Lightweight Traffic Monitoring

HTTP/HTTPS Inspector

Khalegh Salehi

Apr 2016

SSL Inspection?

- Encrypted Traffic, *however, SSL has a potential security gap. It can hide illegal user activity and malicious traffic from the content inspection of Security Gateways*
- SSL/TLS monitoring
  - Security Auditing , *scan this content for either malicious threats or confidential data leakage. What we mean by confidential data leakage is data an employee should not be sending out such as company a financial statement, etc.*
- Privacy and Law

“Ironically, increased use of SSL in attempt to make our online lives more secure can create ‘blind spots’ that can actually reduce security…”

-NSS Labs

HTTPS (Hyper Text Transport Protocol Secure) is inside of a secure tunnel known as SSL (Secure Sockets Layer) is a way of sending data over the web that makes it very difficult for a third party "eavesdropper" to view the data. This added layer of security is used by the large majority of sites that transfer data. Search engines, web based email, web apps, and any site with a login should use HTTPS/ SSL.

Nearly all bot, malware, and data theft tools will use HTTPS/ SSL because network based security tools such as firewalls, malware/ virus inspection devices, Intrusion Detection & Intrusion Prevention Systems (IPS & IDS) do not (or rarely) have the ability to inspect HTTPS /SSL traffic.

How to?

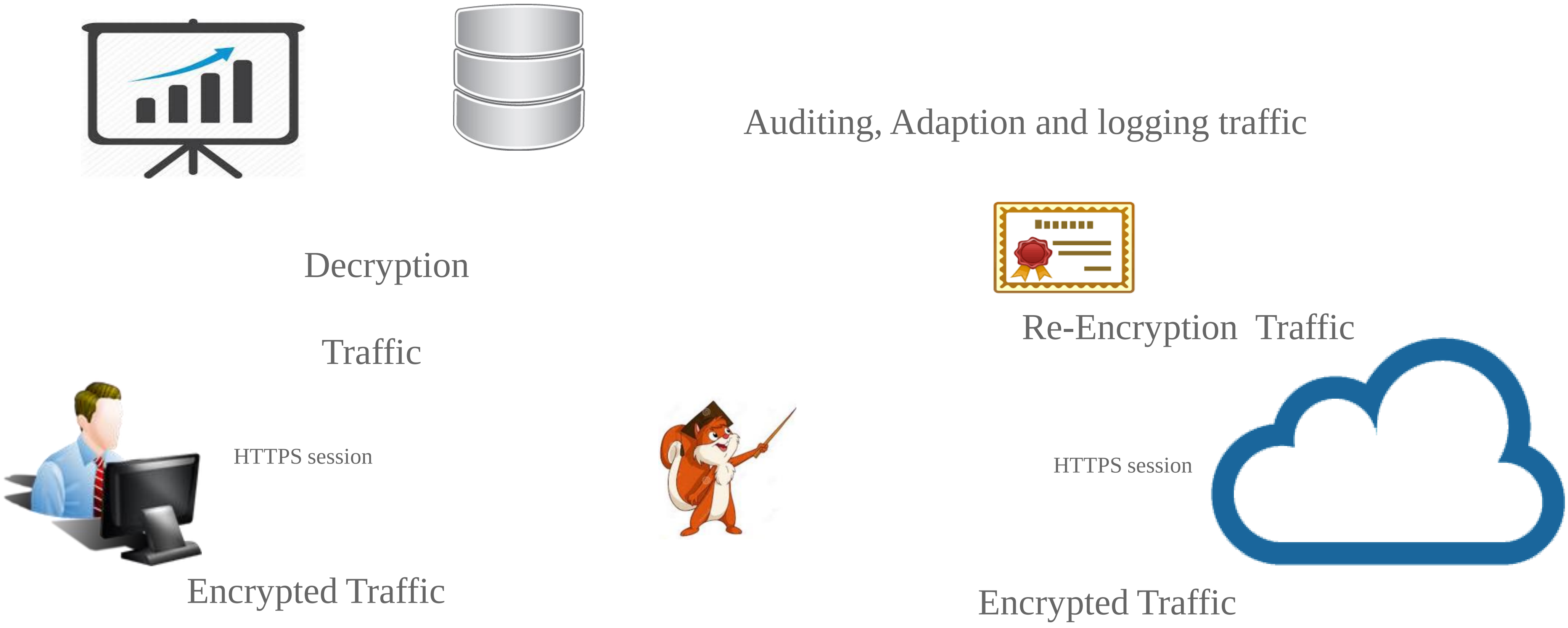
→**Bypassing IDS/IPS**: *Attacker uses any attack against the HTTPS Web site,*

→ *such as SQL injection, buffer overflows,etc*

→**Software Company**: *Source Code easily theft via attachment & uploading*

→ **Military** : *Classification, Information Leaks and insiders attack*

LTM, Lightweight Traffic Monitoring



Auditing, Adaption and logging traffic

Decryption

Traffic

Re-Encryption Traffic

HTTPS session

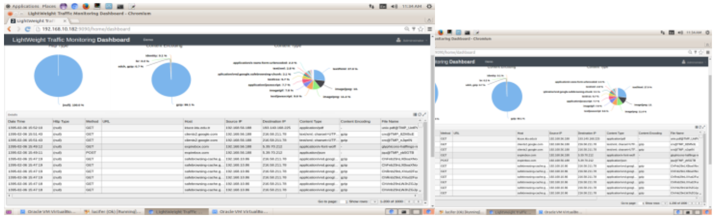
HTTPS session

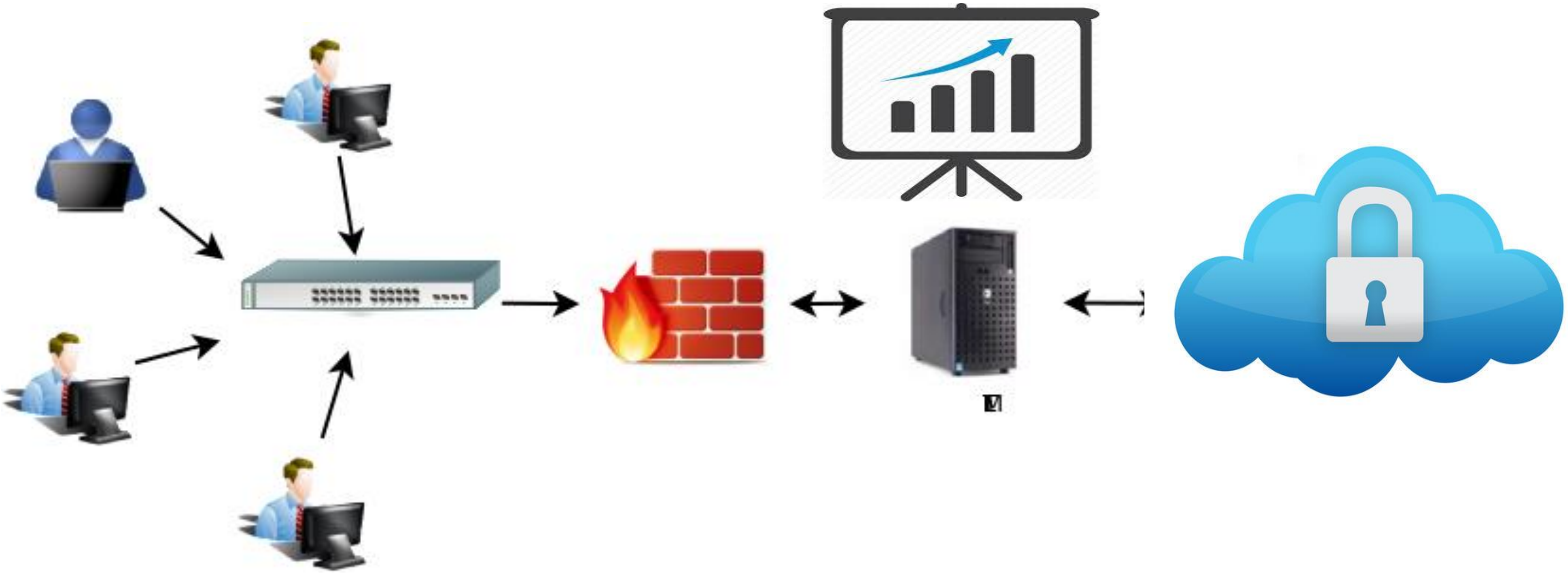
Encrypted Traffic

Encrypted Traffic

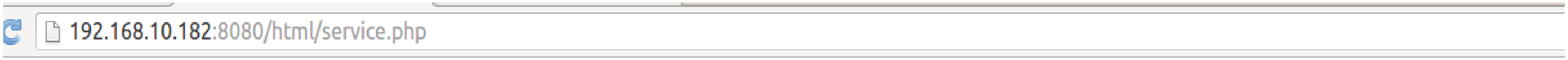
LTM HTTPS traffic inspecting process

LTM deployment scenario


LightWeight Traffic Monitoring Dashboard - Chromium
192.168.10.182:9090/home/dashboard
LightWeight Traffic Monitoring Dashboard
Date Time
Http Type
Method
URL
Host
Source IP
Destination IP
Content Type
Content Encoding
File Name



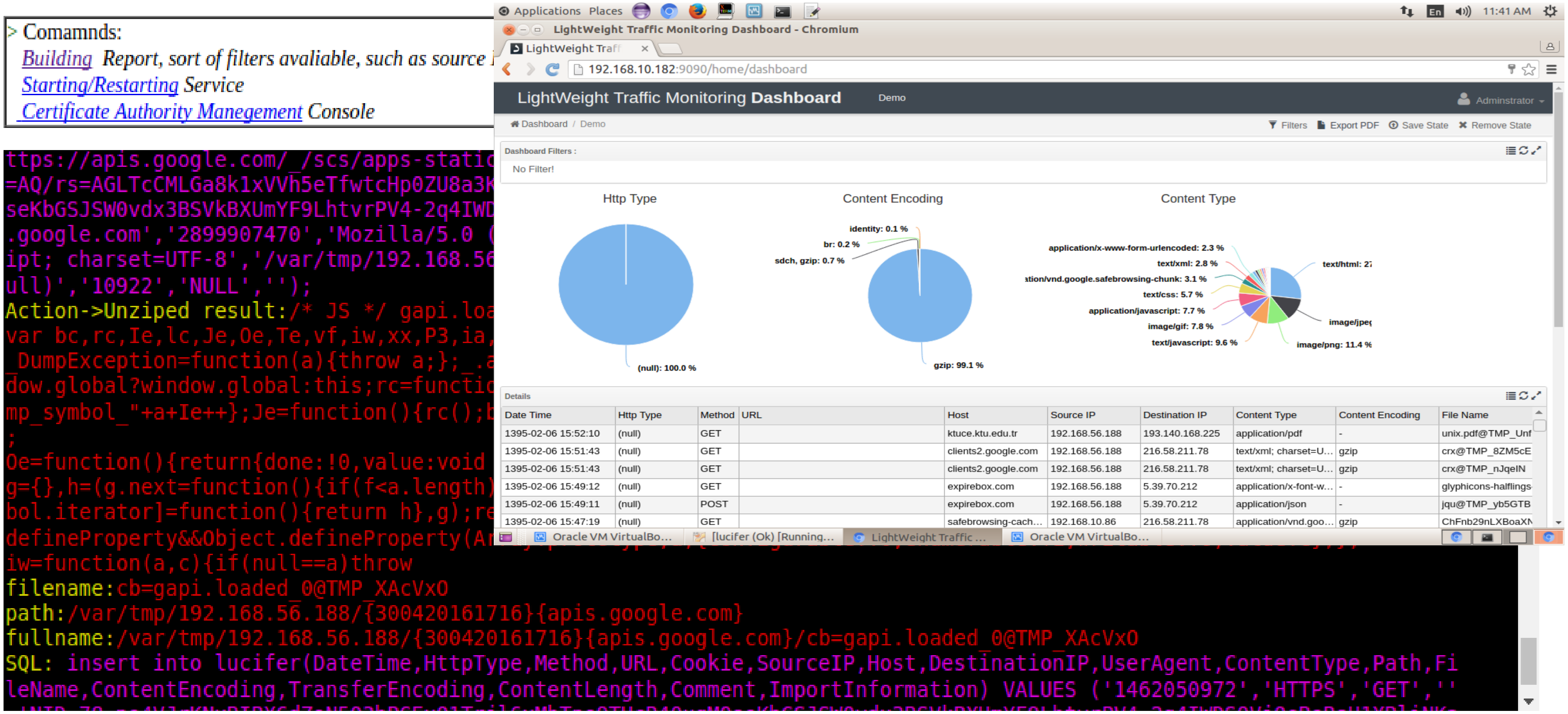
>> This can be done manually from the client by clicking the broken padlock key in your browser and installing the certificate in to the “Trusted Root Certification Authorities”, or you can do this for all clients using Active Directory Group Policies



192.168.10.182:8080/html/service.php

screenshot

Lightweight Traffic Monitoring



> Comamnds:

[Building](#) *Report, sort of filters avaliable, such as source i*

[Starting/Restarting](#) *Service*

[Certificate Authority Manegement](#) *Console*

```
ttps://apis.google.com/_/scs/apps-static
=AQ/rs=AGLTcCMLGa8k1xVVh5eTfwtcHp0ZU8a3K
seKbGSJSW0vdx3BSVkBXUmYF9LhtvrPV4-2q4IWD
.google.com','2899907470','Mozilla/5.0 (
ipt; charset=UTF-8','/var/tmp/192.168.56
ull)','10922','NULL','');
Action->Unziped result:/* JS */ gapi.loa
var bc,rc,Ie,lc,Je,Oe,Te,vf,iw,xx,P3,ia,
_DumpException=function(a){throw a;};_.a
dow.global?window.global:this;rc=functio
mp_symbol_"+a+Ie++};Je=function(){rc();b
;
Oe=function(){return{done:!0,value:void
g={},h=(g.next=function(){if(f<a.length)
bol.iterator]=function(){return h},g);re
defineProperty&&Object.defineProperty(Ar
iw=function(a,c){if(null==a)throw
filename:cb=gapi.loaded_0@TMP_XAcVxO
path:/var/tmp/192.168.56.188/{300420161716}{apis.google.com}
fullname:/var/tmp/192.168.56.188/{300420161716}{apis.google.com}/cb=gapi.loaded_0@TMP_XAcVxO
SQL: insert into lucifer(DateTime,HttpType,Method,URL,Cookie,SourceIP,Host,DestinationIP,UserAgent,ContentType,Path,Fi
leName,ContentEncoding,TransferEncoding,ContentLength,Comment,ImportInformation) VALUES ('1462050972','HTTPS','GET',''
```

LightWeight Traffic Monitoring Dashboard - Chromium

192.168.10.182:9090/home/dashboard

LightWeight Traffic Monitoring **Dashboard**

Dashboard / Demo

Dashboard Filters :

No Filter!

Details

Date Time	Http Type	Method	URL	Host	Source IP	Destination IP	Content Type	Content Encoding	File Name
1395-02-06 15:52:10	(null)	GET		ktuce.ktu.edu.tr	192.168.56.188	193.140.168.225	application/pdf	-	unix.pdf@TMP_Unf
1395-02-06 15:51:43	(null)	GET		clients2.google.com	192.168.56.188	216.58.211.78	text/xml; charset=U…	gzip	crx@TMP_8ZM5cE
1395-02-06 15:51:43	(null)	GET		clients2.google.com	192.168.56.188	216.58.211.78	text/xml; charset=U…	gzip	crx@TMP_nJqeIN
1395-02-06 15:49:12	(null)	GET		expirebox.com	192.168.56.188	5.39.70.212	application/x-font-w…	-	glyphicons-halflings
1395-02-06 15:49:11	(null)	POST		expirebox.com	192.168.56.188	5.39.70.212	application/json	-	jqu@TMP_yb5GTB
1395-02-06 15:47:19	(null)	GET		safebrowsing-cach…	192.168.10.86	216.58.211.78	application/vnd.goo…	gzip	ChFnb29nLXBoaXN

Scenario

- Auditing visited pages & contents
- Auditing files has been downloaded/uploaded
- Sort of keywords & credentials