Advanced Threat Mitigations via SSL Intercept

Jason Rahm, 2016-23-02

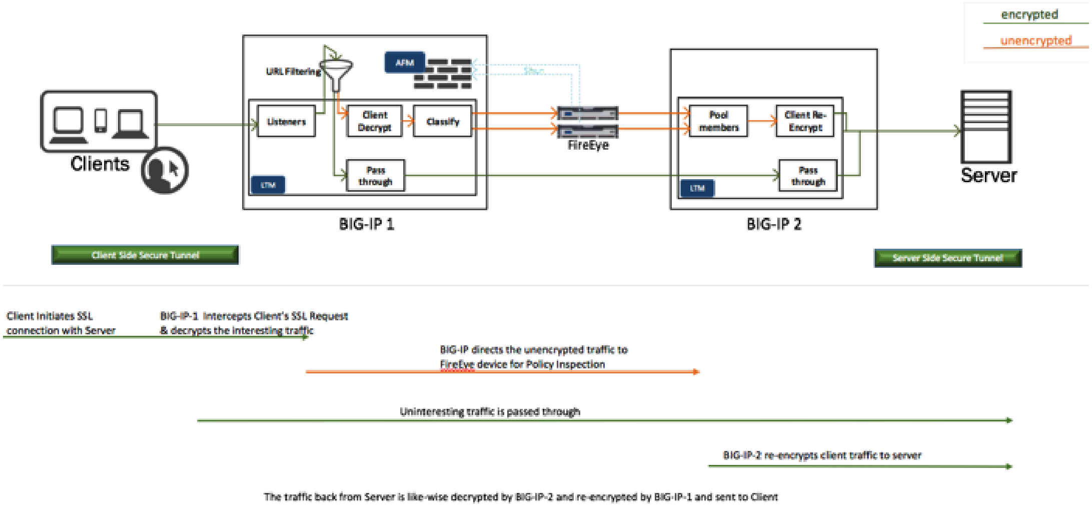
SSL offload has been around for quite some time. But this technology was primarily developed for the web farm audience, offloading SSL traffic from the application servers and putting the load on application delivery controllers like F5's BIG-IP. With the push for SSL Everywhere in the last few years, the need for corporations to have visibility to the traffic from their internal clients (could be employees or internal application services reaching out to external services via APIs) to external services that are encrypted. Without the ability to decrypt and inspect that traffic before it leaves the perimeter and as it returns from the outer reaches of the internet, corporations are exposed to significant risks such as information leakage and loss, general malware at best but botnet command and control communication channels at worst, but corporations are also exposed to the softer productivity risks like employee time management while on the clock.

This is where inspection via SSL intercept comes in. We partner with FireEye to offer combined best in class performance and visibility. Peter also sat down with Sam Ware from FireEye at RSA last year to discuss the solutions and partnership. But enough of the marketing…how does it work? In a traditional reverse proxy scenario, the SSL offload requires that you have the private key and certificate in order to decrypt and inspect. But with the forward proxy scenario, well, we don't have the private keys to all the sites on the internet. So another solution is necessary. I've queued this episode of Whiteboard Wednesday at the point where the process of how to configure and insert the BIG-IP into the trust relationship between client and server is broken down.

Once the air gap is in place with the SSL intercept configuration, this unencrypted traffic can be diverted through inspection devices like FireEye to monitor and act on any disallowed or malicious traffic. There are a couple ways this can be deployed.

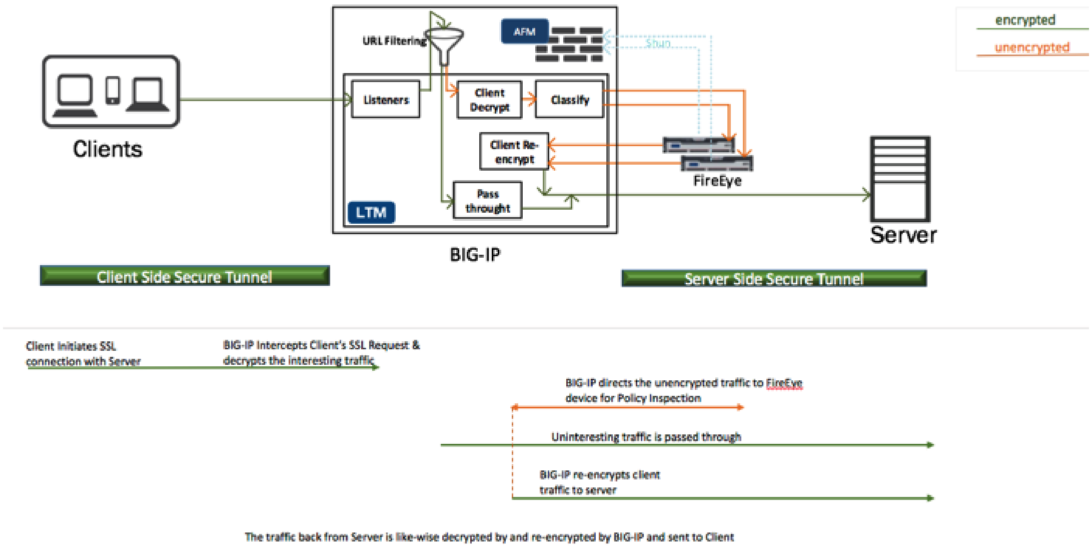
Layered SSL Intercept Solution

In this solution, there is a front-side and a back-side BIG-IP handling the encryption with clients and servers, respectively. In the middle, interesting traffic is unencrypted and passed through the inspect points. The great thing about this solution is the initial inspection point is on the BIG-IP, so if there are some destinations that require no inspection, those can be immediately re-encrypted and sent on without sending through the external inspection point.


encrypted
unencrypted
URL Filtering
AFM
Shun
Listeners
Client Decrypt
Classify
Pass through
LTM
FireEye
Pool members
Client Re-Encrypt
Pass through
LTM
Clients
BIG-IP 1
BIG-IP 2
Server
Client Side Secure Tunnel
Server Side Secure Tunnel
Client Initiates SSL connection with Server
BIG-IP-1 Intercepts Client's SSL Request & decrypts the interesting traffic
BIG-IP directs the unencrypted traffic to FireEye device for Policy Inspection
Uninteresting traffic is passed through
BIG-IP-2 re-encrypts client traffic to server
The traffic back from Server is like-wise decrypted by BIG-IP-2 and re-encrypted by BIG-IP-1 and sent to Client

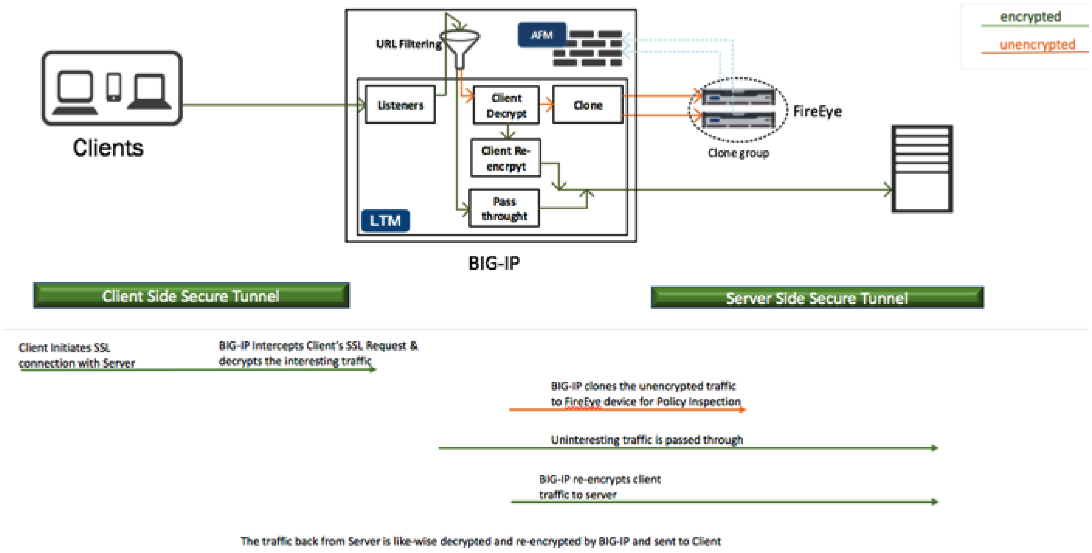
One-Armed SSL Intercept Solution

In this solution, there is only one BIG-IP, and so the front-side and back-side functions of the air gap are combined into the single device. Functionally they are equivalent, just less hardware in the picture.


encrypted
unencrypted
URL Filtering
AFM
Shun
Listeners
Client Decrypt
Classify
Client Re-encrypt
Pass throught
LTM
FireEye
Clients
Server
BIG-IP
Client Side Secure Tunnel
Server Side Secure Tunnel
Client Initiates SSL connection with Server
BIG-IP Intercepts Client's SSL Request & decrypts the interesting traffic
BIG-IP directs the unencrypted traffic to FireEye device for Policy Inspection
Uninteresting traffic is passed through
BIG-IP re-encrypts client traffic to server
The traffic back from Server is like-wise decrypted by and re-encrypted by BIG-IP and sent to Client

Clone Solution

In the event the enforcement angle of the solution is not desired, the traffic can be cloned off to the FireEye for monitoring and alerting, but still be passed along uninhibited by the infrastructure.


encrypted
unencrypted
URL Filtering
AFM
Listeners
Client Decrypt
Clone
Client Re-encrpyt
Pass throught
LTM
FireEye
Clone group
Clients
BIG-IP
Client Side Secure Tunnel
Server Side Secure Tunnel
Client Initiates SSL connection with Server
BIG-IP Intercepts Client's SSL Request & decrypts the interesting traffic
BIG-IP clones the unencrypted traffic to FireEye device for Policy Inspection
Uninteresting traffic is passed through
BIG-IP re-encrypts client traffic to server
The traffic back from Server is like-wise decrypted and re-encrypted by BIG-IP and sent to Client

As simple as the drawings make it all look, the configuration is fairly complex. Thankfully there is a fantastic iApp supported by F5 to assist in the deployment. It is linked below in the resources.

Resources

- FireEye Solutions on F5.com
- Air Gap Egress Inspection with SSL Intercept iApp Template
- Air Gap Deployment Guide
- SSL Everywhere Reference Architecture - Best Practices

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com