PCH
Packet Clearing House

All TLS, All The Time

Using Apache and Let's Encrypt to set up a secure web server

Ashley Jones
Packet Clearing House

South African Network Operators

pch.net/ZATLS

PCH
Packet Clearing House

Requirements

- root
- Supported Let's Encrypt environment (e.g. Ubuntu)
- DNS entry for your server

PCH
Packet Clearing House

Tools

- Ubuntu 16.04 
- Apache v.2.4.x 
- Let’s Encrypt 

PCH
Packet Clearing House

Why Encrypt?

- Public servers are exposed to hackers
- Private servers are exposed to internal hackers ;) *
- Firesheep can hijack sessions
- Man in the middle (MiTM) protection
- Snowden says, “encryption works”

* Let’s Encrypt requires public IP

PCH
Packet Clearing House

Netherlands Vodaphone MiTM

Before:

```
<html><body>Hello World</body></html>
```

PCH
Packet Clearing House

Netherlands Vodaphone MiTM

After:

```
<html>
<script src="http://1.2.3.4/bmi-int-js/bmi.js"
language="javascript"></script>
<body>Hello World</body>
</html>
<script language="javascript"><!-
bmi_SafeAddOnload(bmi_load,"bmi_orig_img",
1);//--></script>
```

PCH
Packet Clearing House

Why encrypt well?

- IPv4 and IPv6 with the same effort
- POODLE, BEAST, Heartbleed, Logjam and more for sure
- Weaponized enables script kiddies
- HTTP Strict Transport Security (HSTS)
- Easy Tools:
  - Cipher List
  - Mozilla TLS Config Generator
  - Qualys SSL Labs

PCH
Packet Clearing House

Install Apache and Git

```
apt-get update&&apt-get upgrade

apt-get install apache2

a2enmod ssl headers rewrite

a2enconf security
```

PCH
Packet Clearing House

Config Edit: ssl.conf

```
<IfModule mod_ssl.c>
SSLRandomSeed startup builtin
SSLRandomSeed startup file:/dev/urandom 512
SSLRandomSeed connect builtin
SSLRandomSeed connect file:/dev/urandom 512
AddType application/x-x509-ca-cert .crt
AddType application/x-pkcs7-crl   .crl
SSLPassPhraseDialog  exec:/usr/share/apache2/ask-for-passphrase
SSLSessionCache shmcb:${APACHE_RUN_DIR}/ssl_scache(512000)
SSLSessionCacheTimeout  300
SSLCipherSuite EECDH+AESGCM:EDH+AESGCM:AES256+EECDH:AES256+EDH
SSLProtocol All -SSLv2 -SSLv3 -TLSv1 -TLSv1.1
SSLHonorCipherOrder On
Header always set Strict-Transport-Security "max-
age=63072000;includeSubDomains; preload"
Header always set X-Frame-Options DENY
Header always set X-Content-Type-Options nosniff
SSLCompression off
SSLUseStapling on
SSLStaplingCache "shmcb:logs/stapling-cache(150000)"
</IfModule>
```

PCH
Packet Clearing House

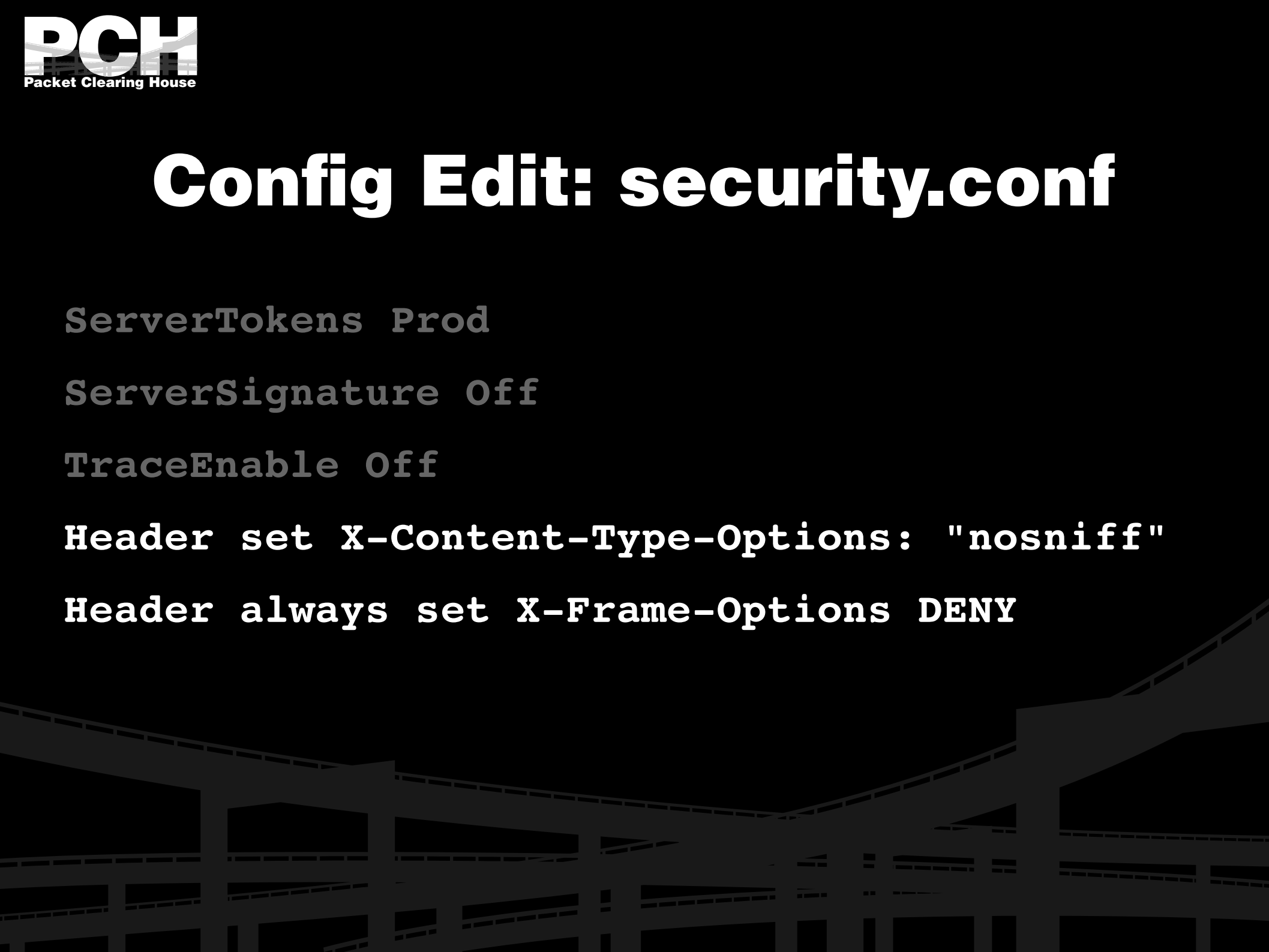
Config Edit: default-ssl.conf

```
<IfModule mod_ssl.c><VirtualHost _default_:443>
ServerAdmin webmaster@localhost
DocumentRoot /var/www/html
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined
SSLEngine on
SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
<FilesMatch "\.(cgi|shtml|phtml|php)$">
  SSLOptions +StdEnvVars
</FilesMatch>
<Directory /usr/lib/cgi-bin>
  SSLOptions +StdEnvVars
</Directory>
BrowserMatch "MSIE [2-6]" \
  nokeepalive ssl-unclean-shutdown \
  downgrade-1.0 force-response-1.0
BrowserMatch "MSIE [17-9]" ssl-unclean-shutdown
</VirtualHost></IfModule>
```

PCH
Packet Clearing House

Config Edit: security.conf

```
ServerTokens Prod
ServerSignature Off
TraceEnable Off
Header set X-Content-Type-Options: "nosniff"
Header always set X-Frame-Options DENY
```



PCH
Packet Clearing House

Config Create: 100-zatls.conf

```
<VirtualHost *:80>
  ServerName zatls.plip.com
  ServerAdmin mrjones@pch.net
  DocumentRoot /var/www/html/
  ErrorLog ${APACHE_LOG_DIR}/error_log
  TransferLog ${APACHE_LOG_DIR}/access_log
  RewriteEngine On
  RewriteRule (.*) https://%{HTTP_HOST}%{REQUEST_URI} [R=301,L]
</VirtualHost>
<VirtualHost *:443>
  ServerName zatls.plip.com
  DocumentRoot /var/www/html/
  ServerAdmin mrjones@pch.net
  ErrorLog ${APACHE_LOG_DIR}/ssl_error_log
  TransferLog ${APACHE_LOG_DIR}/ssl_access_log
  SSLEngine On
  Header always set Strict-Transport-Security "max-age=15768000"
  SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
  SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key
</VirtualHost>
```

PCH
Packet Clearing House

Apache Enable and Restart

```
a2ensite 100-zatls.conf
service apache2 reload
```

PCH
Packet Clearing House

Careful!

- HSTS **`includeSubdomains`**
- SSLUseStapling, SSLCompression, SSLStaplingCache (version 2.4 or higher)
- SSLSessionTickets Requires Apache (version 2.4.11 or higher)
- Reference Mozilla's TLS Config Generator

PCH
Packet Clearing House

Test HTTP

Curl is your friend!

```
curl -I http://zatls.plip.com
```

This is redirected to https (this is good ;)

PCH
Packet Clearing House

Let's Encrypt: Install & Create Cert

```
sudo apt-get install software-properties-common

sudo add-apt-repository ppa:certbot/certbot

sudo apt-get update

sudo apt-get install python-certbot-apache

sudo certbot --apache
```

PCH
Packet Clearing House

Let's Encrypt: Install & Create Cert

```
root@za-tls:~# sudo certbot --apache
Saving debug log to /var/log/letsencrypt/letsencrypt.log
Plugins selected: Authenticator apache, Installer apache
Enter email address (used for urgent renewal and security notices) (Enter 'c' to
cancel): mrjones@plip.com
Starting new HTTPS connection (1): acme-v01.api.letsencrypt.org

-------------------------------------------------------------------------------
Please read the Terms of Service at
https://letsencrypt.org/documents/LE-SA-v1.2-November-15-2017.pdf. You must
agree in order to register with the ACME server at
https://acme-v01.api.letsencrypt.org/directory
-------------------------------------------------------------------------------
(A)gree/(C)ancel: A
```

PCH
Packet Clearing House

Let’s Encrypt: Install & Create Cert

```
-------------------------------------------------------------------------------
Would you be willing to share your email address with the Electronic Frontier
Foundation, a founding partner of the Let's Encrypt project and the non-profit
organization that develops Certbot? We'd like to send you email about EFF and
our work to encrypt the web, protect its users and defend digital rights.
-------------------------------------------------------------------------------
(Y)es/(N)o: N

Which names would you like to activate HTTPS for?
-------------------------------------------------------------------------------
1: zatls.plip.com
-------------------------------------------------------------------------------
Select the appropriate numbers separated by commas and/or spaces, or leave input
blank to select all options shown (Enter 'c' to cancel): 1
```

PCH
Packet Clearing House

Let's Encrypt: Install & Create Cert

```
Obtaining a new certificate
Performing the following challenges:
http-01 challenge for zatls.plip.com
Waiting for verification...
Cleaning up challenges
Deploying Certificate to VirtualHost /etc/apache2/sites-enabled/100-zatls.conf

Please choose whether or not to redirect HTTP traffic to HTTPS, removing HTTP access.
-------------------------------------------------------------------------------
1: No redirect - Make no further changes to the webserver configuration.
2: Redirect - Make all requests redirect to secure HTTPS access. Choose this for
new sites, or if you're confident your site works on HTTPS. You can undo this
change by editing your web server's configuration.
-------------------------------------------------------------------------------
Select the appropriate number [1-2] then [enter] (press 'c' to cancel): 1
```

PCH
Packet Clearing House

Let's Encrypt: Install & Create Cert

```
---------------------------------------------------------------------------
Congratulations! You have successfully enabled https://zatls.plip.com

You should test your configuration at:
https://www.ssllabs.com/ssltest/analyze.html?d=zatls.plip.com
---------------------------------------------------------------------------

IMPORTANT NOTES:
 - Congratulations! Your certificate and chain have been saved at:
   /etc/letsencrypt/live/zatls.plip.com/fullchain.pem
   Your key file has been saved at:
   /etc/letsencrypt/live/zatls.plip.com/privkey.pem
   Your cert will expire on 2018-08-28. To obtain a new or tweaked
   version of this certificate in the future, simply run certbot again
   with the "certonly" option. To non-interactively renew *all* of
   your certificates, run "certbot renew"
 - Your account credentials have been saved in your Certbot
   configuration directory at /etc/letsencrypt. You should make a
   secure backup of this folder now. This configuration directory will
   also contain certificates and private keys obtained by Certbot so
   making regular backups of this folder is ideal.
 - If you like Certbot, please consider supporting our work by:

   Donating to ISRG / Let's Encrypt:   https://letsencrypt.org/donate
   Donating to EFF:                    https://eff.org/donate-le
```

PCH
Packet Clearing House

Resulting 100-tls-test.conf

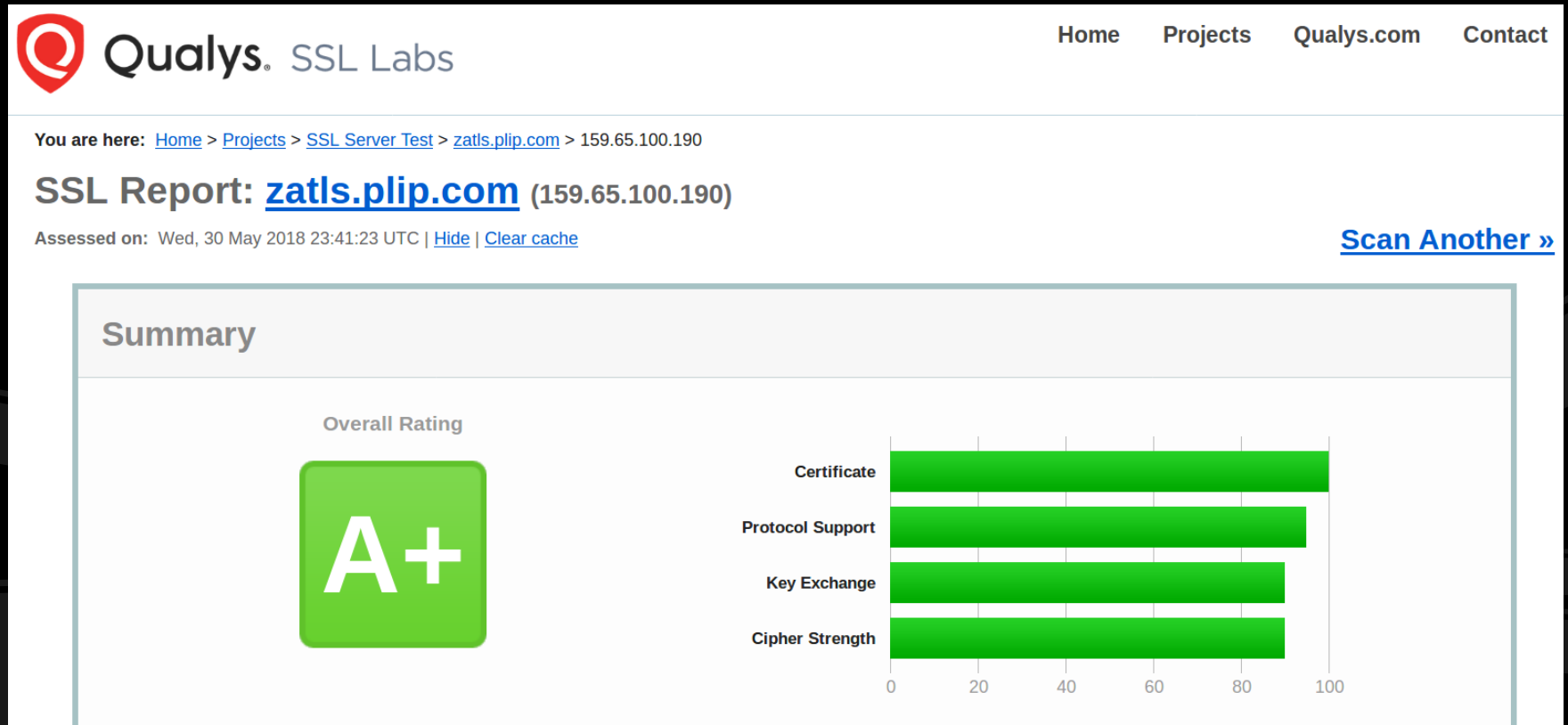
```
<VirtualHost *:443>
[SNIP]
SSLCertificateFile
/etc/letsencrypt/live/zatls.plip.com/cert.pem
SSLCertificateKeyFile
/etc/letsencrypt/live/zatls.plip.com/privkey.pem
SSLCertificateChainFile
/etc/letsencrypt/live/zatls.plip.com/chain.pem
</VirtualHost>
```

PCH
Packet Clearing House

Test HTTPS

Curl is still your friend! (so is SSL Labs)

```
curl -I https://1.tls-test.plip.com
```



PCH
Packet Clearing House

Myth: TLS is slow

"On our production machines, TLS accounts for less than 1% CPU load, less than 10 KB RAM per connection and less than 2% of network overhead. People believe that TLS takes a lot of CPU...we hope our numbers will dispel that."

-Adam Langley, Google "Overclocking SSL"

PCH
Packet Clearing House

Myth: TLS is slow

"On our production machines, TLS accounts for less than 1% CPU load, less than 10 KB RAM per connection and less than 2% of network overhead. People believe that TLS takes a lot of CPU...we hope our numbers will dispel that."

-Adam Langley, Google "Overclocking SSL" 2010

PCH
Packet Clearing House

Myth: TLS is slow

"On our production machines, TLS accounts for less than 1% CPU load, less than 10 KB RAM per connection and less than 2% of network overhead. People believe that TLS takes a lot of CPU...we hope our numbers will dispel that."

-Adam Langley, Google "Overclocking SSL" 2010

It is 2018!!

PCH
Packet Clearing House

Myth: TLS is slow

"On our production machines, TLS accounts for less than 1% CPU load, less than 10 KB RAM per connection and less than 2% of network overhead. People believe that TLS takes a lot of CPU...we hope our numbers will dispel that."

-Adam Langley, Google "Overclocking SSL" 2010

See https://istlsfastyet.com/

It is 2018!!

PCH
Packet Clearing House

Myth: Let's Encrypt requires root

- Non-root solution is available!
- Let's Encrypt has APIs and SDKs which don't all require root

PCH
Packet Clearing House

Myth: Managing certs is hard

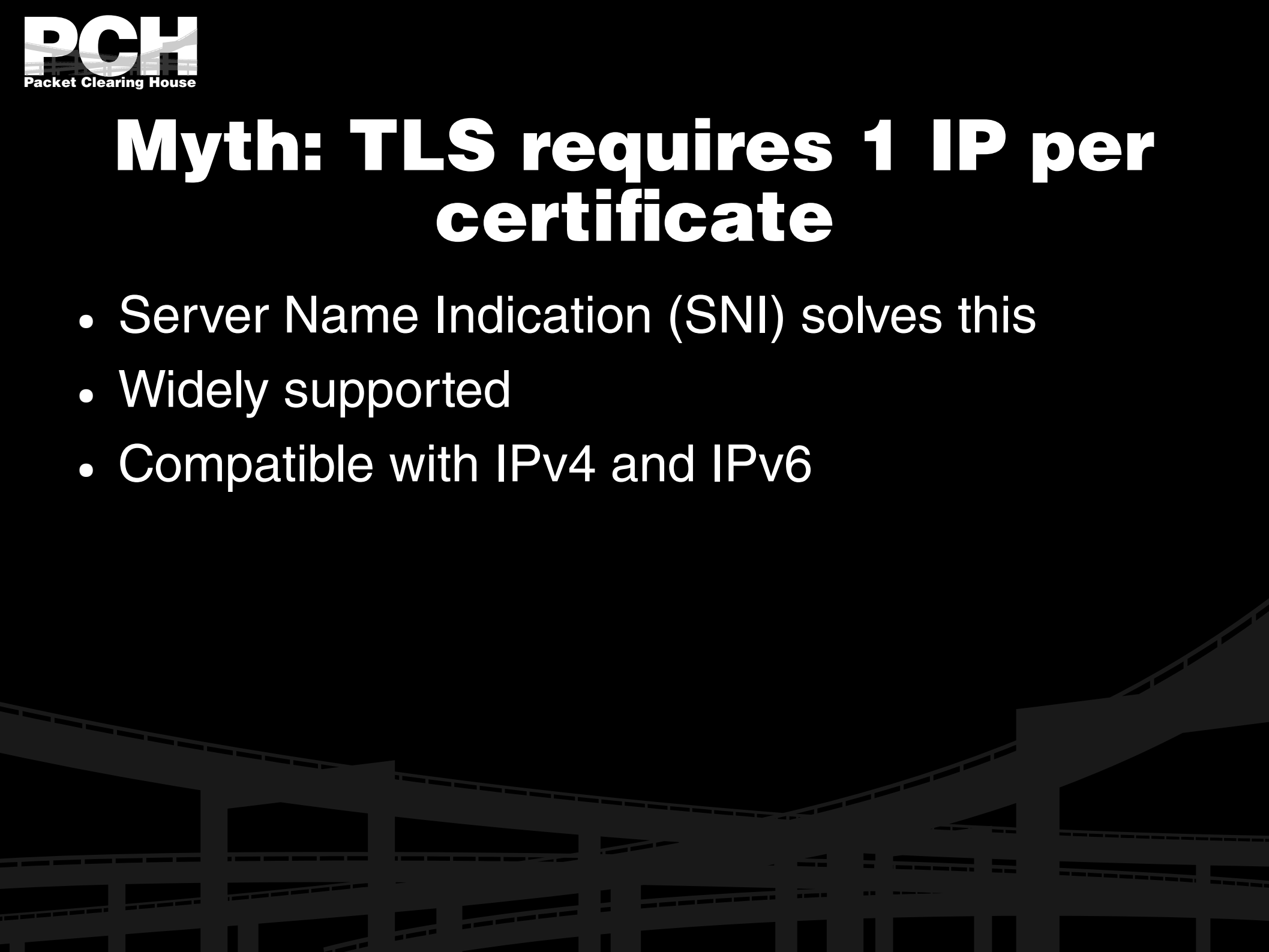
- 100% automated
- Command line works with no options
- cronjob installed automatically

```
root@za-tls:~# certbot renew
Saving debug log to /var/log/letsencrypt/letsencrypt.log

-------------------------------------------------------------------------------
Processing /etc/letsencrypt/renewal/zatls.plip.com.conf
-------------------------------------------------------------------------------
Cert not yet due for renewal

-------------------------------------------------------------------------------

The following certs are not due for renewal yet:
  /etc/letsencrypt/live/zatls.plip.com/fullchain.pem expires on 2018-08-28 (skipped)
No renewals were attempted.
-------------------------------------------------------------------------------
```

PCH
Packet Clearing House

Myth: TLS requires 1 IP per certificate

- Server Name Indication (SNI) solves this
- Widely supported
- Compatible with IPv4 and IPv6



PCH
Packet Clearing House

Caveats

- Requires Public IP
- Let’s Encrypt is in beta - errors?!#
- No Wildcards (*.zatls.plip.com)
- Short certs - currently 3 months
- Only specific platform supported
- Related packages auto-installed
- Non HTTPS assets (eg JS) cause warnings
- Orphaned browsers

PCH
Packet Clearing House

Caveats

- Requires Public IP
- ~~Let's Encrypt is in beta - errors?!#~~ as of Apr 12, 2016
- ~~No Wildcards (*.zatls.plip.com)~~ as of Mar 13, 2018
- Short certs - currently 3 months
- ~~Only specific platform supported~~
- Related packages auto-installed
- Non HTTPS assets (eg JS) cause warnings
- Orphaned browsers

PCH
Packet Clearing House

Thanks! Questions? https://pch.net/ZATLS

- Ashley Jones - mrjones@pch.net - personal blog https://blog.plip.com
- PCH https://pch.net
- Vodaphone in Netherlands: https://web.archive.org/web/20170610010435/http://www.sphaero.org/blog:2012:0418_am_i_hacked_oh_it_s_just_vodafone
- Let's Encrypt https://letsencrypt.org
- Apache https://httpd.apache.org
- Ubuntu https://ubuntu.com
- Cipherli.st https://cipherli.st
- iptables http://www.netfilter.org/projects/iptables
- POODLE https://en.wikipedia.org/wiki/POODLE
- BEAST https://en.wikipedia.org/wiki/Transport_Layer_Security#BEAST_attack
- Heartbleed http://heartbleed.com/
- Logjam https://weakdh.org/
- RFC2246 https://tools.ietf.org/html/rfc2246
- List of all Let's Encrypt client https://letsencrypt.org/docs/client-options/#acme-v2-compatible-clients
- No Root Let's Encrypt How-To https://github.com/diafygi/letsencrypt-nosudo
- Mozilla's TLS Config Generator https://mozilla.github.io/server-side-tls/ssl-config-generator/
- Is TLS Fast Yet? https://istlsfastyet.com/