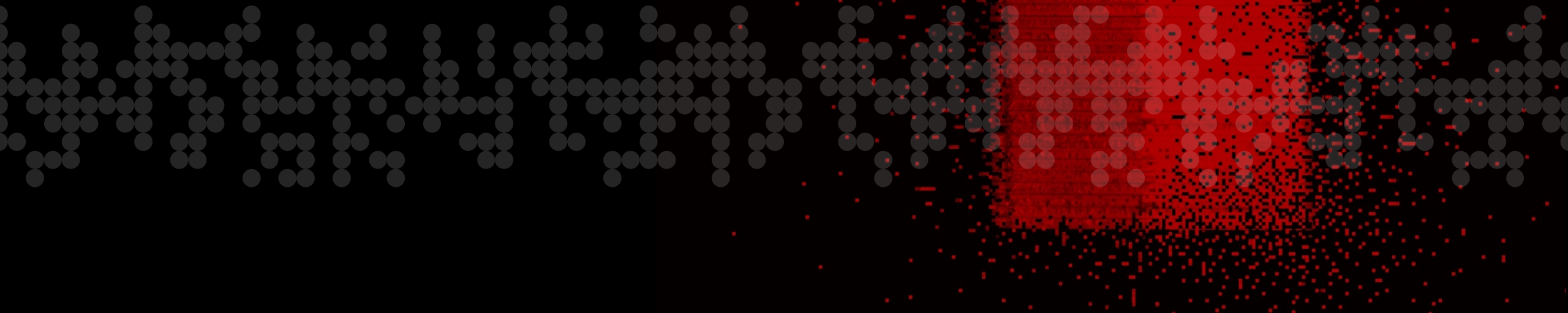




Is Encryption Smuggling Exploits Into Your Company?

Keiron Shepherd – Snr Security Systems Engineer



Secure by default

“SSL Everywhere is a fundamental shift in the natural state of IT services, by which nothing is trusted and everything is encrypted.”

Zero Trust





{Security Starts Here}

Robust encryption is the next step toward protecting our networks and data from unauthorized surveillance. The **Data Security Action Plan** offers 7 security-enhancing steps that every internet platform should take to safeguard our data.

[HTTPS://ENCRYPTALLTHETHINGS.NET/](https://encryptallthethings.net/)

Industry trends

External pressures are mounting to move to SSL



Google using HTTPS as a ranking signal.



PCI DSS 3.1 requires TLS1.1+ for all new deployments.



Firefox is deprecating HTTP!

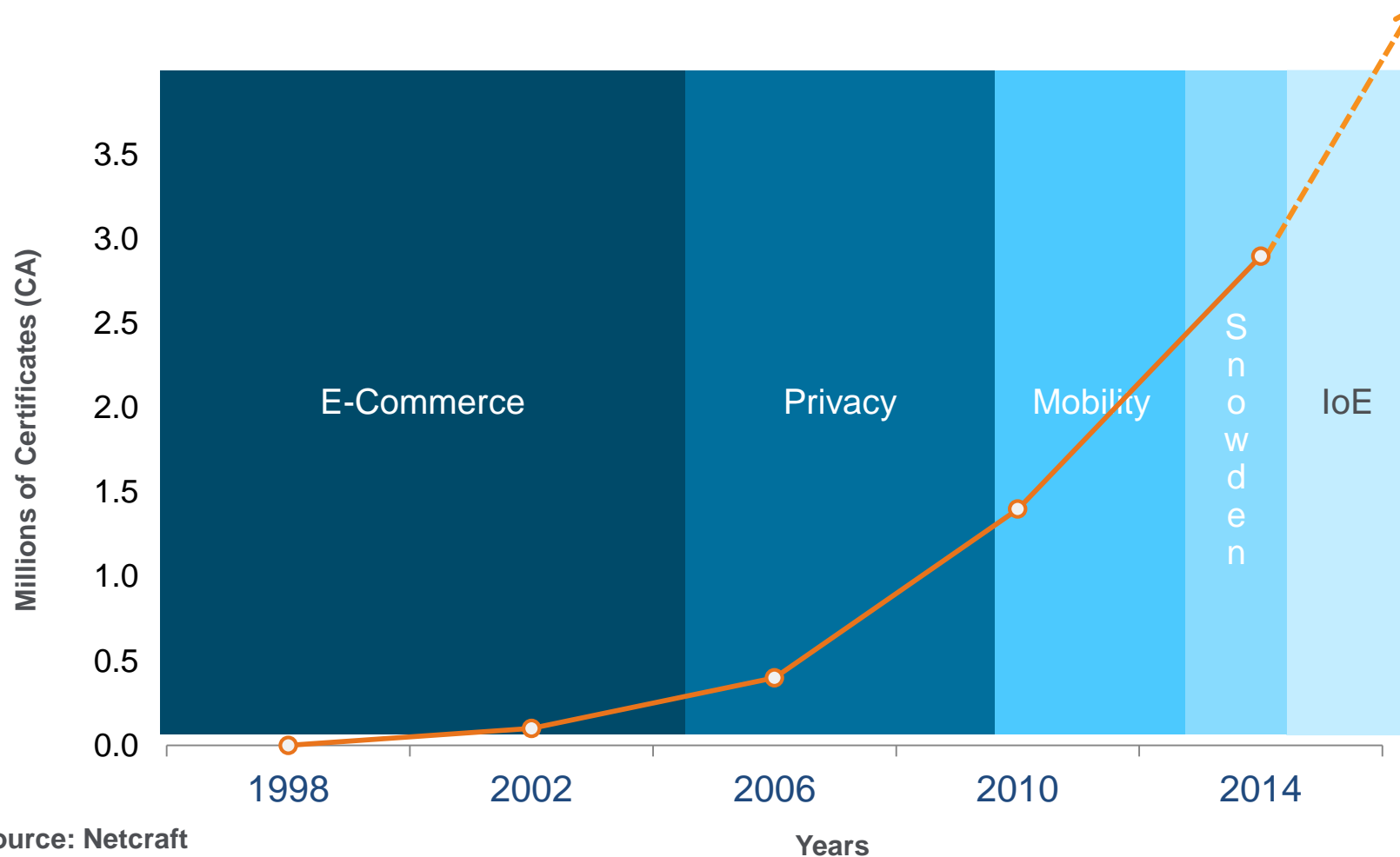


HTTP/2 is only supported over TLS.

<http://googlewebmastercentral.blogspot.com/2014/08/https-as-ranking-signal.html>
https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-1.pdf
<https://blog.mozilla.org/security/2015/04/30/deprecating-non-secure-http/>

Trajectory and Growth of Encryption

SSL growing ~30% annually. Entering the Fifth wave of transition (IoE)



MARKET AMPLIFIERS

Customer Trends:

- Higher Security Standards
- Security more mobile

Emerging Standards:

- TLS 1.3, HTTP 2.0/SPDY
- RSA -> ECC

Thought Leaders and Influence:

- Google: SHA2, SPDY, Search Ranking by Encryption
- Microsoft: PFS Mandated

Source: Netcraft

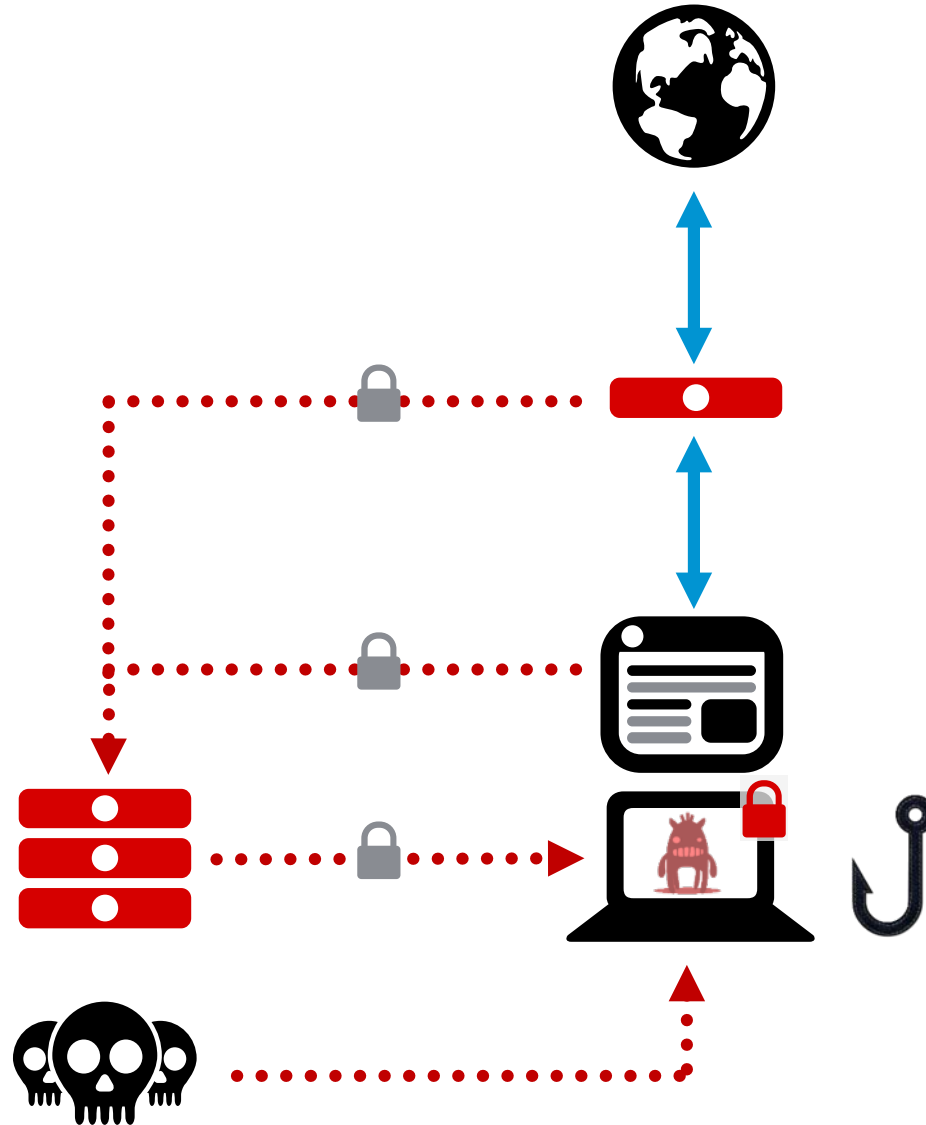




Sometimes those really are the droids you are looking for.

Trojan droppers using SSL

Two stage droppers contacts
command & control servers for the
rest of Malware... *Over SSL!*



**LESS THAN
20%**

Of Organizations
with a FW, IPS/IDS,
or UTM decrypt
SSL/TLS traffic

Gartner®





[Blog](#)

[Technology ▾](#)

[Contribute ▾](#)

[Support ▾](#)

[About ▾](#)

Let's Encrypt is a new Certificate Authority:
It's free, automated, and open.

[Get Started](#)

SSL1 and

SSL2

Created by Netscape and contained significant flaws

SSL3

Created by Netscape to address SSL2 flaws

TLS 1.0

Standardized SSL3 with most no changes
RFC2246

TLS 1.1

Security fixes and TLS extensions
RFC4346

TLS 1.2

Added support for authenticated encryption (AES-GCM, CCM modes) and removed hard-coded primitives
RFC5246

TLS1.3

Protocol fixes, enforced ciphers.

1994

1996

1999

2006

2008

2017 (?)

SSL (Its All In The Handshake)

- NO Forward Secrecy
 - Can be decrypted by passive devices
 - If private key compromised all data
 - Poor performance of passive decryption devices
- With Forward Secrecy
 - Browsers are preferring FS
 - No decryption on passive devices

That awkward moment
you go for a handshake...



... and they go for a hug.



ANALYST BRIEF

SSL Performance Problems

SIGNIFICANT SSL PERFORMANCE LOSS LEAVES MUCH ROOM FOR IMPROVEMENT

Author – John W. Pirc

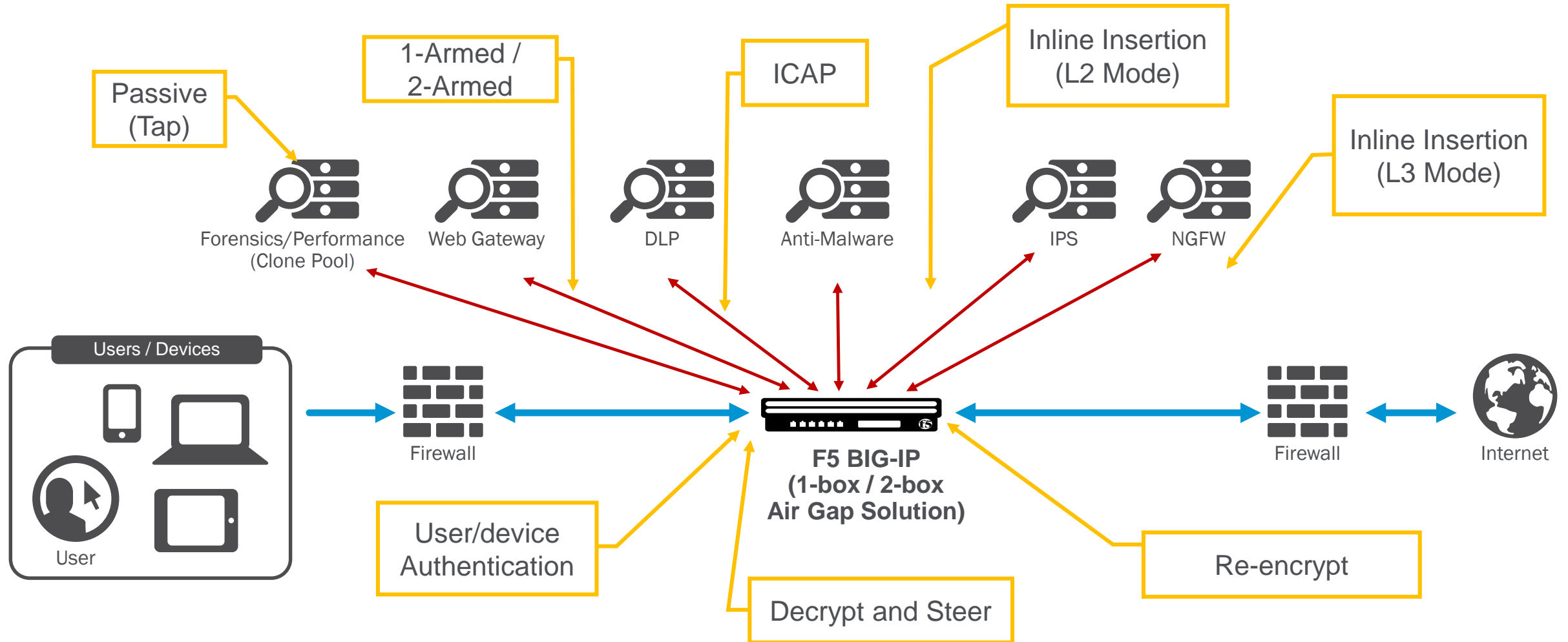
Overview

In early 2013, NSS Labs released the results of its analysis of SSL performance (CARs). As part of the analysis, NSS assessed the performance of seven of the eight NGFWs that were included in the study.

Vendor	2048 bit Cipher Performance Loss
Juniper SRX3600	36%
Palo Alto Networks PA-5020	79%
SourceFire 8250	83%
Check Point 12600	87%
Dell SonicWall E10800	94%
Fortinet 3600C	94%
SourceFire 8290	96%

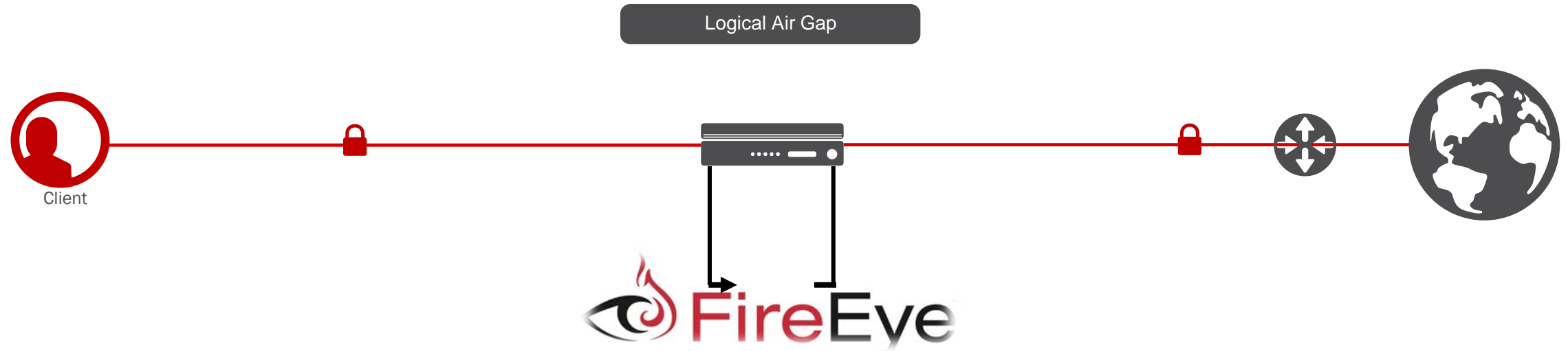
SSL/TLS Visibility and Security Service Chaining

Robust Traffic Steering Options



SSL visibility and inspection

Active mode or “inline” visibility

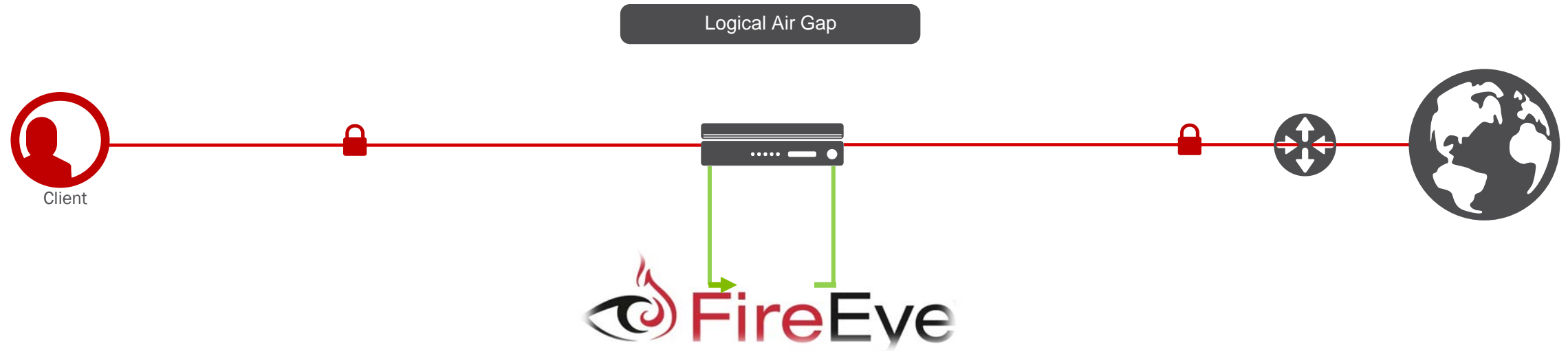




Demo

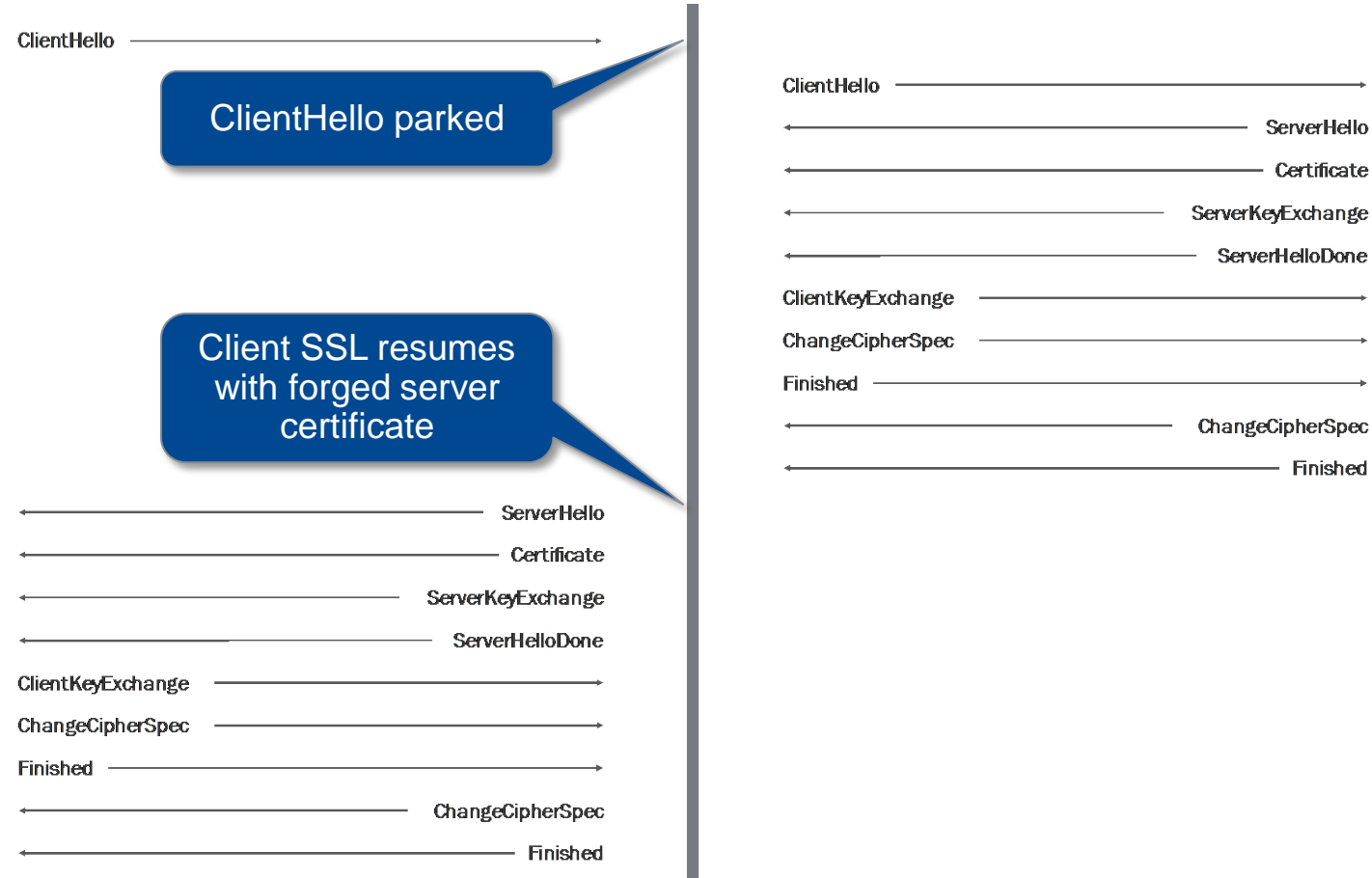
SSL visibility and inspection

Active mode or “inline” visibility



SSL visibility and inspection

Forward Proxy SSL protocol flow



SSL visibility and inspection

Forward Proxy SSL configuration

SSL Forward Proxy: **Advanced** ▼

SSL Forward Proxy	Enabled... ▼
CA Certificate	sub1.homelab.com ▼
CA Key	sub1.homelab.com ▼
CA Passphrase
Confirm CA Passphrase
Certificate Lifespan	30 day(s)
Certificate Extensions	Extensions List... ▼
Certificate Extensions List	<div>Enabled Extensions Basic Constraints Subject Alternative Name</div> <div>Disable</div> <div>Available extensions Authority Key Identifier Certificate Policies CRL Distribution Points Extended Key Usage Fresh CRL (a.k.a. Delta CRL Distribution Point) ▼</div> <div>Enable</div>
Cache Certificate by Addr-Port	<input type="checkbox"/>
SSL Forward Proxy Bypass	Disabled ▼

Issuer configuration

Lifespan

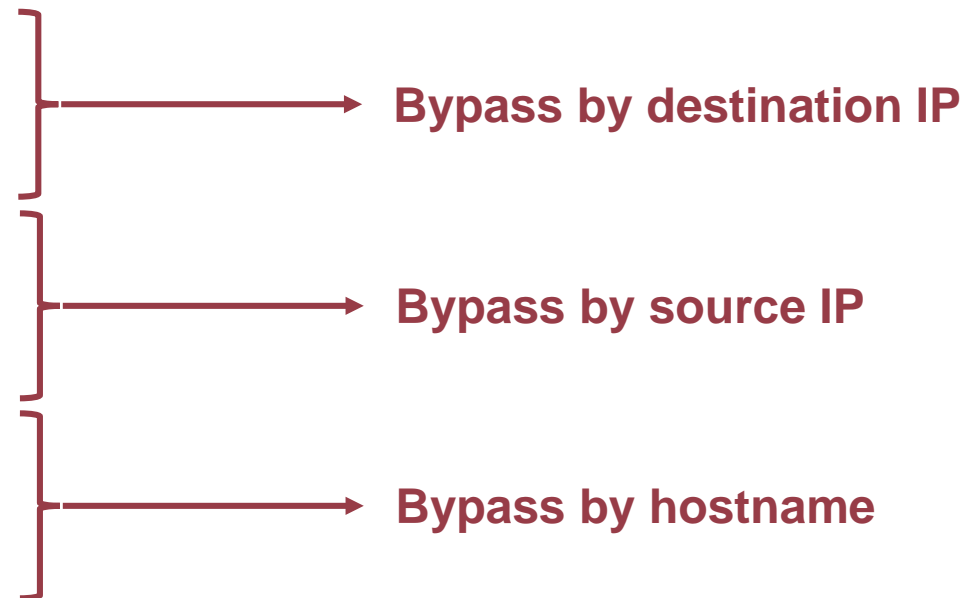
Transferred attributes

Caching

SSL visibility and inspection

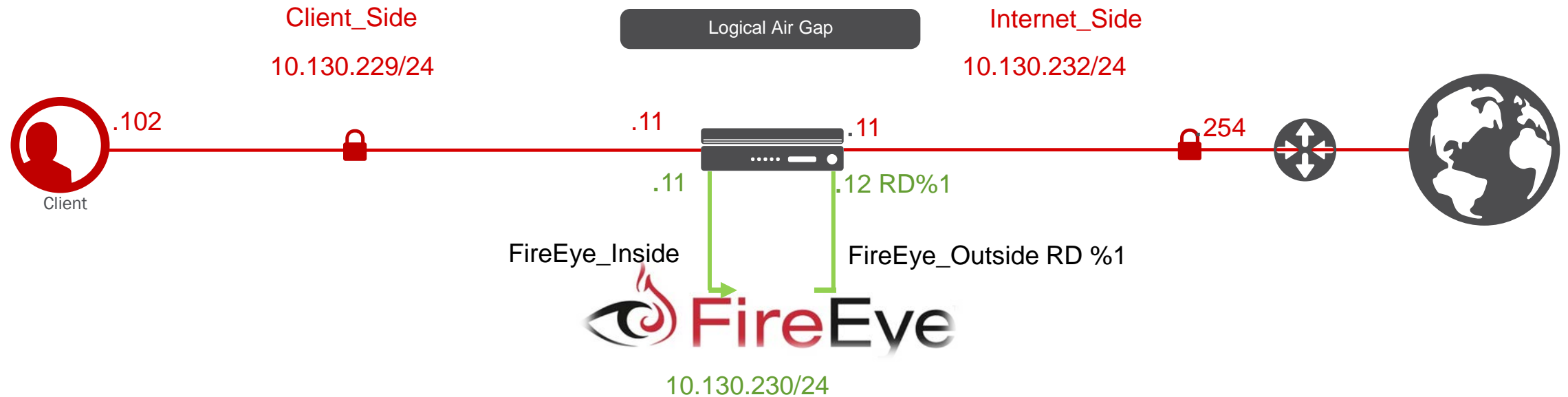
Forward Proxy SSL bypass

SSL Forward Proxy Bypass	Enabled... ▼
Bypass Default Action	Intercept ▼
Destination IP Bypass	private_net ▼
Destination IP Intercept	None ▼
Source IP Bypass	None ▼
Source IP Intercept	None ▼
Hostname Bypass	url_list ▼
Hostname Intercept	None ▼



SSL visibility and inspection

Active mode or “inline” visibility



The Malware



SHA256:

eb51d36ace1e480439e4ed14f9bf2fb8f40fe3cd9dc0f1973d24a94a7046162c

File name:

STOP_DONT_PUT_THIS_IN_DROPBOX_EXE.zip

Detection ratio:

2 / 56

Analysis date:

2016-04-19 17:13:54 UTC (0 minutes ago)

Analysis

File detail

Additional information

Comments

Votes

Antivirus	Result
VBA32	suspected of Trojan.Downloader.gen.h
Zillya	Trojan.Farfli.Win32.23199



SOLUTIONS FOR AN ~~APPLICATION~~ WORLD

^
SSL