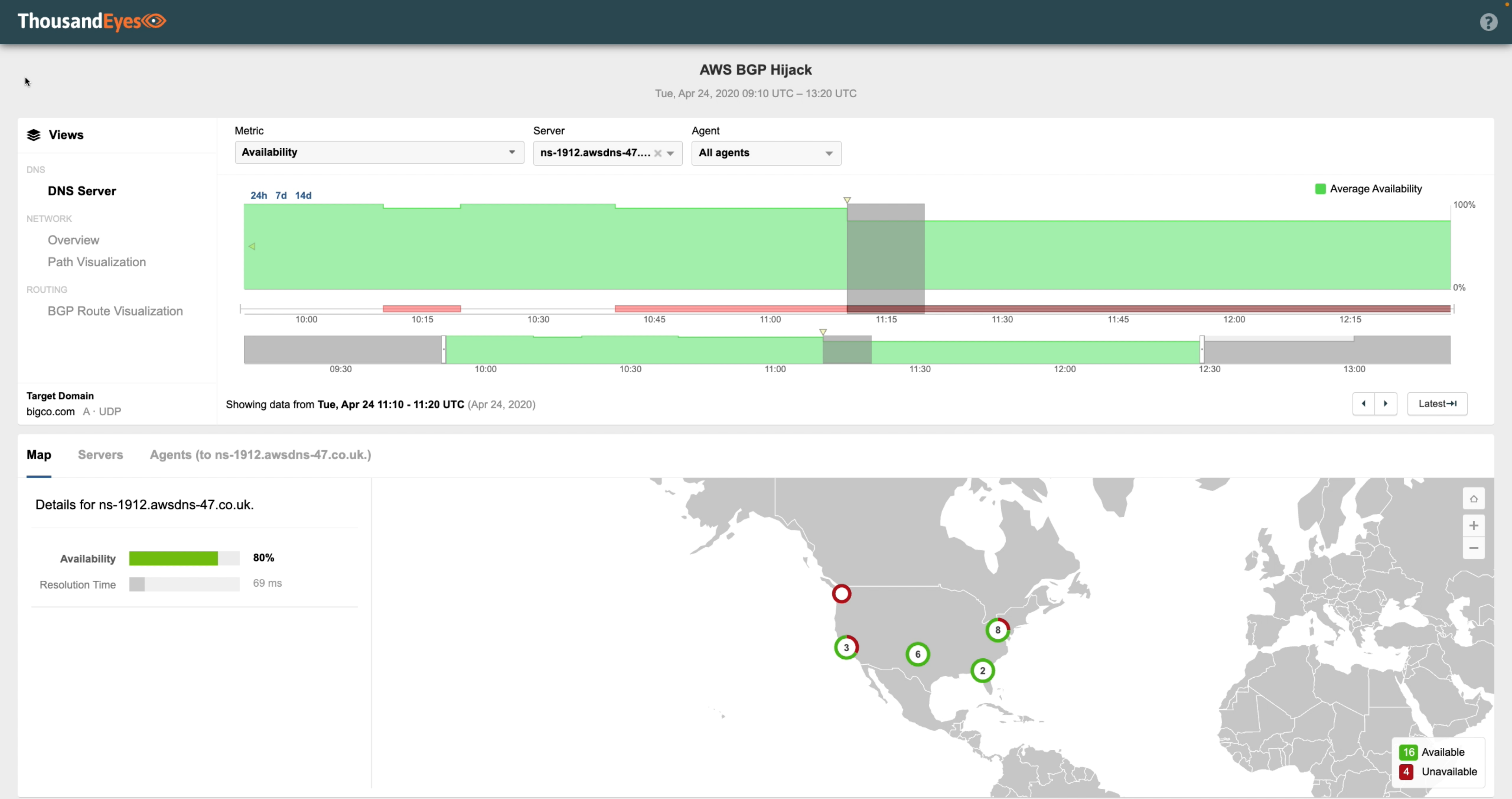


Showing data from **Thu, Jul 25 03:30 - 03:45 -03** (Jul 25, 2019)

Google BGP hijack pulls G-Suite traffic into Russia, China and Nigeria.

When BGP and DNS are weaponized!

Malicious BGP Hijack Example



AWS BGP Hijack

Tue, Apr 24, 2020 09:10 UTC – 13:20 UTC

DNS Server

Metric: Availability

Server: ns-1912.awsdns-47....

Agent: All agents

Target Domain
bigco.com A · UDP

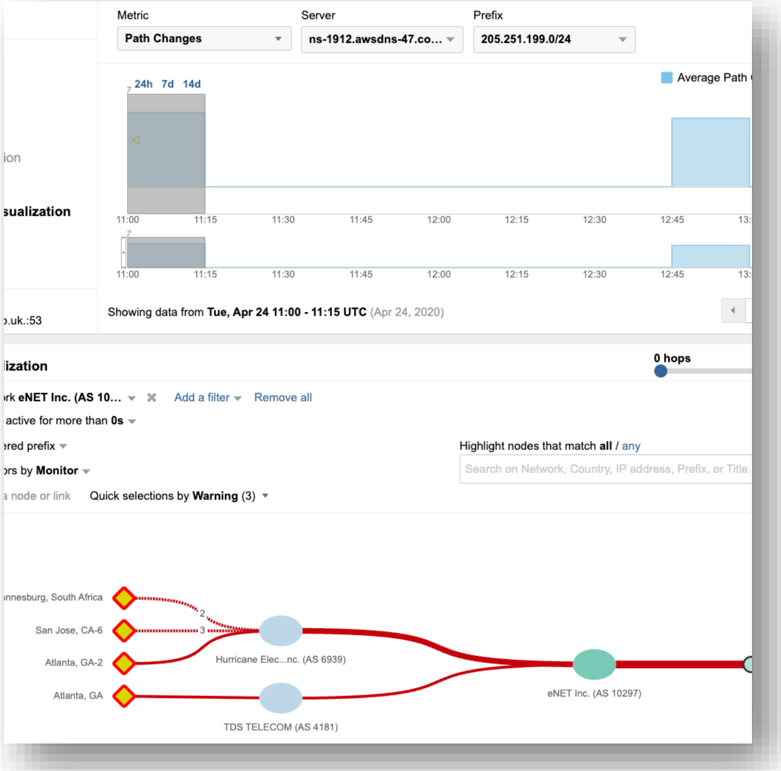
Showing data from **Tue, Apr 24 11:10 - 11:20 UTC** (Apr 24, 2020)

Details for ns-1912.awsdns-47.co.uk.

Availability	80%
Resolution Time	69 ms

16 Available
4 Unavailable

Attacks against third party networks often have major impacts on their customers. Timely data can empower you to act and mitigate sooner, reducing the impact.



Metric: Path Changes

Server: ns-1912.awsdns-47.co...

Prefix: 205.251.199.0/24

Showing data from Tue, Apr 24 11:00 - 11:15 UTC (Apr 24, 2020)

Hackers hijacked an AWS Route 53 prefix pulling traffic to a compromised network where a rogue DNS server route traffic to a bogus website in order to steal cryptocurrency.

Requirements for successful BGP monitoring

Monitor the routine

- Operational policy changes
- Peering changes
- Maintenance
- Intentional handovers (DDoS)

And the unexpected

- Local misconfigurations
- Upstream ISP failures
- Route hijacking and leaks
- Instability and flapping

Correlate BGP visibility with Layer 3 network visibility and application data

Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!

- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.

- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.

Cisco Learning and Certifications

From technology training and team development to Cisco certifications and learning plans, let us help you empower your business and career. www.cisco.com/go/certs

Pay for Learning with Cisco Learning Credits

(CLCs) are prepaid training vouchers redeemed directly with Cisco.

Learn

Cisco U.
IT learning hub that guides teams and learners toward their goals

Cisco Digital Learning
Subscription-based product, technology, and certification training

Cisco Modeling Labs
Network simulation platform for design, testing, and troubleshooting

Cisco Learning Network
Resource community portal for certifications and learning

Train

Cisco Training Bootcamps
Intensive team & individual automation and technology training programs

Cisco Learning Partner Program
Authorized training partners supporting Cisco technology and career certifications

Cisco Instructor-led and Virtual Instructor-led training
Accelerated curriculum of product, technology, and certification courses

Certify

Cisco Certifications and Specialist Certifications
Award-winning certification program empowers students and IT Professionals to advance their technical careers

Cisco Guided Study Groups
180-day certification prep program with learning and support

Cisco Continuing Education Program
Recertification training options for Cisco certified individuals

Here at the event? Visit us at **The Learning and Certifications lounge at the World of Solutions**

Continue your education

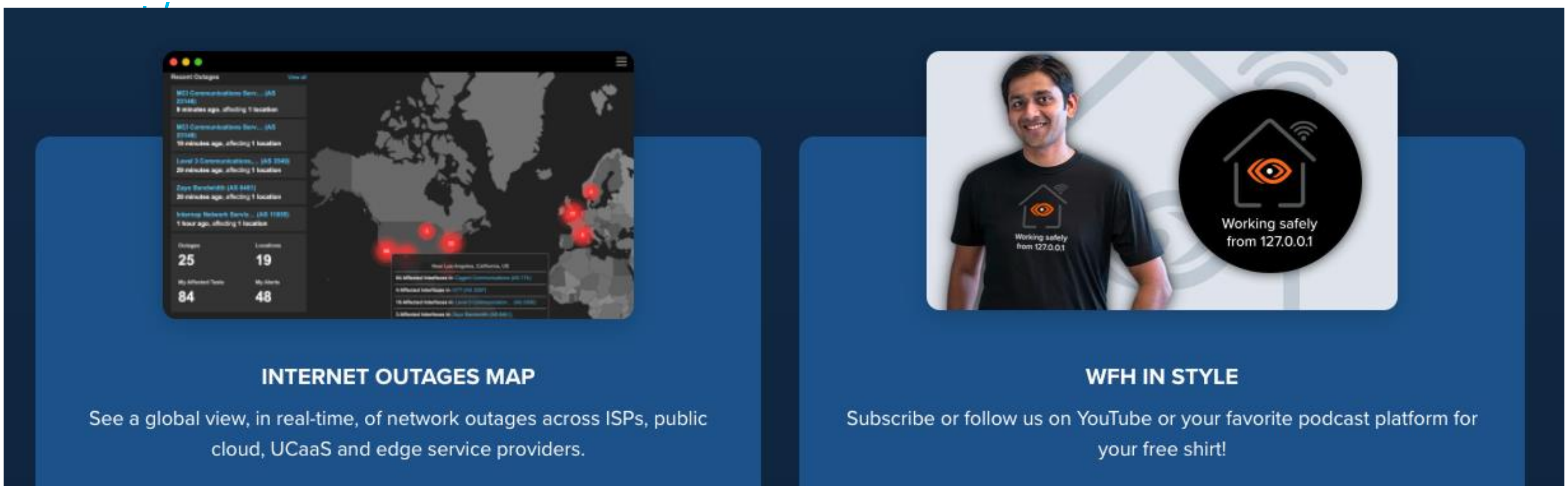
- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Want to know more?

Blog: https://www.thousandeyes.com/blog/

Free trial: https://www.thousandeyes.com/signup/

The internet report: https://www.thousandeyes.com/the-internet-



INTERNET OUTAGES MAP

See a global view, in real-time, of network outages across ISPs, public cloud, UCaaS and edge service providers.

WFH IN STYLE

Subscribe or follow us on YouTube or your favorite podcast platform for your free shirt!

The bridge to possible

Thank you

cisco Live!

#CiscoLive