Enabling Active Flow Manipulation In Silicon-based Network Forwarding Engines

Tal Lavian  - 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

Active Nets Community
Active Nets
Ideas

Realistic
Mechanisms

Real AN Network Products

Internet

Great Ideas

Usable/Realizable
Mechanisms/Products
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

Application services:
- OpletService, Shell, Logger

User Oplets
- ORE
- JVM
- MEM
- CPU

Standard Services
- JFWD

Function Services
- ANTS
  - Firewall, DiffServ
  - Jcapture, HTTP, IpPacket

Control Plane:
- Filtered packets
- Monitor status
- New forwarding rules

Data Plane

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?

Active Nets Community
Active Nets
Ideas

Realistic
Mechanisms

Experimental/Laboratory Platforms

Commercial AN Platform?

Nortel Networks
AN Products

SSL
ASF
IDS
VPN
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

1. User opens session
2. Sends server certificate
3. Requests client certificate
4. Client sends the certificate with public key
5. Validates the client certificate info.
6. Send encrypted data to back end
7. Serves request/response

HTTP
HTTPS

Public key
Published

Private key
Confidential

DANCE Exposition
ASF – Alteon Switched Firewall

Traditional Firewall Solution

Alteon Switched Firewall System

Security Revolution

90% of all packets are accelerated

Innovative Firewall Platform

Switched Firewall System
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

Management Plane
- Single point of secure central management
- BBI, CLI, SSI, Plug and Play

Application Plane
- SSL
- Firewall
- IDS
- VPNs
- Virus Scan
- URL Filtering

Control Plane
- Security Appliance
- Controller of accelerated sessions

Data Plane
- Security Accelerator
- Switch based acceleration of session data

Nortel Appliance Acceleration Protocol
(Enables application control of switch sessions)
What next?
Disaster Recovery concept

1. Normal App flow: Client X -> Server Z
2. Disaster Strikes at Location Z
3. EvaQ8 OG 3 sends a signal[RSPV] to OG1
4. OG1 instructs Omnit net to connect B2 & B3; Server Z and Server Y data sync'd
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)*

Actions

- Drop
- NAT
- IP TOS rewrite
- Redirect (to IP or server group)
- Allow / express forward

Frame Ingress

Iterate per unmatched frame / session

DANCE Exposition
Secure XL & NAAP in Action
TCP session

1. Policy Check
2. SYN/ACK
3. Update Conn.
4. TCP 3-way handshake complete, data for the session accelerated
5. Update Conn.
6. Update Conn.
7. Delete Conn.

Alteon Switched Firewall (ASF)

Clients

Servers

1. SYN
2. ACK
3. (TCP 3-way handshake complete)
4. TCP 3-way handshake complete, data for the session accelerated
5. FIN-1
6. FIN-2
7. ACK

DANCE Exposition
Secure XL & NAAP in Action
UDP session

1. Policy Check
2. Data for the session accelerated
3. Delete Conn. after UDP timeout if session is inactive

Alteon Switched Firewall (ASF)

Clients

1st pkt

Servers

Add Conn.
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