

# Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines

**Tal Lavian** - [tlavian@ieee.org](mailto:tlavian@ieee.org)

Nortel Networks

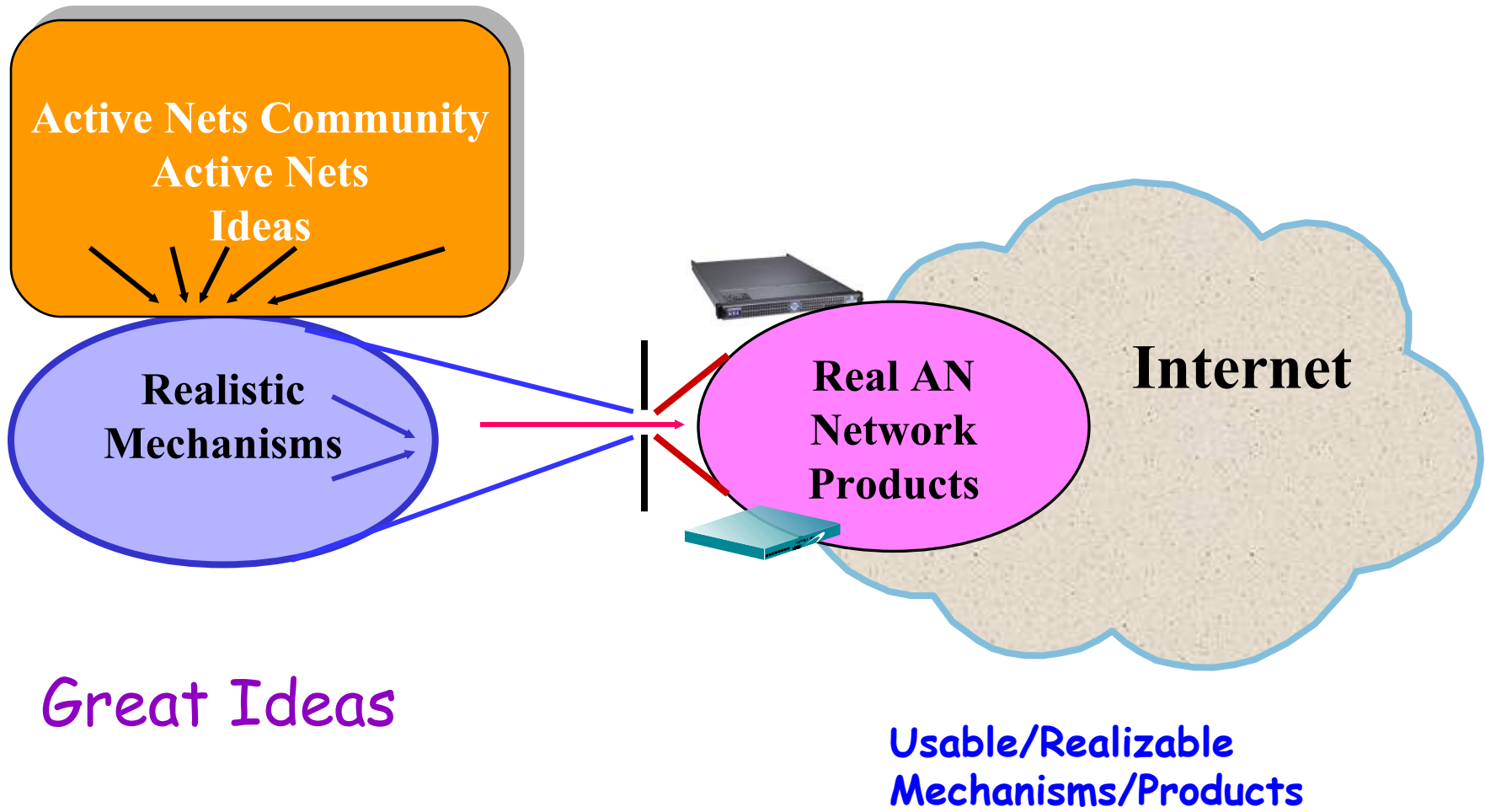
Advanced Technology Labs

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

# Outline of the talk

- **AN technologies => Real Network Devices**
- **Main thrust of the paper**
- **Commercial Active Nets Platform**
- **Application Example 1 – SSL**
- **Application Example 2 – ASF**
- **Next Generation AN Platform**
- **Conclusion**

# AN Technology Transfer



# 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**

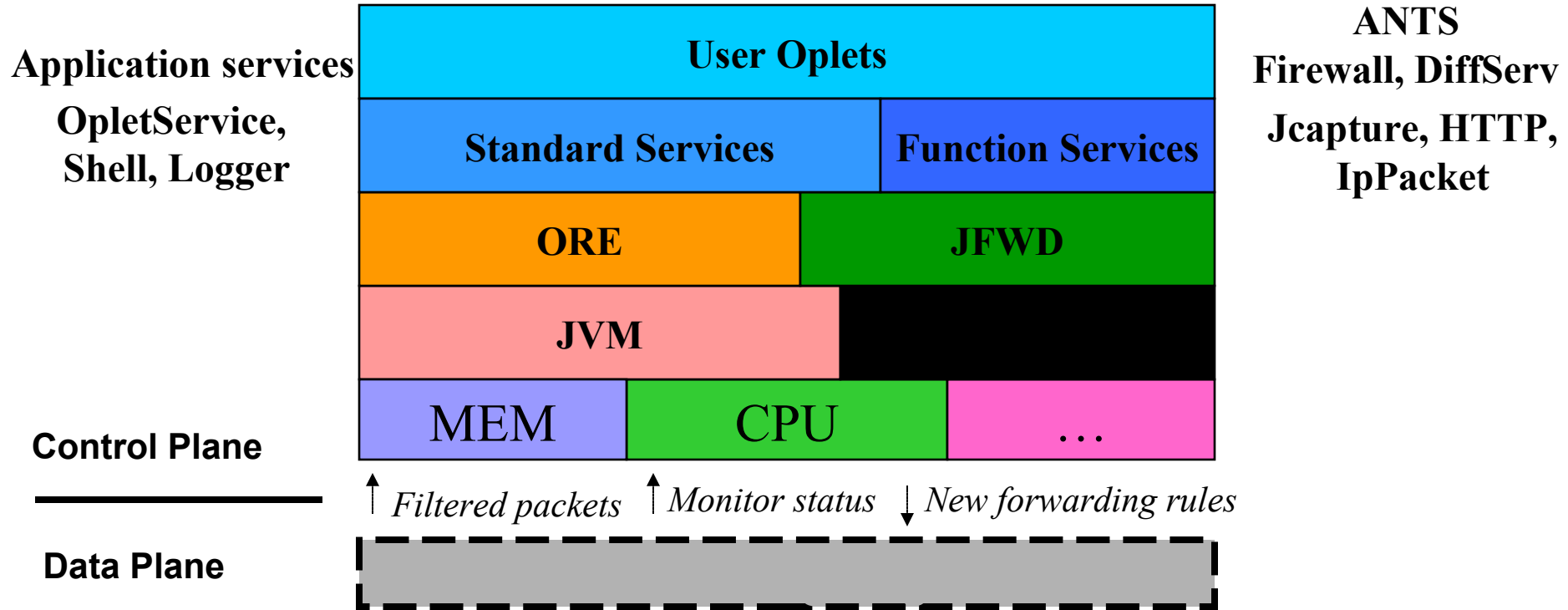
**Lack of industrial-strength Active Network devices that dispel major concerns:**

- **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.**

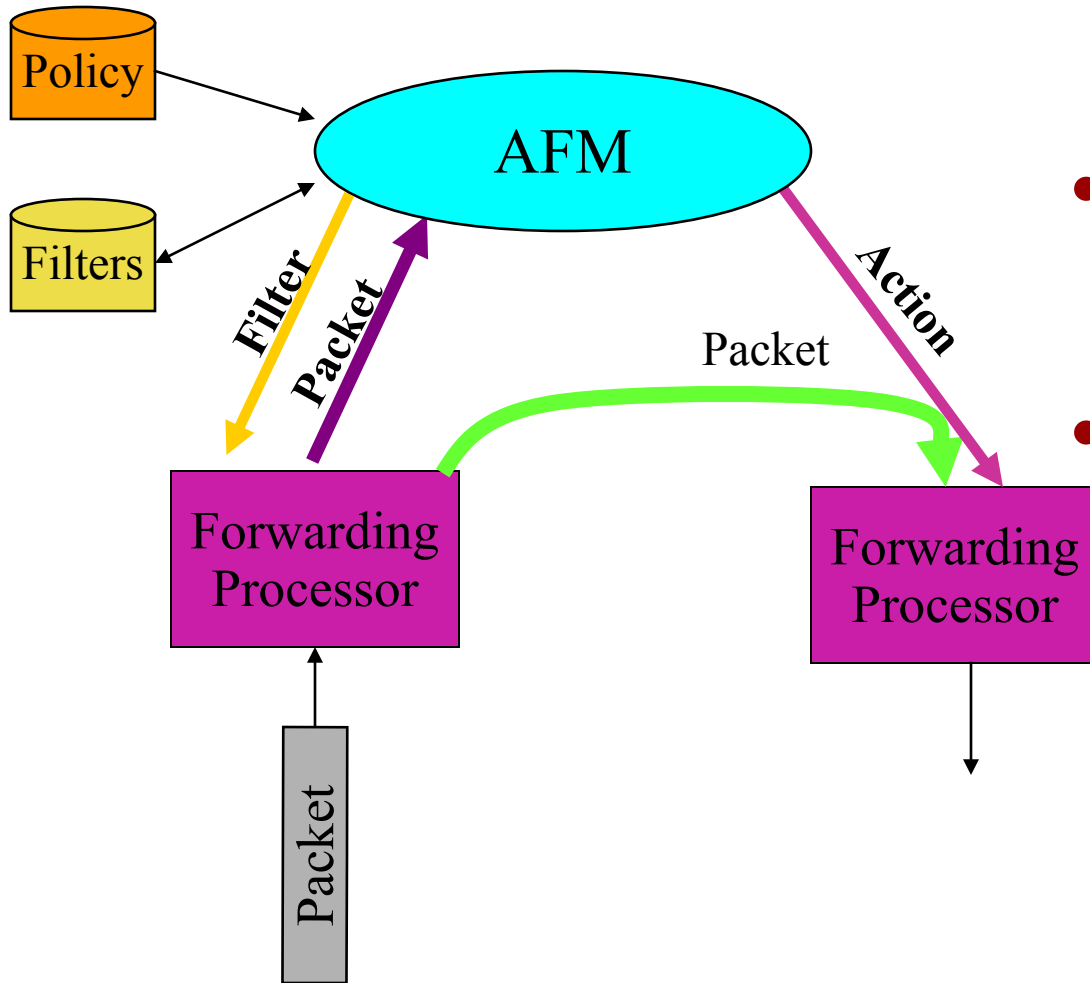
# Main contributions of the paper

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

# Openet: An active service platform



# Active Flow Manipulation

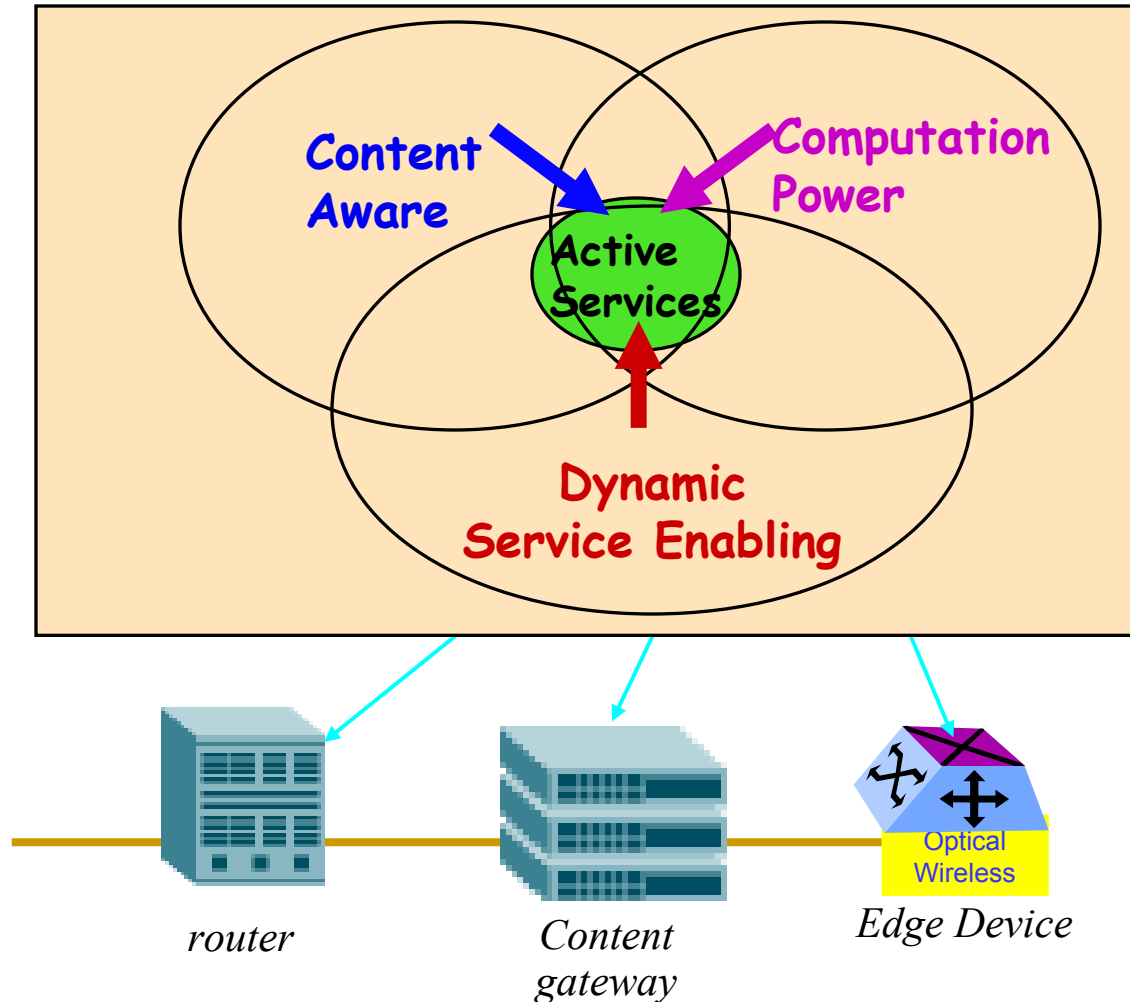


- **A key enabling technology of Openet**
- **Two abstractions**
  - Primitive flows
  - Primitive actions
- **Customer network services exercise active network control**
  - Identifying specific flows
  - Apply actions to alter network behavior in real-time

# Openet Alteon Active Nets Platform = A Powerful Platform for AN Technologies Transfer

- **A powerful and extensible control and computational plane**

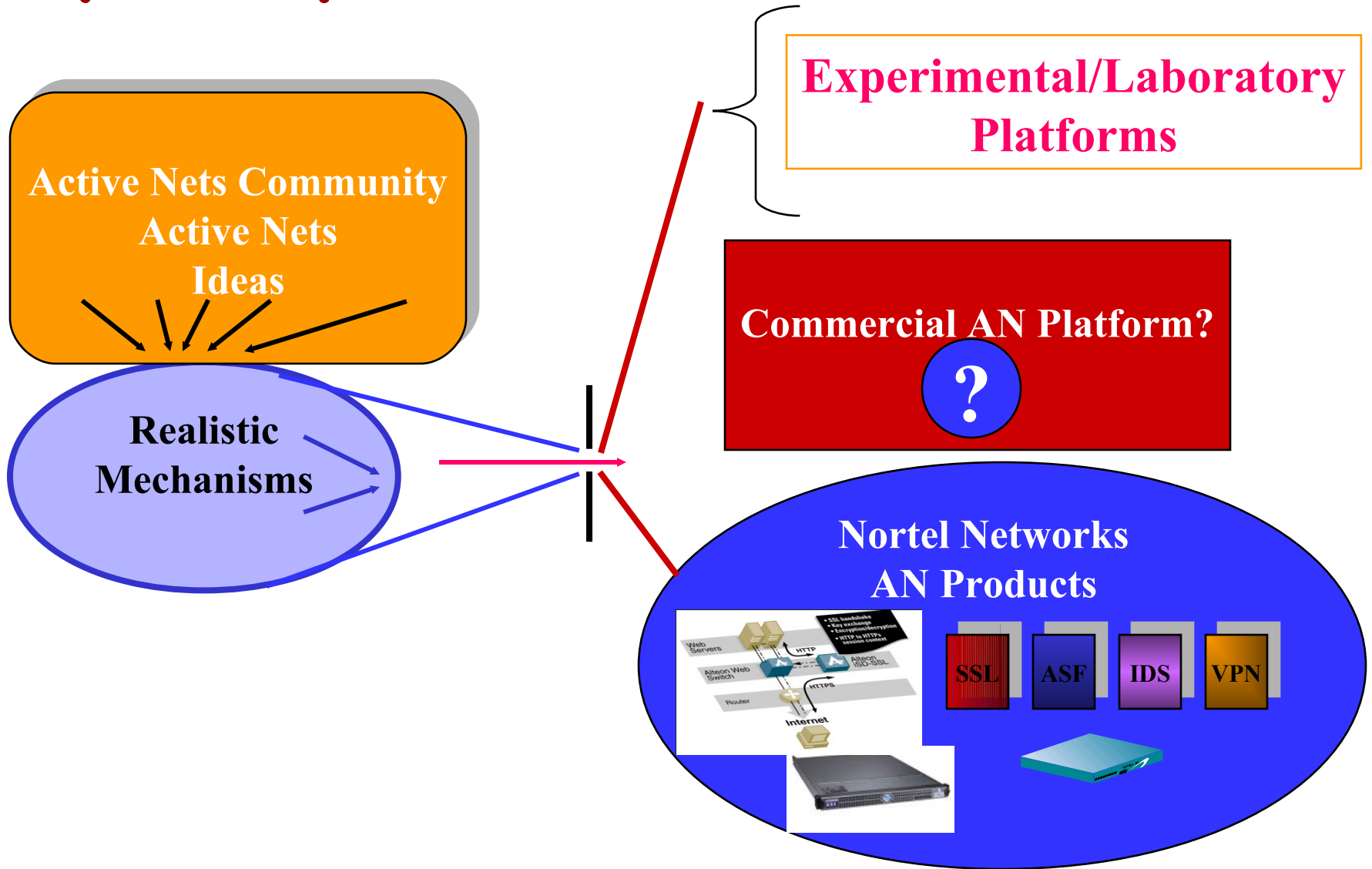
- Partitioning hardware/software resources
- Active service enabling
- Content filtering in real-time
- Active services accommodation



# **Nortel Networks' contributions to Active Networks**

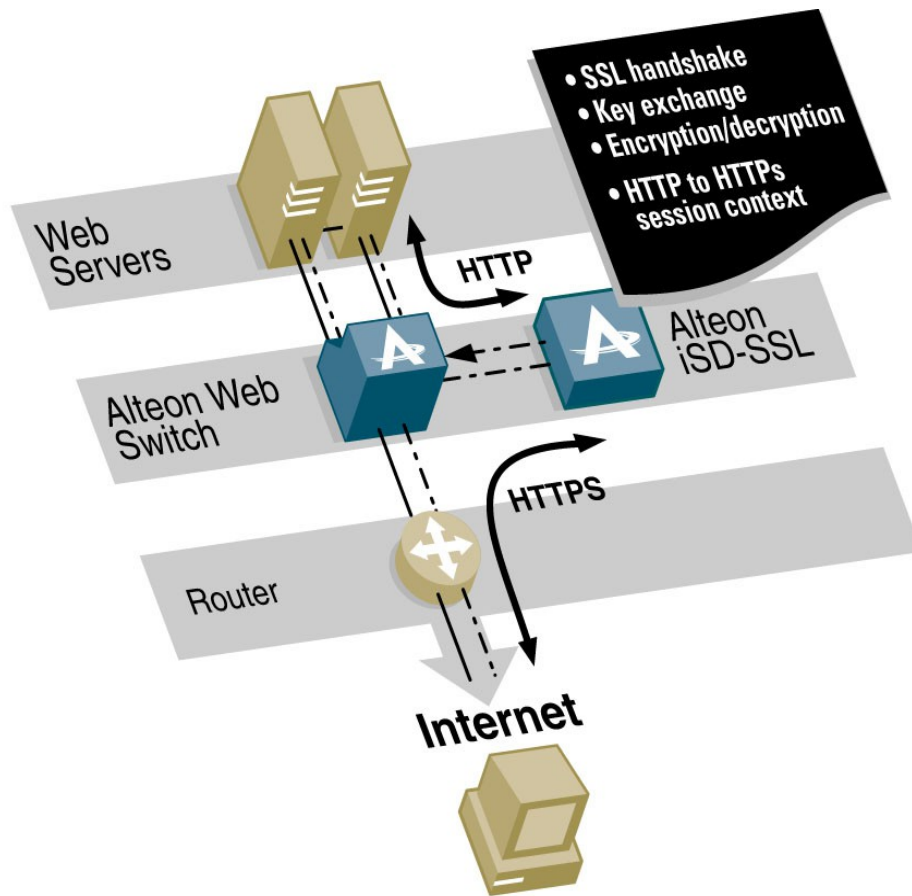
- **Practical Active Networks Architecture on real network device.**
- **First Commercial Active Networks platform.**

# Any AN products?



# SSL Acceleration

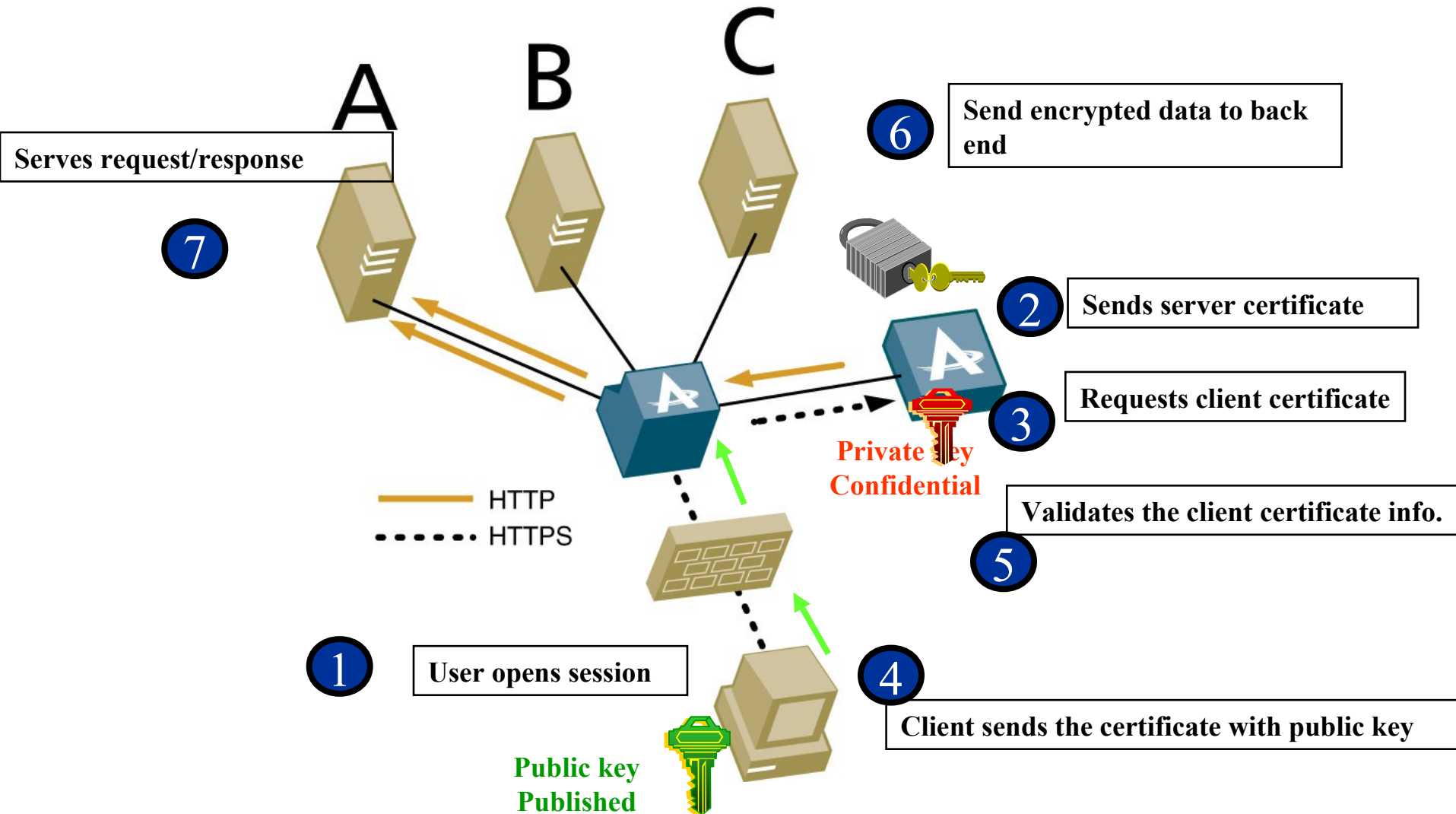
## *How Does the iSD-SSL Accelerator work?*



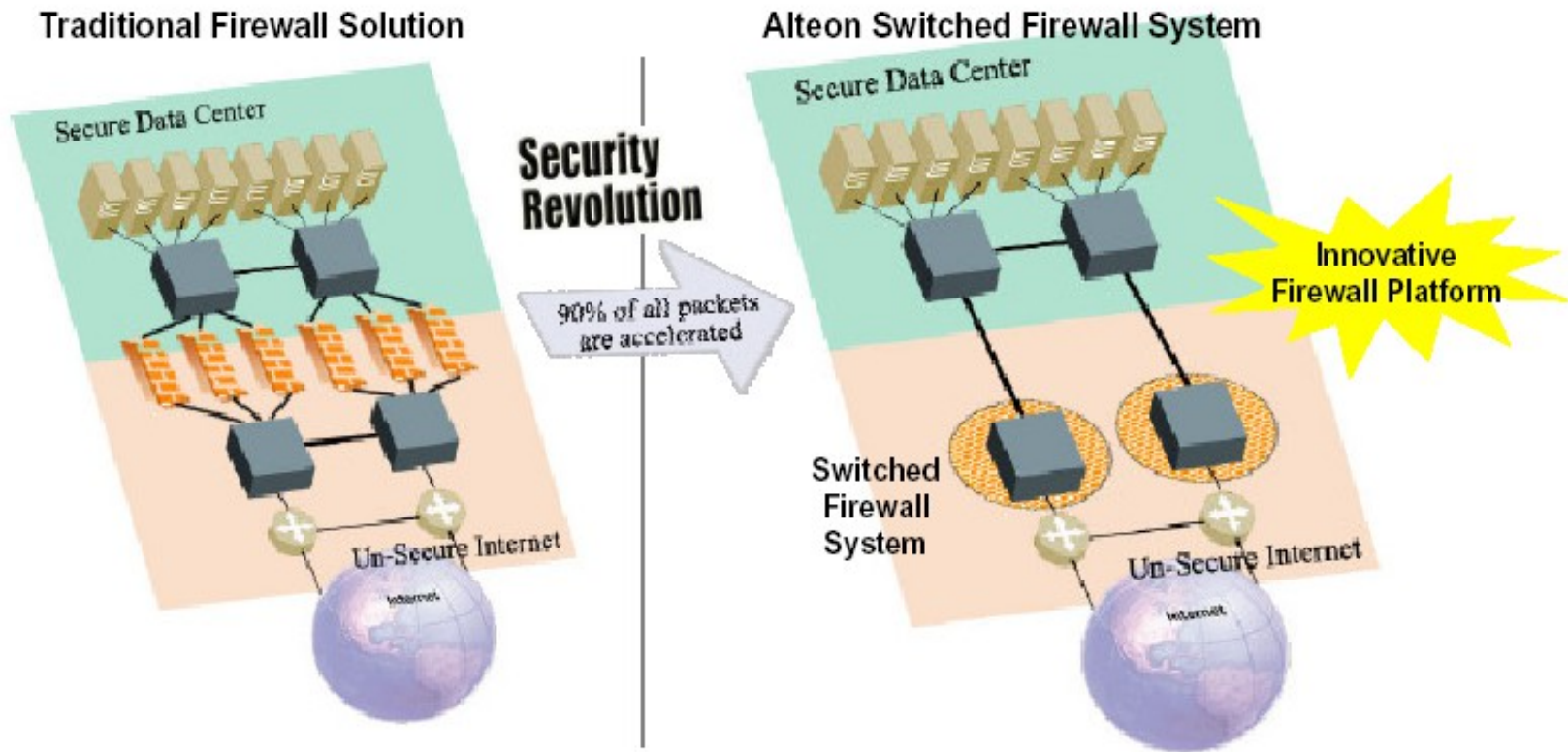
- Client sends an HTTPS request
- Switch redirects request on port 443 to iSD-SSL
- iSD-SSL completes SSL handshake
- iSD-SSL initiates HTTP connection to server on port 80
- Switch selects real server based on configured LB policy
- Server responds to HTTP request and replies to the iSD-SSL
- iSD-SSL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

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

# Client And Server Authentication



# ASF – Alteon Switched Firewall

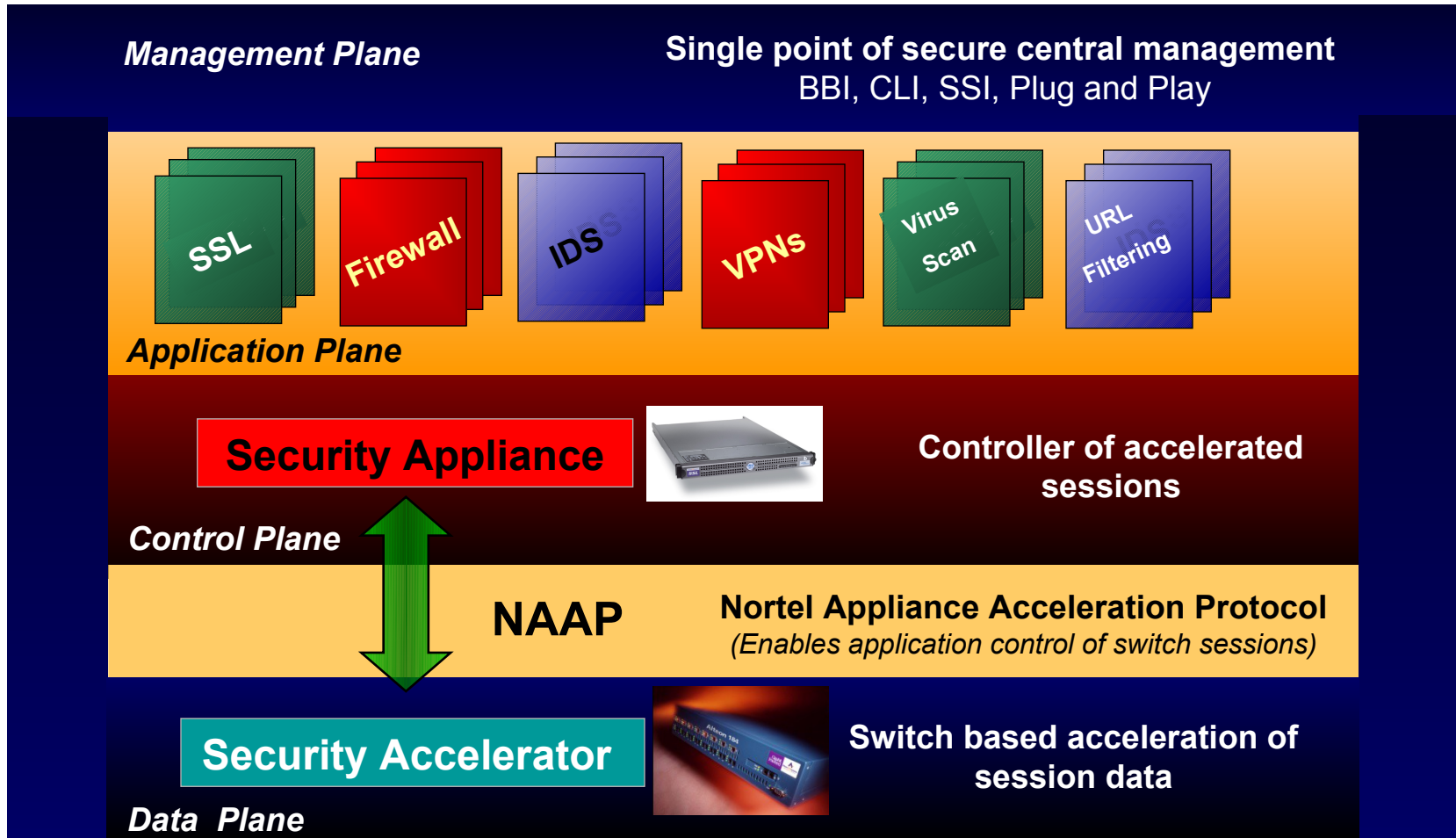


# Relate AFS to AN Technology

- **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.**

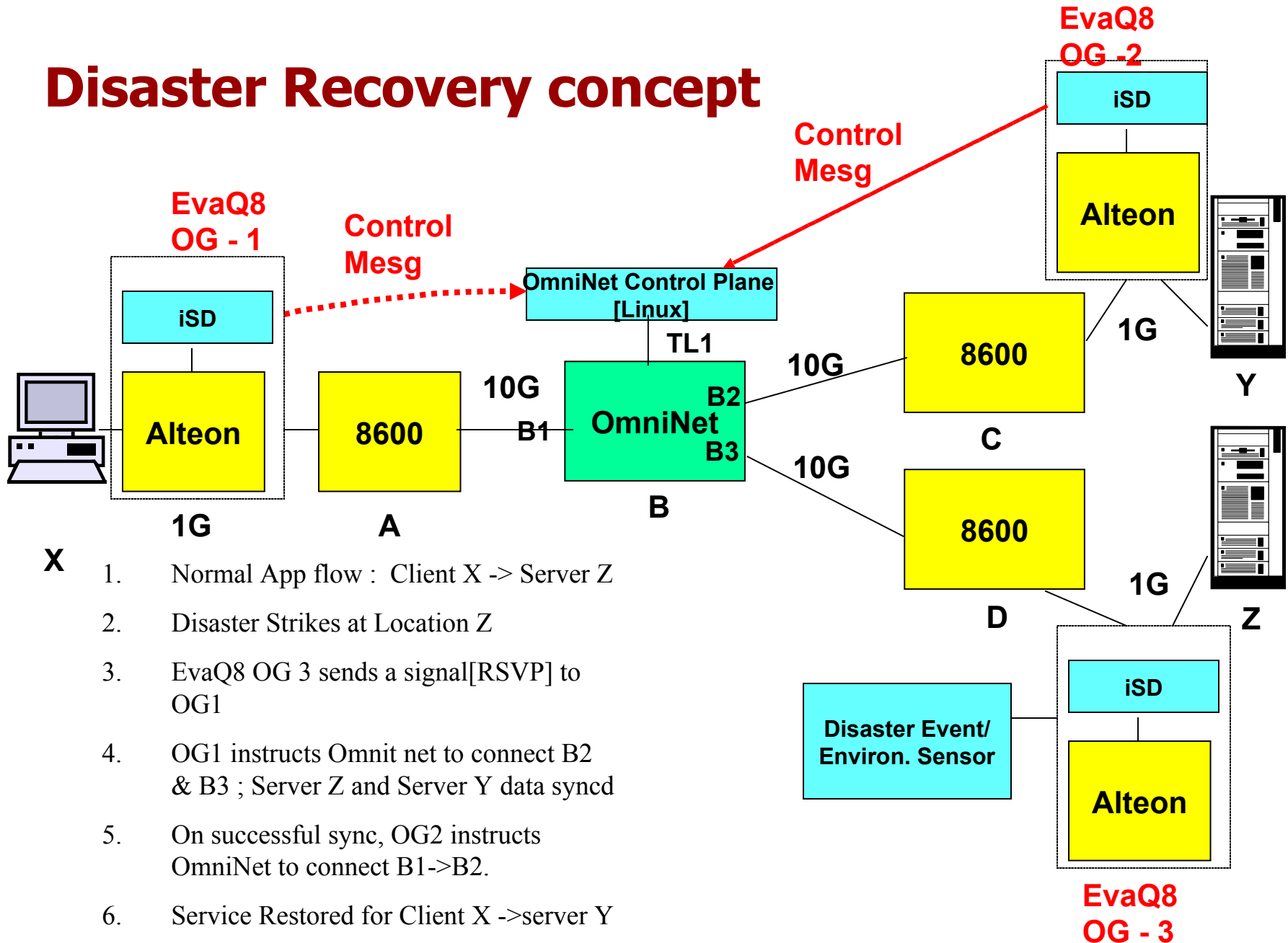
# Alteon Security Cluster

*Acceleration and intelligent integration of security applications*



# What next?

# Disaster Recovery concept



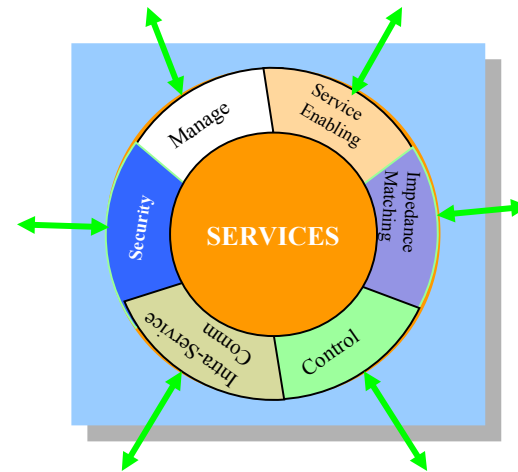
- X
1. Normal App flow : Client X -> Server Z
  2. Disaster Strikes at Location Z
  3. EvaQ8 OG 3 sends a signal[RSVP] to OG1
  4. OG1 instructs Omnit net to connect B2 & B3 ; Server Z and Server Y data synced
  5. On successful sync, OG2 instructs OmniNet to connect B1->B2.
  6. Service Restored for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

# What next? Quotes from VIPs

# What after next?

## Service-centric Active Nets Platform

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



# Summary

- **AN Technologies Transfer => Nortel AN Platform**
- **New AN platform: Openet + Alteon + iSD**
  - Alteon: AN platform advanced content filtering
  - iSD: powerful & extensible computation plane
- **Important Applications**
- **Impact of AN on next generation networks**

**OpenetLab – Nortel Networks:** <http://www.openetlab.org/>

**Q&A**

# Backup Slides

# Policy Engine Enhancement

## WebOS Policy Engine

MAC source/dest address  
IP /not  
IP source/dest address /range  
Protocol  
IP TOS  
IP Options /not  
ICMP message types  
TCP/UDP source/dest port  
TCP flags  
URL and Cookie  
**VLAN ID (New)**

Frame  
Ingress



## Actions

Drop

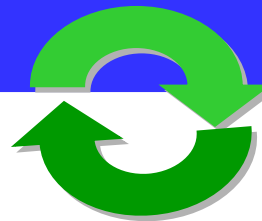
NAT

IP TOS rewrite

Redirect  
(to IP or server group)

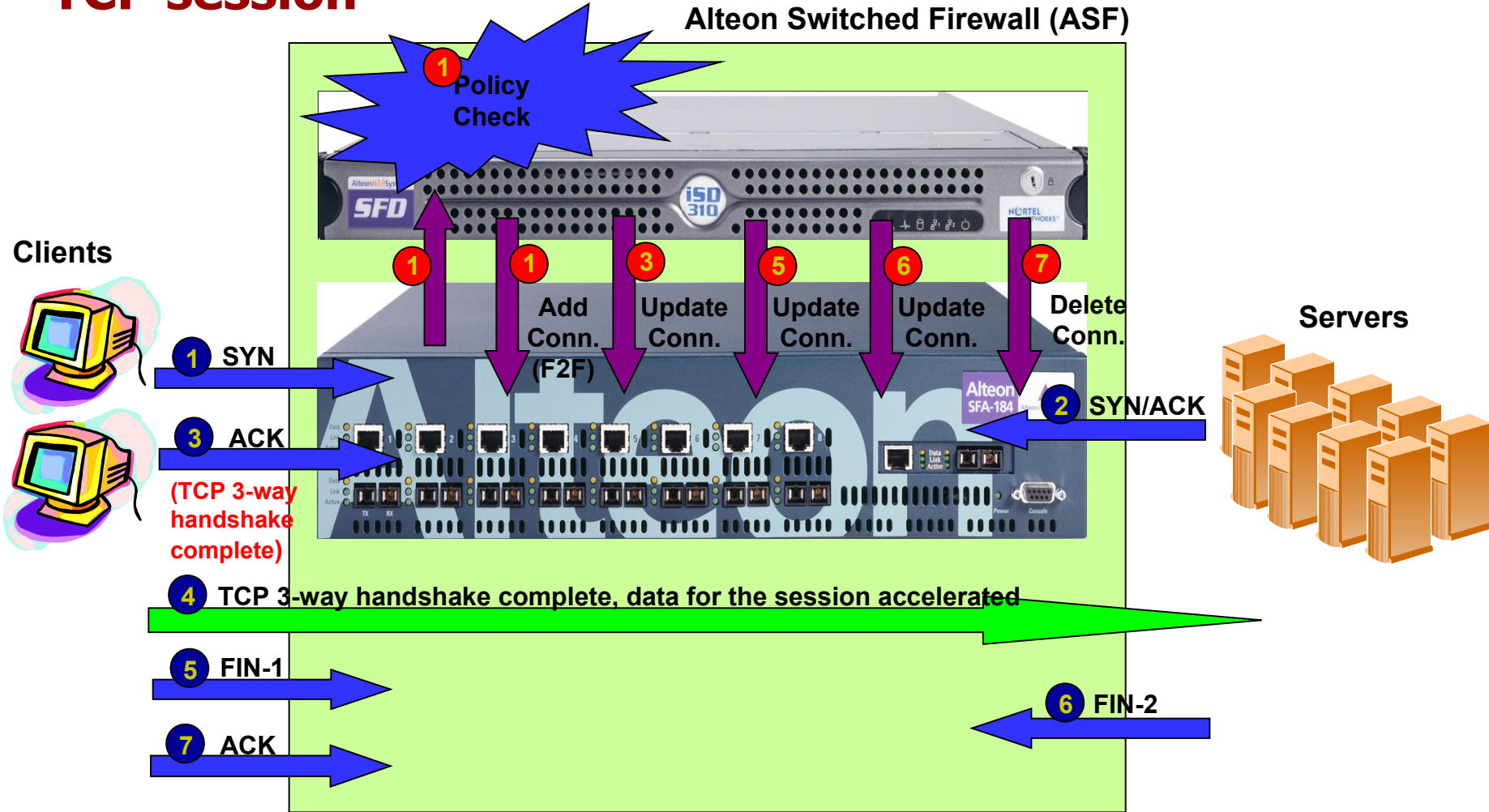
Allow /  
express forward

Iterate per unmatched  
frame / session



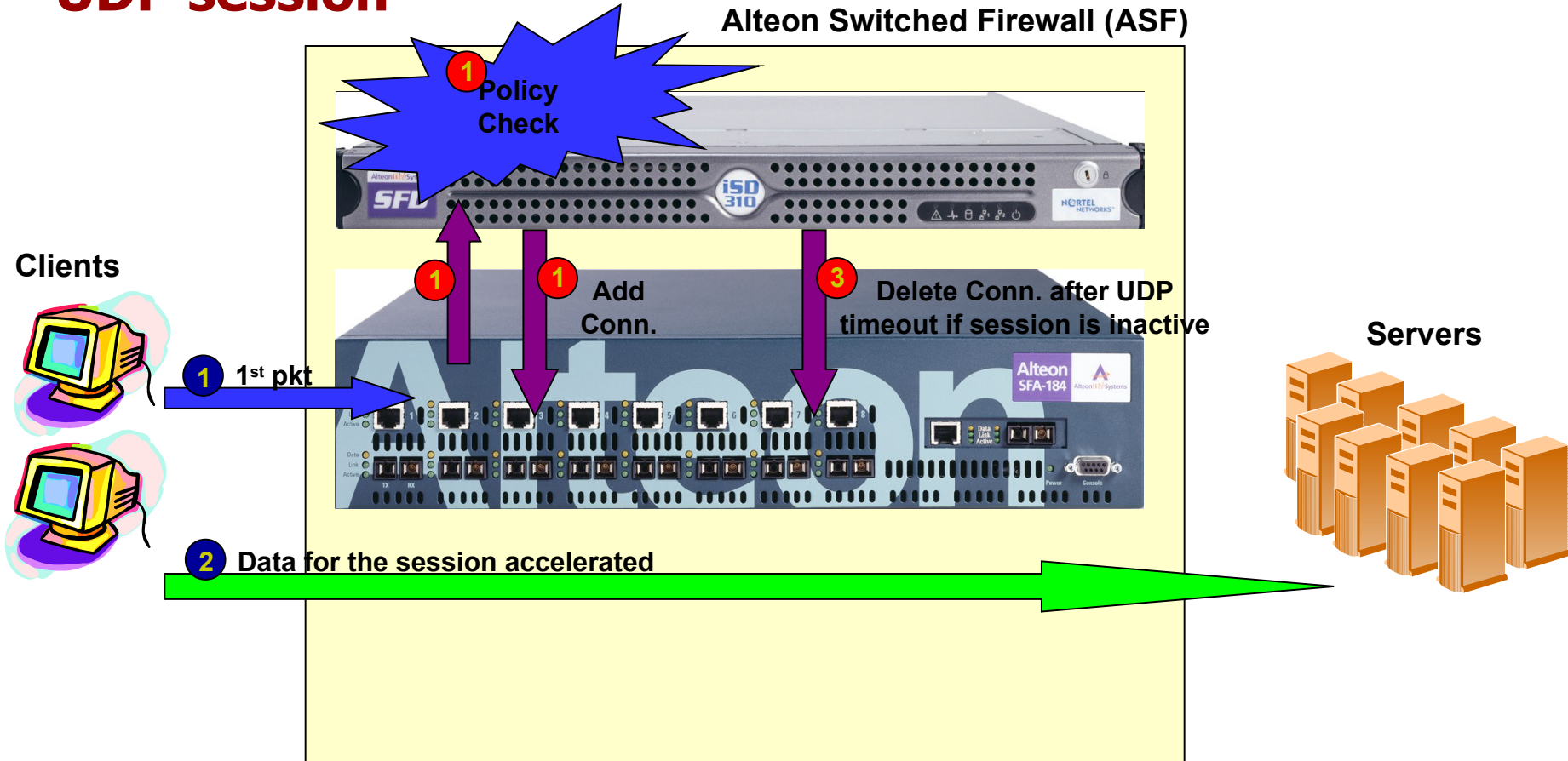
# Secure XL & NAAP in Action

## TCP session

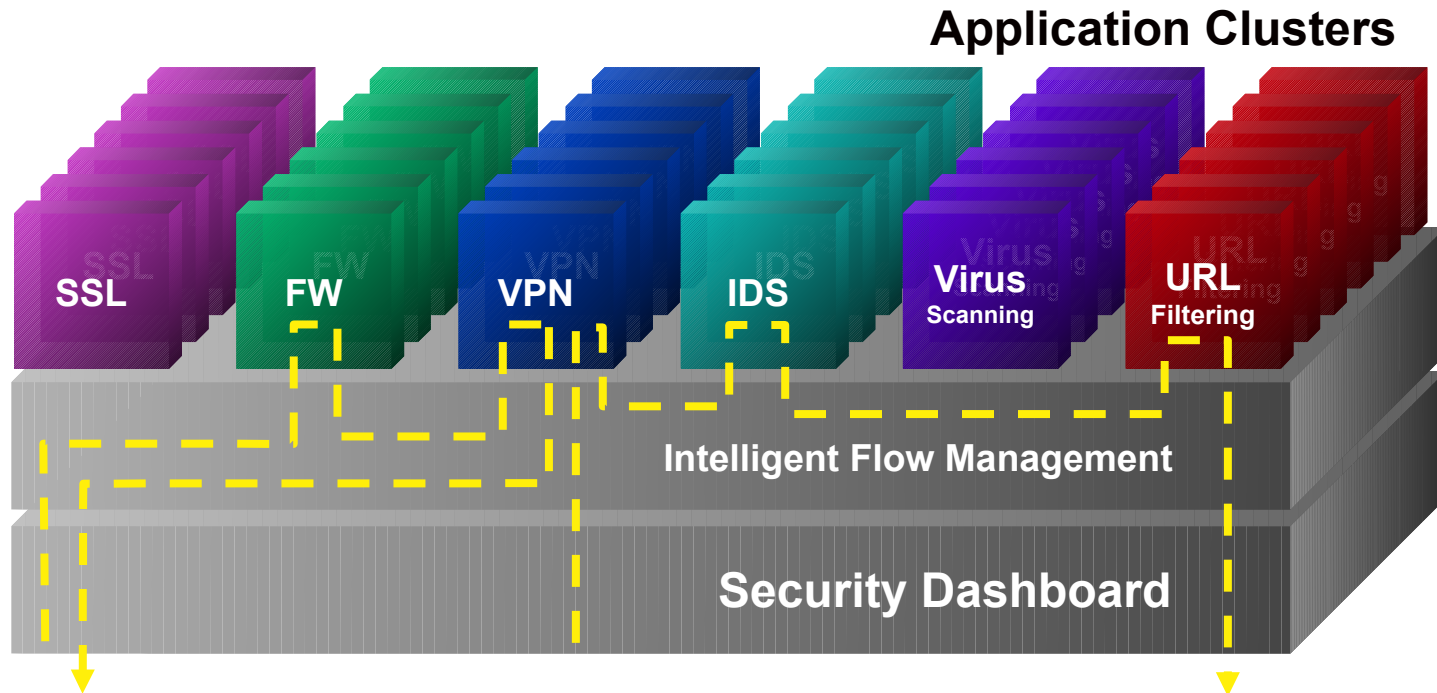


# Secure XL & NAAP in Action

## UDP session



# New Focus on Integrated Management and Flow



- Shift from physical management to logical management
- Central management of multiple services
- Plug and play simplicity and scalability