

HTTPS kui infoturbe risk

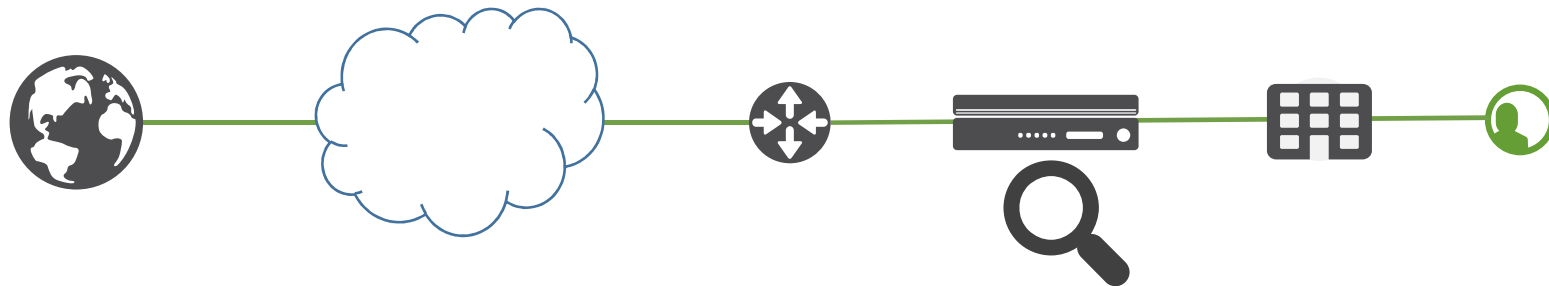
ja mida selle riski vähendamiseks ette võtta

Tarmo Mammers



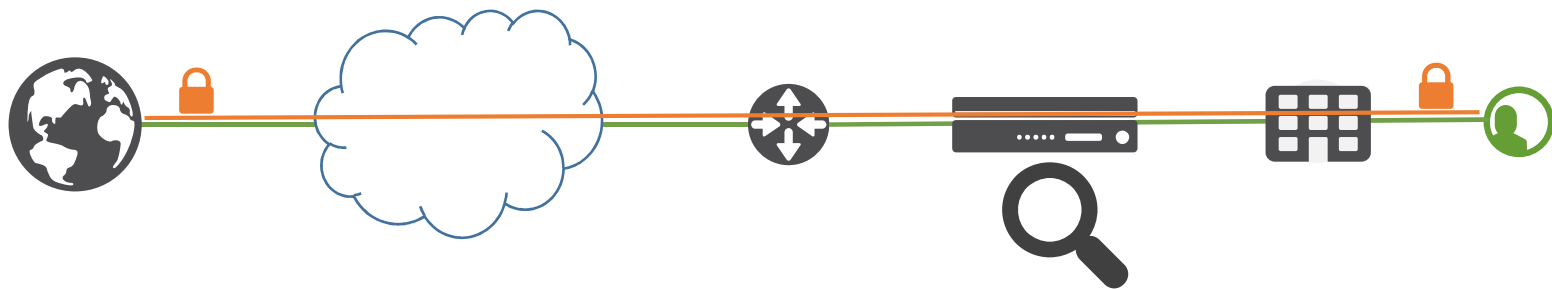
HTTP

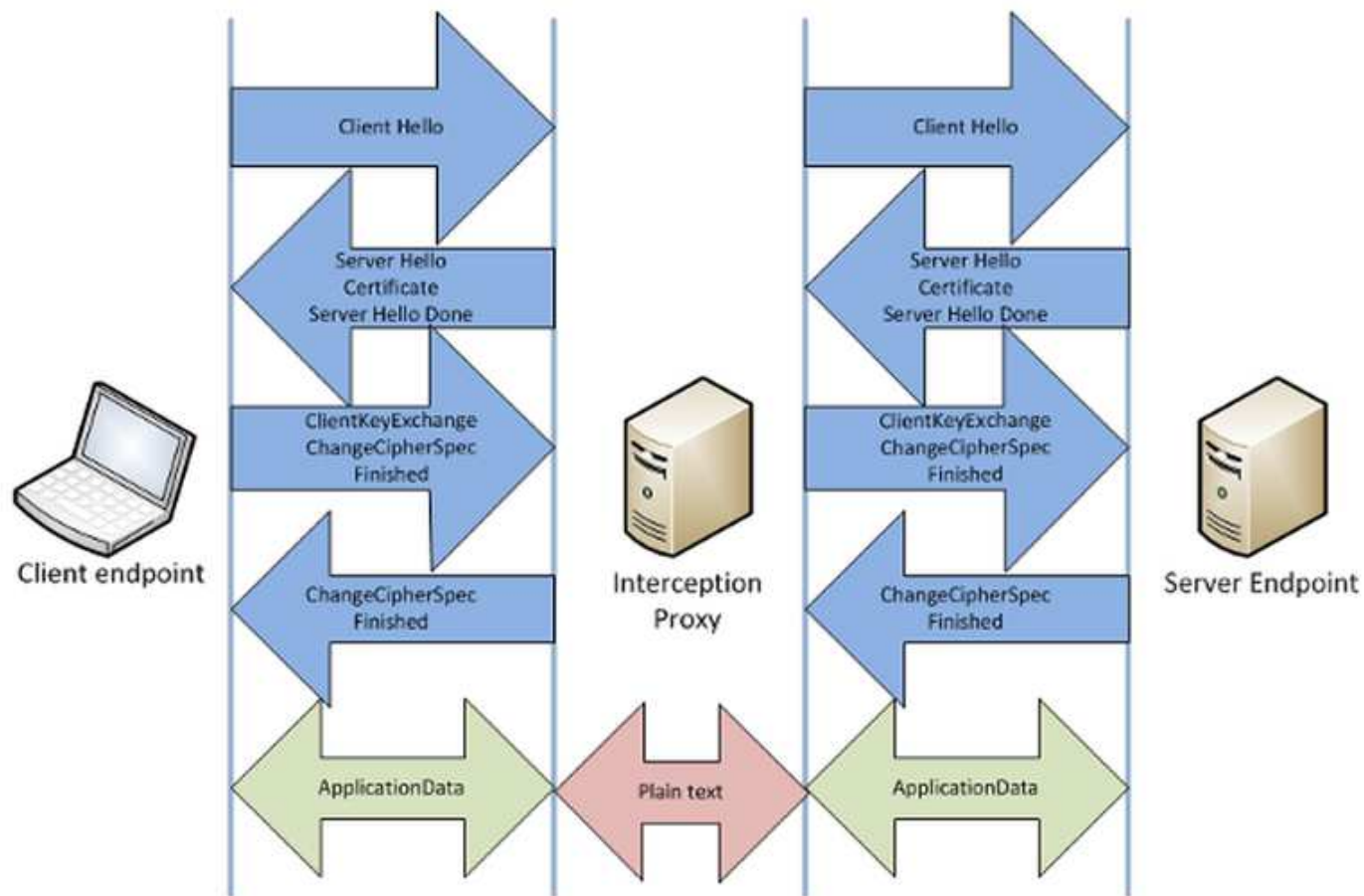
Everything over HTTP



HTTPS

Everything over HTTPS







Your connection is not secure

The owner of arstechnica.com has configured their website improperly. To protect your information from being stolen, Firefox has not connected to this website.

[Learn more...](#)

[Go Back](#)

Report errors like this to help Mozilla identify and block malicious sites

Certificates

Intended purpose: <All>

Intermediate Certification Authorities | **Trusted Root Certification Authorities** | Trusted Publ

Issued To	Issued By	Expiratio...	Friend
RSA Security 2048 V3	RSA Security 2048 V3	2/22/2026	RSA S...
SecureTrust CA	SecureTrust CA	12/31/2029	Trustw...
SonicWALL Engineering	SonicWALL Engineering	3/14/2023	<None
SSL Insp Device's or Enterprise CA's Certificate		3/4/2029	<None
Starfield Class 2 Certification ...	Starfield Class 2 Certificati...	6/29/2034	Starfie
Starfield Root Certificate Aut...	Starfield Root Certificate A...	12/31/2037	Starfie
StartCom Certification Autho...	StartCom Certification Aut...	9/17/2036	StartC
sw0dc03	sw0dc03	3/1/2017	<None

Import... Export... Remove Advanced

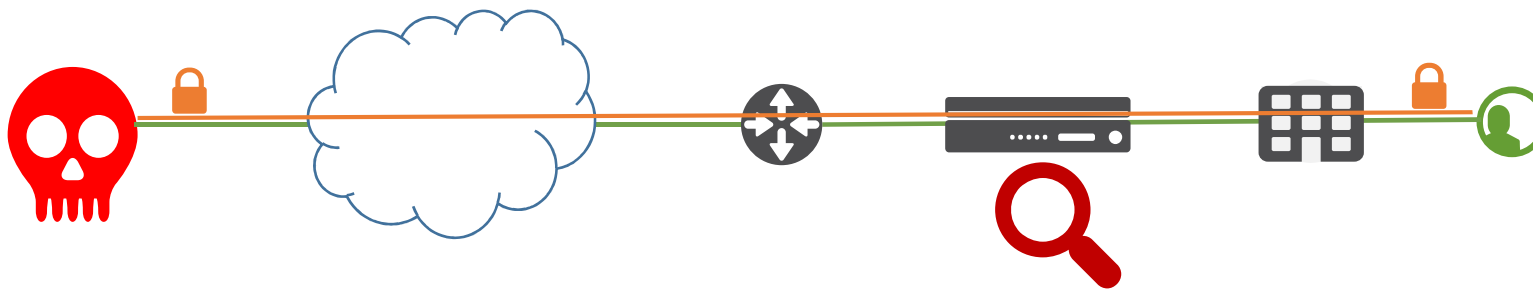
Certificate intended purposes

Server Authentication, Client Authentication, Secure Email, Code Signing, Time Stamping, Encrypting File System, IP security tunnel termination, IP security user [View](#)

[Learn more about certificates](#) [Close](#)

HTTPS

Threats over HTTPS



F5 Networks: SSL Orchestrator

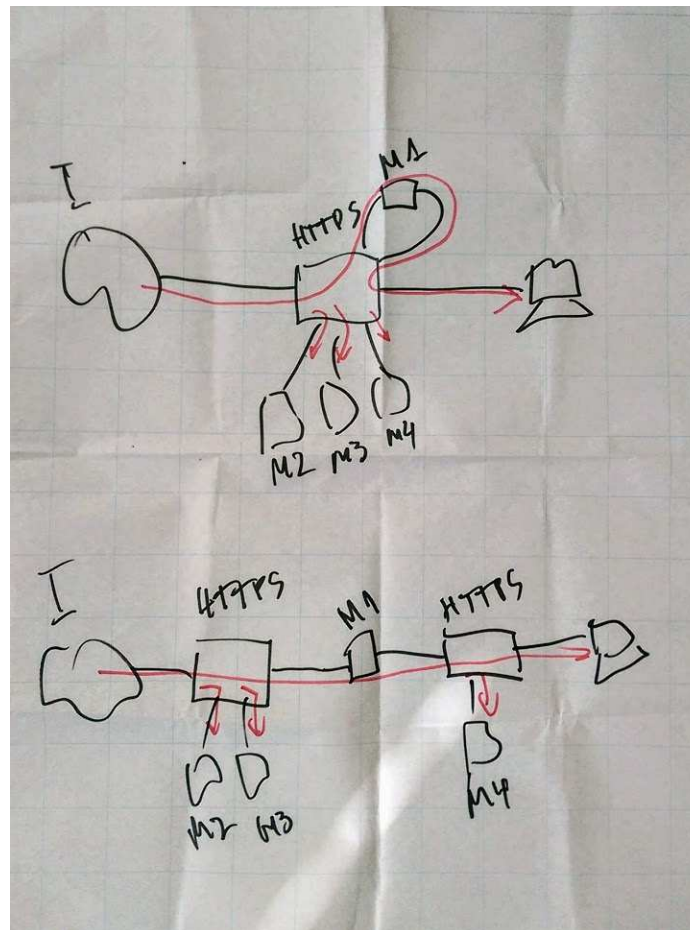
- 1-box
- 2-box

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

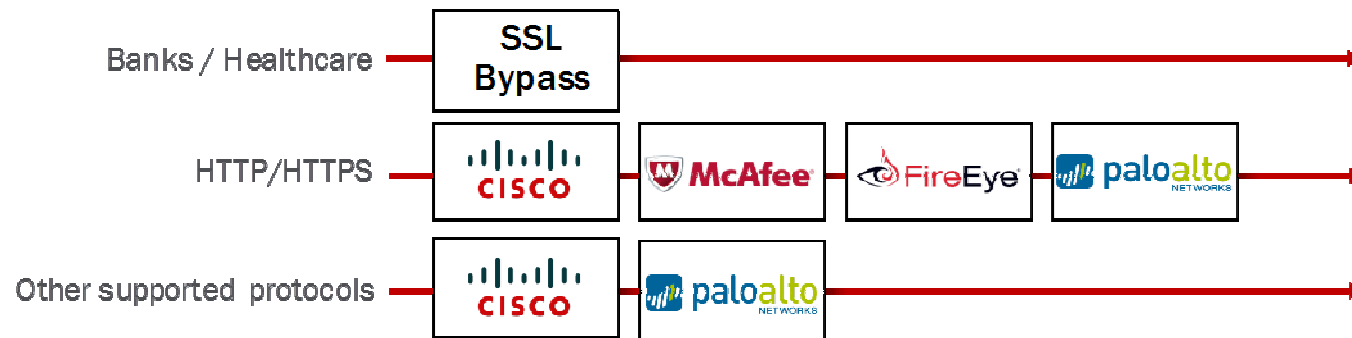
F5 Networks: SSL Orchestrator

- 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




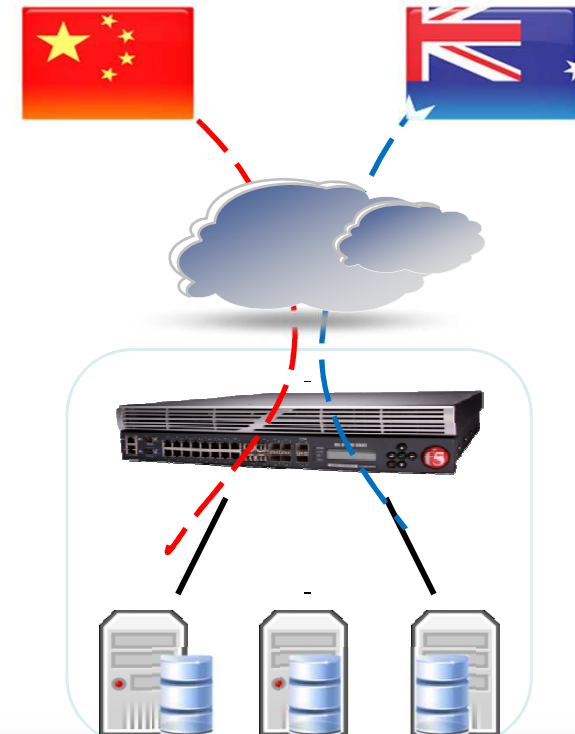
DSC Policies

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

IP Reputation Services

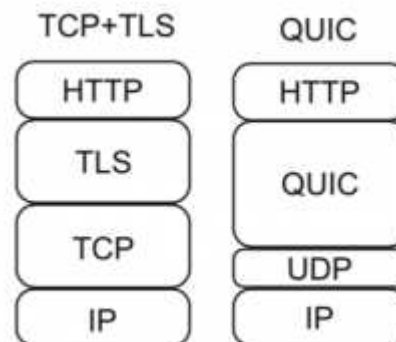
Know where traffic is coming from...
 Make intelligent decisions based on a client's IP address.
 Cloud based services provide location and reputation information.

		
IP Reputation	IP Location	Spam Reputation
<ul style="list-style-type: none"> OS Exploits 	<ul style="list-style-type: none"> Continent 	<ul style="list-style-type: none"> Spam Source
<ul style="list-style-type: none"> Web Attacks 	<ul style="list-style-type: none"> Country 	
<ul style="list-style-type: none"> Botnets 	<ul style="list-style-type: none"> State 	
<ul style="list-style-type: none"> Scanners 	<ul style="list-style-type: none"> Carrier 	
<ul style="list-style-type: none"> DoS Attacks 	<ul style="list-style-type: none"> Registered Org 	
<ul style="list-style-type: none"> Proxy 	<ul style="list-style-type: none"> City 	
<ul style="list-style-type: none"> Phishing 	<ul style="list-style-type: none"> Post / Zip Code 	
	<ul style="list-style-type: none"> 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