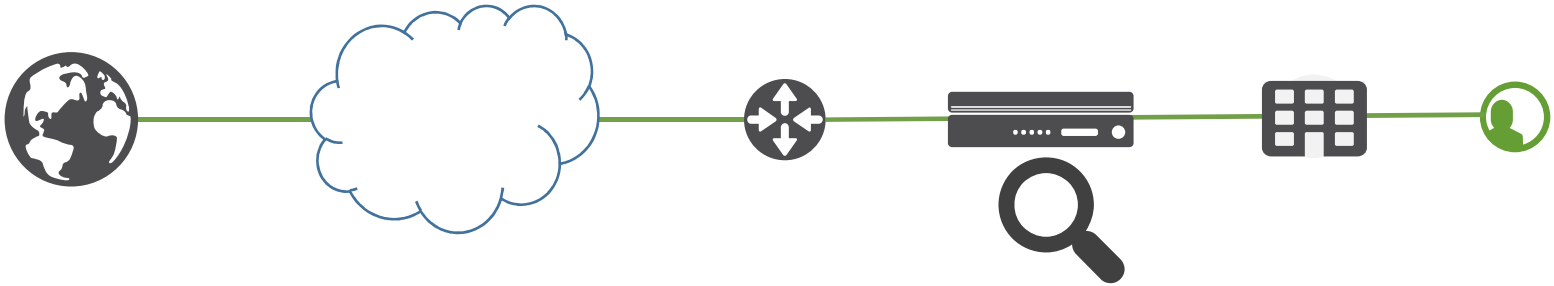
HTTPS kui infoturbe risk

ja mida selle riski vähendamiseks ette võtta

Tarmo Mamers

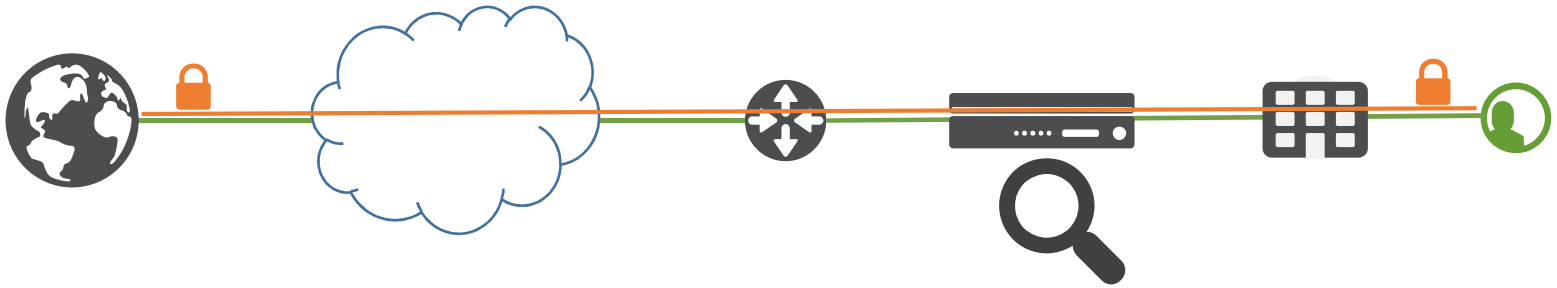
HTTP

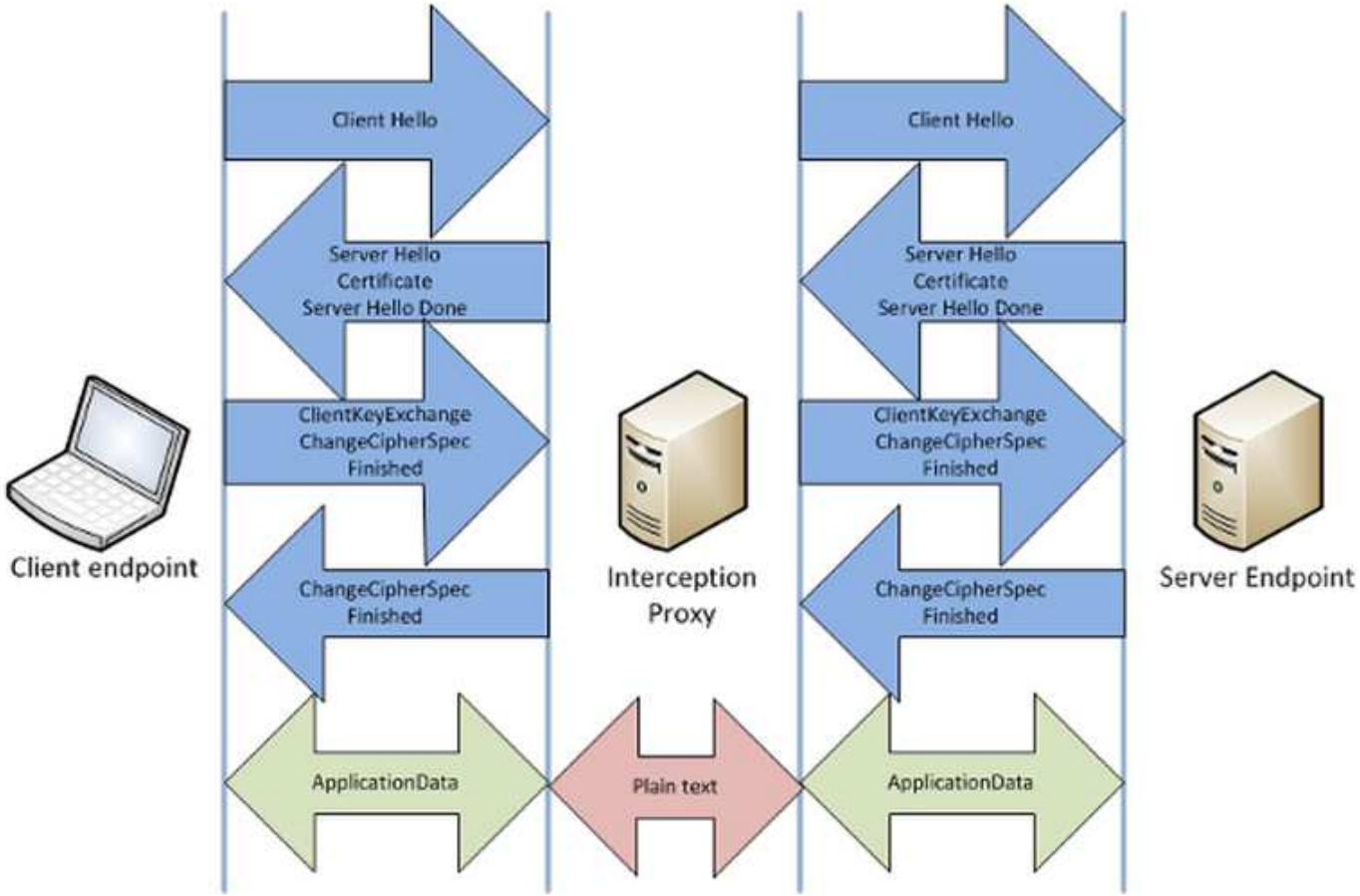
Everything over HTTP

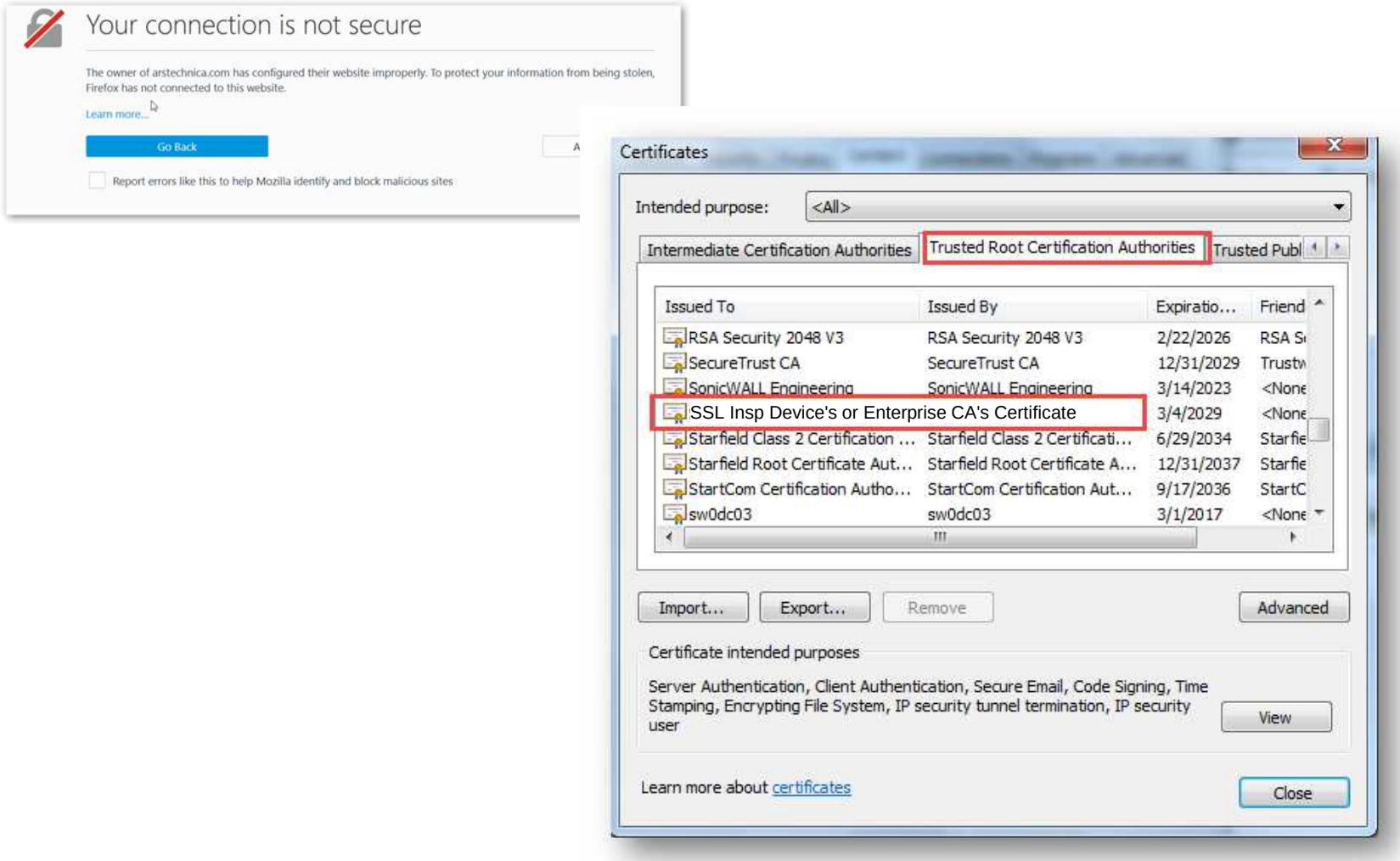


HTTPS

Everything over HTTPS

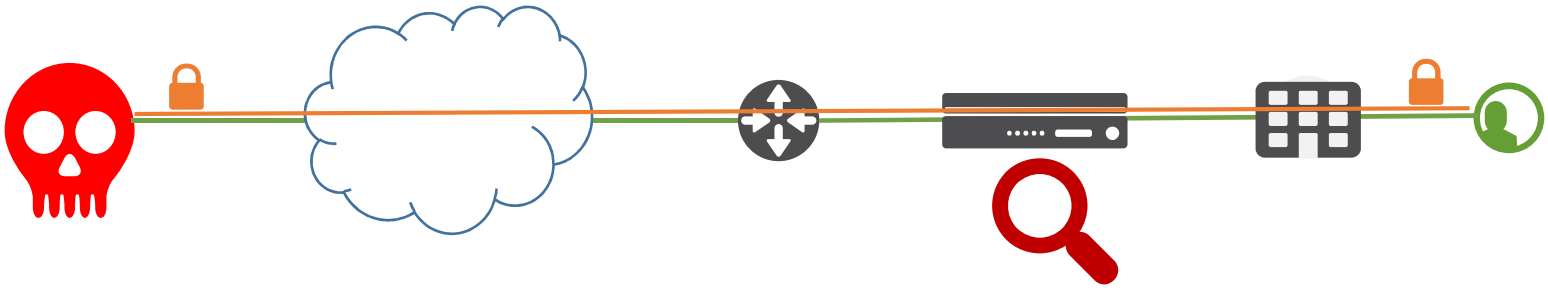






HTTPS

Threats over HTTPS



F5 Networks: SSL Orchestrator

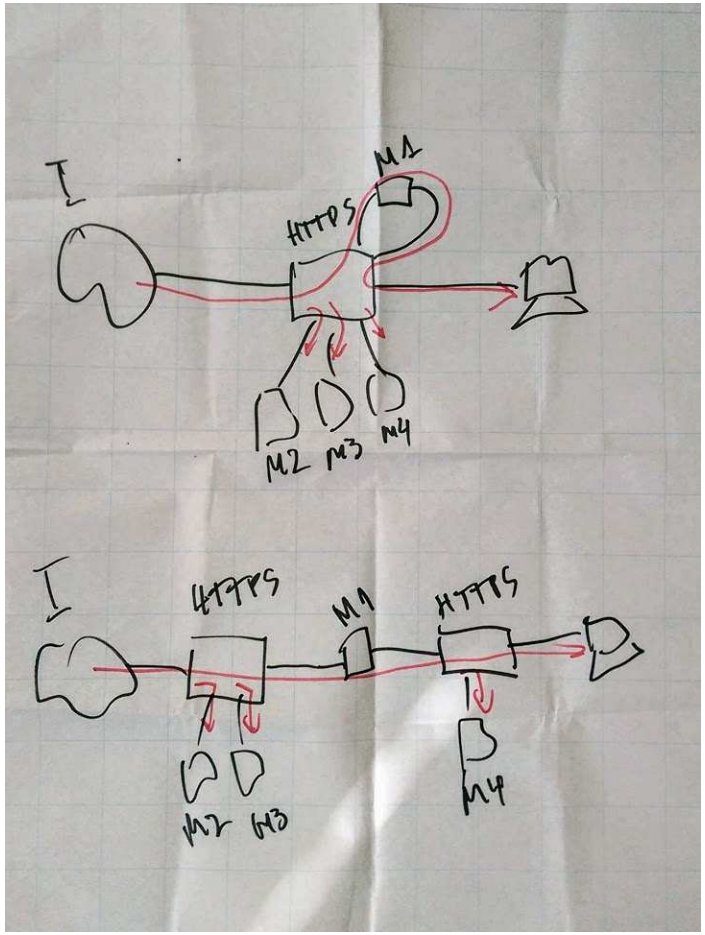
- 1-box
- 2-box

- L2 in-line
- L3 in-line
- ICAP
- receive-only

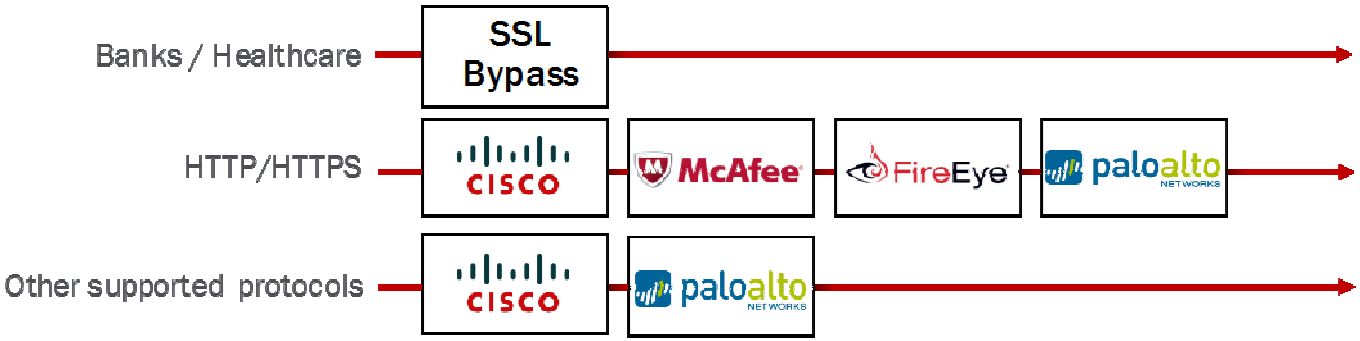
F5 Networks: SSL Orchestrator

- Herculon SSLO appliance
- iApp on BIGIP (v12.1+)
  - appliance: LTM + SSL Forward Proxy
  - VE: LTM + SSL Forward Proxy
- IPI subscription
- URLF subscription

Deployment modes



Dynamic Service Chaining



DSC Policies

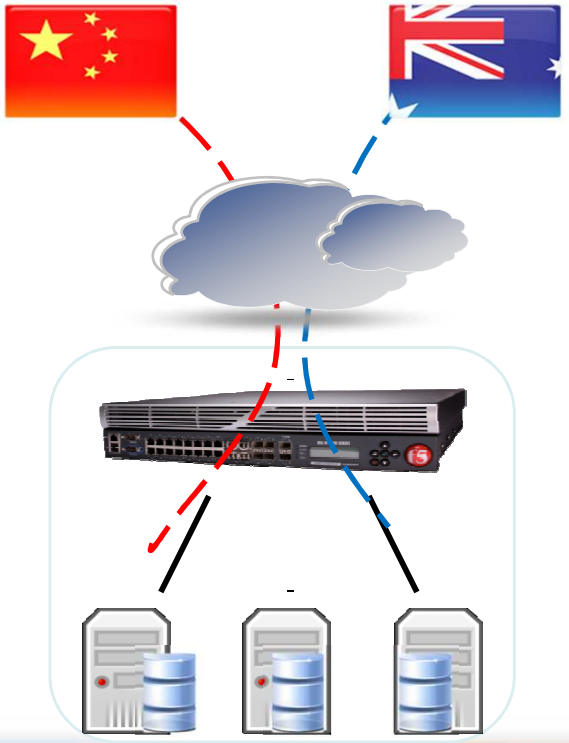
- Source IP
- Destination IP
- IP intelligence [subscription]
- IP geolocation
- Domain name
- URL category [subscription]
- Destination port
- Protocol

IP Reputation Services

Know where traffic is coming from…
Make intelligent decisions based on a client's IP address.
Cloud based services provide location and reputation information.

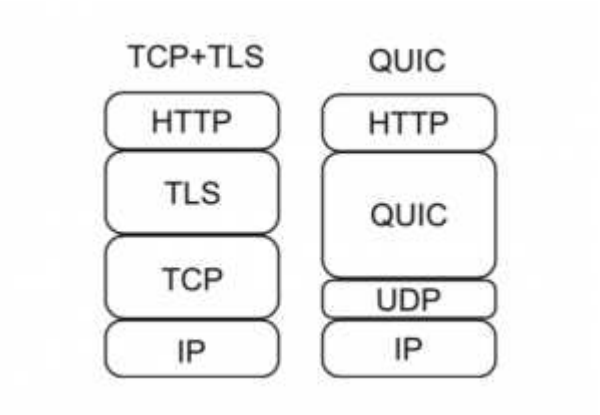
WEBROOT digital envoy McAfee An Intel Company

IP Reputation	IP Location	Spam Reputation
• OS Exploits	• Continent	• Spam Source
• Web Attacks	• Country	
• Botnets	• State	
• Scanners	• Carrier	
• DoS Attacks	• Registered Org	
• Proxy	• City	
• Phishing	• Post / Zip Code	
	• Lat / Long	



HTTPS is not alone

Try blocking all outbound tcp/443 in your firewall
You're still able to surf Google and Youtube



Hint: QUIC udp/443 Quick UDP Internet Connections