

Contextual Forwarding

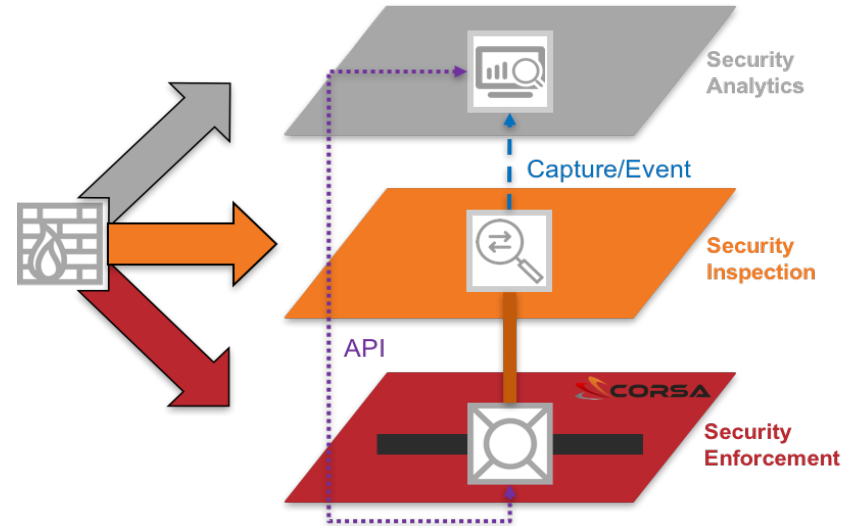
Ed Lopez – Security Architect
ed.lopez@corsa.com

Geo-Political Pressure

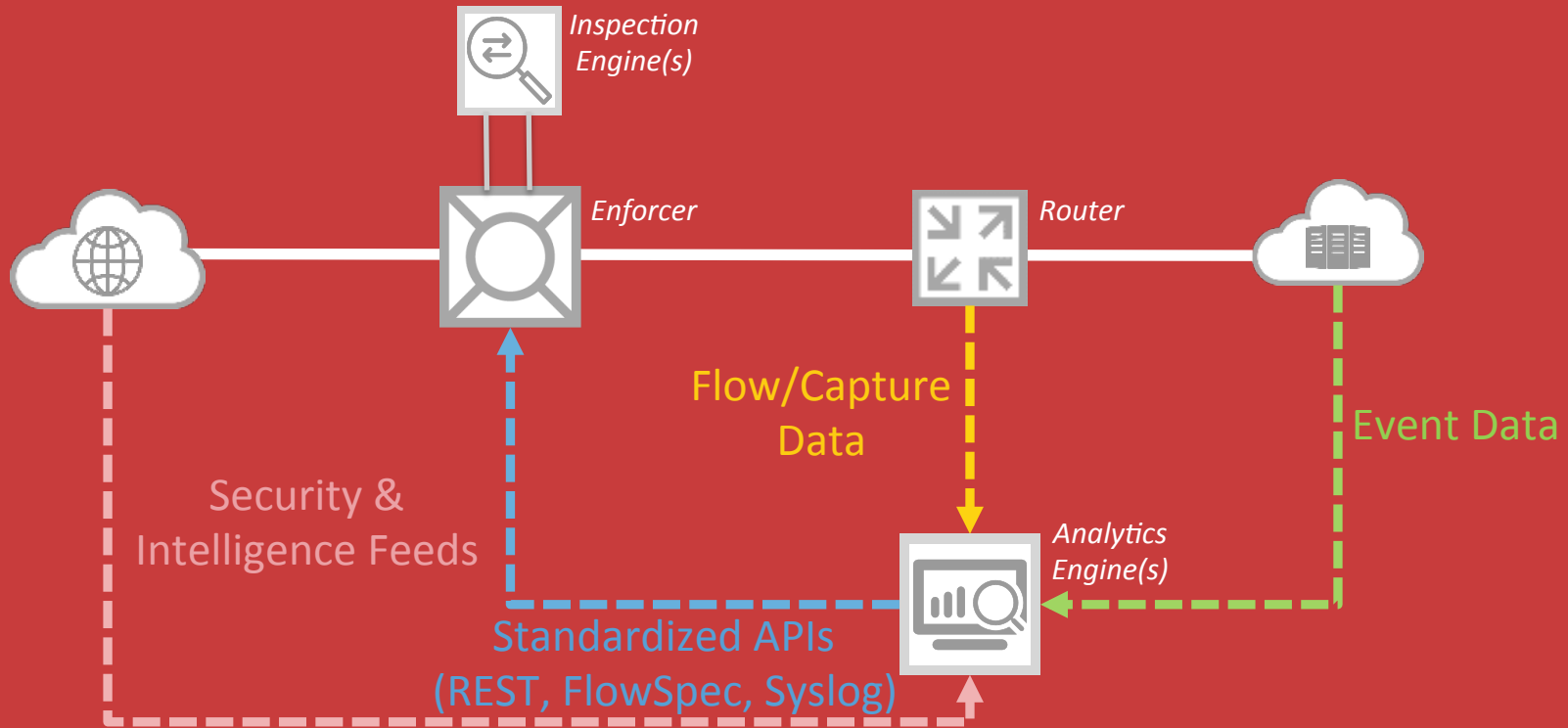
- Renewed calls for “Regulating the Internet” following London Bridge attack
- Concern regarding state-sponsored cyber-events
- Increasing use of device and traffic encryption leading to calls to provide decrypted access
- While much of this pressure is currently directed towards content, application, and device providers, in many cases government intervention into peering is being considered

What is Contextual Forwarding?

- The use of programmable data planes to forward packets based on traffic analysis or inspected content
- Decoupling 'middleboxes' to scale security solutions to meet architectural performance requirements



Implementing Contextual Forwarding



Scaling With Enforcers

- An enforcer evaluates packets of a virtual-wire, using dynamic ACLs and multi-tuple programmable flow rules
 - Unlike SDN, enforcers use standardized APIs to convert contextual analytics into ACL/flow entries
 - DevOps integration is key
- The enforcer can directly mitigate traffic (pass/block/limit), or can redirect traffic towards near-line inspection engines
 - Support for virtualization and scaling of solutions to meet performance requirements
 - Amplification of security intelligence

Open Is Key

- Use of standardized protocols/APIs
 - BGP FlowSpec, Syslog, REST
 - Emerging standards work is being done (ex DOTS, I2NSF)
- Decoupling ‘middleboxes’ into open-compute for CPU-intensive analytics/inspection and open-networking for contextual forwarding
 - Solutions that scale to meet 100G peer performance
- Many sources of intelligence feeds
- DevOps integration

Thanks!

Questions/Comments Are
Always Welcome!

ed.lopez@corsa.com



REDARMOR