Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines

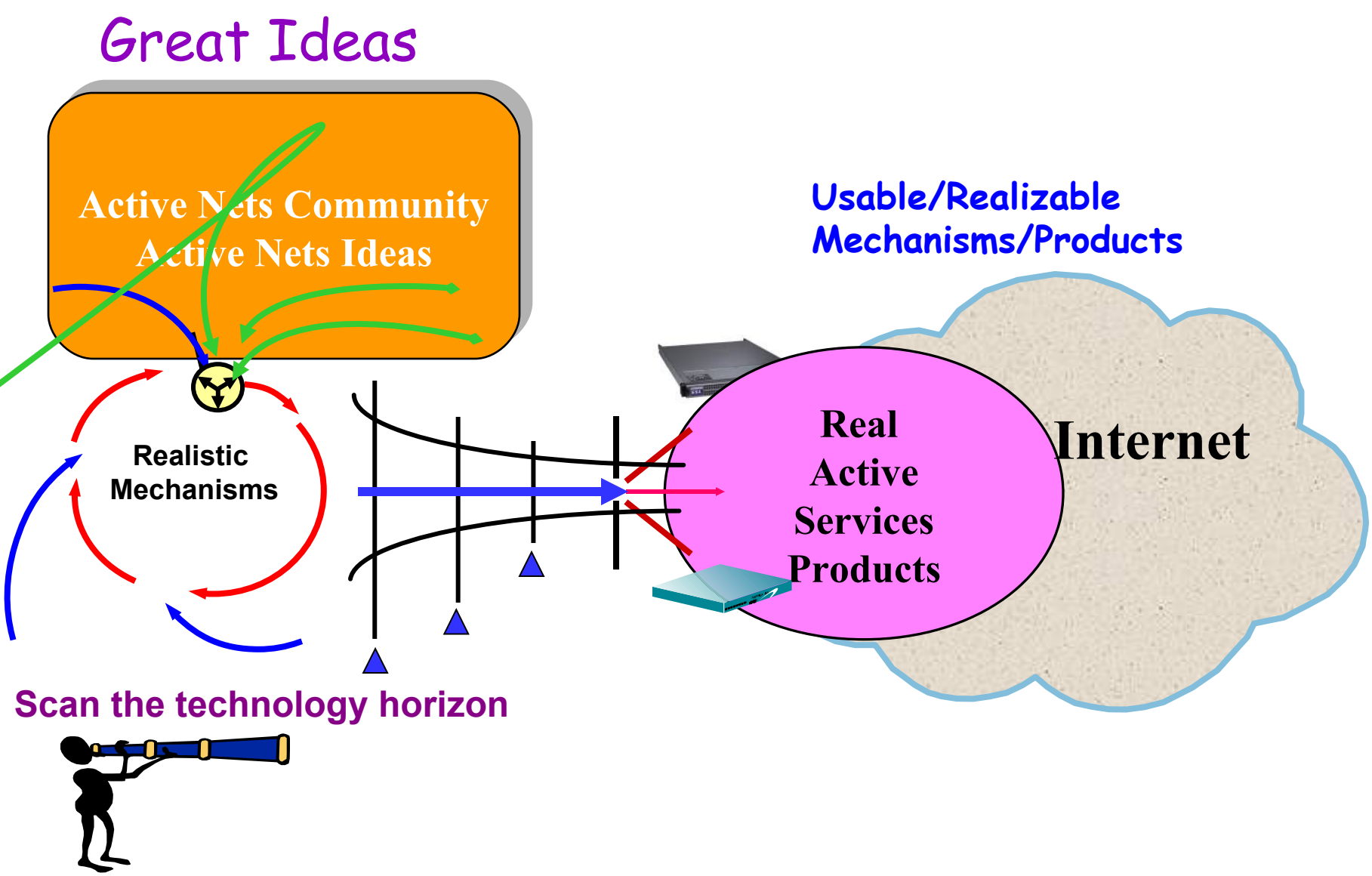
Tal Lavian - tlavian@ieee.org
Phil Wang, Ramesh Durairaj, Jennifer Rasimas, Doan Hoang, Franco Travostino.
Nortel Networks, Advanced Technology Labs

Open Source - http://www.openetlab.org

Outline of the talk

- AN technology Transfer
- Issues in the realization of AN technologies
- Main contributions of the paper.
- Commercial Active Services Platform
- Application Example 1 – SSL
- Application Example 2 – ASF
- A Demo Application
- Next Generation Active Services Platform
- Conclusion

AN Technology Transfer



Any AN products?

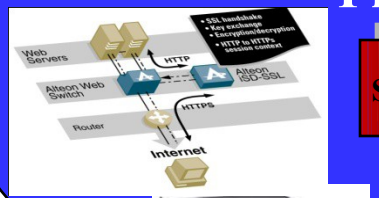
Active Nets Community
Active Nets
Ideas

Realistic
Mechanisms

Experimental/Laboratory
Platforms

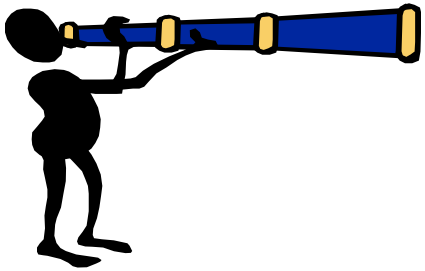
Commercial
Active Services Platform?
?

Nortel Networks
Active Services
Products



SSL ASF IDS VPN

Scan the technology horizon



Great Active Nets Community Solutions

- Active networks (AN) approach opens an exciting opportunity for individual applications to define the service provided by the network through programmability.
- Active Networks technologies expose a novel approach that allows customer value-added services to be introduced to the network "on-the-fly".
- Active Nets program has produced a new network platform flexible and extensible at runtime to accommodate the rapid evolution and deployment of network technologies.
- The exciting opportunity exists for network service providers and third parties, not just the network device providers, to program the network infrastructure and services.

AN issues

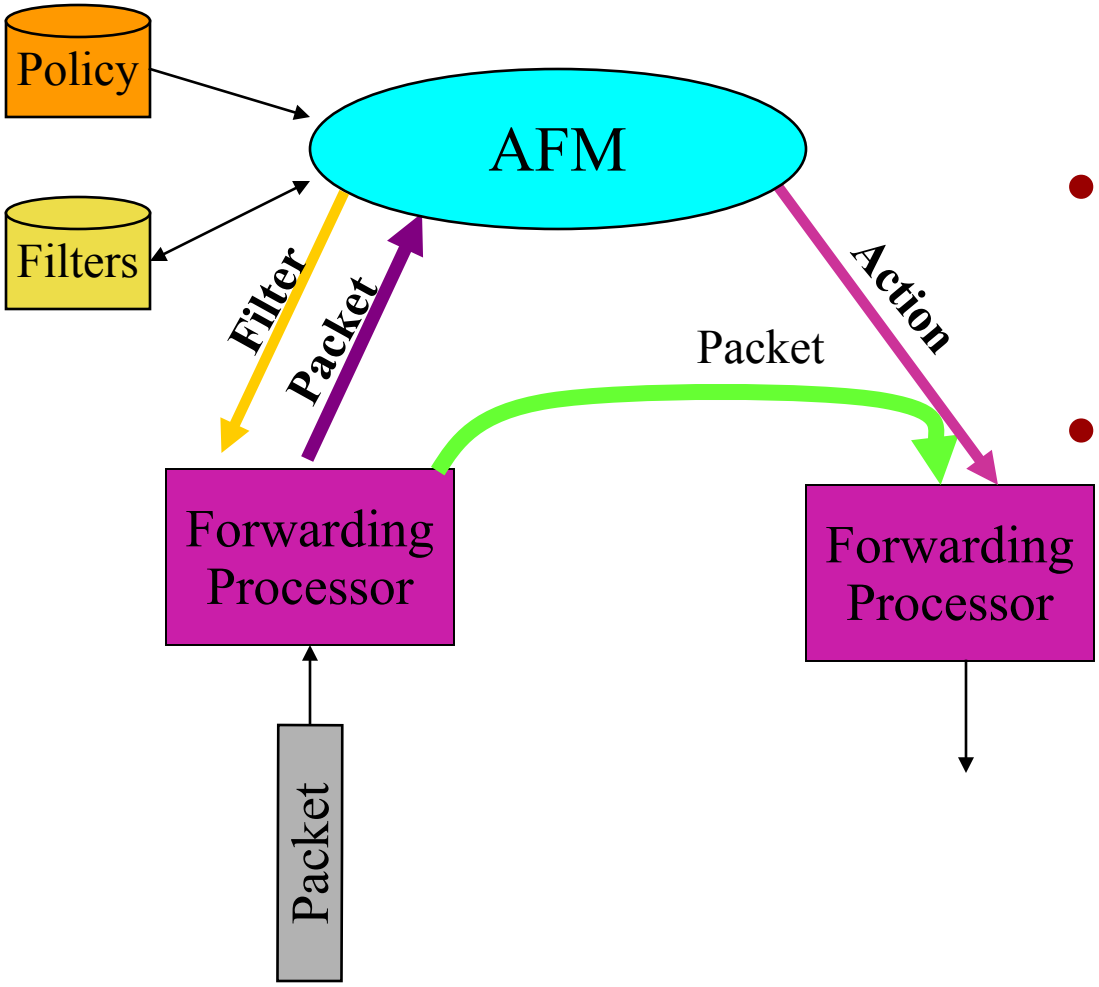
Lack of industrial-strength Active Network devices that dispel major concerns:

- **AN requires substantial supports from a NOS**
- **AN introduces substantial software component, hence delay on the data path**
- **AN lacks adequate measures to addressing integrity and security of network devices.**

Main contributions of the paper

- **Active Flow Manipulation Concept**
  - Flow abstraction
  - Actions on Flows
  - Control/Data separation
- **Openet Platform**
  - Commercial Network Devices
  - Runtime Environment
  - Active Services
- **Applications**

Active Flow Manipulation

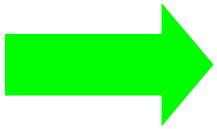


- **A key enabling technology of Openet**
- **Two abstractions**
  - Primitive flows
  - Primitive actions
- **Customer network services exercise active network control**
  - Identifying specific flows
  - Apply actions to alter network behavior in real-time

Dynamic L2-L7 Filtering

L2-L7 Filtering Capability

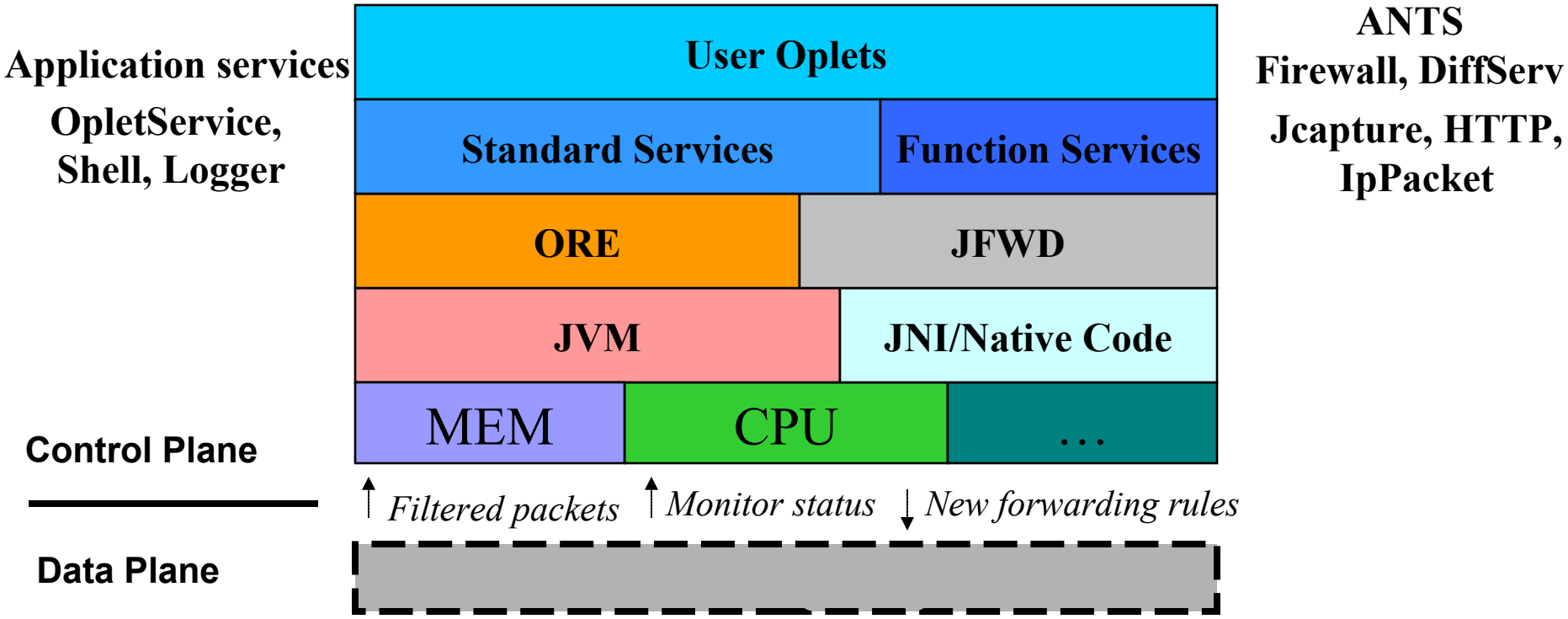
- Source Address
- Source Port
- Destination Address
- Destination Port
- Protocol
- VLAN
- Diffserv Code Points
- Content Filtering
- Cookies Filtering



Active Flow Manipulation

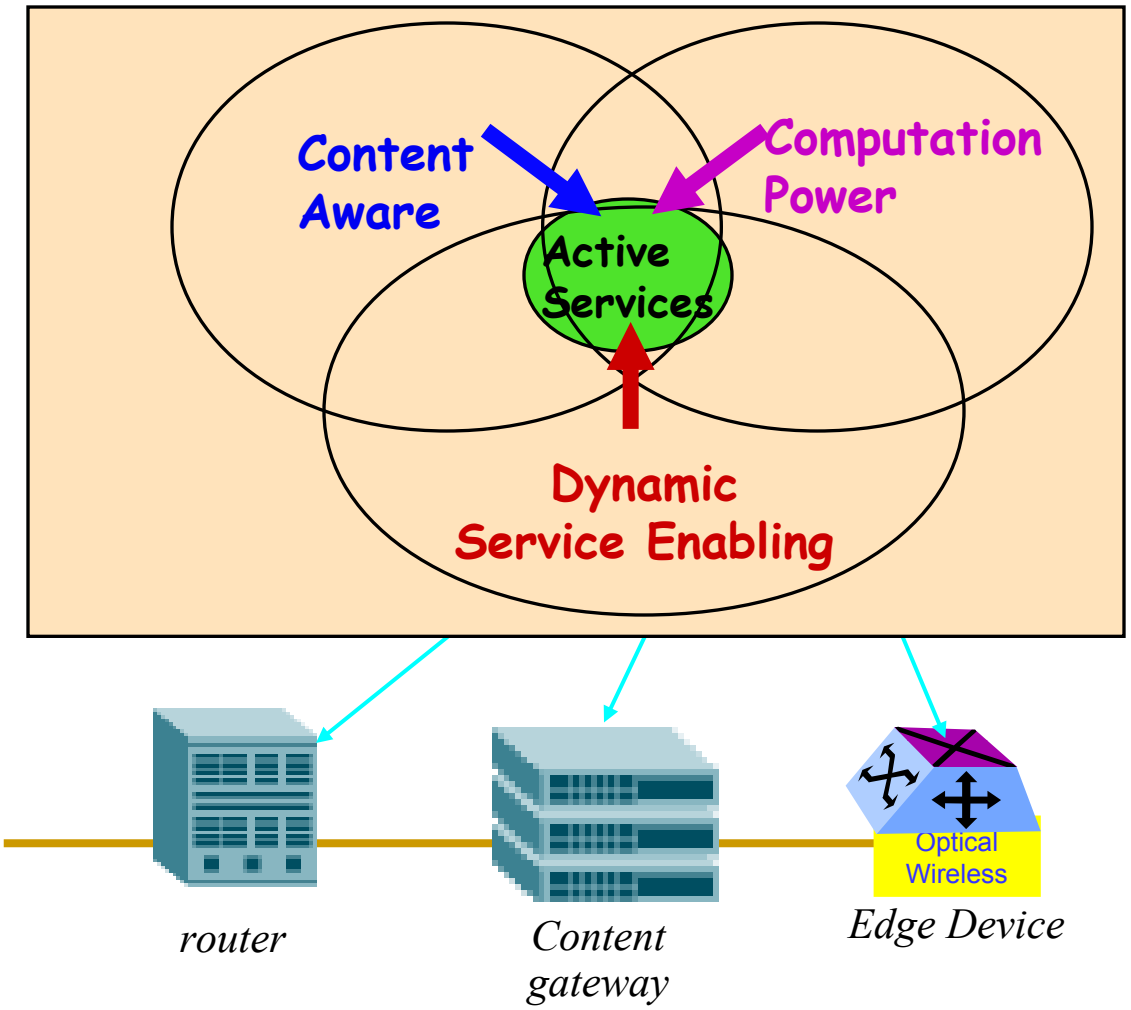
- Flow redirection
- Stop/Forward flow
- Change DSCP field
- Set VLAN priority
- Adjust priority queue
- Modify session table
- Parsing request header
- Parsing application contents

Openet: An active service platform



Openet Alteon Active Services Platform = A Powerful Platform for AN Technologies Transfer

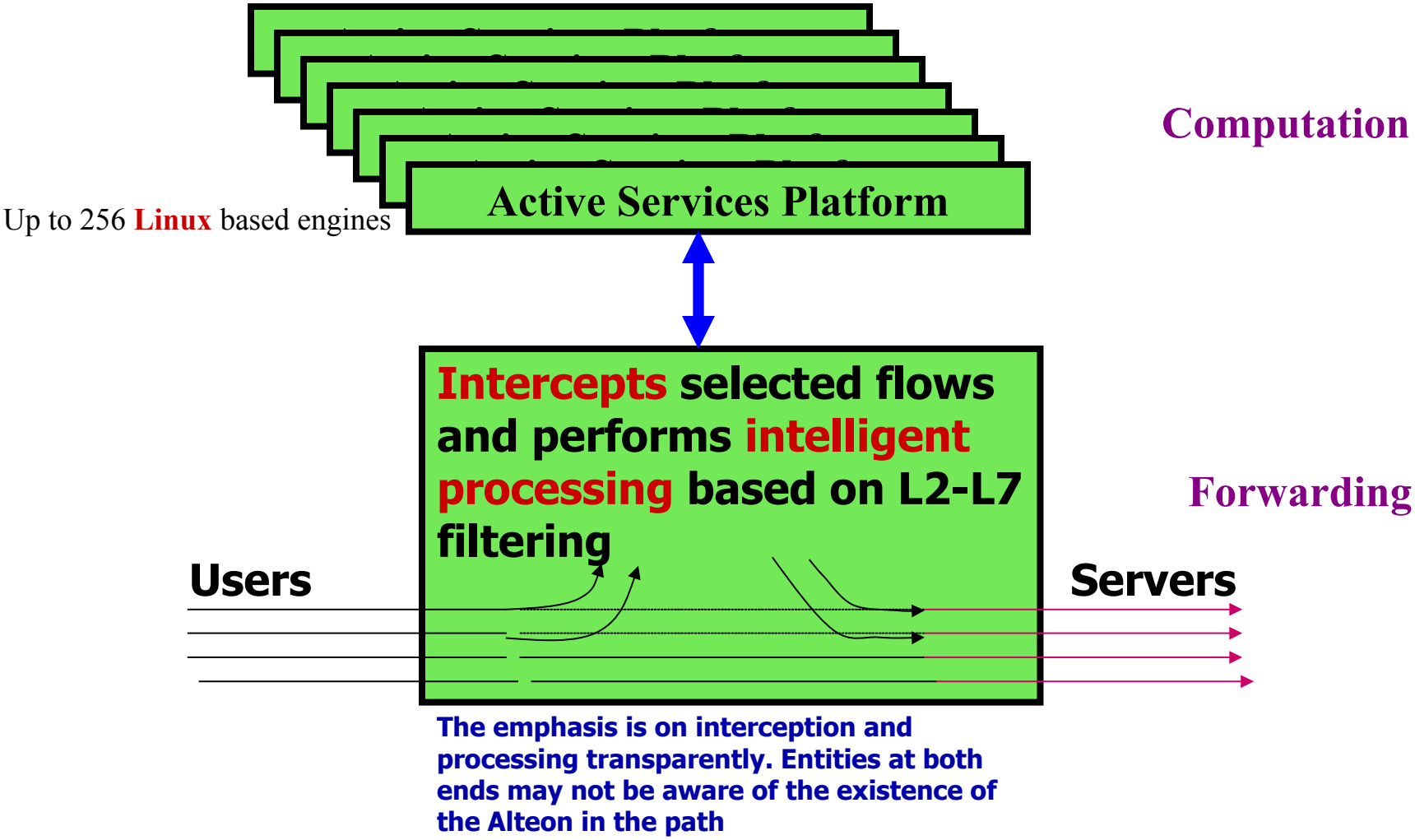
- **A powerful and extensible control and computational plane**
  - Partitioning hardware/software resources
  - Active service enabling
  - Content filtering in real-time
  - Active services accommodation



Nortel Networks' contributions to Active Services

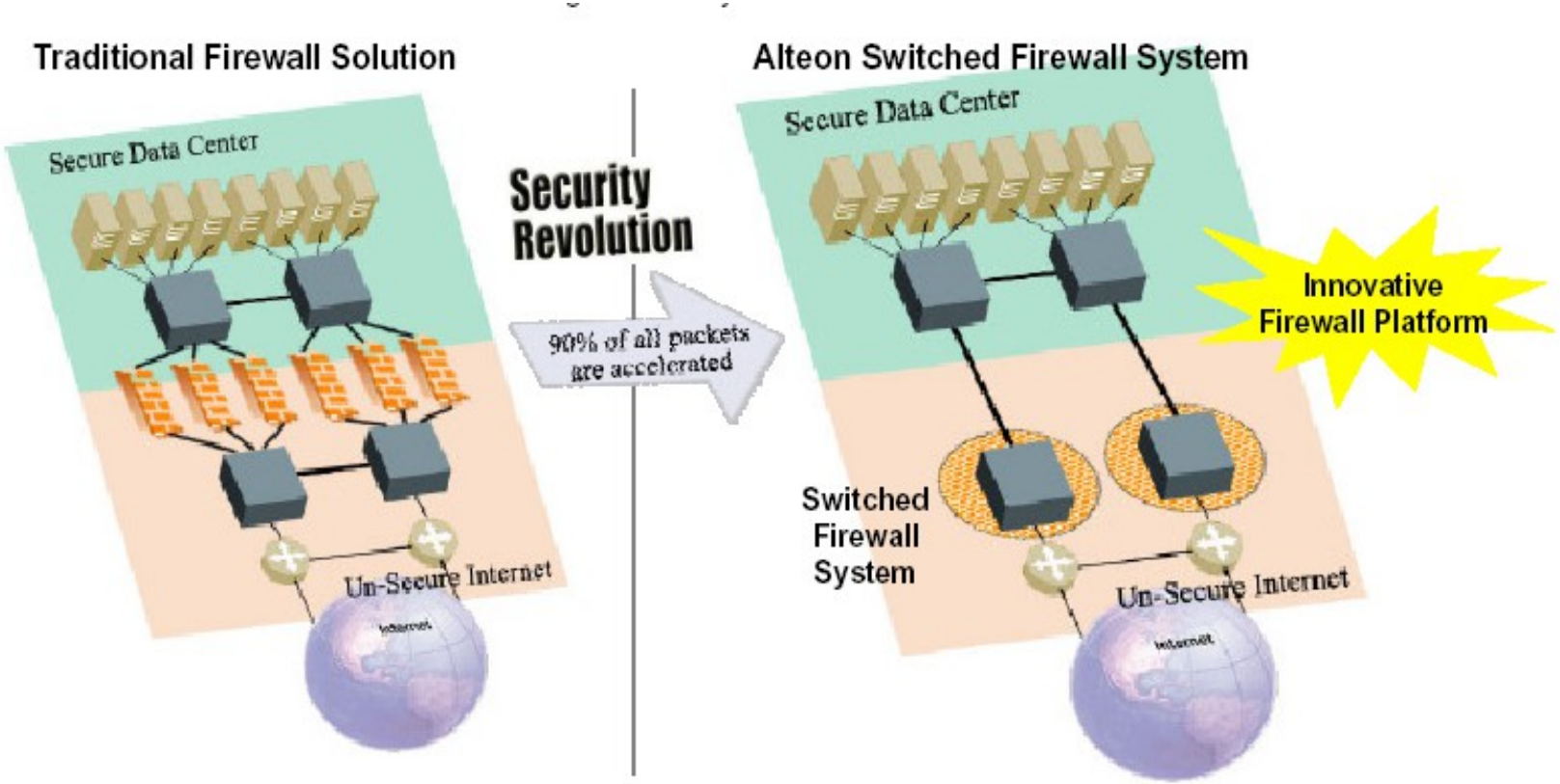
- **Practical Active Services Architecture on real network device.**
- **First Commercial Active Services platform.**
  - ASF - Product
  - SSL – Product
  - Open Active Architecture for more product
  - Alteon+iSD as a research platform
  - L3 programmable routing switch PP8600 – used by research community
  - Photonic Switch – Early prototype
- **Identify Active applications (More than Ping☺)**
  - Active VPN – Carrier A
  - Active fault diagnostic – Carrier A
  - Active SLA reliability
  - Active Extranet on Demand – CeNTIE- Media post production industry
  - Early stages in disaster recovery and fault tolerant networks

Strong computation power inside network device.

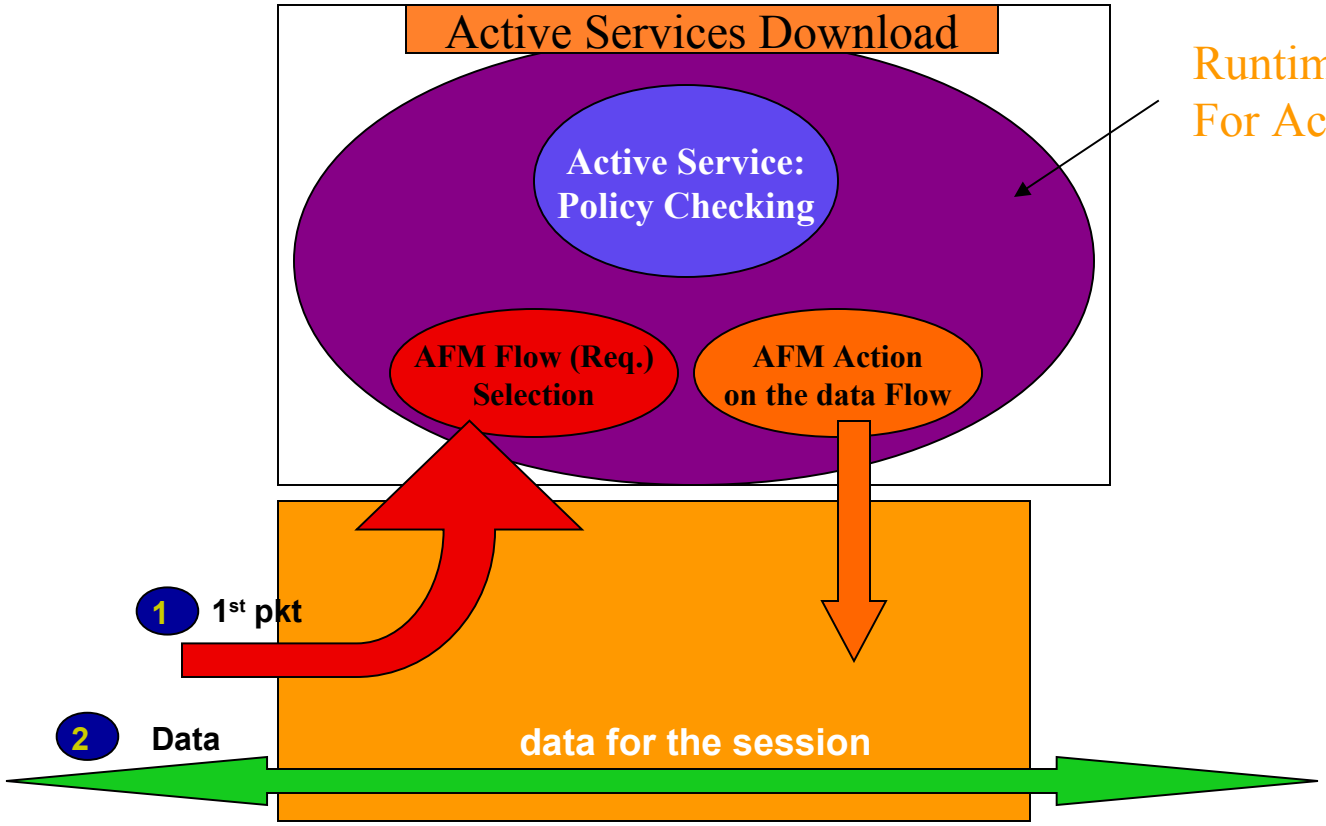


This slide is from the official product literature!!!

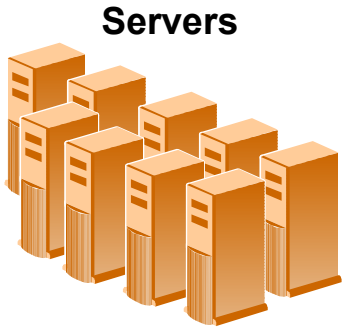
Active Service – Example 1
ASF – Alteon Switched Firewall
A Real Product



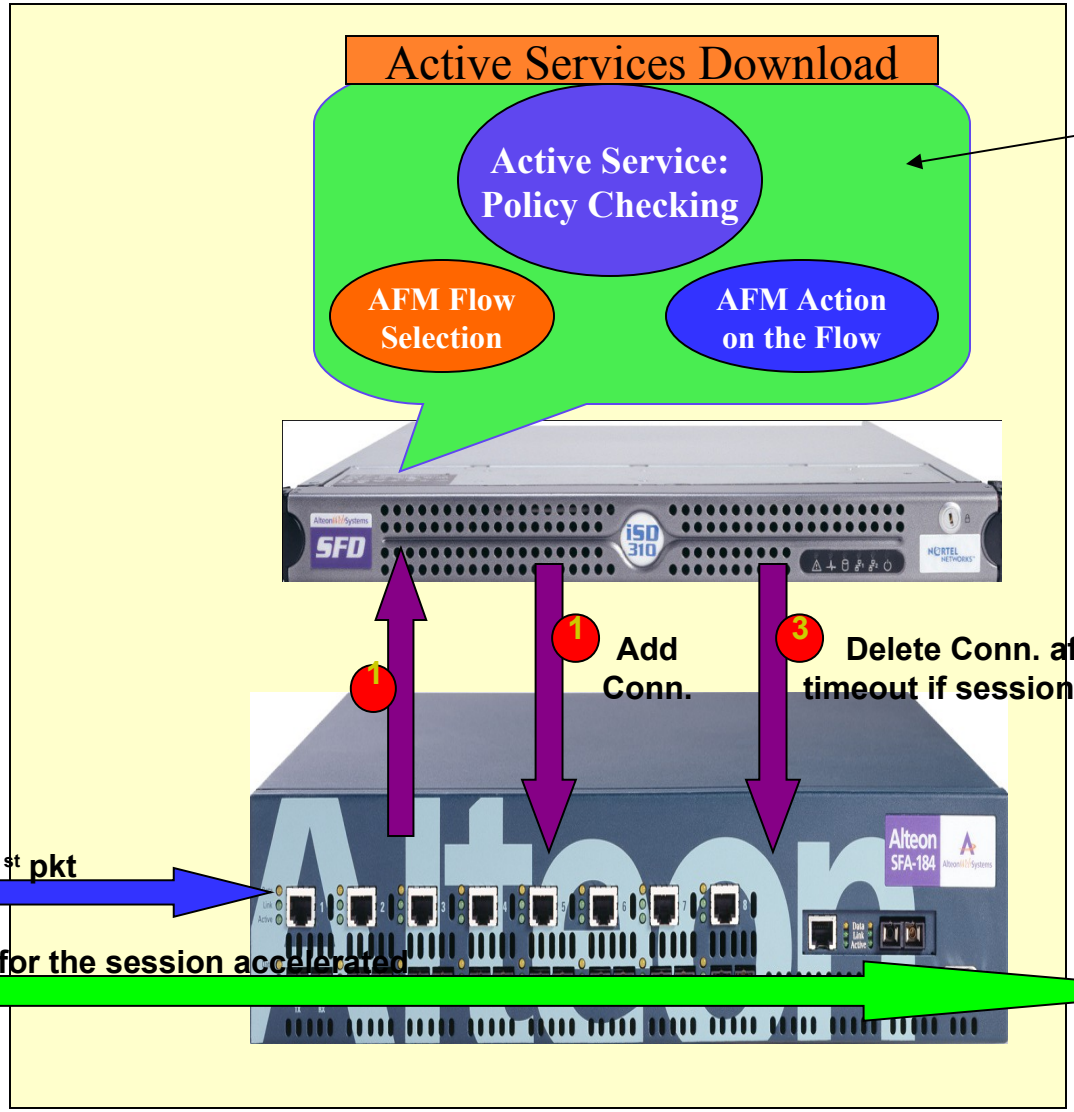
Alteon Switched Firewall (ASF)
A Real Product



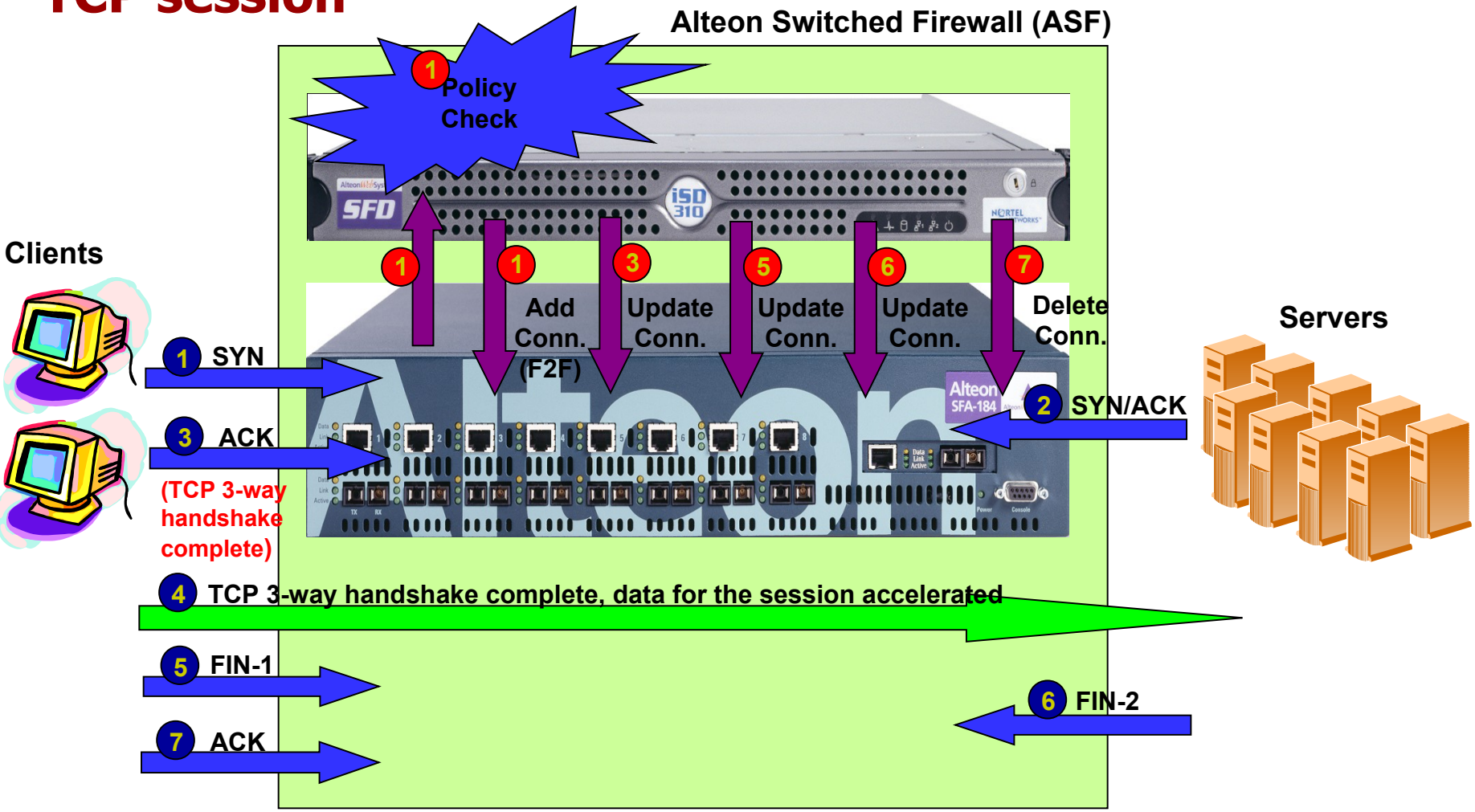
Runtime Environment
For Active Services



Alteon Switched Firewall (ASF)
A Real Product



Secure XL & NAAP in Action
TCP session



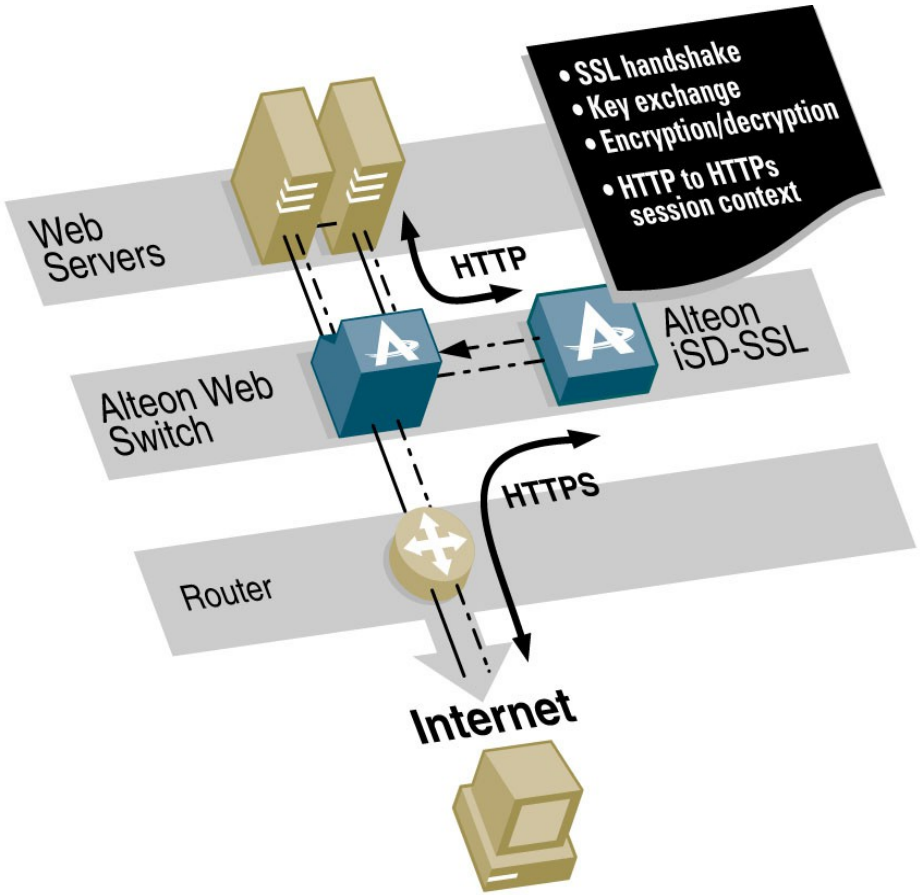
AFS as an Active Service Technology

- **The Alteon selectively redirects new connection requests to the Alteon Switched Firewall Director to perform policy checking.**
- **The Director runs the Check Point FireWall-1 engine as an Active Service.**
- **The Active Service manages the connection table, specifies rules for handling packets in the session, passes the connection table to the Alteon Switched Accelerator.**
- **90% of traffic is accelerated, supporting a throughput of 3.2 Gbps.**

This slide is from the official product literature!!!

SSL Acceleration

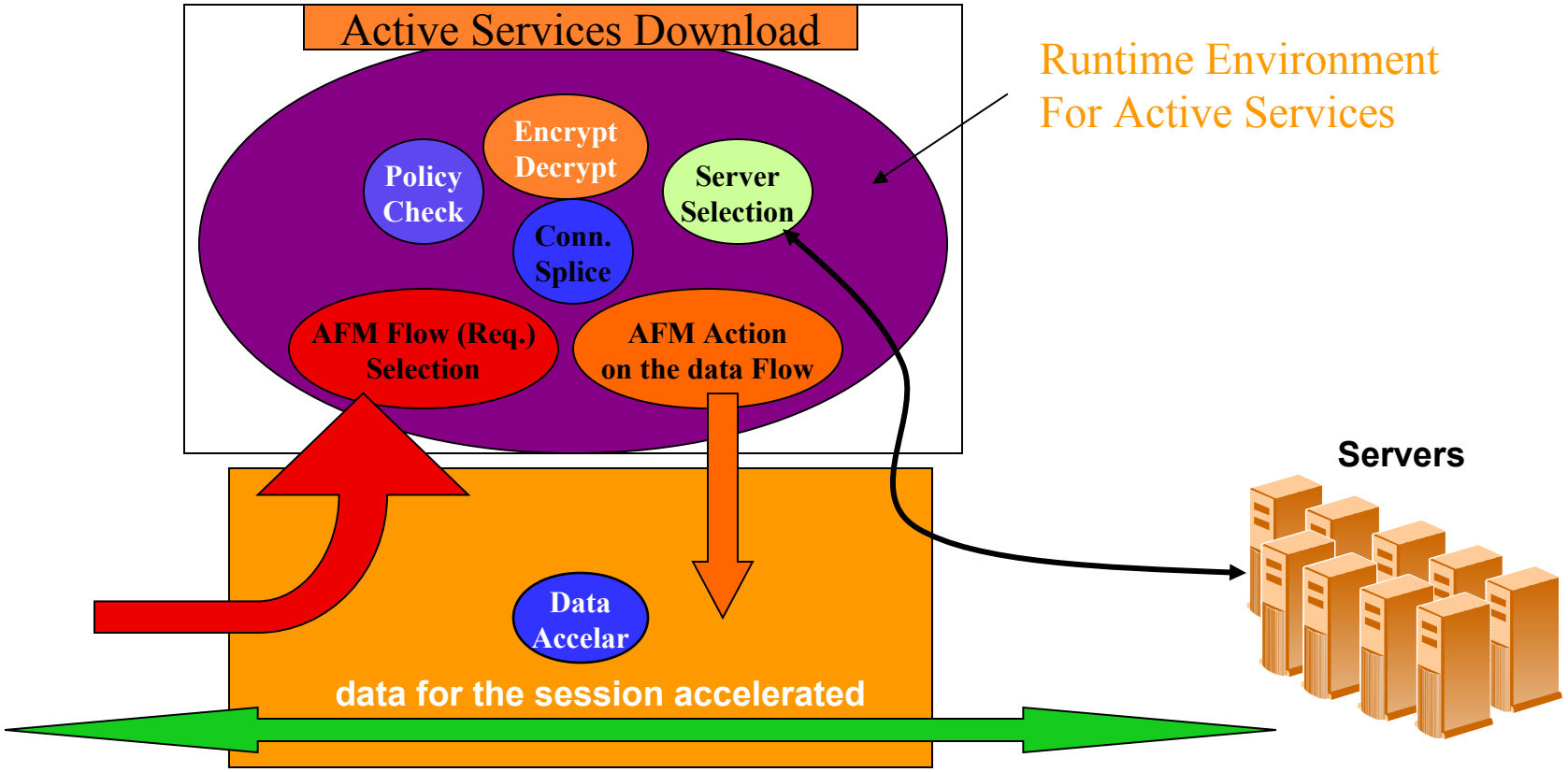
How Does the iSD-SSL Accelerator work?



- **Client sends an HTTPS request**
- **Switch redirects request on port 443 to iSD-SSL**
- **iSD-SSL completes SSL handshake**
- **iSD-SSL initiates HTTP connection to server on port 80**
- **Switch selects real server based on configured LB policy**
- **Server responds to HTTP request and replies to the iSD-SSL**
- **iSD-SSL encrypts session and sends HTTPS response to client**

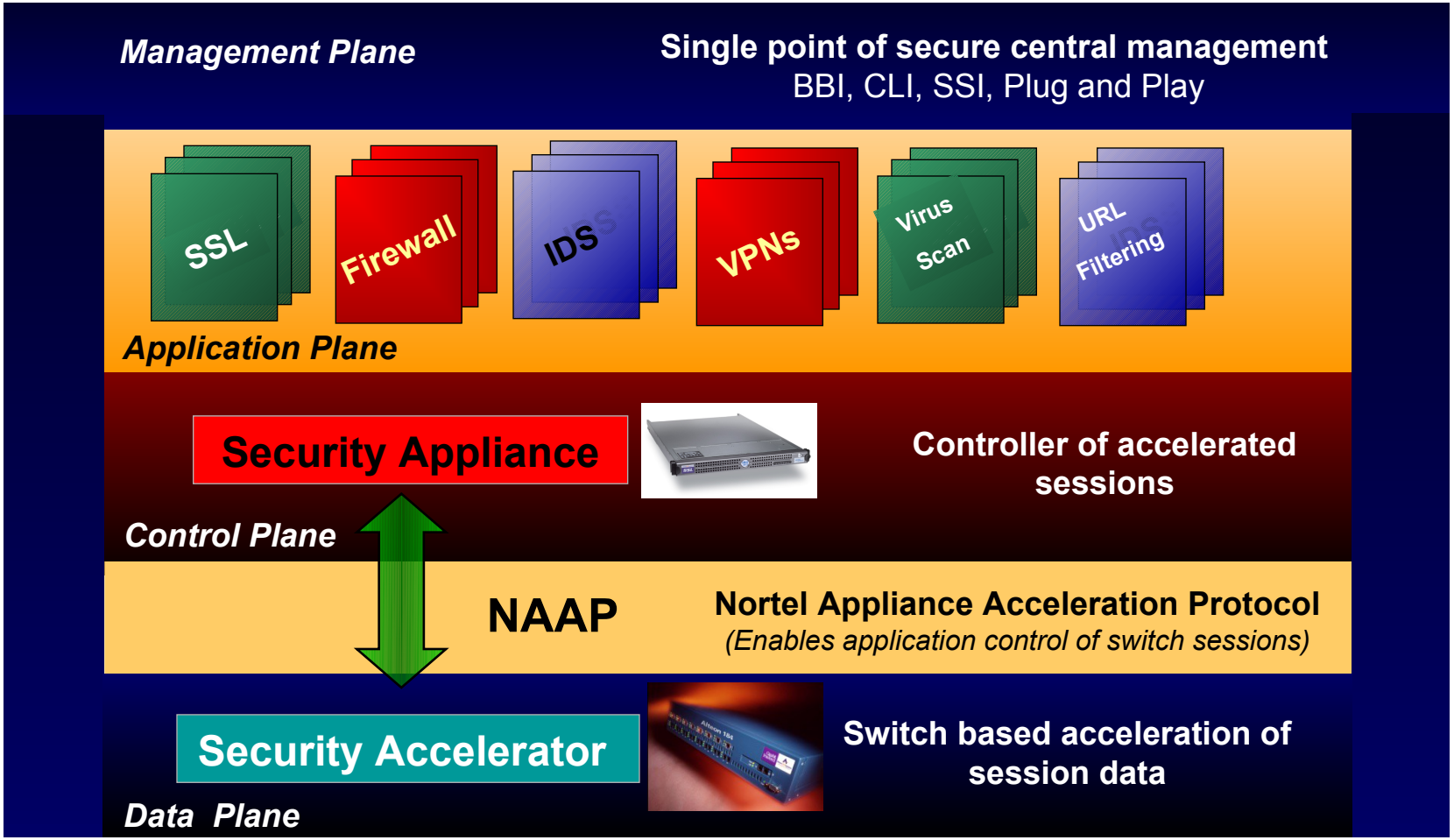
HTTPS, SMTP-S, POP3-S and IMAP-S services

SSL Acceleration Cont

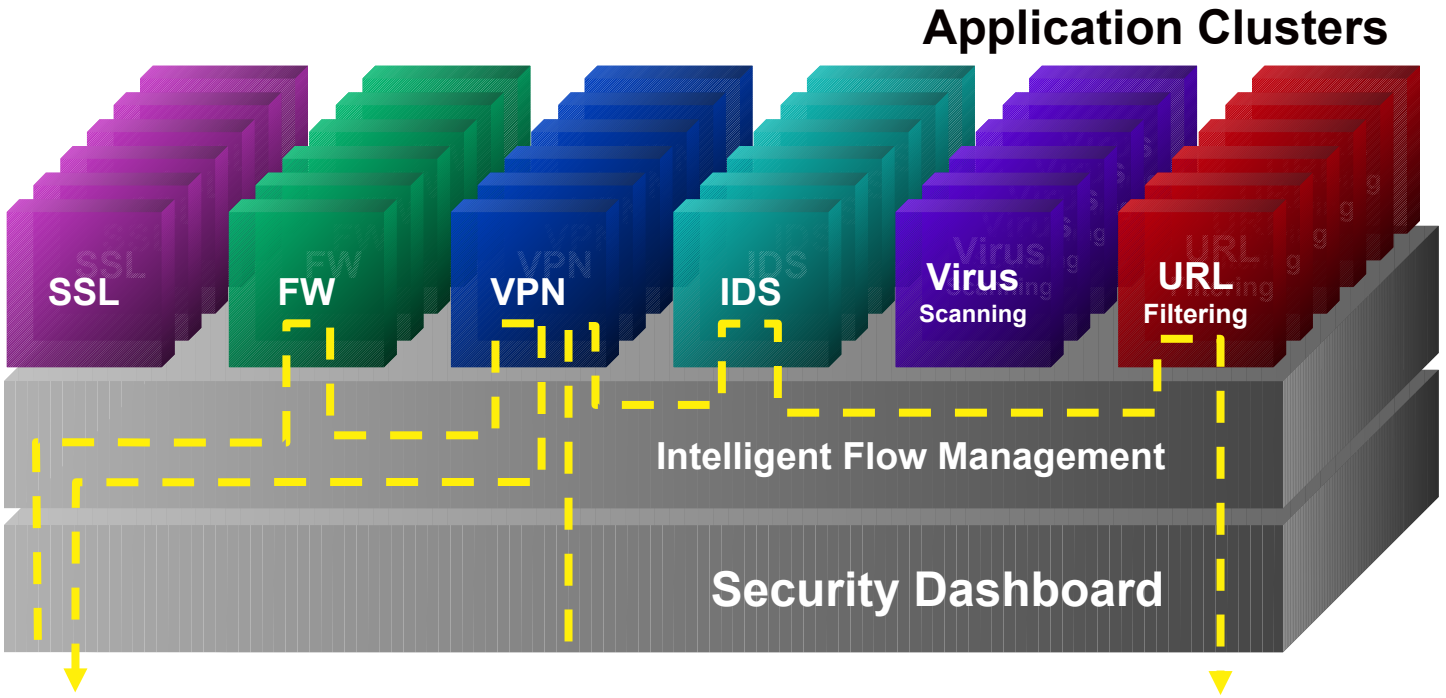


On the Horizon: Alteon Security Cluster

Acceleration and intelligent integration of security applications



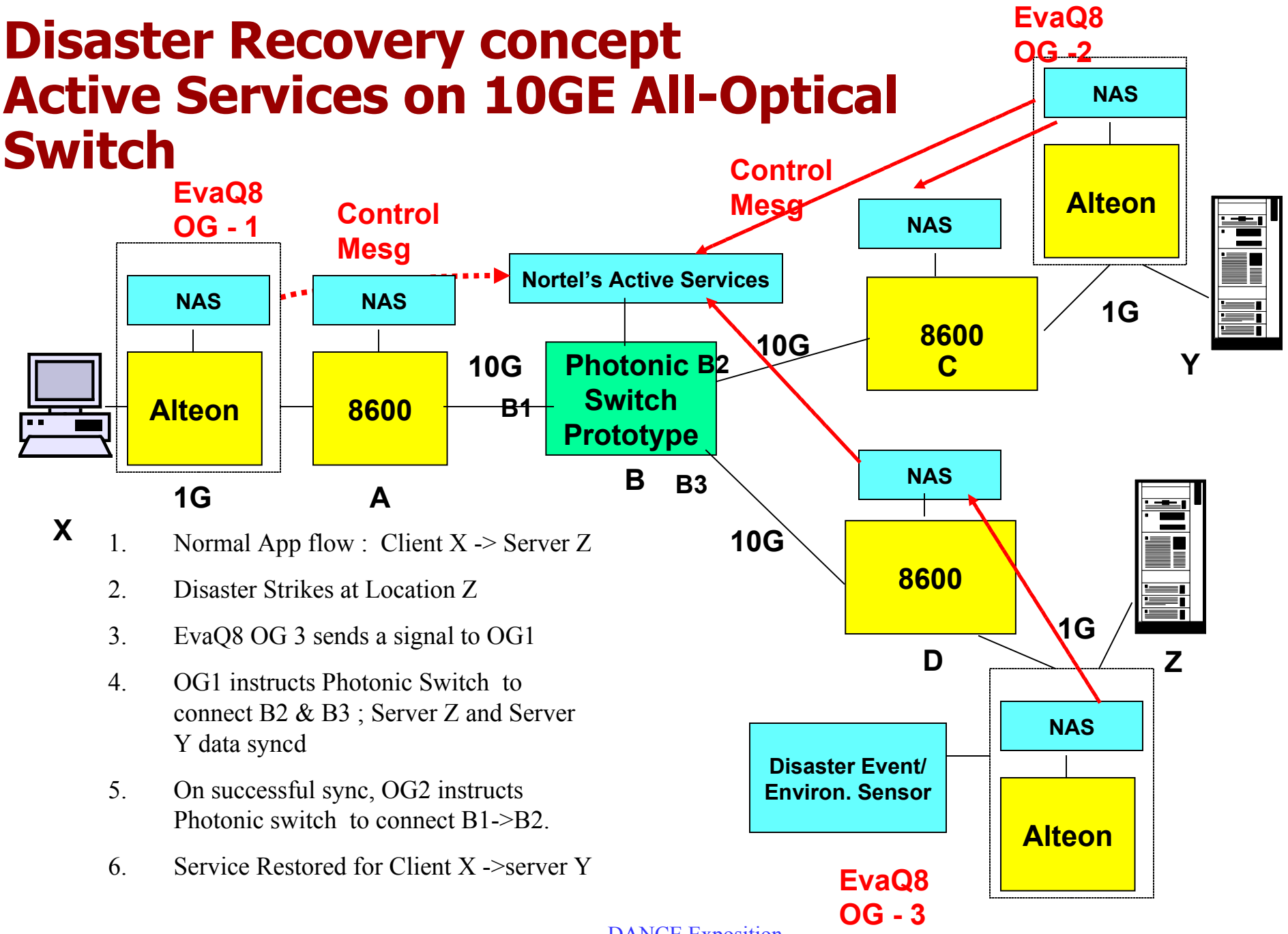
Security Cluster



Disaster Recovery Demonstration

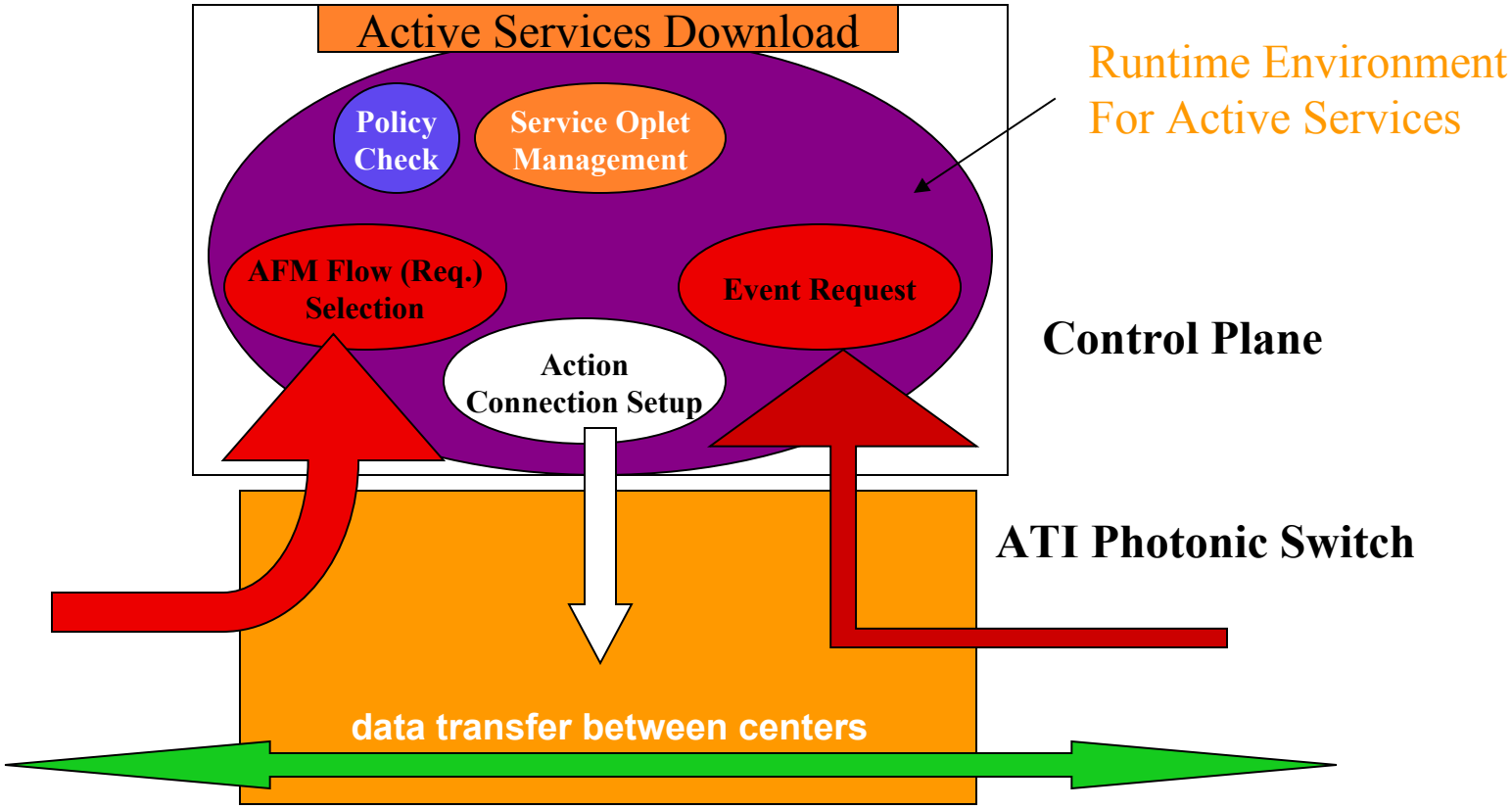
- **Early Prototype**

Disaster Recovery concept Active Services on 10GE All-Optical Switch



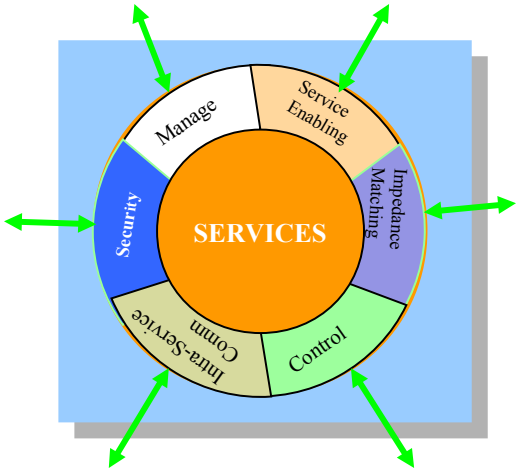
1. Normal App flow : Client X -> Server Z
2. Disaster Strikes at Location Z
3. EvaQ8 OG 3 sends a signal to OG1
4. OG1 instructs Photonic Switch to connect B2 & B3 ; Server Z and Server Y data syncd
5. On successful sync, OG2 instructs Photonic switch to connect B1->B2.
6. Service Restored for Client X ->server Y

A Disaster Discovery Application



What after next?
Service-centric Active Nets Platform

- Service Enabling API
- Control API
- Impedance Matching API
- Security API
- Management API
- Intra-service Communications API



AN Collaboration: CeNTIE – CSRIO- Nortel

Center for Networking Technologies for Information Economy (CeNTIE) - a CSIRO-led consortium including Nortel Networks, Amcom Telecommunications, the UNSW, UTS and the WA Interactive Virtual Environments Centre (IVEC).
www.centie.net

Tele-Health Focus Group

- Royal Australian College of Surgeons
- Medic Vision
- University of Sydney
- NSW Health
- Royal Prince Alfred
- Interactive Virtual Environment Centre (IVEC).
- Centre for Medical and Surgical Skills (CTEC).

Media Systems Focus Group

- Fox Studios
- Animal Logic
- GMD
- Ambience
- Film Industry Broadband Resource Enterprise (FIBRE)
- WAM!NET
- Australian Broadcasting Corporation (ABC)
- ScreenWest

1st Expl: Collaboration with a Major Carrier

- A major Carrier is interested in some aspects of the research and technologies incubated by the AN community ☺
- The main value is to role out new services – and fast
  - Active VPN
  - Active Fault diagnostic
- Unfortunately - the current market condition slowed down the interest (great direction – but no money now) ☹

Summary of Our Work

- **We have inspired ourselves to active networks concepts**
- **Demonstrate Active Networks technology transfer through Nortel Active Services platform.**
- **We have implemented programmable Gigabit Routing Switch (backplane 256 Gbs)**
  - New Active Services platform: Openet + Alteon + iSD
- **Active Services in the control plane (slows down in the data plane)**
  - AFM abstraction
- **Capable of dynamic monitoring and modification of silicon knobs**
  - The granularity is streams and not packets
  - Short time granularity (part of apps and not human intervention, keyboard, telnet, cli, snmp)

Summary of Our Our Work (cont.)

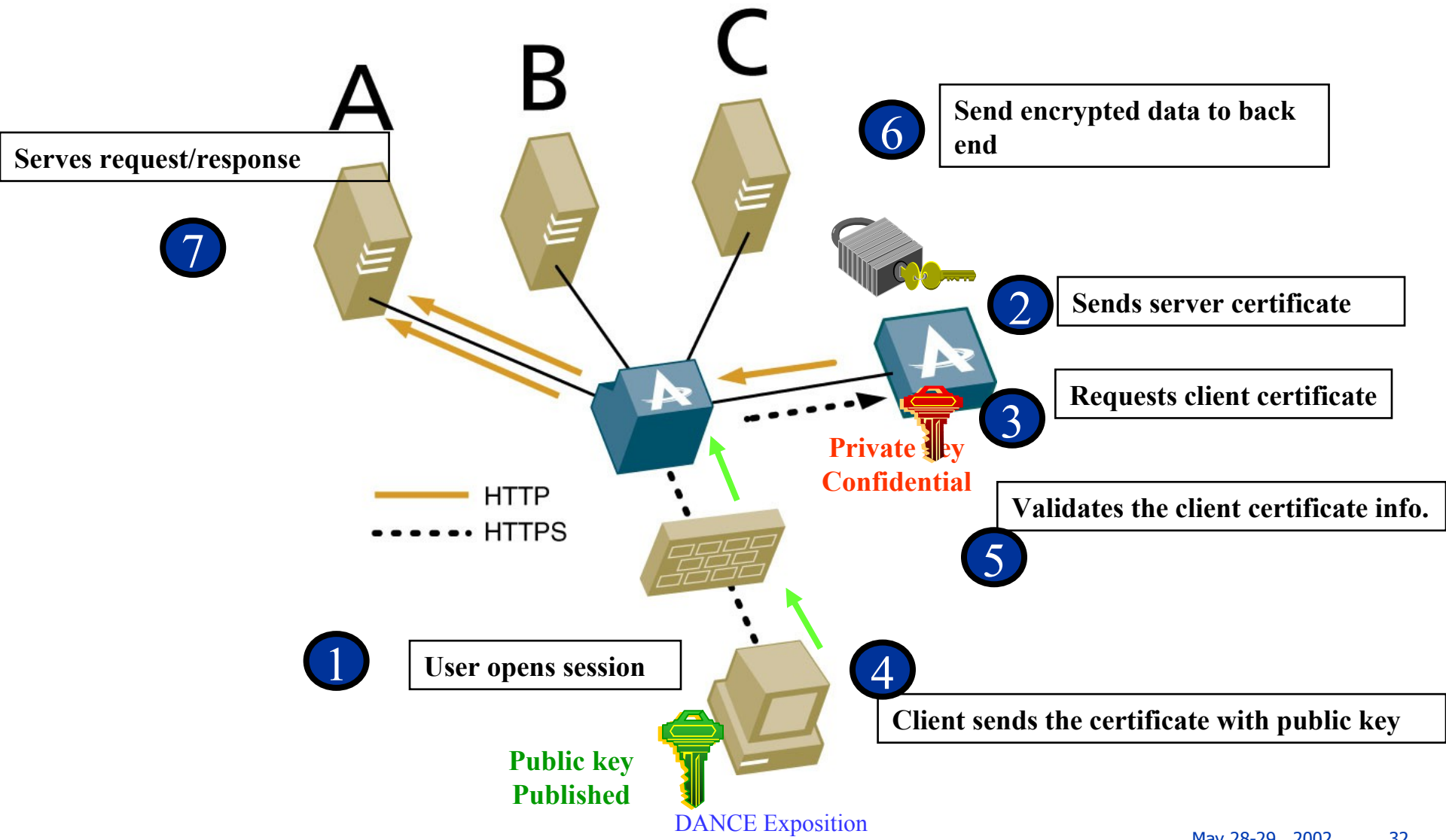
- **Enabling New Types of intelligence on programmable network device to handle Infinite Bandwidth resources, Wire speed routing capability, and nontrivial Streaming media application.**

- **Important next step is the development of a *Service-centric Active Services Platform.***

OpenetLab – Nortel Networks: http://www.openetlab.org/

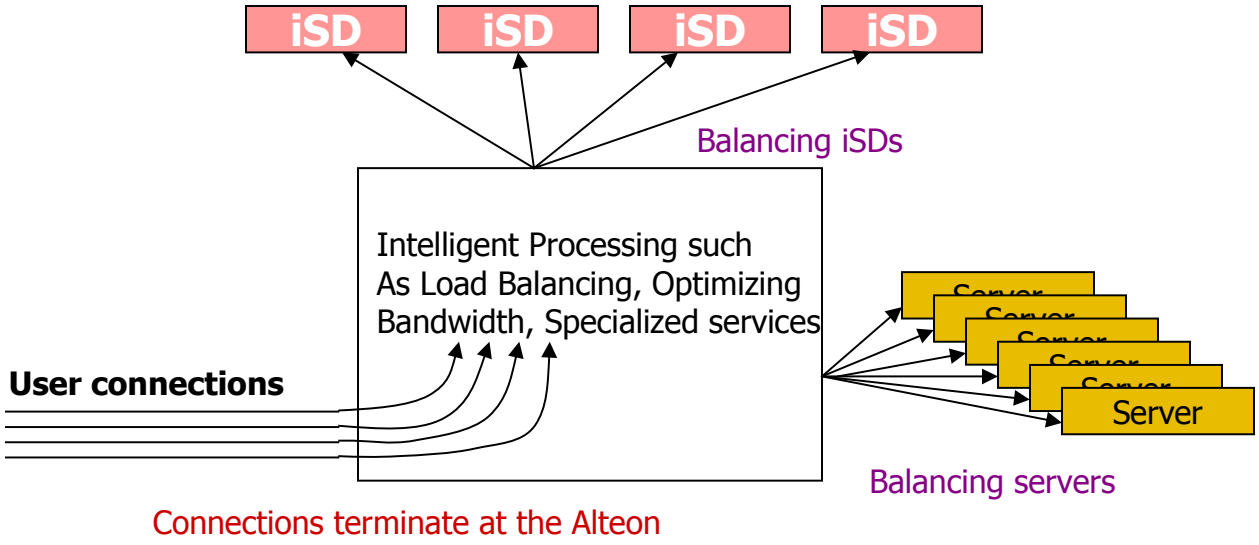
Q&A

Client And Server Authentication



Strong computation power inside network device.

Load balance of iSDs (and servers)



Balancing can be based on

- **load, or**
- **Functionality**

Powerful generic processors do not have the filtering capability of the Alteon. That is if they have to do the same thing as the Alteons, they have to do filtering in software, hence slow.

- **An API is needed for exploring this filtering capacity**

Content Re-route

- **Resource optimization (route 2)**
  - Alternative lightpath
- **Route to mirror sites (route 3)**
  - Lightpath setup failed
  - Load balancing
  - Long response time
    - Congestion
    - Fault