IETF New WG: I2NSF (Interface to Network Security Functions) to Mitigate DDoS attacks

I2NSF Co-Chair:

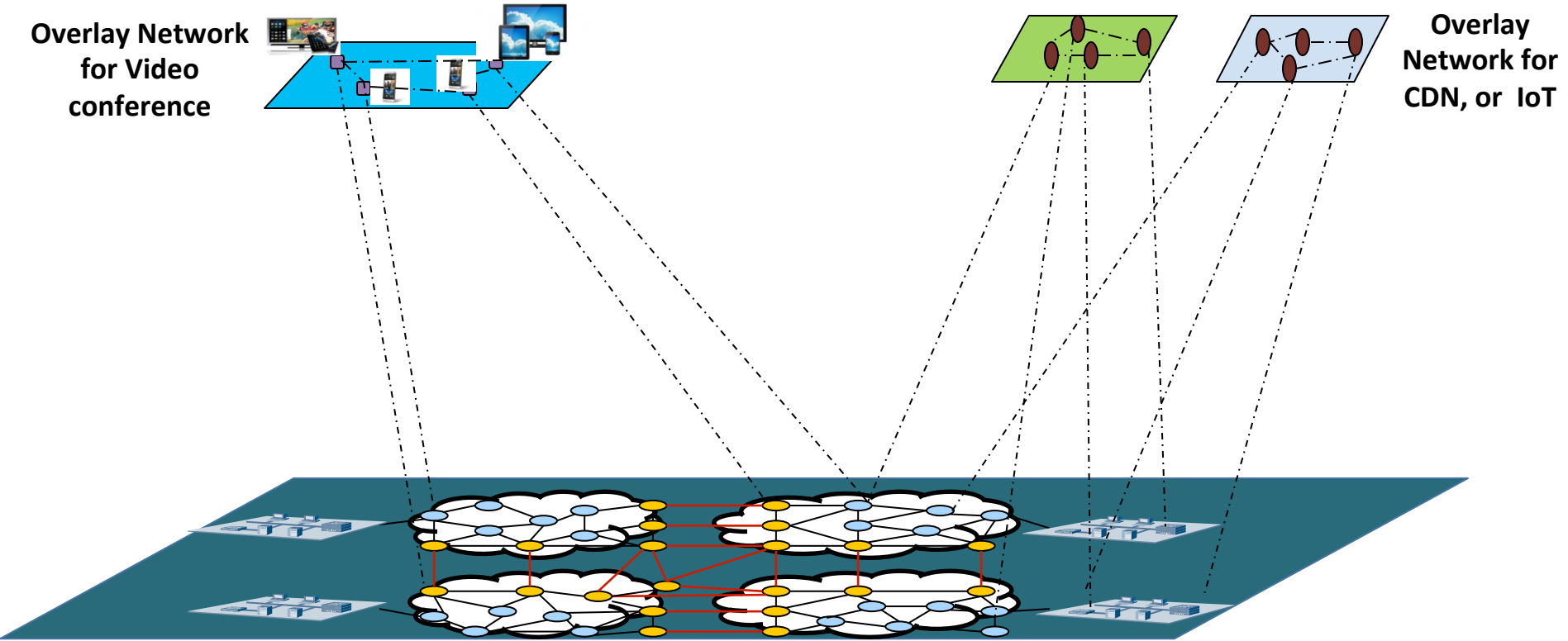
Linda Dunbar (Linda.Dunbar@huawei.com)

Adrian Farrel (adrian@olddog.co.uk)

Implementation slide by

rkkumar@juniper.net

More and More Overlay Networks

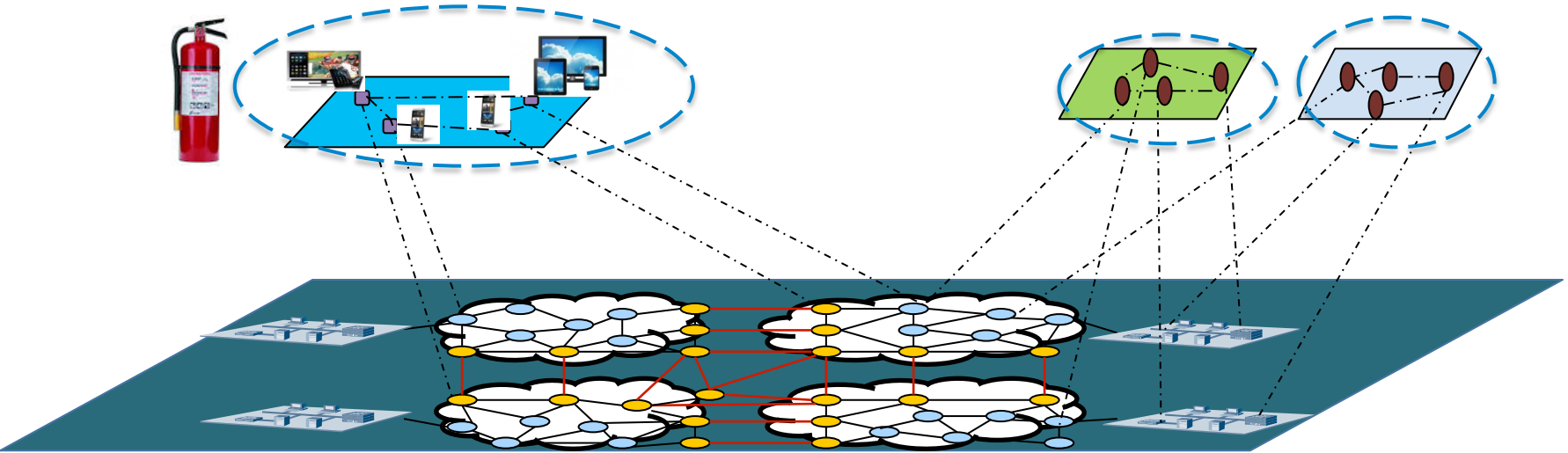


Shared Network: routers, switches, service functions (virtual/physical)

Security for Overlay Network

The State of Being Free from Danger or Threat:

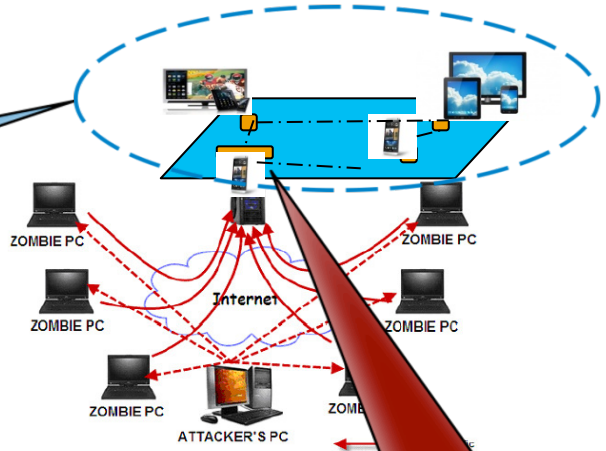
- Confidentiality, Integrity, Authentication, Access control } Overlay Network
- Shelter from unwanted data (DDoS attack, malicious attack, etc) } Underlay Network
- Guaranteed delivery among the nodes in the overlay



Security and Privacy are the Cornerstones for Overlay Network

- BYOD on steroid, Billions moving end points,
- DDoS attacks: more diverse, sophisticated and larger

pre-defined packet header (e.g. Src/ Dst, TCP/UDP) can be compromised



- inline dedicated devices not only are too expensive, but also becomes bottleneck
- E2E encryption no longer enough.
- Today's static security solutions can no longer catch up with the ever changing and complex security threats.

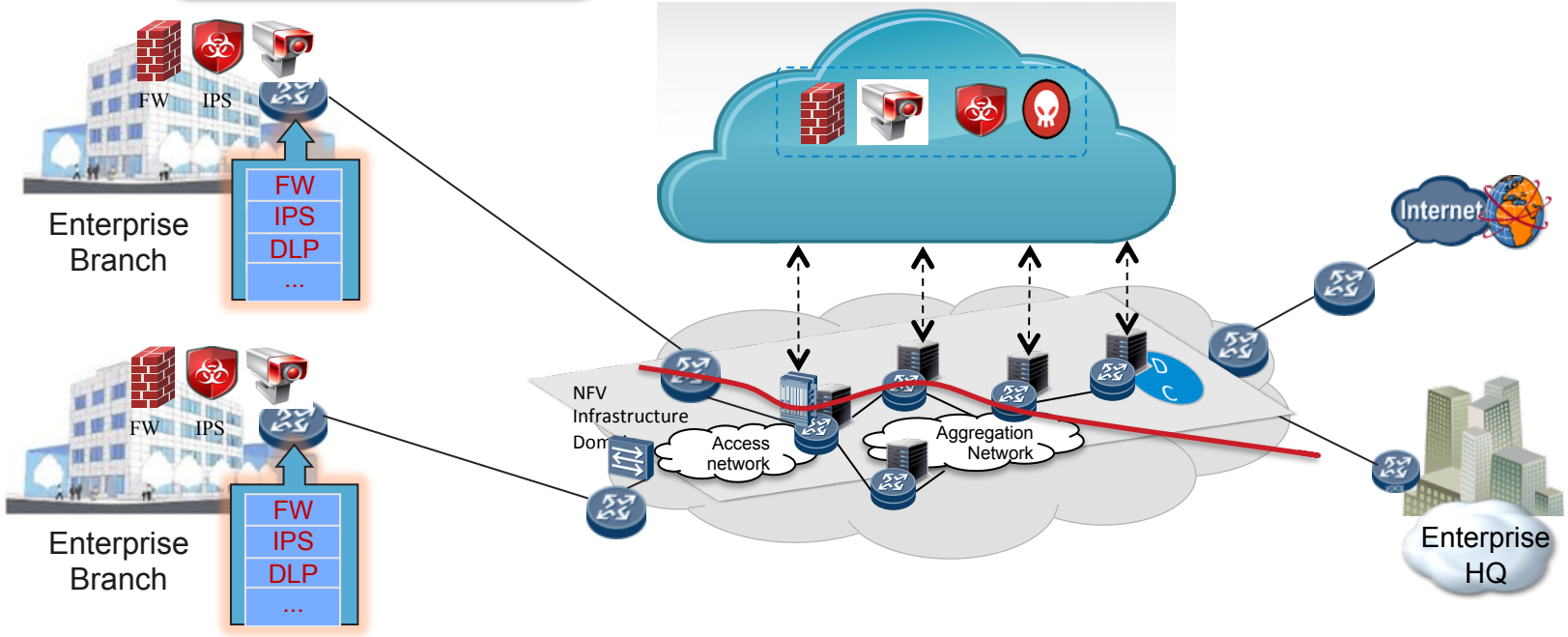
Key:
Allow Applications/clients to control what traffic they are willing to receive, when to receive, and how.

Automation with Virtual Network Functions in Networks ➔ Key Driver for Standardized Interface for Dynamic Rules

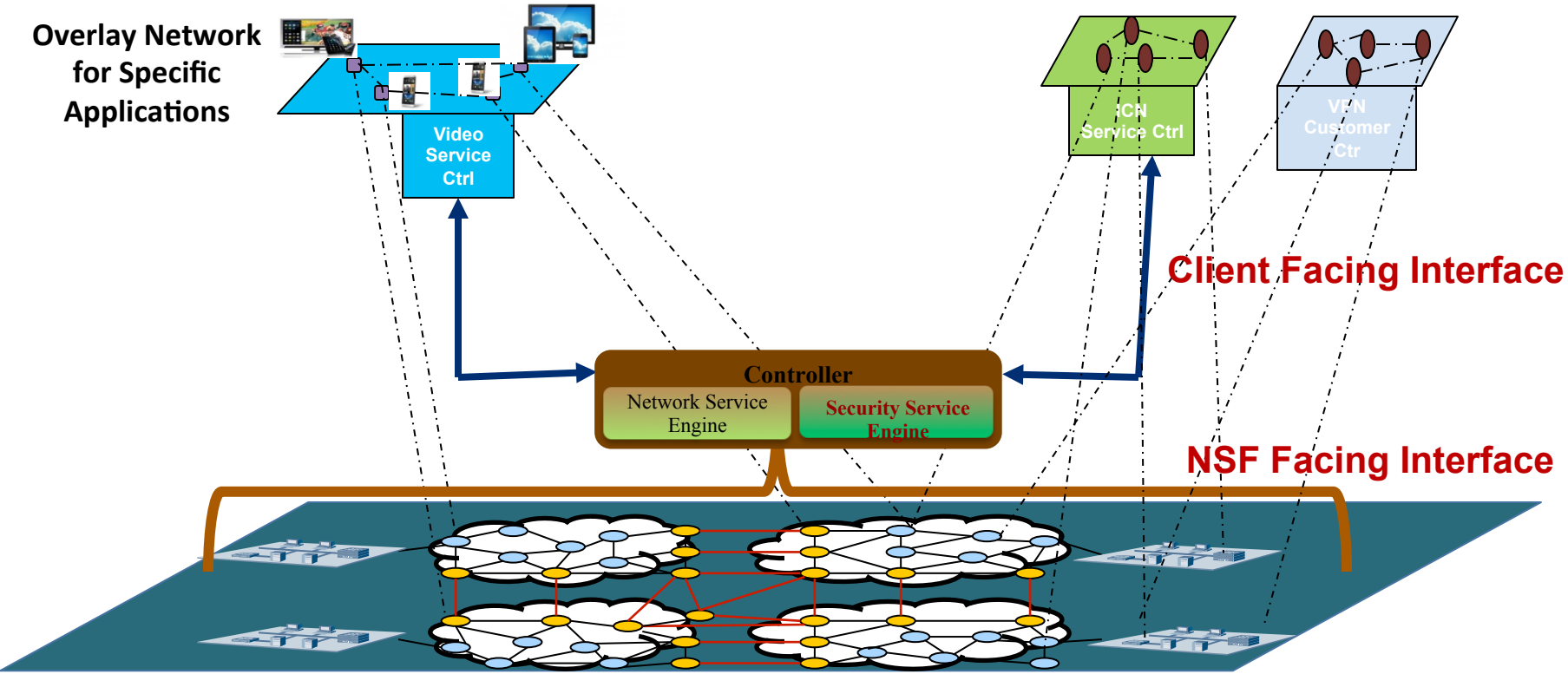
- Reduced need for appliances at the branch
- Easy service delivery
- Open、unified interface to NSF

- Results

- Simpler Branch network security
- Lower OPEX/CAPEX for enterprise
- New revenue opportunity for operator
- Automated deployment



I2NSF Framework

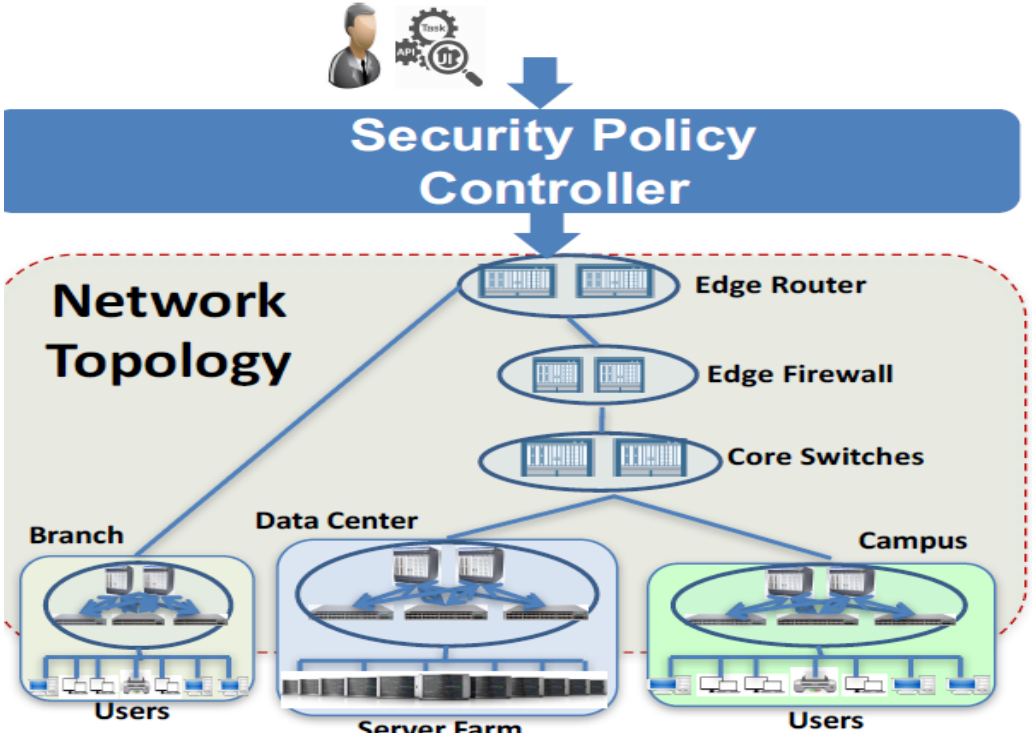


Interface to Network Security Functions – I2NSF

- **Charter:**
  http://datatracker.ietf.org/wg/i2nsf/charter/
- **Mailing List:**
  https://www.ietf.org/mailman/listinfo/i2nsf
- **Working Group Drafts (need your input):**
  - draft-ietf-i2nsf-problem-and-use-cases-02
    I2NSF Problem Statement and Use cases
  - draft-ietf-i2nsf-framework-03
    Framework for Interface to Network Security Functions
  - draft-ietf-i2nsf-terminology-01
    Interface to Network Security Functions (I2NSF) Terminology
  - draft-ietf-i2nsf-gap-analysis-02
    Analysis of Existing work for I2NSF

One vendor implementation

https://youtu.be/MXzJump81zA



- Security Controller
  - A policy controller
- Northbound Interface
  - Security admin interface
  - Policy abstraction
  - Data model driven
- Southbound Interface
  - Security function interface
  - Vendor, Device, Feature agnostic
  - Data model driven
- Secure Network Fabric
  - Policy Enforcement Points

Thank You
Any Questions?