

23 September 2020

Open Standards Everywhere (OSE)

2020 Africa Chapters Workshop



Dan York

Project Lead, Open Standards Everywhere

york@isoc.org

Training Objective

Improve the availability and security
of your web server(s)
using open Internet standards.



The Open Standards Everywhere project team



Dan York, Project Lead

- Overall coordination, testing, speaking, writing, GitHub, Docker



Gregg Lechner, Implementation Lead

- Building/configuring servers, creating raw documentation, fixing ISOC sites



Ashlyn Wittwer, Documentation Lead, French assistance

- Documenting what we did to make the servers work, delivering French training



Susannah Gray, Communications Lead

- Developing and executing our plans to communicate about the project



Israel Rosas, Spanish assistance

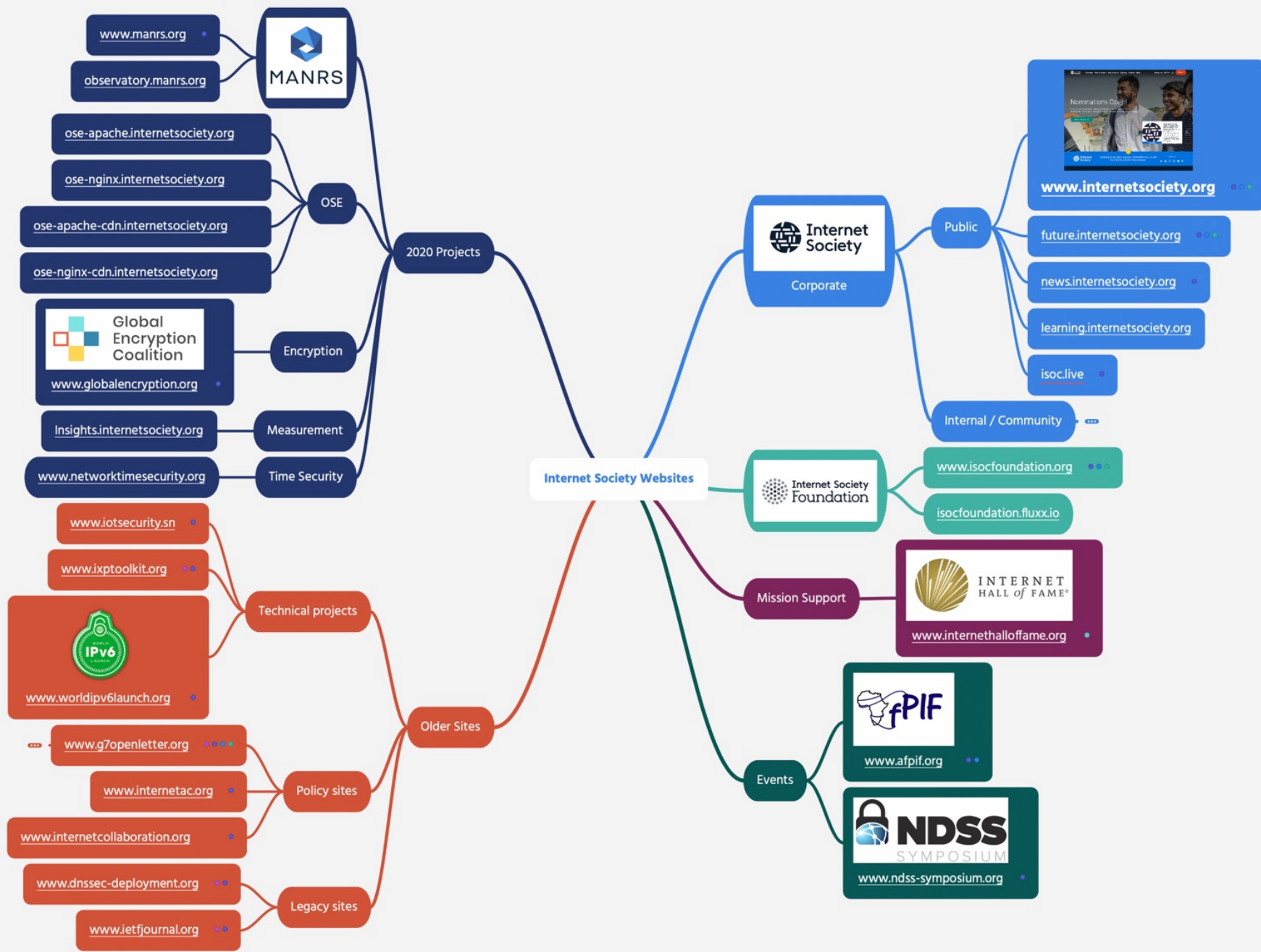
- Delivering Spanish training, engaging with our community in Spanish



<https://www.internetsociety.org/ose/>

Once upon a time...







Internet.nl supported by Dutch Internet Standards Platform



Modern Internet standards

Connection test

- IPv6
- DNSSEC

Website test

- IPv6
- DNSSEC
- HTTPS
- Application security & privacy options

Email test

- IPv6
- DNSSEC
- DMARC, DKIM, SPF
- STARTTLS + DANE



Running the Website Test (March 2019)...

Site	IPv6	DNSSEC	HTTPS	HSTS	Internet.nl	TLS 1.3	HTTP/2	Audit date
www.internetsociety.org	Y	Y	Y	Y	100%	N	Y	3/25/19
future.internetsociety.org	N	Y	Y	N	78%	N	N	3/25/19
assets.internetsociety.org	N	N	Y	Y	55%	N	Y	3/25/19
apps.internetsociety.org	Y	Y	Y	N	94%	N	N	3/25/19
inforum.internetsociety.org	N	Y	Y	Y	81%	Y	N	4/8/19
www.isocfoundation.org	N	N	Y	N	52%	N	Y	3/25/19
www.manrs.org	Y	N	Y	N	70%	N	Y	3/25/19
observatory.manrs.org	N	Y	Y	N	94%	N	N	3/26/19
www.internethalloffame.org	Y	Y	Y	Y	100%	N	N	3/26/19
www.afpif.org	Y	N	Y	N	70%	N	N	3/26/19
www.ndss-symposium.org	Y	N	Y	N	71%	N	Y	3/26/19
www.ietfjournal.org	Y	N	Y	N	70%	N	N	3/26/19
www.dnssec-deployment.org	Y	Y	Y	N	94%	N	N	3/26/19
www.internetac.org	Y	N	Y	N	70%	N	Y	3/26/19
www.ixptoolkit.org	Y	Y	Y	N	91%	N	N	3/26/19
www.iotsecurity2018.ca	N	N	Y	N	37%	N	N	3/26/19
www.iotsecurity.sn	Y	N	Y	N	70%	N	Y	3/26/19
www.worldipv6launch.org	Y	N	Y	N	68%	N	Y	3/25/19
Percentage compliant	67%	44%	100%	22%	76%	6%	44%	
The sites below are additional websites where changes may be made in the future.								
www.connect-smart.org	N	N	Y	N	52%	N	N	3/26/19
www.openwsis2015.org	Y	Y	Y	N	94%	N	N	4/8/19
www.otalliance.org	N	Y	Y	N	79%	N	N	4/8/19
Percentage compliant	33%	67%	100%	0%	76%	0%	0%	



Activity – Test your site with Internet.nl

Go to <https://internet.nl/> and do the website test



“Oh, sure, we can fix those up!”



...





...

...



...

...

...

“So, about those web servers...”



*“We need to make this easier for
system administrators like me!”*



Sli.do – How did your site do?



The Open Standards Everywhere Project

An Internet Society Action Plan 2020 Project



Open standards are a fundamental
building block
of an
open Internet



IP TCP UDP HTTP(S)

SSH TLS SMTP FTP

QUIC NTP XMPP

DNS BGP SNMP

WebRTC SIP



Open Internet standards are...

... open to all to read/access

... open to all to create

... open / free to all to use



Open Architecture of Interoperable and Reusable Building Blocks

based on open standards
development processes voluntarily
adopted by a user community.

IWN Critical Property #2



We want **open standards** to be **everywhere!**

(Including our own sites and services)



Open Standards Everywhere (OSE) Project Goals - 2020

Build and deploy reference web servers

- Show what a "good site" looks like

Document our work

- Explain how we configured the servers

Promote the documentation

- Share the documentation so that people can learn how to configure their web servers

Lead by example

- Configure as many Internet Society sites as possible



Open

- Based on agreed-upon, voluntary standards that anyone can use to connect with other systems

Globally-connected

- **IPv6** – Native connections for new networks (especially mobile)
- **HTTP/2** – Faster connections work better for low bandwidth, mobile

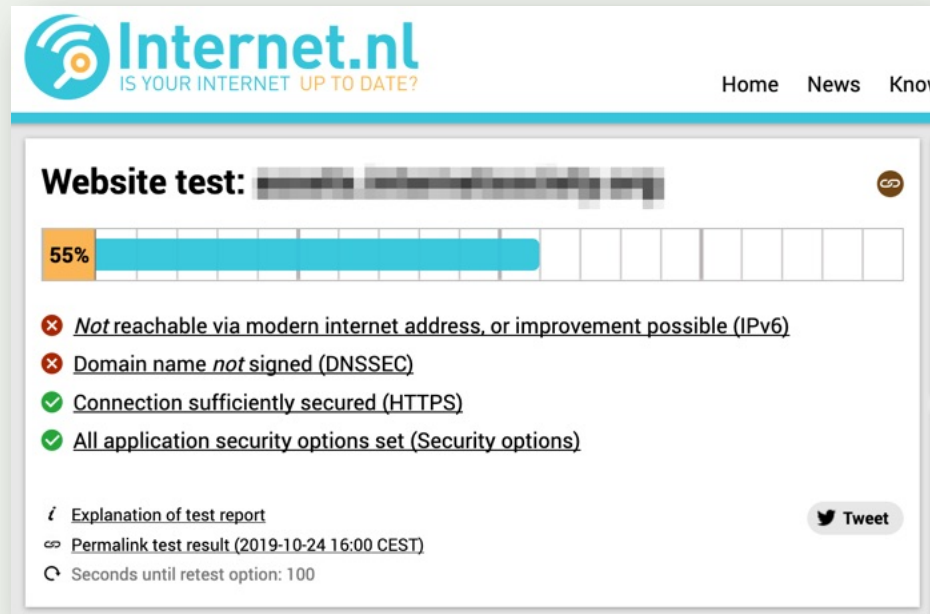
Secure and trustworthy

- **DNSSEC**
- **TLS 1.3**, HSTS, and more



Test framework – Internet.nl and http2.pro

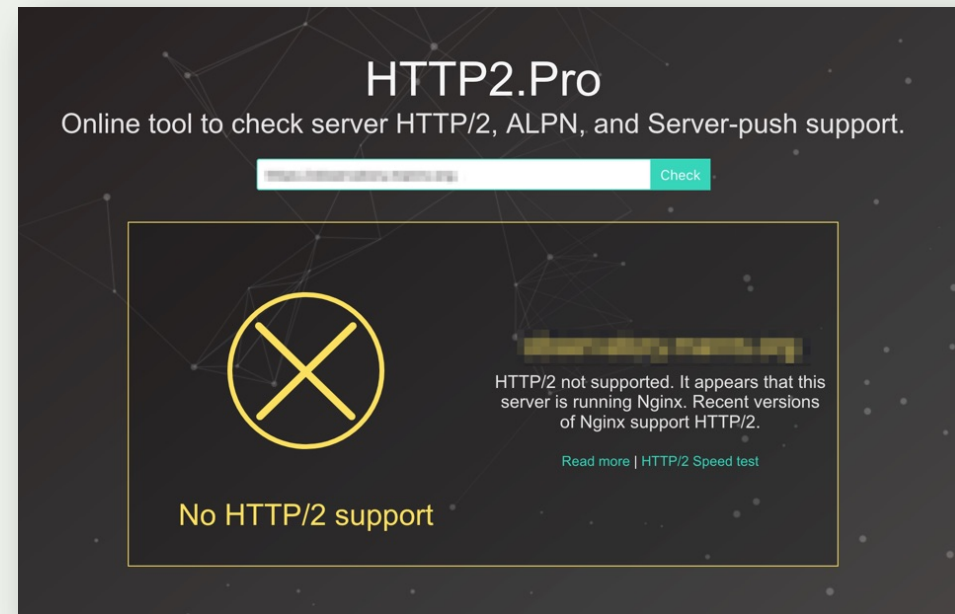
- <https://internet.nl/>
 - IPv6, DNSSEC, HTTPS/TLS, including TLS 1.3, HSTS, more
- <https://http2.pro/>
 - HTTP/2



The screenshot shows the Internet.nl website with the header "Internet.nl IS YOUR INTERNET UP TO DATE?". The main content area is titled "Website test:" and displays a progress bar at 55%. Below the progress bar, there are four items in a list:

- ✗ Not reachable via modern internet address, or improvement possible (IPv6)
- ✗ Domain name *not* signed (DNSSEC)
- ✓ Connection sufficiently secured (HTTPS)
- ✓ All application security options set (Security options)

At the bottom, there is a "Tweet" button and a "Permalink test result (2019-10-24 16:00 CEST)" link. A small icon in the bottom left corner indicates the time until the next test: "Seconds until retest option: 100".

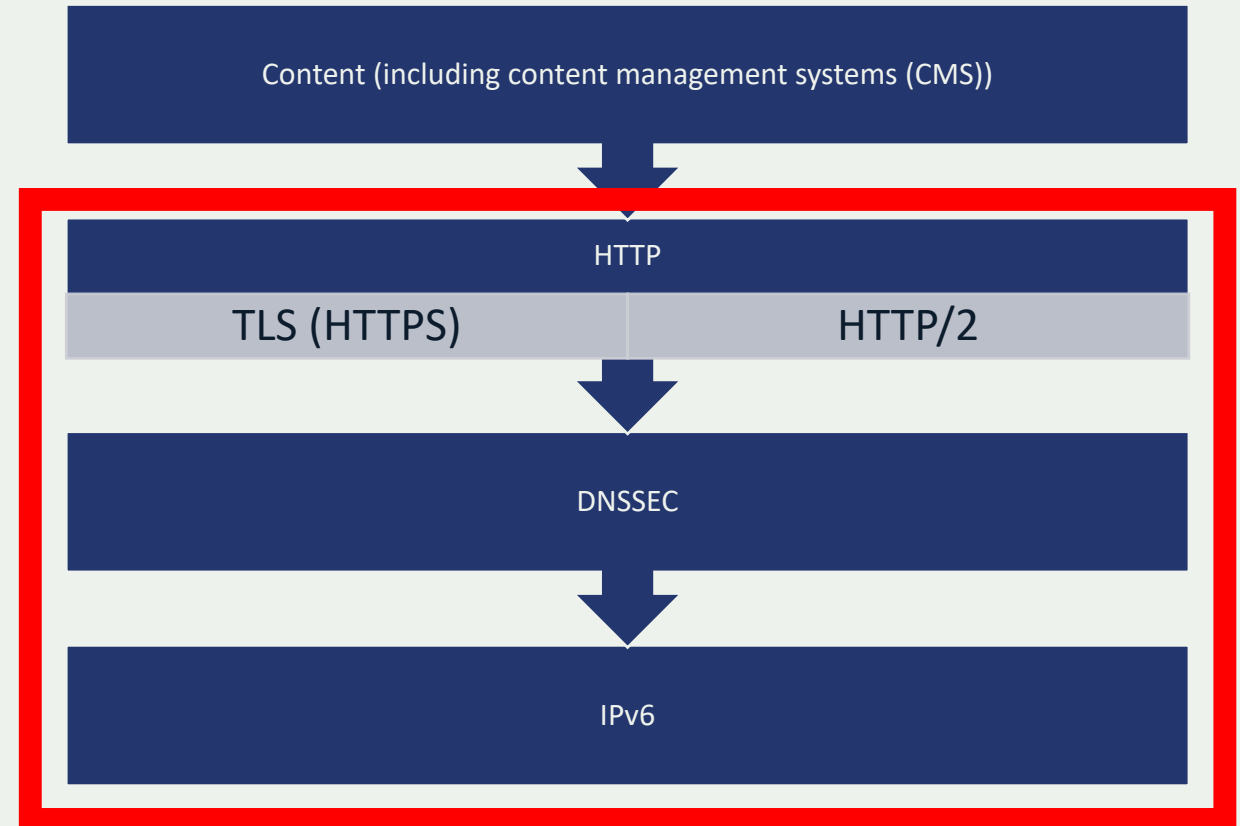


The screenshot shows the HTTP2.Pro website with the header "HTTP2.Pro Online tool to check server HTTP/2, ALPN, and Server-push support.". The main content area features a large yellow "X" icon and the text "No HTTP/2 support". Below this, a message states: "HTTP/2 not supported. It appears that this server is running Nginx. Recent versions of Nginx support HTTP/2." A link "Read more | HTTP/2 Speed test" is provided at the bottom.



Scope in 2020 – Web servers

- OSE project is focusing on security and standards of **the connections to a web server**
- **NOT** focused on **content** of web sites.
- Out of scope:
 - Web site design, presentation
 - Content management systems
 - Accessibility
 - Mobile usability
 - Page speed performance



Scope - Three types of web servers

"Self-hosted" on a server or virtual machine

- You have command-line access and can configure files.

Hosted with a website hosting provider

- You do NOT have command-line access. You typically use web administration forms and are limited in what you can do.

Content delivery networks (CDNs)

- You use a CDN in front of your self-hosted or hosted website.

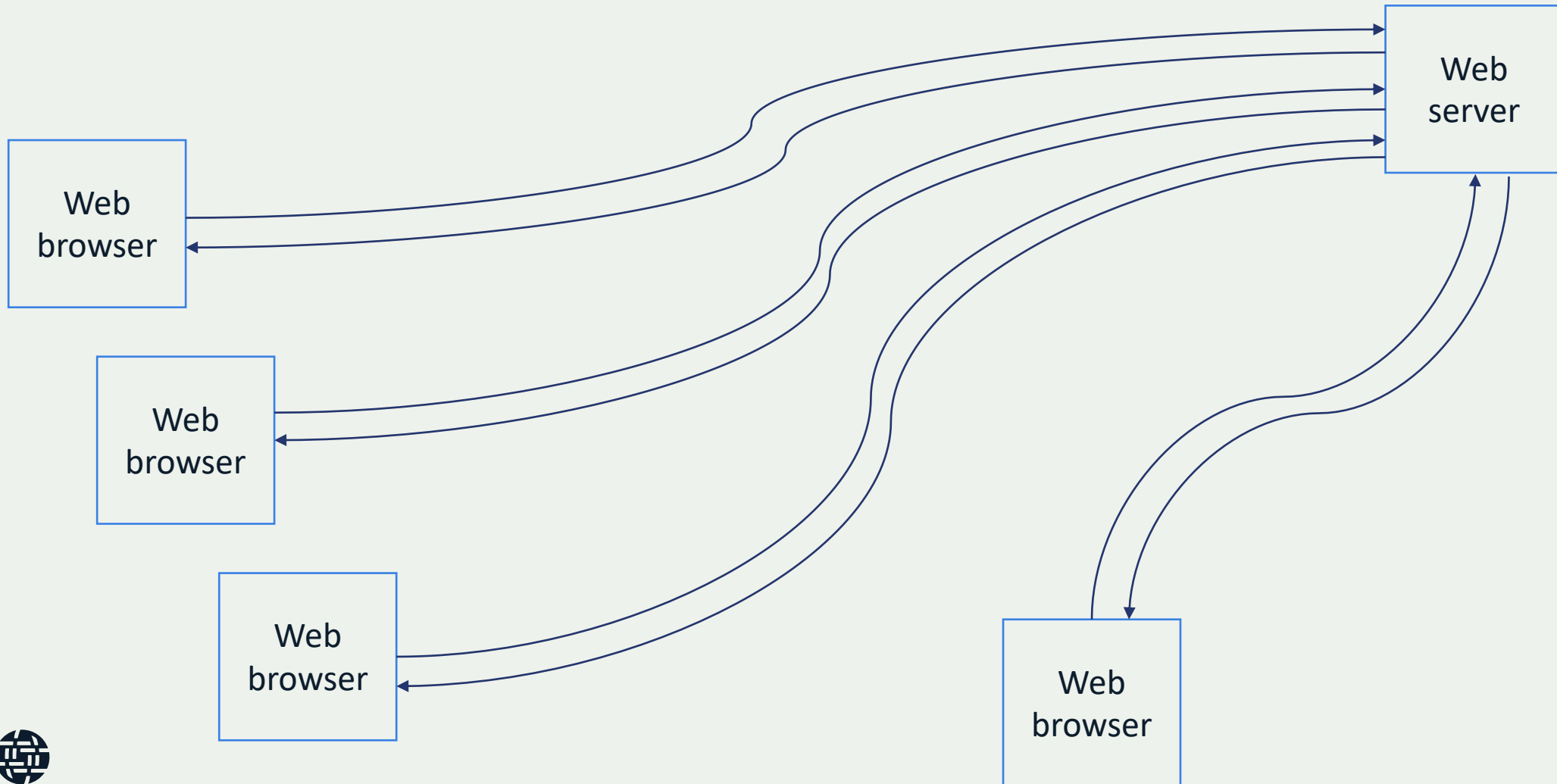


Website Hosting Providers

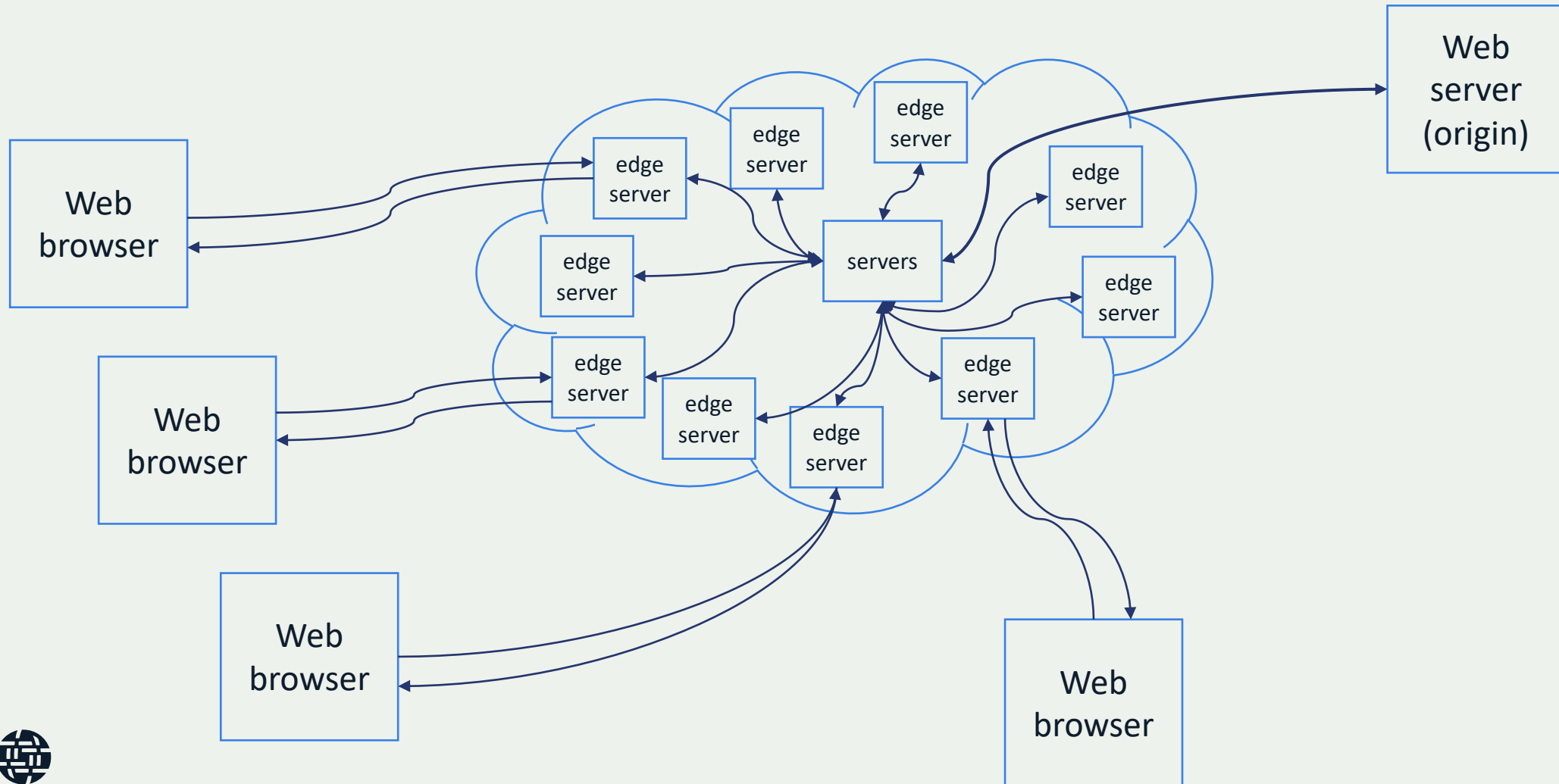
- Often very limited in what you can do.
- Some providers allow limited control through “Cpanel” or similar programs
- Contact support team at hosting provider and request a standard
 - At least one provider indicated they offer a service, but only if you request it
 - Now, you can point them to OSE documentation.
- Or, move to another hosting provider?



About CDNs – A website connection without a CDN



About CDNs – A website connection WITH a CDN



About CDNs

- A CDN can provide IPv6, HTTP/2, TLS, DNSSEC, *even if your original web server does not*
- CDNs can dramatically improve speed of your site, and protection from some attacks
- Some CDNs offer free services, others require payment for some or all services
- Long list, including: Akamai, Amazon CloudFront, Cloudflare, Fastly, Google Cloud, Microsoft Azure, Verizon Edgecast, *many more*



CDNs and DNS

CDNs typically involve one of two configurations

- **CDN provides authoritative DNS**

- You set the CDNs DNS server as the name servers for your domain (“NS” records)

```
example.com. 43200 IN NS art.ns.cloudflare.com.  
example.com. 43200 IN NS eva.ns.cloudflare.com.
```

- **You use a CNAME record to point to CDN**

- You retain control of your DNS records

```
www.internetsociety.org. 300 IN CNAME d229qzkrjypvi4.amimoto-cdn.com.
```



Either one can work – it is a choice for you.

Sli.do – What type of site do you have?



?



BUILD reference servers

- Four servers using two major open source web servers, with and without a Content Delivery Network (CDN)
- Standards/practices supported:
 - IPv6
 - DNSSEC
 - TLS 1.3 (using Let's Encrypt certificates)
 - HSTS
 - HTTP/2

Apache

Apache with
CDN

NGINX

NGINX with
CDN



DOCUMENT how we set up those servers

- Easy-to-understand (and easy-to-find) documentation will be key.
- Current plans include:
 - Web pages with step-by-step tutorials
 - Videos / "screencasts" showing the precise configuration steps
 - Links to testing tools and environments
 - Links to more details on specific standards, protocols, and practices
 - Materials about why this is important, including business cases

Where we are RIGHT NOW!



DOCUMENTATION – Available on GitHub

- We are developing the documentation on GitHub:
- **<https://github.com/internetsociety/ose-documentation>**
- Once complete, documentation will be moved to main ISOC website
- Will be published in English, French, and Spanish

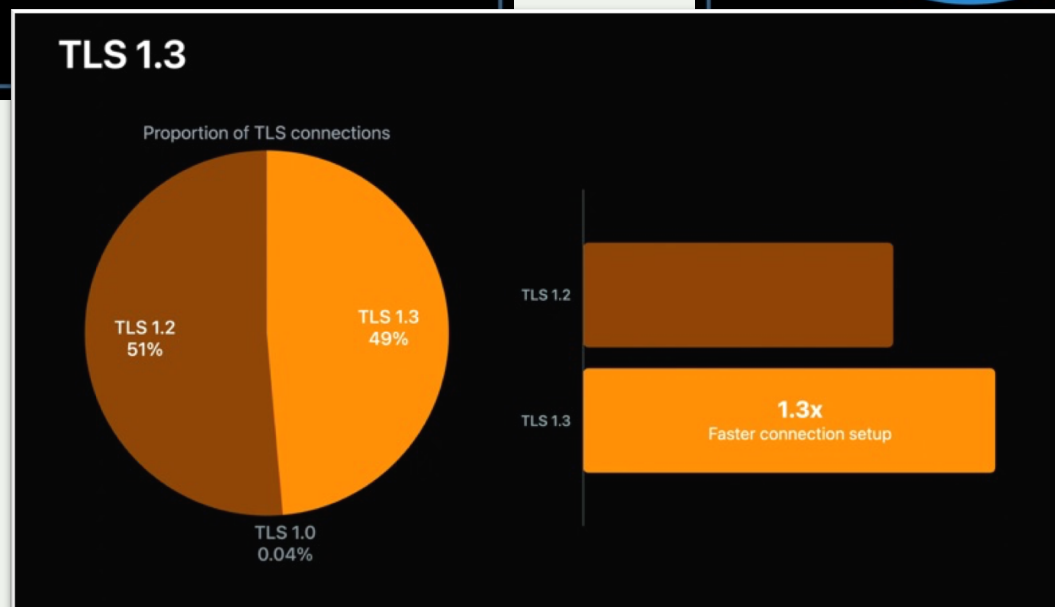
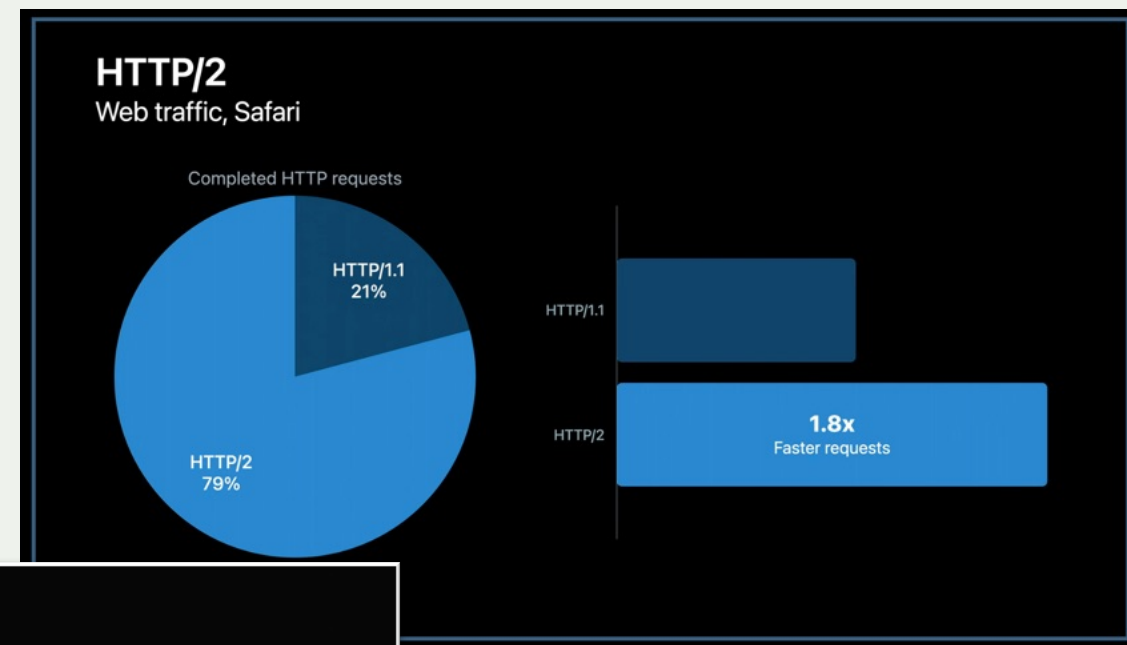
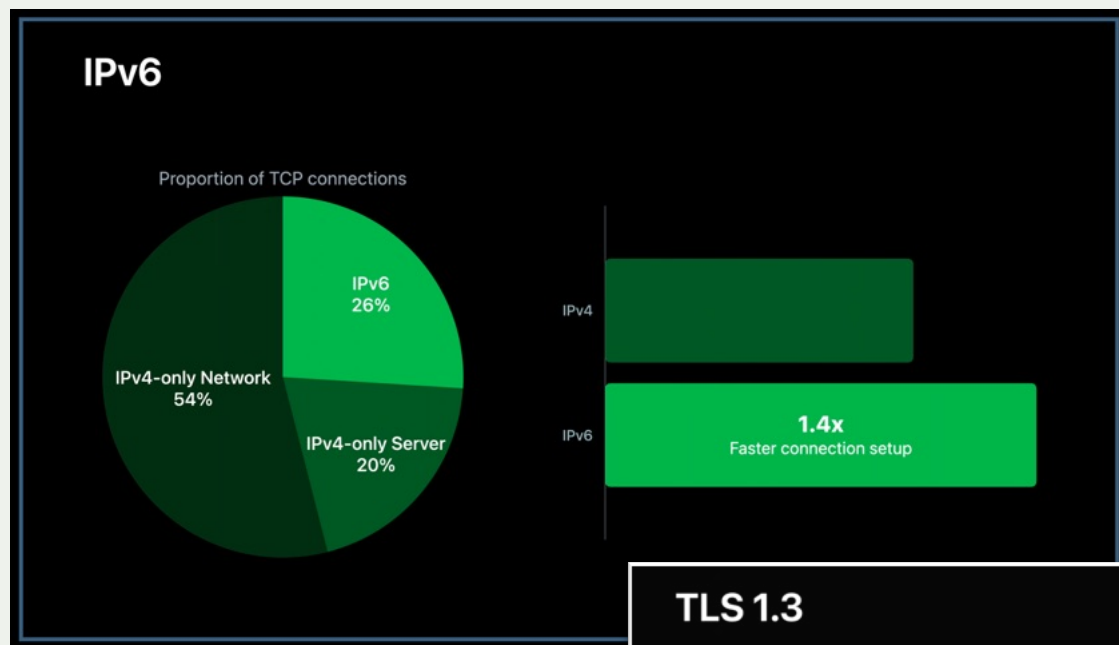


PROMOTE the information

- Sharing this information, incorporating feedback, and helping more people:
 - Presentations to online conferences
 - Network operator groups (NOGs) meetings
 - Websites and media channels focused on
 - website operators and developers
 - open source / free software
 - security and privacy
 - Events within the web community (ex. WordCamp events for WordPress)
 - Events within the open source community
 - Events within the security community
 - Podcasts (audio and video) on these topics
- If you have ideas – york@isoc.org



PROMOTION – the performance business case



Source: Apple WWDC 2020

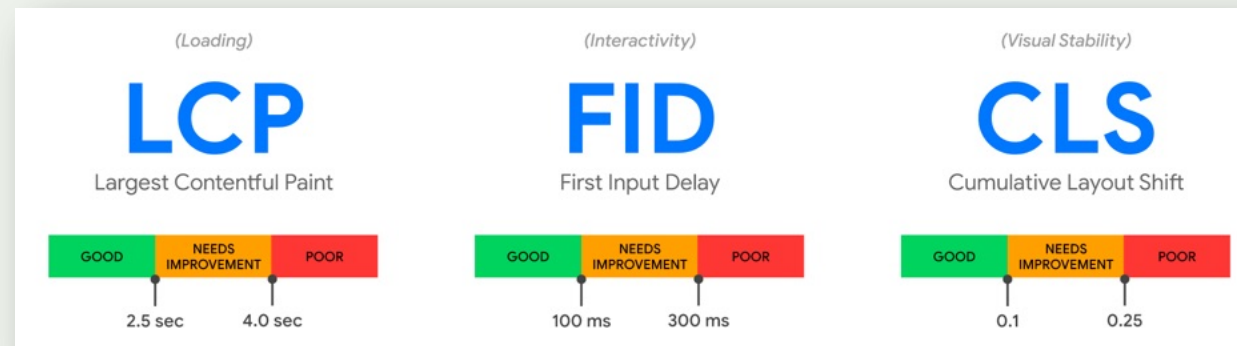


PROMOTION – the performance business case



Results showed that **by decreasing load time by 0.1s**, the average conversion rate **grew by 8%** for retail sites and **by 10%** for travel sites.

- Deloitte study commissioned by Google



Google search ranking factor in 2021.
<https://web.dev/vitals/>



LEAD BY EXAMPLE – our Internet Society sites

- We will “practice what we promote”
- Audit of all of our corporate sites
- Working on changes

Site	IPv6	DNSSEC	HTTPS	HSTS	NOT TLS 1.0/1.1	Cipher Order	Internet.nl	TLS 1.3	HTTP/2
www.internetsociety.org	Y	Y	Y	Y	Y	N	97%	N	Y
future.internetsociety.org	Y	Y	Y	Y	Y	N	97%	N	Y
apps.internetsociety.org	Y	Y	Y	Y	N	N	97%	N	N
www.isocfoundation.org	Y	N	Y	Y	Y	N	70%	N	Y
news.internetsociety.org	Y	Y	Y	Y	Y	N	97%	N	Y
www.manrs.org	Y	Y	Y	Y	Y	N	97%	N	Y
observatory.manrs.org	Y	Y	Y	Y	N	N	92%	N	N
ose.apache.internetsociety.org	Y	Y	Y	Y	Y	Y	100%	Y	Y
ose.apache-cdn.internetsociety.org	Y	Y	Y	Y	Y	N	97%	Y	Y
ose.nginx.internetsociety.org	Y	Y	Y	Y	Y	Y	100%	Y	Y
ose.nginx-cdn.internetsociety.org	Y	Y	Y	Y	Y	N	97%	Y	Y
www.internethalloffame.org	Y	Y	Y	Y	N	N	97%	N	N
www.afpif.org	Y	N	Y	Y	Y	N	70%	N	Y
www.ndss-symposium.org	Y	N	Y	N	Y	N	69%	N	Y
www.ietfjournal.org	Y	N	Y	N	N	N	68%	N	Y
www.dnssec-deployment.org	Y	Y	Y	N	N	N	95%	N	Y
www.internetac.org	Y	Y	Y	Y	Y	N	97%	N	Y
www.internetcollaboration.org	Y	Y	Y	Y	Y	N	97%	N	Y
www.ixptoolkit.org	Y	N	Y	N	N	N	68%	N	Y
www.networktimesecurity.org	Y	Y	Y	Y	Y	Y	100%	Y	Y
www.worldipv6launch.org	Y	N	Y	Y	Y	N	68%	Y	Y
Percentage compliant	100%	71%	100%	81%	71%	14%	89%	29%	86%



Future Years

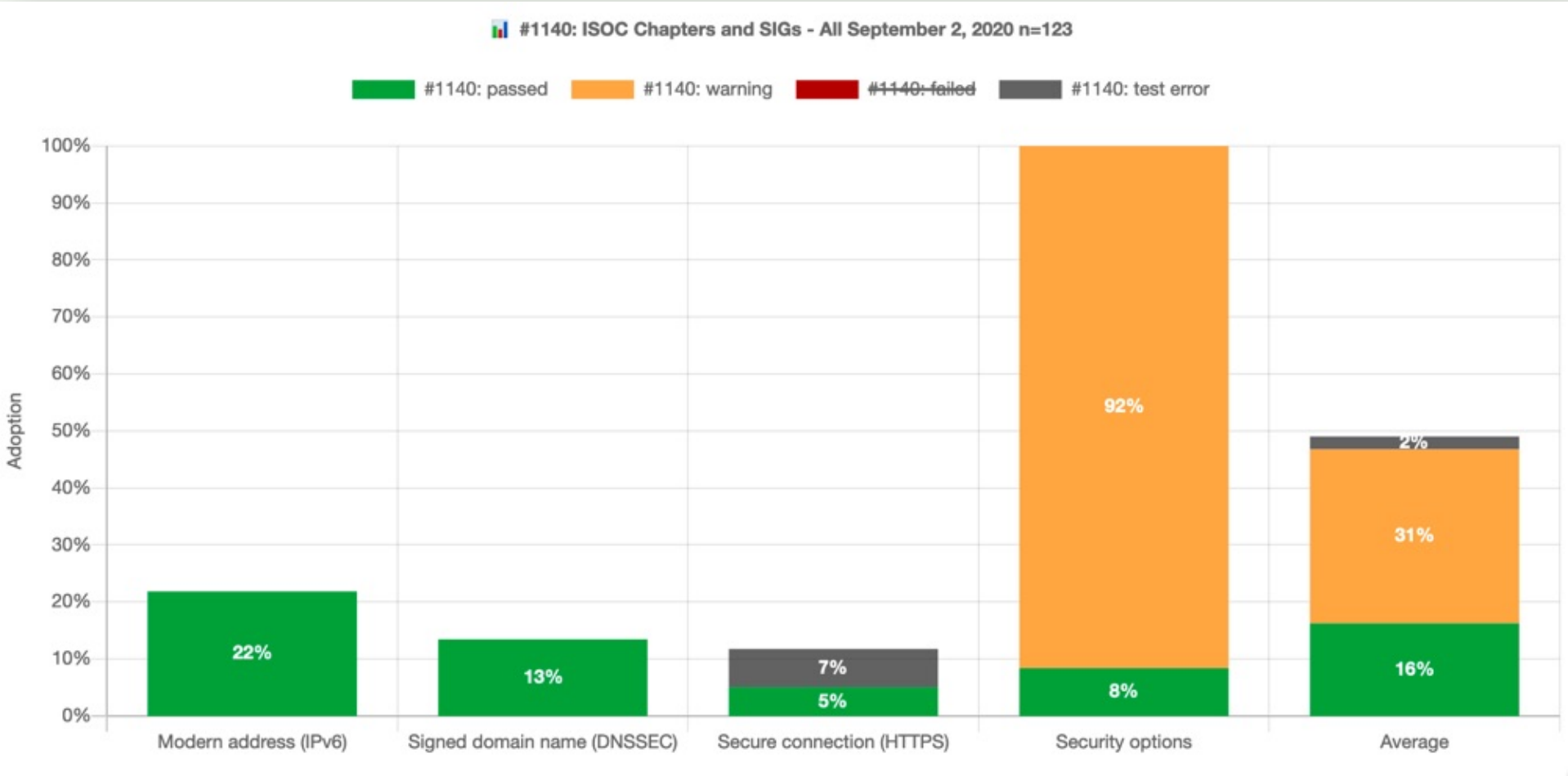
- Expanding web server documentation as standards evolve:
 - **HTTP/3** (also known as QUIC)
 - **Website packaging standards**
- In 2021, our focus will expand to:
 - **Mail servers**, embracing security standards such as DMARC, DKIM, SPF, DANE
- In the next years, possible ideas include:
 - **DNS servers**, promoting DNSSEC validation, DNS-over-HTTPS (DoH), and DNS-over-TLS (DoT)
 - **Time servers**, adding support for Network Time Security (NTS) to complement our Time Security project
 - **Communication servers**, embracing WebRTC and similar standards



Leading By Example



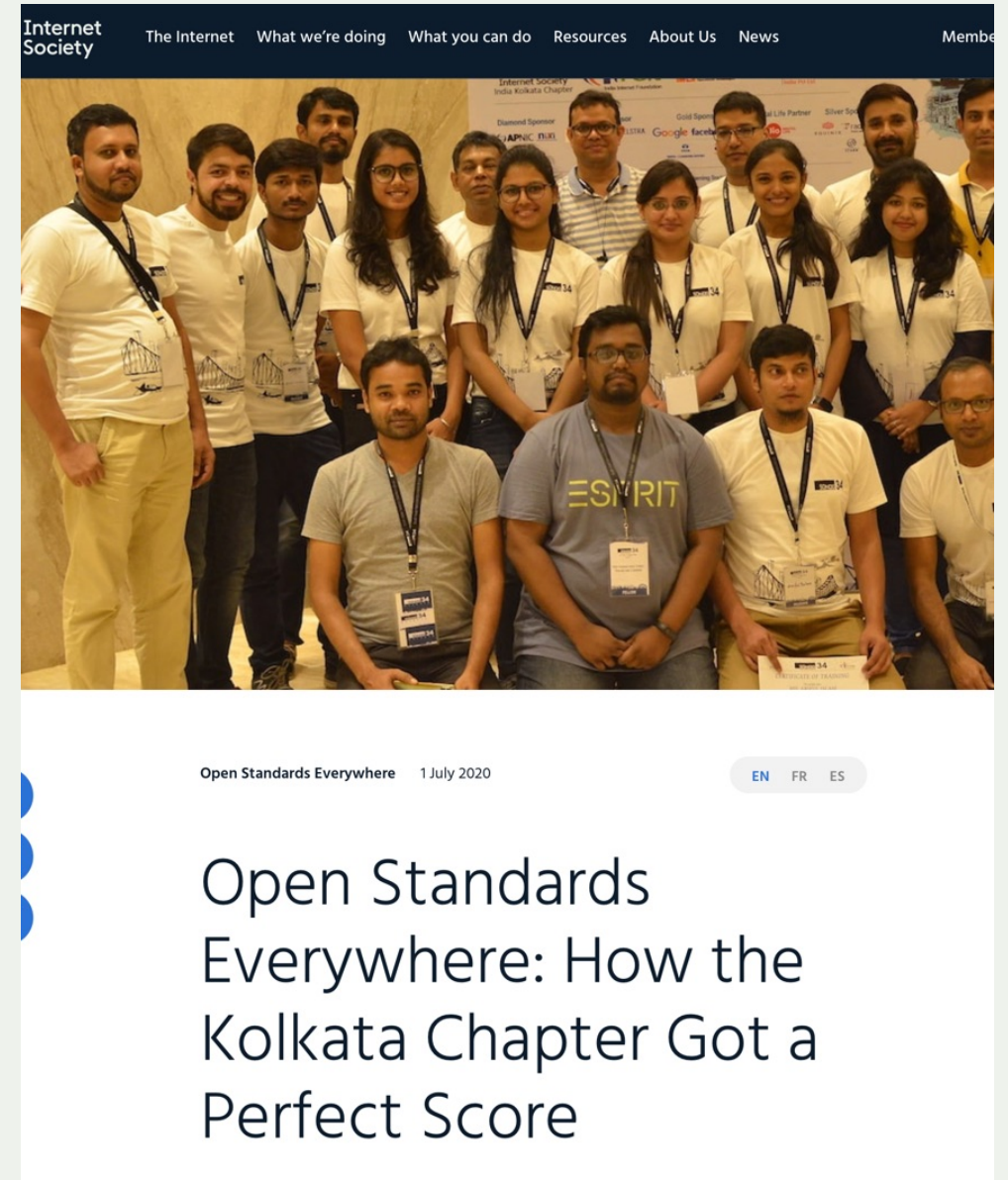
Internet.nl Test – All ISOC Chapter/SIG Sites – 2 September 2020



ISOC Kolkata Chapter

After Global Chapter Training in May 2020, made changes to bring their site to 100% from 32%

<https://www.internetsociety.org/blog/2020/07/open-standards-everywhere-how-the-kolkata-chapter-got-a-perfect-score/>



ISOC Madagascar Chapter – 55%

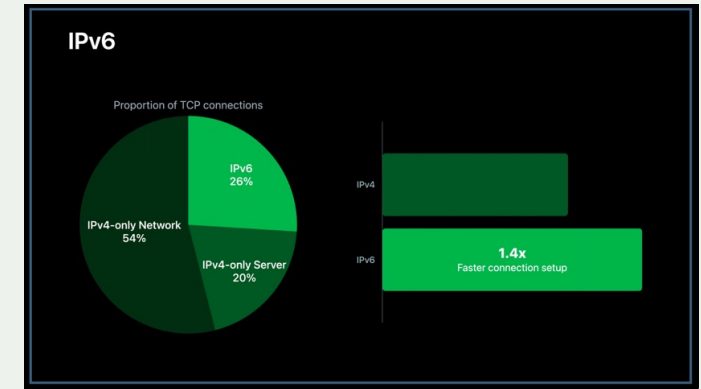


IPv6



IPv6

- Web server needs IPv6 connectivity
- If unable to get IPv6 address, consider a CDN
- See: *Making Content Available Over IPv6*
 - <https://www.internetsociety.org/resources/deploy360/2013/making-content-available-over-ipv6/>
- For more background, watch our tutorial: *Introduction to IPv6*
 - English: <https://www.internetsociety.org/tutorials/introduction-to-ipv6>
 - Spanish: <https://www.internetsociety.org/es/tutorials/introduction-to-ipv6>
 - Unfortunately a French version is not available.



Source: Apple WWDC 2020



How do I know if I have IPv6?

Open a terminal window and type:

```
$ dig +short aaaa <domain name>
```

```
$ dig +short aaaa www.google.com
2607:f8b0:4006:81a::2004
$
$ dig +short aaaa facebook.com
2a03:2880:f112:83:face:b00c:0:25de
$
$ dig +short aaaa www.internetsociety.org
d229qzkrjypvi4.amimoto-cdn.com.
2600:9000:21b8:e00:9:4aa:6f00:93a1
2600:9000:21b8:3400:9:4aa:6f00:93a1
2600:9000:21b8:4000:9:4aa:6f00:93a1
2600:9000:21b8:5c00:9:4aa:6f00:93a1
2600:9000:21b8:5e00:9:4aa:6f00:93a1
2600:9000:21b8:6000:9:4aa:6f00:93a1
2600:9000:21b8:ca00:9:4aa:6f00:93a1
2600:9000:21b8:dc00:9:4aa:6f00:93a1
$
$
$
$
$ dig +short aaaa reddit.com
$
$ dig +short aaaa live.com
$
$ dig +short aaaa www.amazon.com
tp.47cf2c8c9-frontier.amazon.com.
d3ag4hukkh62yn.cloudfront.net.
$
$
```

Single IPv6 address

CDN name and multiple IPv6 addresses

No IPv6 address

CDN names but **no** IPv6 address

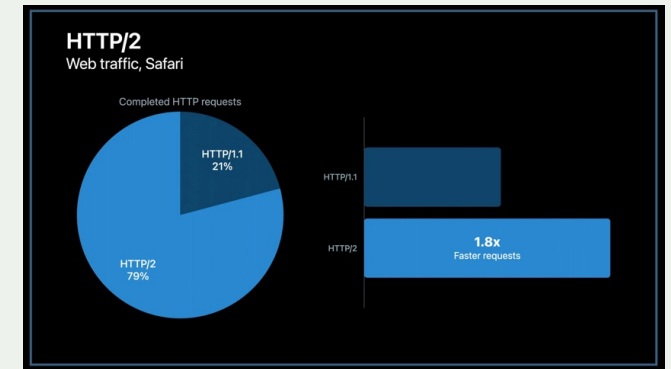


HTTP/2



HTTP/2

- Hypertext Transfer Protocol Version 2 ("HTTP/2", "HTTP2", "H2") - RFC 7540 – May 2015
- Speeds web server performance and reduces latency by:
 - Allowing multiple exchanges of data on a single connection
 - Compressing headers
 - Enabling web servers to “push” data to web browsers



Source: Apple WWDC 2020



HTTP/2 – Self-hosted – NGINX

- Open your NGINX configuration file (usually `nginx.conf`)
- Add the text below in bold:

```
server {  
    listen 443 http2 ssl;  
    listen [::]:443 http2 ssl;
```

- Save the file and restart the NGINX service



<https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-http2-nginx.md>

TLS



TLS

- Transport Layer Security (TLS) Version 1.3 – RFC 8446 – August 2018
- Encrypts connection between web browser and web server
- Previously known as “Secure Sockets Layer” or “SSL”
- Web servers should only support TLS versions 1.2 (2008) and 1.3 (2018). Need to disable TLS 1.0 (1999) and 1.1 (2006).
- If you do not have TLS active on your server:
 - Install Let’s Encrypt: <https://letsencrypt.org/>
 - Free, no-cost TLS certificates
 - Consider using a CDN



TLS – Self-hosted – Apache

- Go to directory where you installed Let's Encrypt, usually `/etc/letsencrypt`
- Edit `options-ssl-apache.conf`
- Find the `SSLProtocol` line and set it to:

```
SSLProtocol all -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
```

- Save the file and restart apache.

Note: This will enable support for TLS 1.2 and 1.3, and remove support for TLS 1.0 and 1.1.



<https://github.com/InternetSociety/ose-documentation/blob/master/ose-web-tls-1-3-apache.md>

HSTS

- HTTP Strict Transport Security – RFC 6787 – 2012
- After first visit, requires web browsers to *only* connect to your site via HTTPS. Can protect against man-in-the-middle (MiTM) attacks.
- Typically set for a 6-month period (31536000 seconds)
- NOTE: If you *disable* TLS, web browsers that have already visited your site will not be able to connect over insecure HTTP until HSTS expiration.



HTTP Security Headers

- Best practices are to include several HTTP headers to protect against common attacks.
- Exercises show simple configurations. You may need to adjust for your site.
- Recommend adding headers one at a time and testing.



DNSSEC

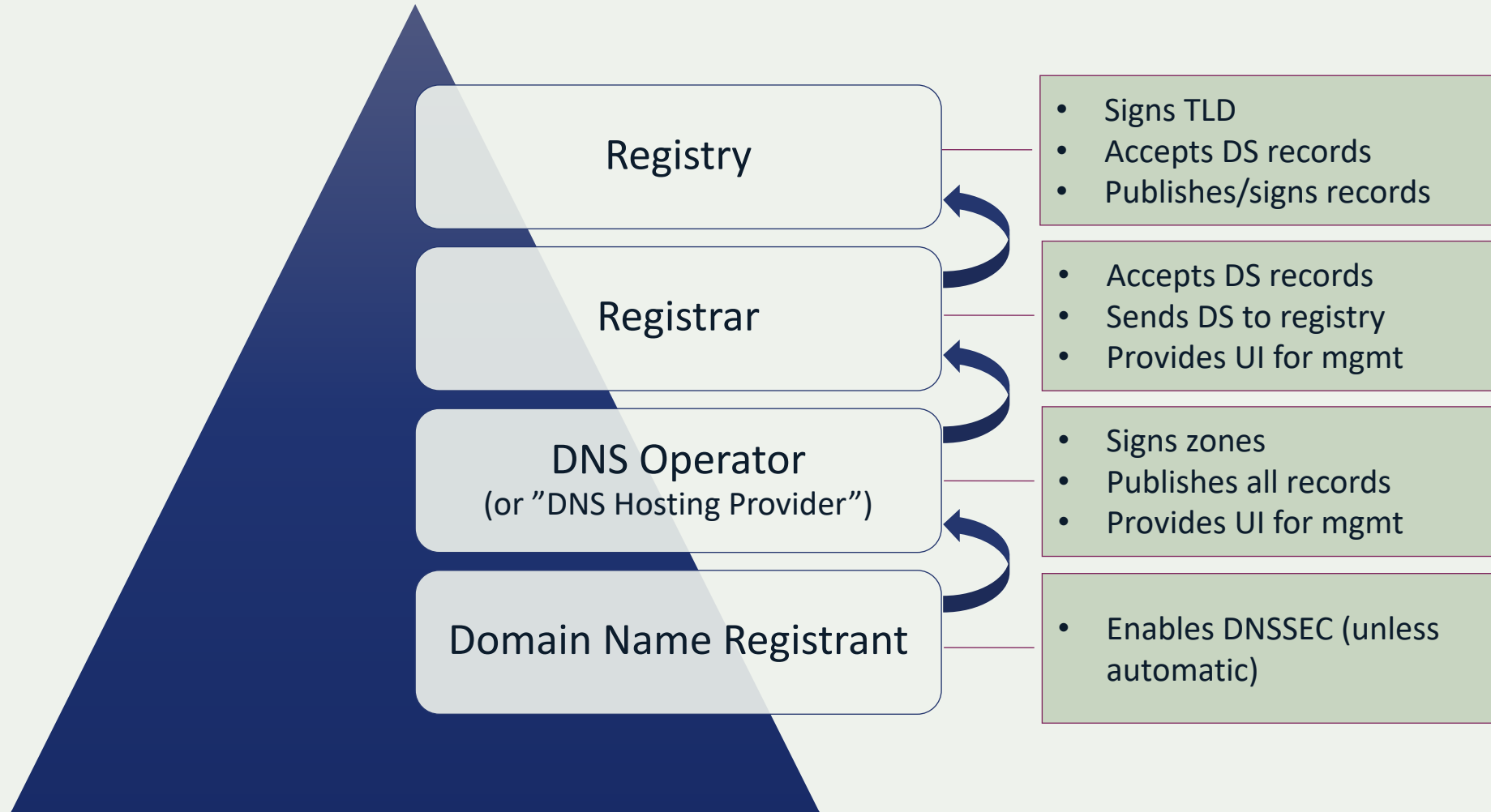


DNSSEC

- DNS Security Extensions, “DNSSEC”, provides a way to be sure you are getting accurate information from DNS
- Resources
 - <https://www.internetsociety.org/deploy360/dnssec/>



DNSSEC Signing - The Individual Steps



Sli.do – What will you work on next?



How You Can Help

Next Steps



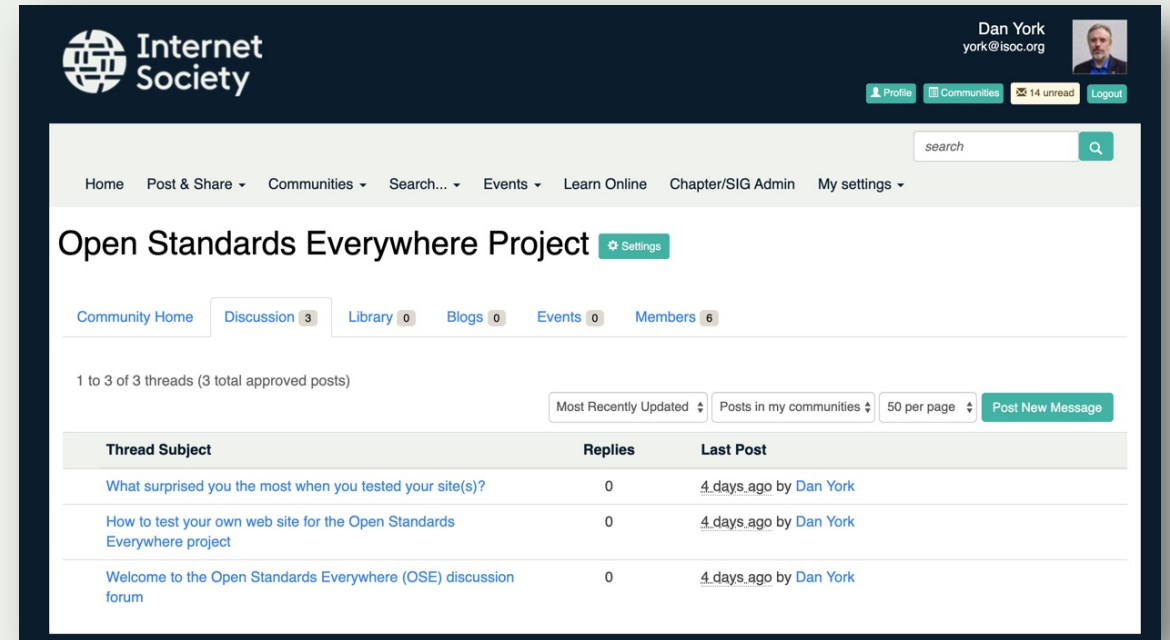
How You Can Help

- **Test your site with Internet.nl** – and help spread the word about site
- **Review / comment on the documentation on GitHub:**
 - <https://github.com/internetsociety/ose-documentation>
- **Share** this info and encourage others to join in
 - <https://www.internetsociety.org/ose/>
 - **Invite our team to participate in events, podcasts, articles, more**

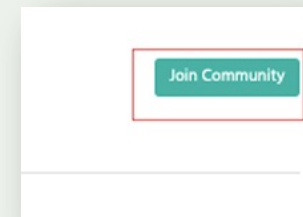


Connect Community

- You can join the “Open Standards Everywhere Project” community in Connect.
- This community will be used for ongoing updates throughout the project.



- Link to join: <http://connect.internetociety.org/communities/community-home?CommunityKey=f35f6fff-56d8-496a-9477-317926ec16d1>
- Choose the “Join Community” button and select how you want to receive email. (Individual messages or as a periodic digest.)



Next Steps

- We want to continue working with you to improve your server
- Please join us in the Connect community
- Additionally, you can contact:
 - york@isoc.org – Dan York
 - lechner@isoc.org – Gregg Lechner
- Please spread the word and share the OSE documentation. Share your stories with us!
- You can join us on GitHub to improve the documentation
- Watch for our survey about email servers!



An open Internet is based on
open standards

Please join us!



?



Thank you.

Dan York
Project Lead, Open Standards Everywhere
york@isoc.org

Twitter: [@danyork](https://twitter.com/danyork)

Mastodon: [@danyork@mastodon.social](https://mastodon.social/@danyork)

GitHub: [danyork](https://github.com/danyork)

Rue Vallin 2
CH-1204 Geneva
Switzerland

Rambla Republica de Mexico 6125
11000 Montevideo,
Uruguay

Science Park 400
1098 XH Amsterdam
Netherlands

11710 Plaza America Drive
Suite 400
Reston, VA 20190, USA

66 Centrepont Drive
Nepean, Ontario, K2G 6J5
Canada

3 Temasek Avenue, Level 21
Centennial Tower
Singapore 039190

internet-society.org
[@internet-society](https://twitter.com/internet-society)



BUILD reference servers

- <https://ose-apache.internetsociety.org/>
- <https://ose-apache-cdn.internetsociety.org/>
- <https://ose-nginx.internetsociety.org/>
- <https://ose-nginx-cdn.internetsociety.org/>

Apache

Apache with
CDN

nginx

nginx with
CDN



You are NOT alone! A survey of the Alexa Top 25 sites

Alexa Top 25 Sites - 19 Feb 2020 - OSE Standards Audit										
#	Site	IPv6	DNSSEC	HTTPS	HSTS	NOT TLS 1.0/1.1	Cipher Order	Internet.nl	TLS 1.3	HTTP/2
1	Google.com	Y	N	Y	N	N	N	66%	Y	Y
2	YouTube.com	Y	N	Y	Y	N	N	70%	Y	Y
3	Tmall.com	N	N	Y	N	N	N	32%	N	Y
4	Facebook.com	Y	N	Y	Y	N	N	68%	Y	Y
5	Baidu.com	N	N	Y	N	N	N	28%	N	N
6	Qq.com	N	N	Y	N	N	N	37%	N	Y
7	Sohu.com	N	N	Y	N	N	N	32%	Y	Y
8	Login.tmall.com	N	N	Y	N	N	N	35%	N	Y
9	Taobao.com	N	N	Y	N	N	N	32%	N	Y
10	360.cn	N	N	Y	N	N	N	28%	N	N
11	jd.com	N	N	Y	N	N	N	32%	Y	N
12	Yahoo.com	Y	N	Y	Y	N	N	73%	N	Y
13	Wikipedia.org	N (NS)	N	Y	Y	Y	Y	58%	N	Y
14	Amazon.com	N	N	Y	N	N	Y	52%	N	Y
15	Sina.com.cn	N	N	Y	N	N	N	28%	Y	Y
16	Weibo.com	N	N	Y	N	N	N	28%	N	Y
17	Pages.tmall.com	N	N	Y	Y	N	N	37%	N	Y
18	Live.com	N	N	Y	N	N	N	47%	N	Y
19	Reddit.com	N	N	Y	Y	N	N	52%	N	Y
20	Vk.com	N	N	Y	Y	N	N	52%	Y	Y
21	Netflix.com	Y	N	Y	Y	N	N	63%	N	N
22	Xinhuanet.com	N	N	N	N	N	N	21%	N	N
23	Okezone.com	N	N	Y	N	N	N	30%	N	Y
24	Bongacams.com	N	N	Y	N	N	N	30%	N	Y
25	Blogspot.com	Y	N	Y	N	N	N	66%	Y	Y
Percentage compliant		22%	0%	96%	35%	4%	9%	44%	30%	78%
List from https://www.alexa.com/topsites on 19 Feb 2020										

