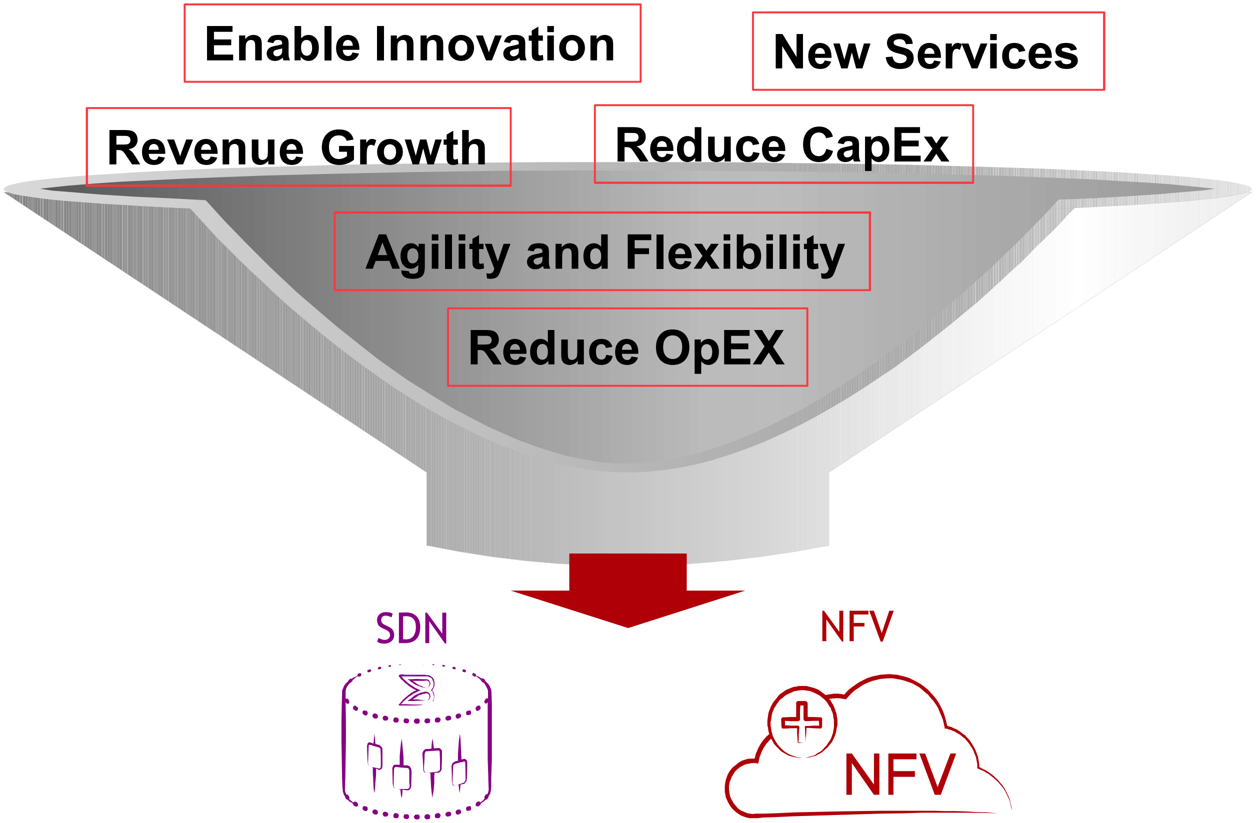
What's driving SDN/NFV?

Ivan Wong

Senior IP Architect

Why Company want SDN/NFV?



Enable Innovation

New Services

Revenue Growth

Reduce CapEx

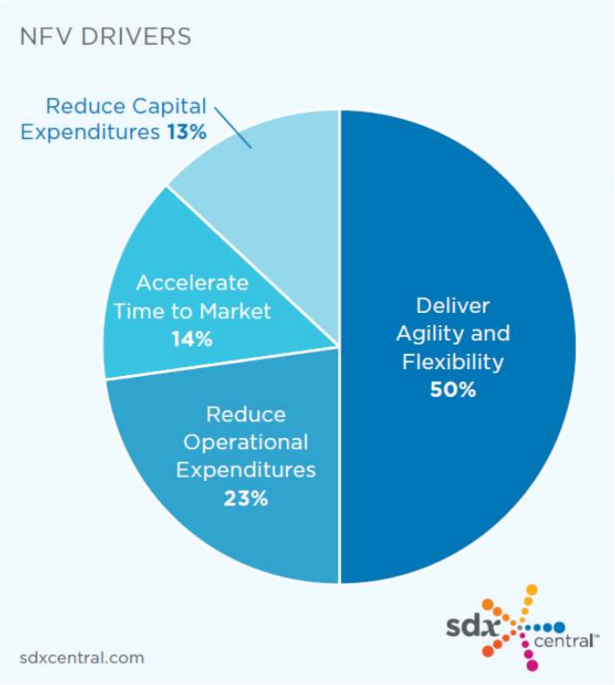
Agility and Flexibility

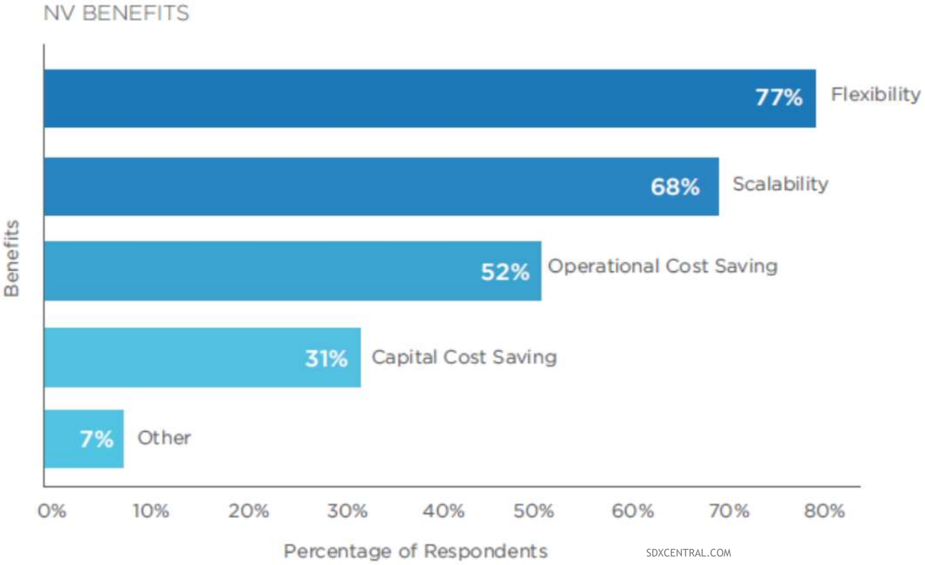
Reduce OpEX

SDN

NFV

Why Company want SDN/NFV?

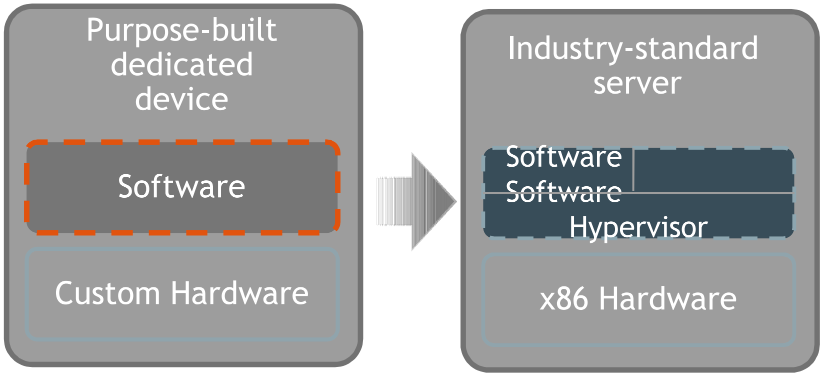




What is the Difference between SDN and NFV?

Complimentary, but independent technologies

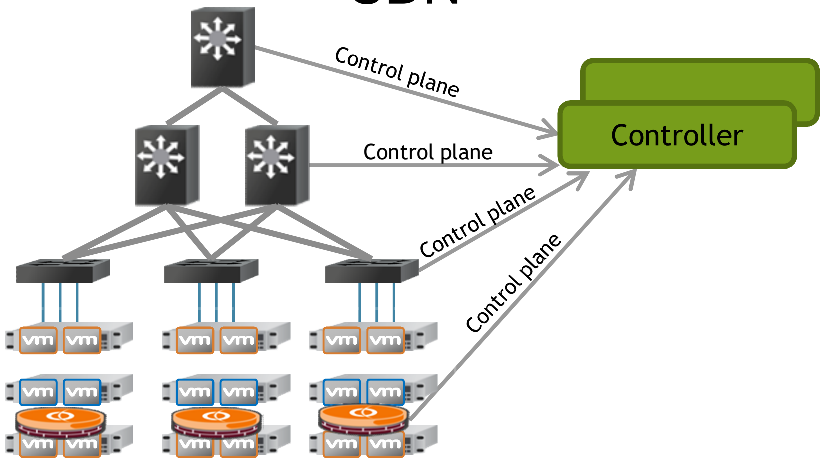
NFV



Consolidate diverse network equipment types (firewall, switching, routing, ADC, BRAS, EPC, etc.) onto industry-standard x86 servers using virtualization.

Benefits: Reduced cost and increased agility

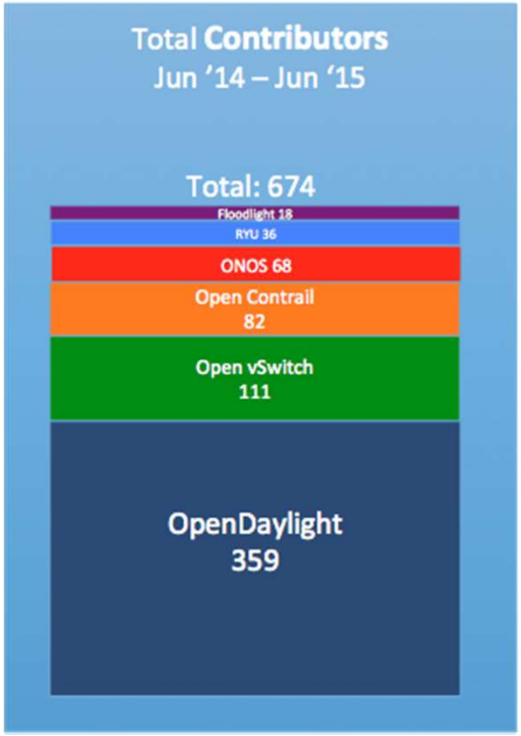
SDN

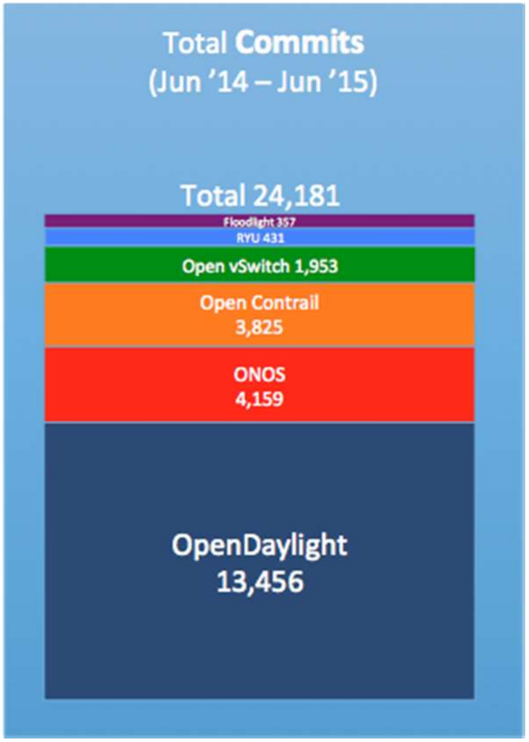


Separate control plane from the data plane in network devices (physical and virtual) with intelligence and programmability centralized in a controller.

Benefits: Increased agility via automation and increased innovation via programmability

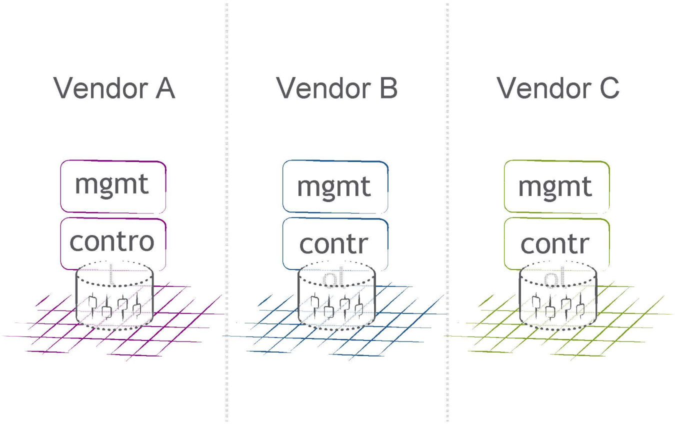
The brain of SDN, Opendaylight?



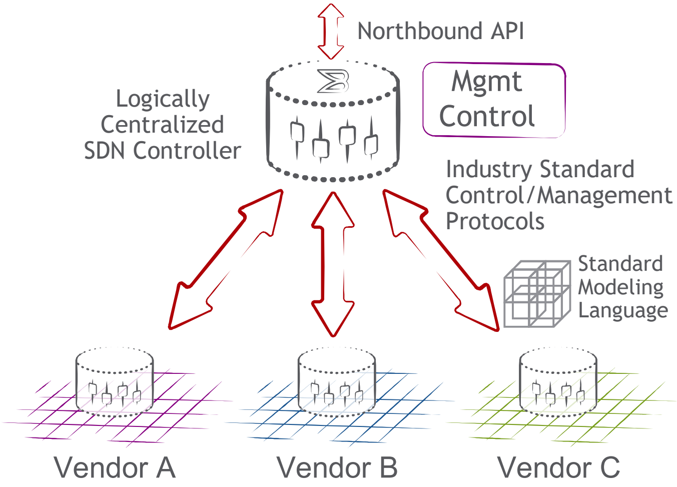


OPEN
DAYLIGHT
SUMMIT

Disaggregation and Open, Scalable Platform



- Device-by-device operation
- Proprietary, vendor-specific vertical stacks for control, management and orchestration
- Limited innovation in individual silos


Northbound API
Logically Centralized SDN Controller
Mgmt Control
Industry Standard Control/Management Protocols
Standard Modeling Language
Vendor A
Vendor B
Vendor C

- Network-wide operation
- Open control, management and orchestration using open control protocols/modeling languages
- Independent innovation at each layer of the stack

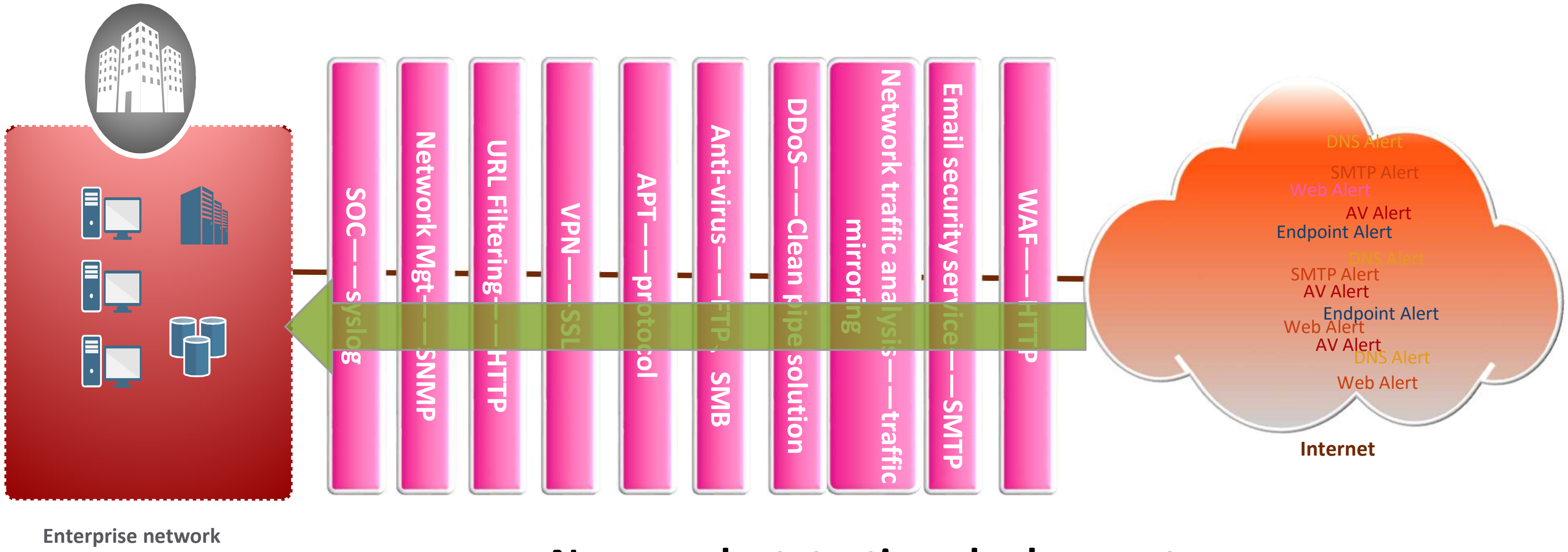
Software-Defined Networking

New levels of automation, agility and innovation

PROGRAMMATIC
CONTROL

SDN Use Case

Traditional security service infrastructure



New product, testing, deployment

Limited GUI

In series design, reliability?

Multiple devices transition, increasing latency

Performance Bottleneck?

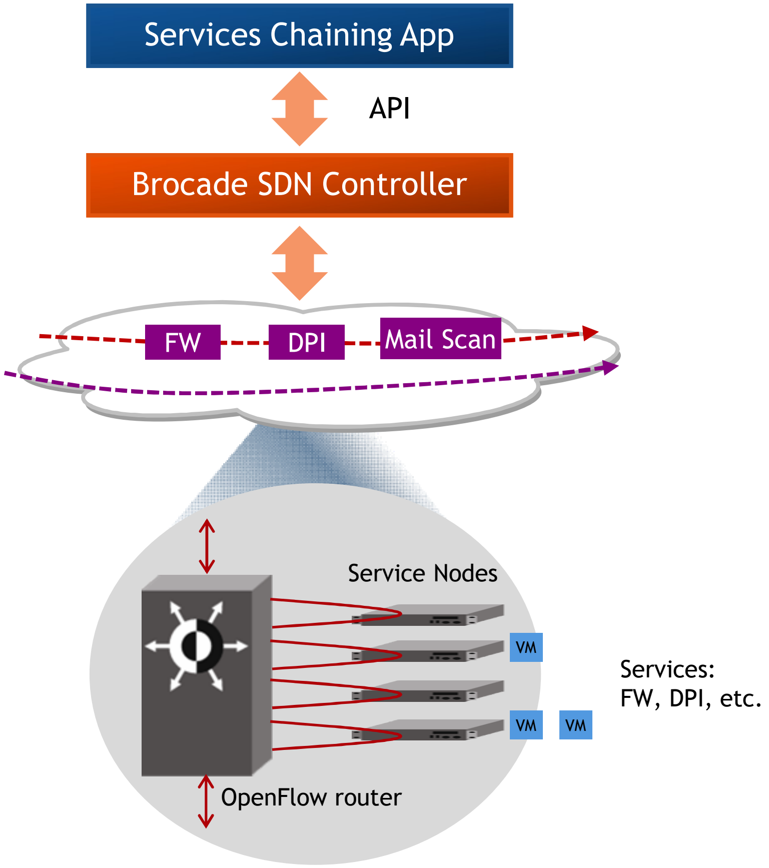
Trouble shooting difficulty

Maintenance down time for replacement

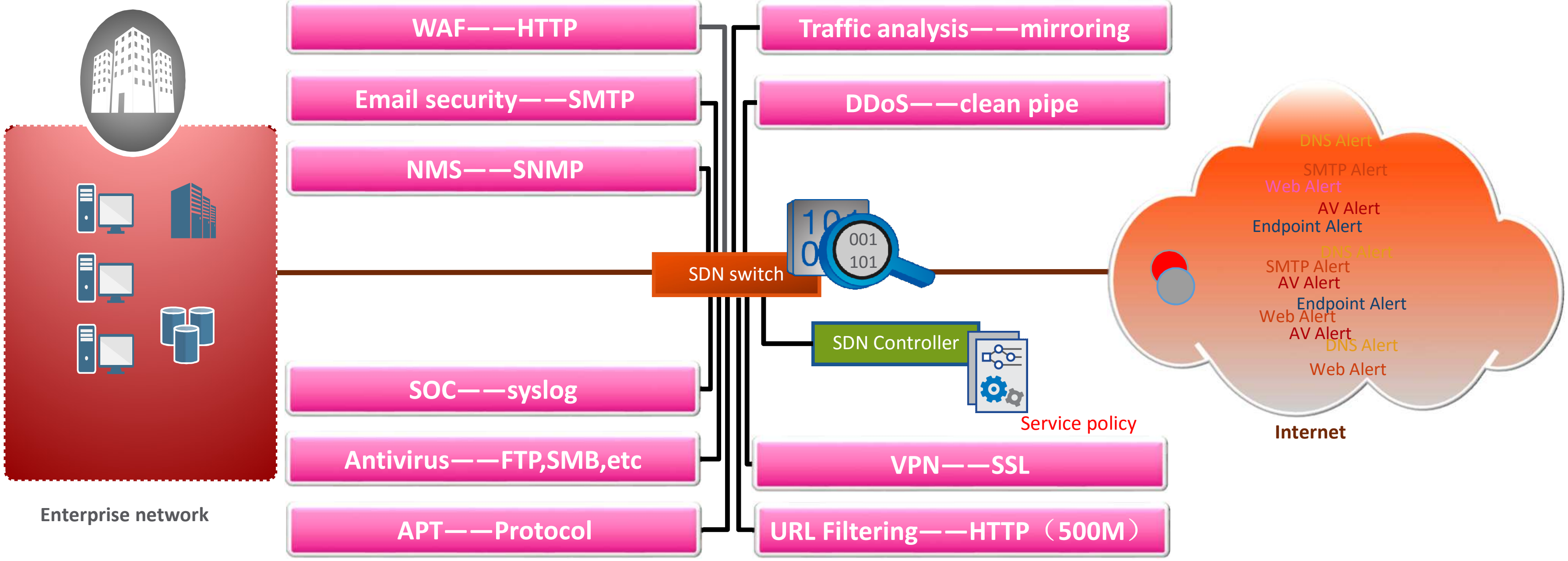
Slow emergency react plan

Security Service Chaining

- All service nodes are offline mode
  - Node failures are automatically bypassed
- No more single-point-of-failure or performance bottleneck
- Customization of services according to customer/application needs
- Simple to implement using SDN application (GUI-based)



SDN Security infrastructure



WAF——HTTP

Email security——SMTP

NMS——SNMP

SOC——syslog

Antivirus——FTP,SMB,etc

APT——Protocol

Traffic analysis——mirroring

DDoS——clean pipe

VPN——SSL

URL Filtering——HTTP（500M）

SDN switch

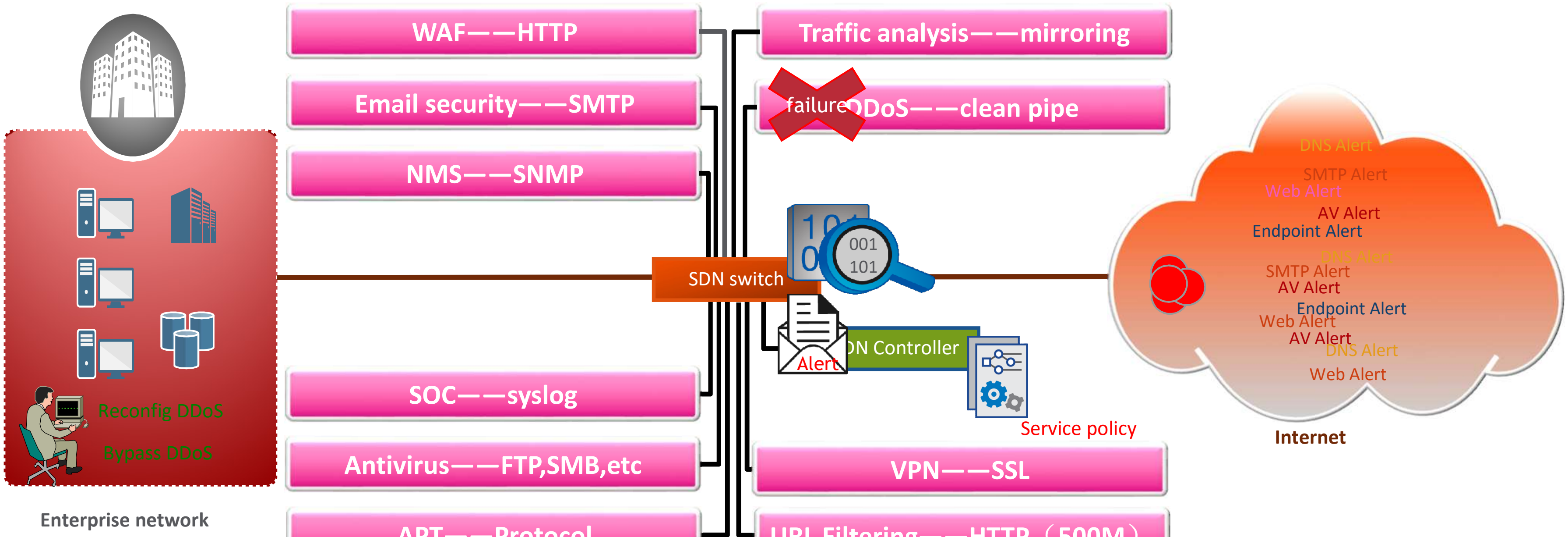
SDN Controller

Service policy

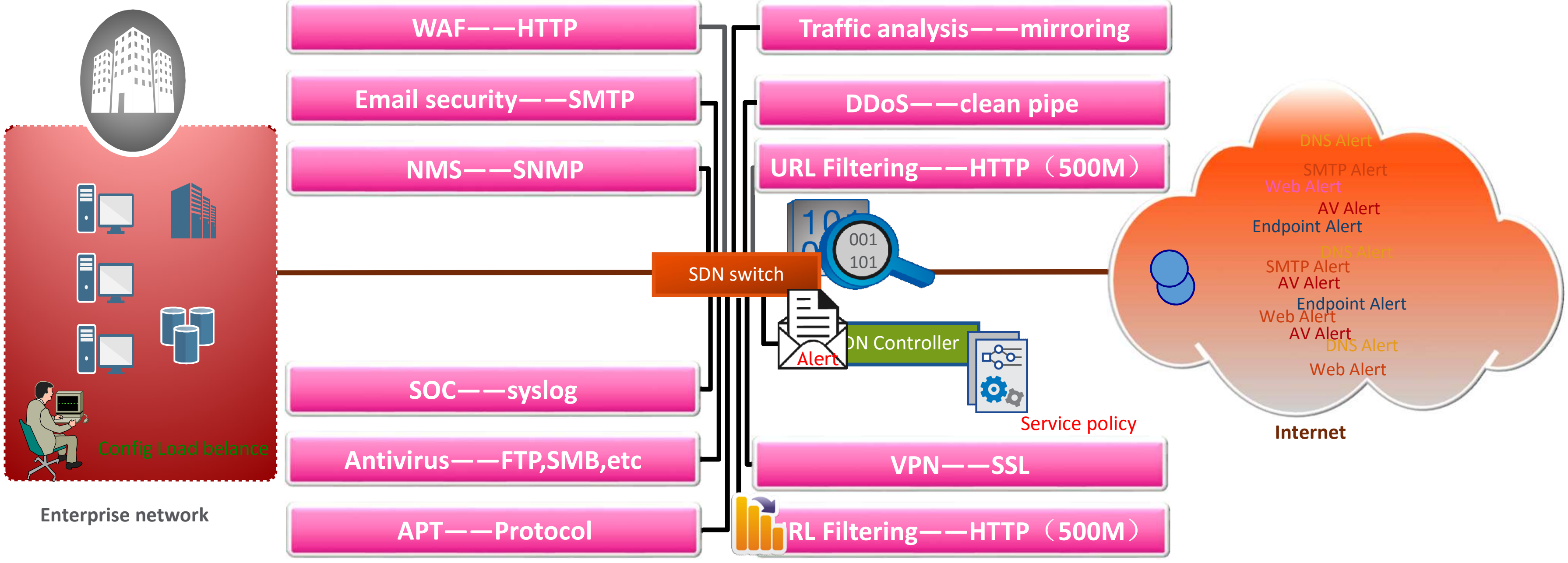
Enterprise network

Internet

SDN Security infrastructure



SDN Security infrastructure



WAF——HTTP

Email security——SMTP

NMS——SNMP

SOC——syslog

Antivirus——FTP,SMB,etc

APT——Protocol

Traffic analysis——mirroring

DDoS——clean pipe

URL Filtering——HTTP（500M）

SDN switch

Alert

DN Controller

Service policy

VPN——SSL

RL Filtering——HTTP（500M）

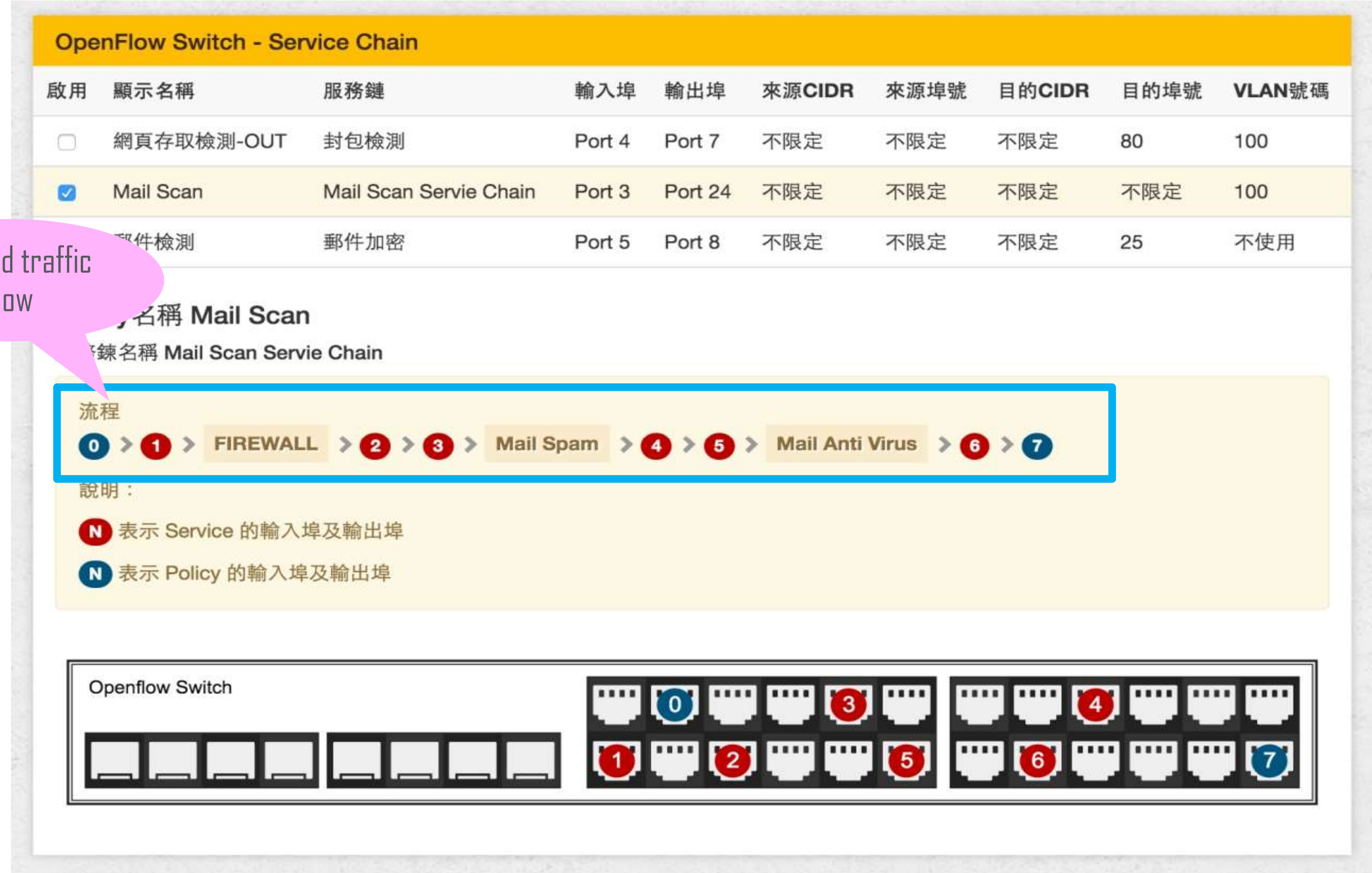
Config Load belance

Enterprise network

DNS Alert
SMTP Alert
Web Alert
AV Alert
Endpoint Alert
DNS Alert
SMTP Alert
AV Alert
Endpoint Alert
Web Alert
AV Alert
DNS Alert
Web Alert

Internet

Service Chaining Application - Actions



OpenFlow Switch - Service Chain

啟用	顯示名稱	服務鏈	輸入埠	輸出埠	來源CIDR	來源埠號	目的CIDR	目的埠號	VLAN號碼
☐	網頁存取檢測-OUT	封包檢測	Port 4	Port 7	不限定	不限定	不限定	80	100
☑	Mail Scan	Mail Scan Servie Chain	Port 3	Port 24	不限定	不限定	不限定	不限定	100
	郵件檢測	郵件加密	Port 5	Port 8	不限定	不限定	不限定	25	不使用

Defined traffic flow

名稱 Mail Scan

鍊名稱 Mail Scan Servie Chain

流程

0 > 1 > FIREWALL > 2 > 3 > Mail Spam > 4 > 5 > Mail Anti Virus > 6 > 7

說明：

N 表示 Service 的輸入埠及輸出埠

N 表示 Policy 的輸入埠及輸出埠

Brocade Flow Optimizer

VISIBILITY

- L2-L4 Flow Monitoring
- MPLS and VXLAN Monitoring
- IPsec (IPv4, IPv6) Monitoring
- SDN Based Wiretap
- Flow Accounting

CONTROL

- Volumetric Attack Mitigation
- BGP RTBH (Drop, Re-direct)
- Elephant Flow Management (Drop, Metering, Re-direct)
- Firewall Bypass/Insertion
- White-listing and Black-listing

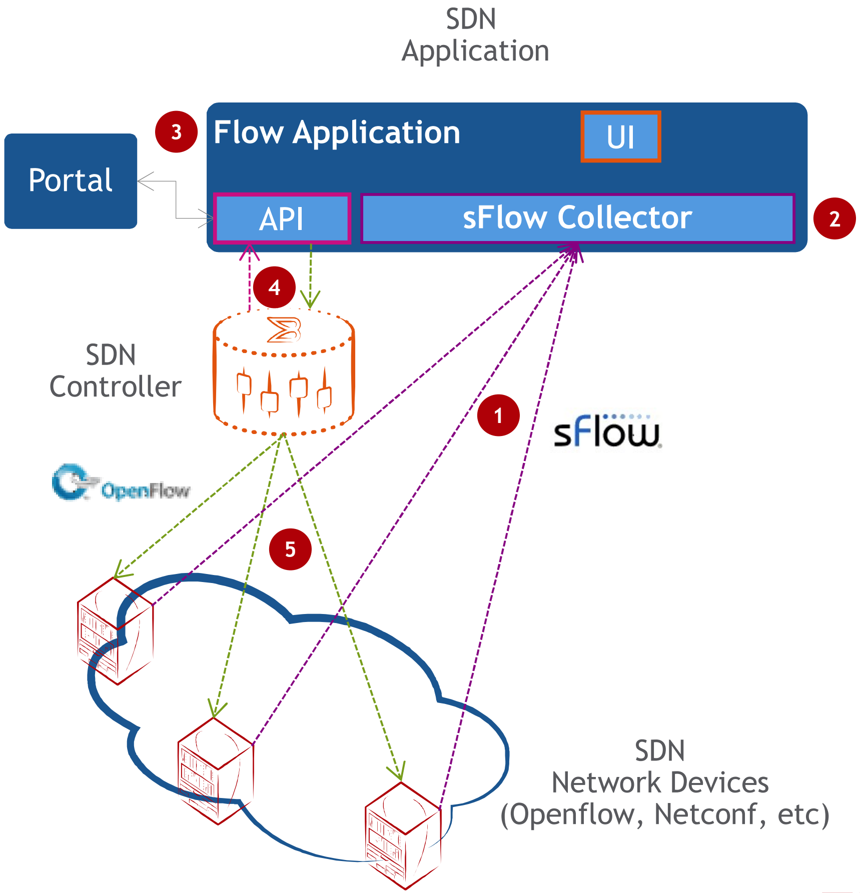
AUTOMATION

- Automated Threat Mitigation
- Automated BGP RTBH
- Automated Flow Tap
- Automated Firewall Bypass
- Automated Flow Management

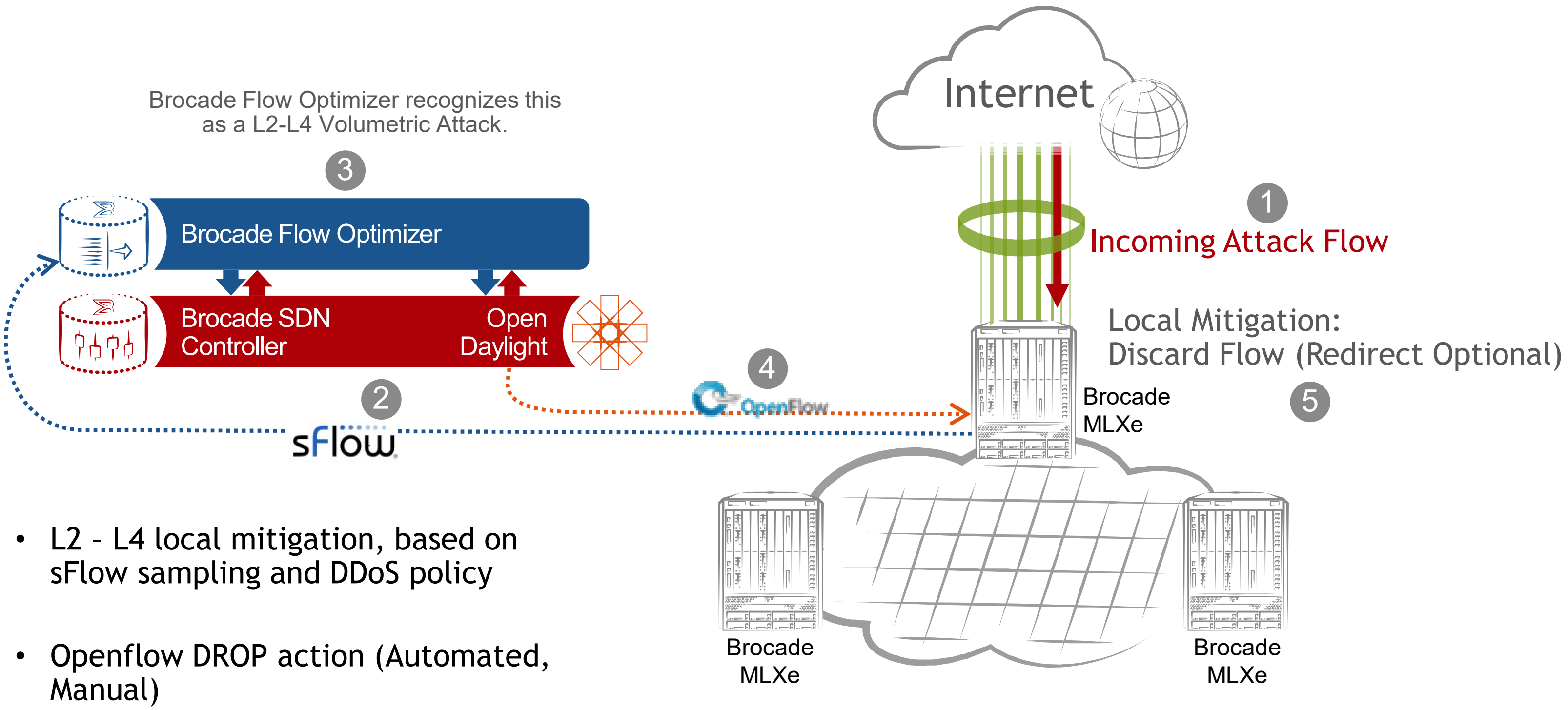
SDN Use Case

A Closed-Loop Control and Automation

1. Network devices send flow sampling records
2. Flow Collector collect sampled data
3. Flow App present “abnormal” flows to dashboard
4. Flow App “ask” SDN controller to “handle” the flows by request
5. SDN controller “program” network devices to
   - DROP traffic
   - REDIRECT to clean pipe
   - RATE-LIMIT traffic
   - MIRROR to probe`

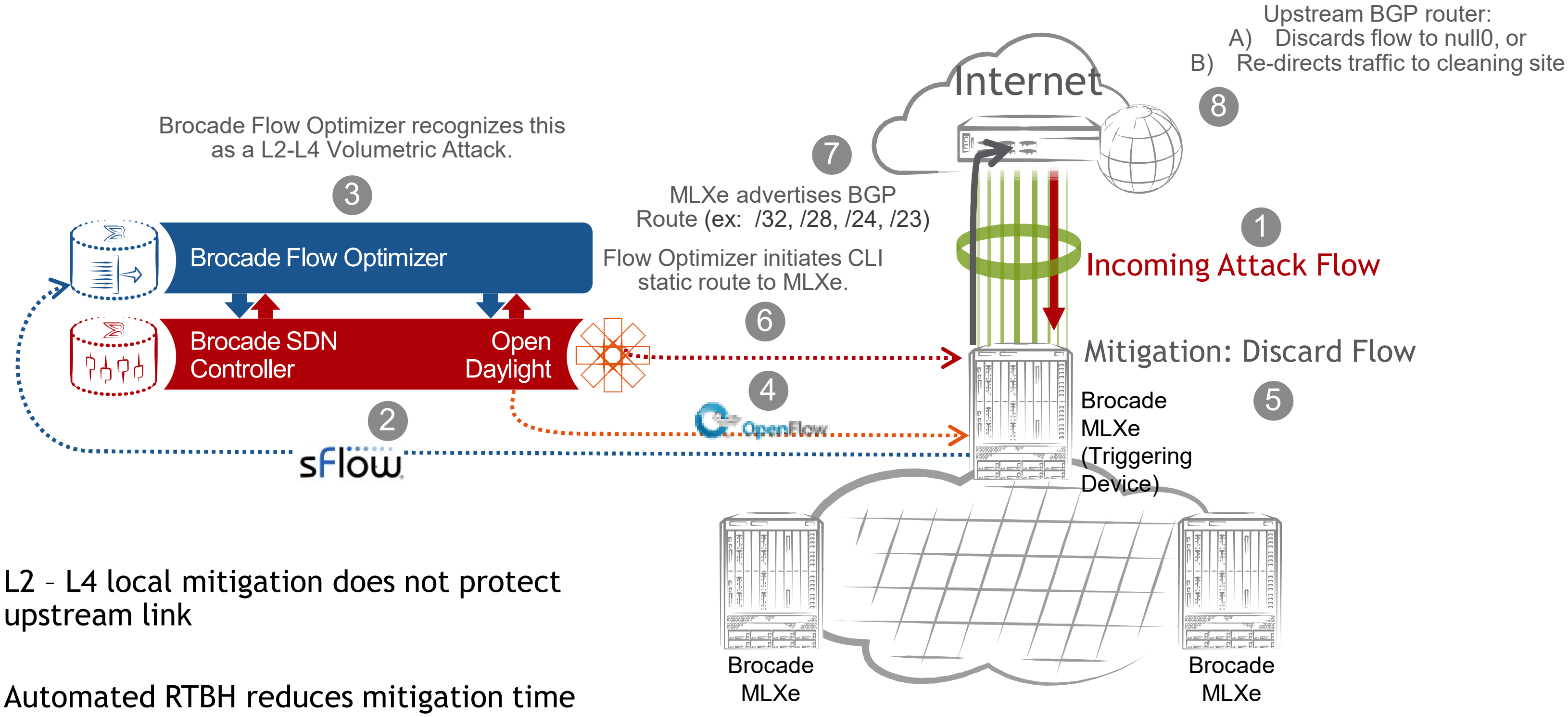


L2-L4 Volumetric Attack Mitigation



- L2 – L4 local mitigation, based on sFlow sampling and DDoS policy
- Openflow DROP action (Automated, Manual)
- 1/10GbE, 40GbE and 100GbE support

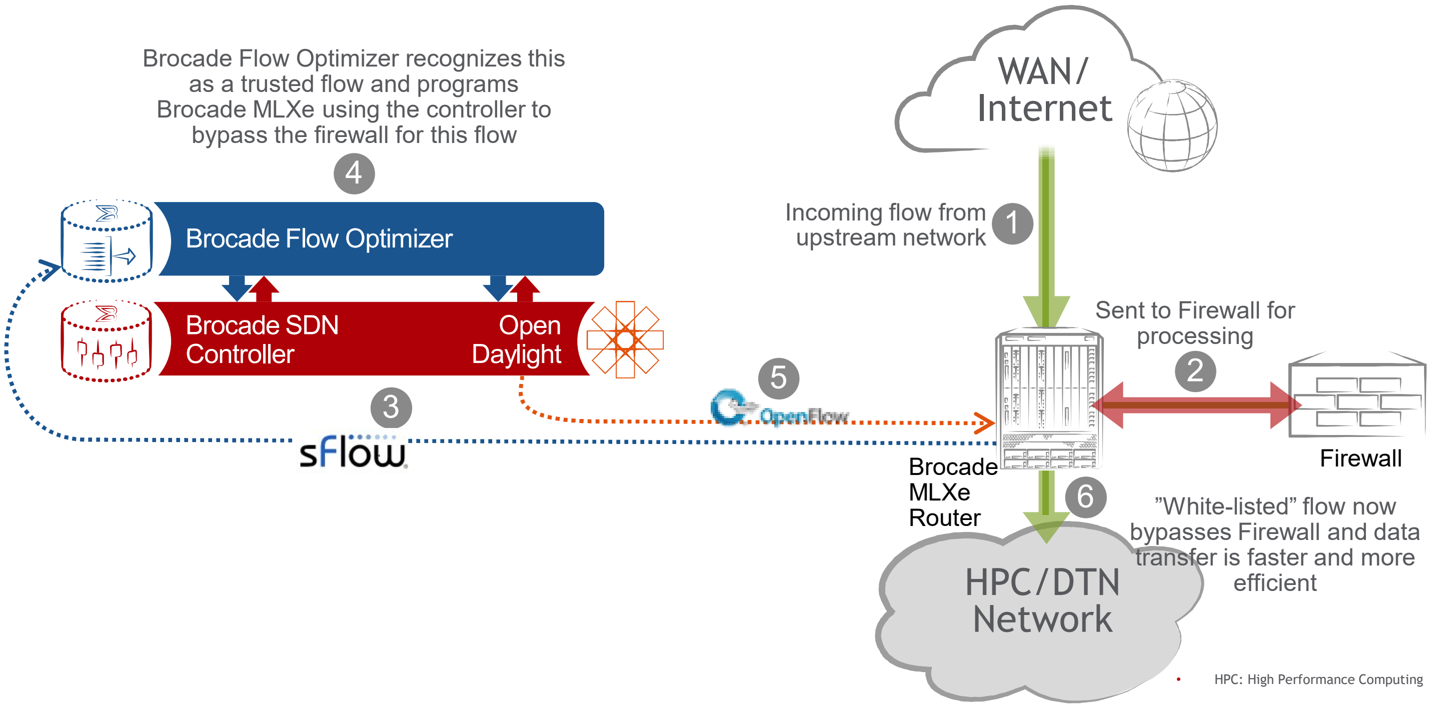
BGP Remote Triggered Black-Hole (RTBH) Mitigation


Upstream BGP router:
A) Discards flow to null0, or
B) Re-directs traffic to cleaning site
8
Internet
Brocade Flow Optimizer recognizes this as a L2-L4 Volumetric Attack.
3
7
MLXe advertises BGP Route (ex: /32, /28, /24, /23)
1
Incoming Attack Flow
Brocade Flow Optimizer
Flow Optimizer initiates CLI static route to MLXe.
6
Brocade SDN Controller
Open Daylight
Mitigation: Discard Flow
4
OpenFlow
2
sFlow
Brocade MLXe (Triggering Device)
5
Brocade MLXe
Brocade MLXe

- L2 – L4 local mitigation does not protect upstream link
- Automated RTBH reduces mitigation time from 15 minutes or hours -> under 1 minute

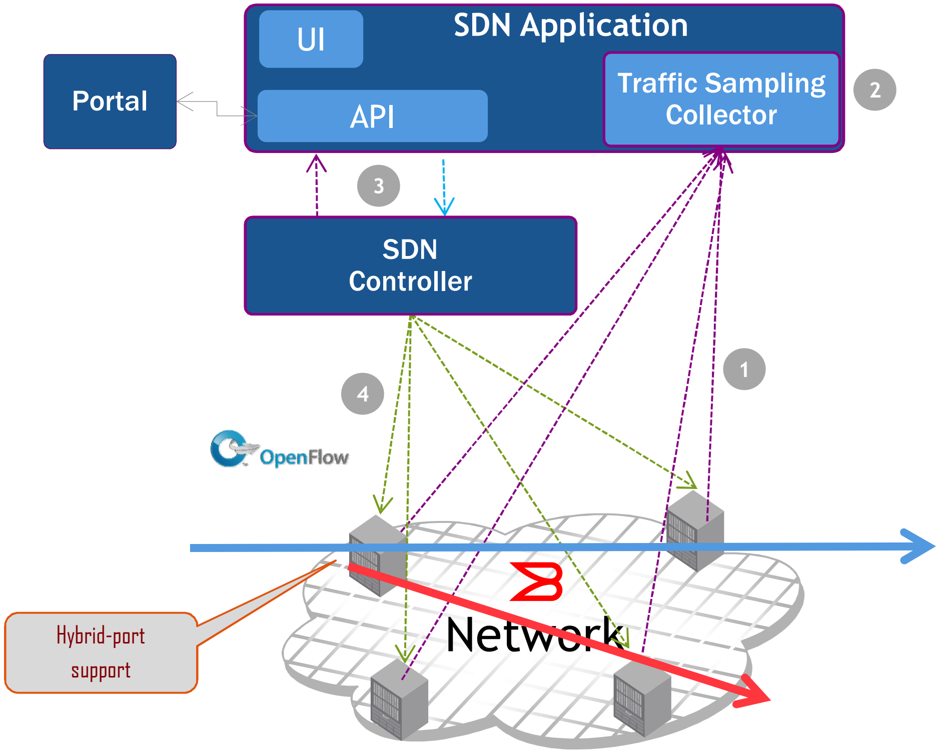
Firewall Bypass

Science-DMZ Use Case


Brocade Flow Optimizer recognizes this as a trusted flow and programs Brocade MLXe using the controller to bypass the firewall for this flow
4
Brocade Flow Optimizer
Brocade SDN Controller
Open Daylight
3
sFlow
5
OpenFlow
WAN / Internet
Incoming flow from upstream network
1
Sent to Firewall for processing
2
Firewall
Brocade MLXe Router
6
"White-listed" flow now bypasses Firewall and data transfer is faster and more efficient
HPC / DTN Network

- HPC: High Performance Computing
- DTN: Data Transfer Nodes

Why Hybrid-Port Mode ?



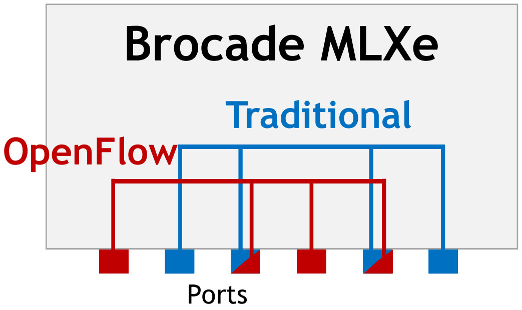
- Real-time, closed-loop control
- An open, scalable architecture for best-of-breed solutions putting together
- Support different traffic handling actions
  - DROP
  - REDIRECT
  - METERING
  - MIRROR
- With all above, traffic are forwarded by hybrid-port like normal router/switch port

Hybrid-Port Support

Brocade Innovation

- Hybrid Switch Mode
  - OpenFlow only on certain ports
  - Other ports run existing features, e.g., IP routing/switching, etc

- Hybrid Port Mode
  - Any port supports Openflow (1.3) and existing routing/switching features at the same time

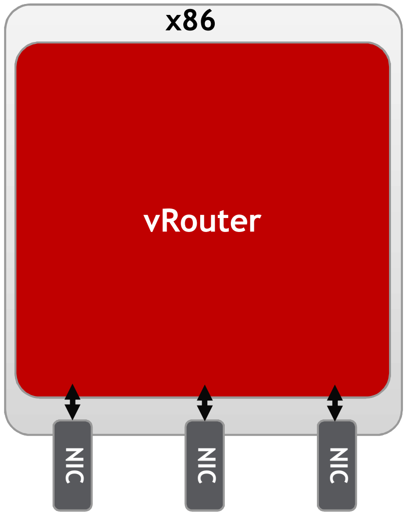


🟦 Traditional Features

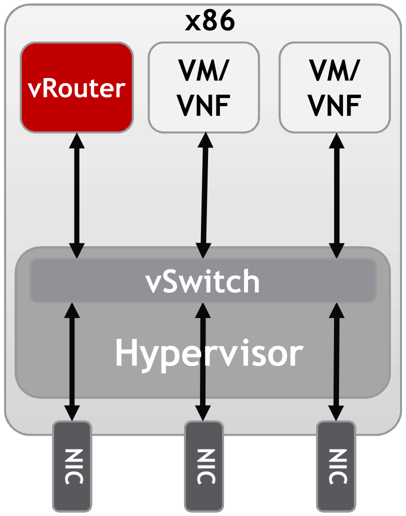
🟥 OpenFlow only (hybrid switch mode)

◩ OpenFlow + Traditional Features (hybrid port mode)

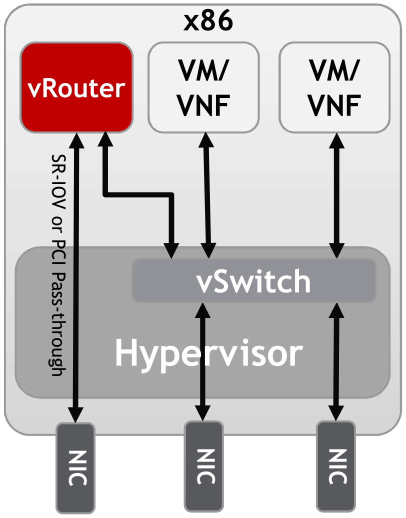
NFV Deployment Models



Bare Metal

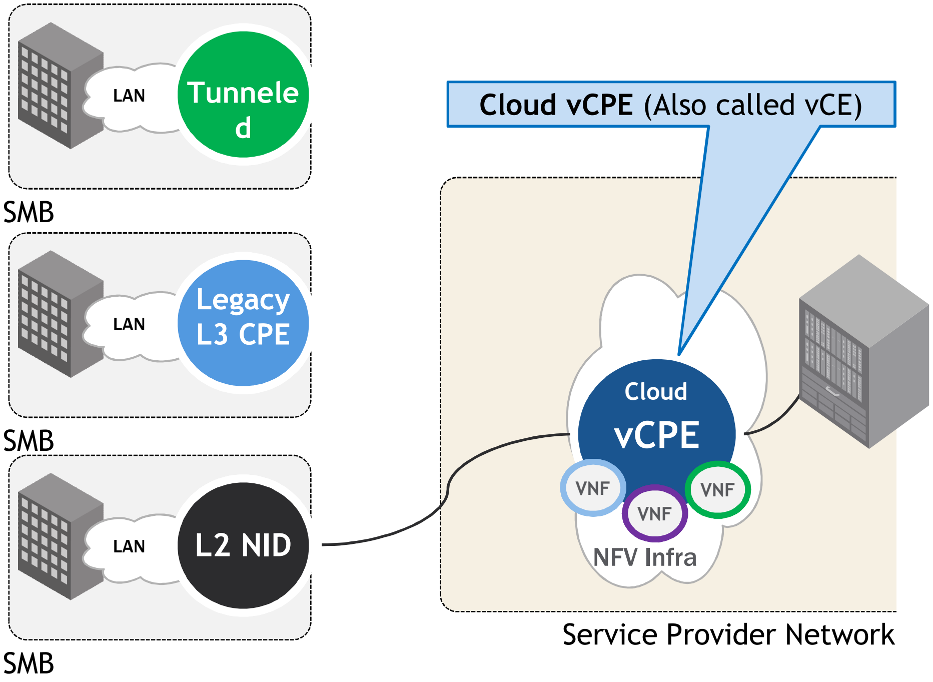


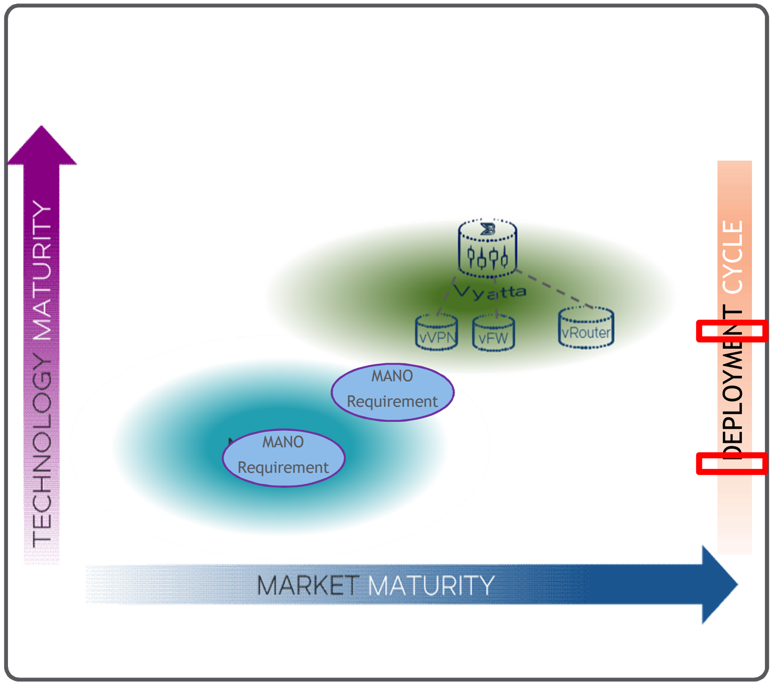
Virtualized Deployment



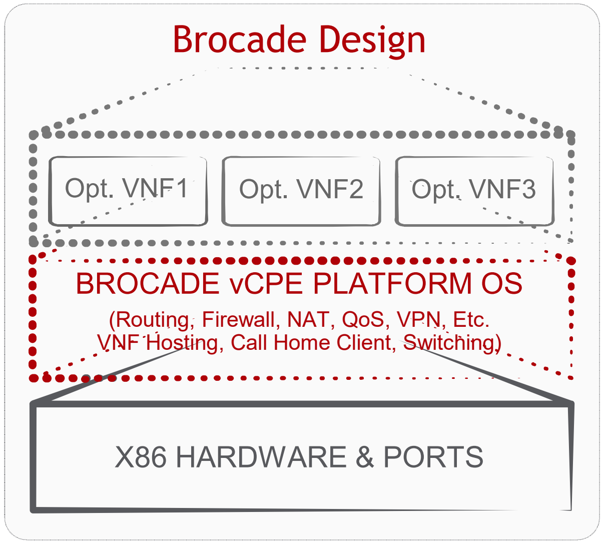
SR-IOV / PCI Pass-through

Use Case – Cloud vCPE

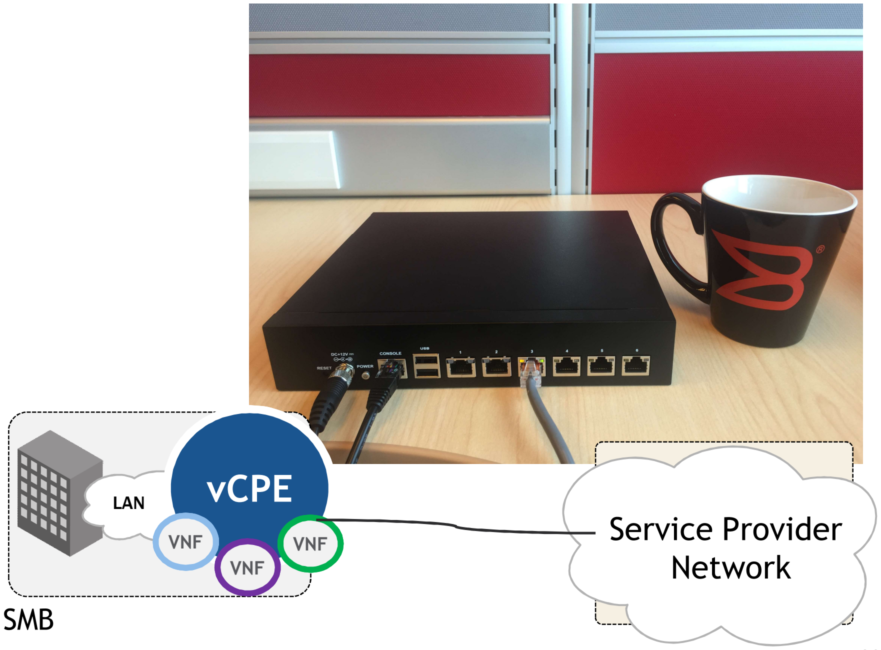




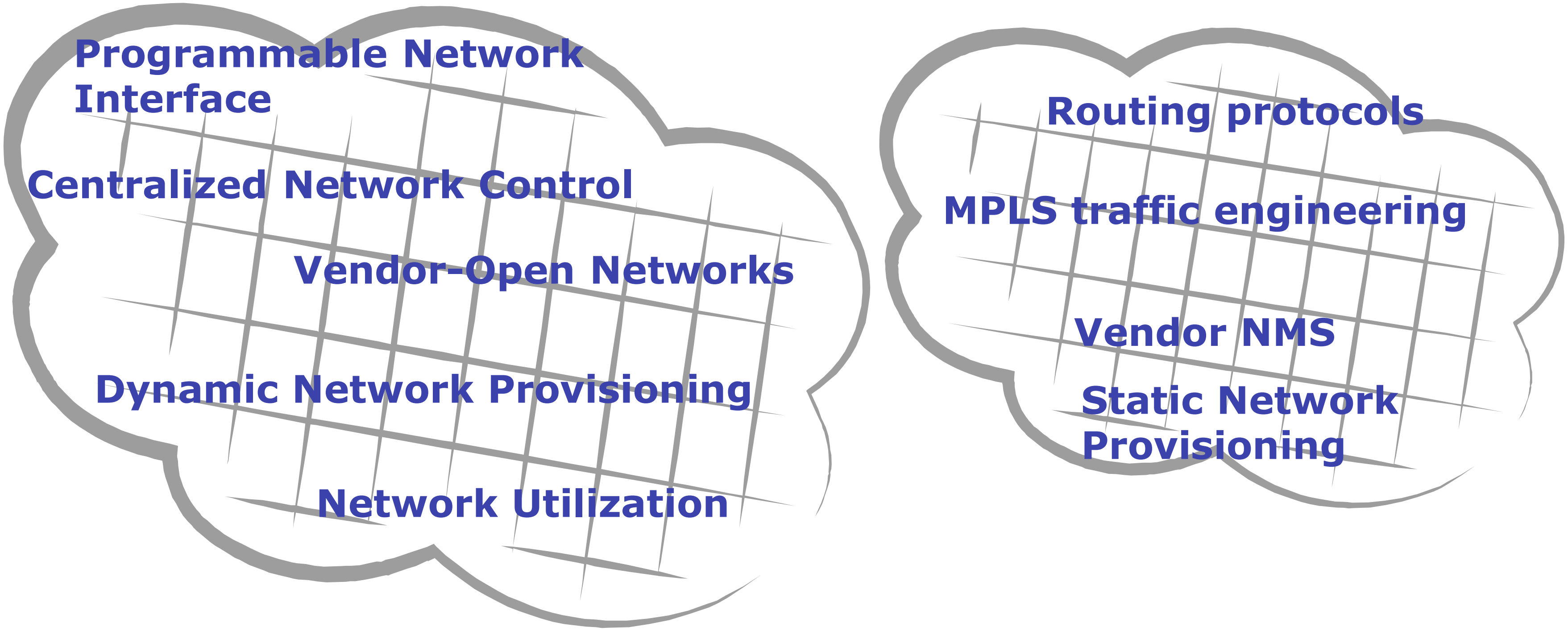
Use Case – On-Premise vCPE



Open X86 HW Platform



Network architecture



Programmable Network Interface

Centralized Network Control

Vendor-Open Networks

Dynamic Network Provisioning

Network Utilization

Routing protocols

MPLS traffic engineering

Vendor NMS

Static Network Provisioning

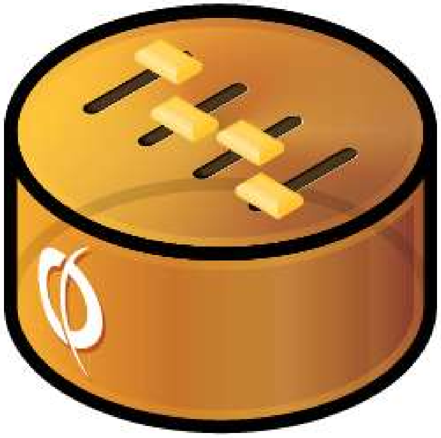
Network vendor solution and management

Common NMS

SDN Controller as high level management tool

OpenFlow

SDN-enabled hybrid devices



Vendor specific NMS

vendor-specific forwarding planes

vendor-specific control planes

Proprietary Protocols

Professionals skills

Research and Protocols

Understand the new technology, protocol

Business context

Understand the context of their businesses

business need

Adoption of a new technology to control and manage the network based on business need

Q & A

BROCADE

Thank you