The SDN Applications for Data Transfer & Network Security @ IHEP

Fazhi Qi
CC,IHEP

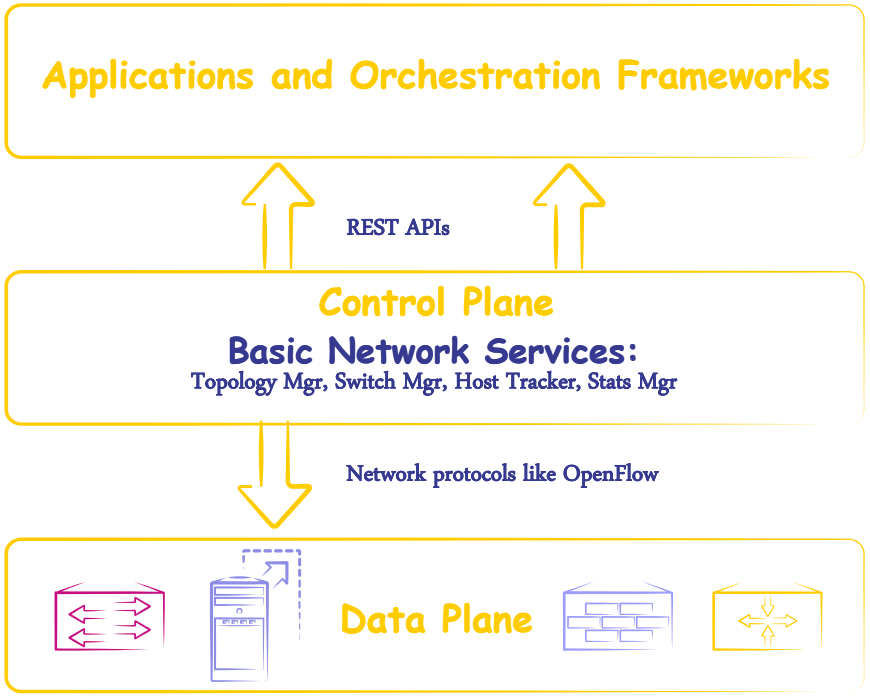
9th Mar,2017

Agenda

- About SDN
- SDN for HEP Data Transfer
- SDN for Security
- Summary

Software Defined Networking (SDN)

A Programmable Network—Design, Build, Manage



Key Features

- Network algorithms decoupled from Hardware

Advantages

- Network automation can integrate with other disciplines
- Less lock-in; Users can choose features to suit needs
- Networking control can innovate at software speeds

Agenda

- About SDN
- SDN for HEP Data Transfer(SDN-WAN)
- SDN for Security
- Summary

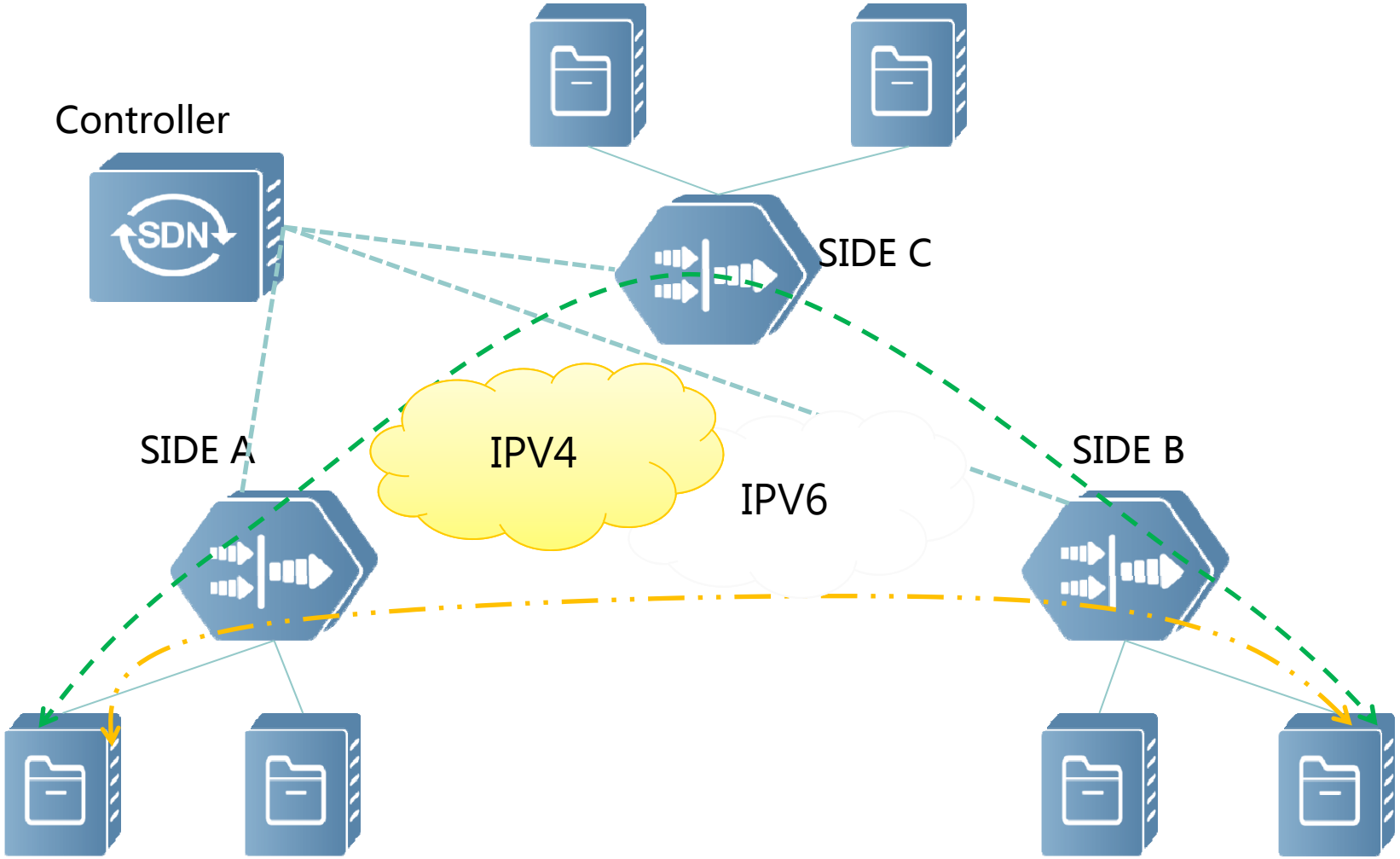
Goals & Thoughts

- Refer to :
  - **A virtual private network based on software-defined network architecture for high energy physics scientific data exchange**
  - https://indico.cern.ch/event/466991/contributions/1143596/ (HEPiX 2016 Spring)
- Improve the data exchange performance, based on the current
  - Network infrastructure
  - Applications
- Provide a simple, flexible, robust, high performance and Easy/Central - controlled network environment for HEP members in China
  - Overlay: use IPv4 & IPv6 network link
  - Automatically and Dynamically network path choosing based on the application requirements and network performance status

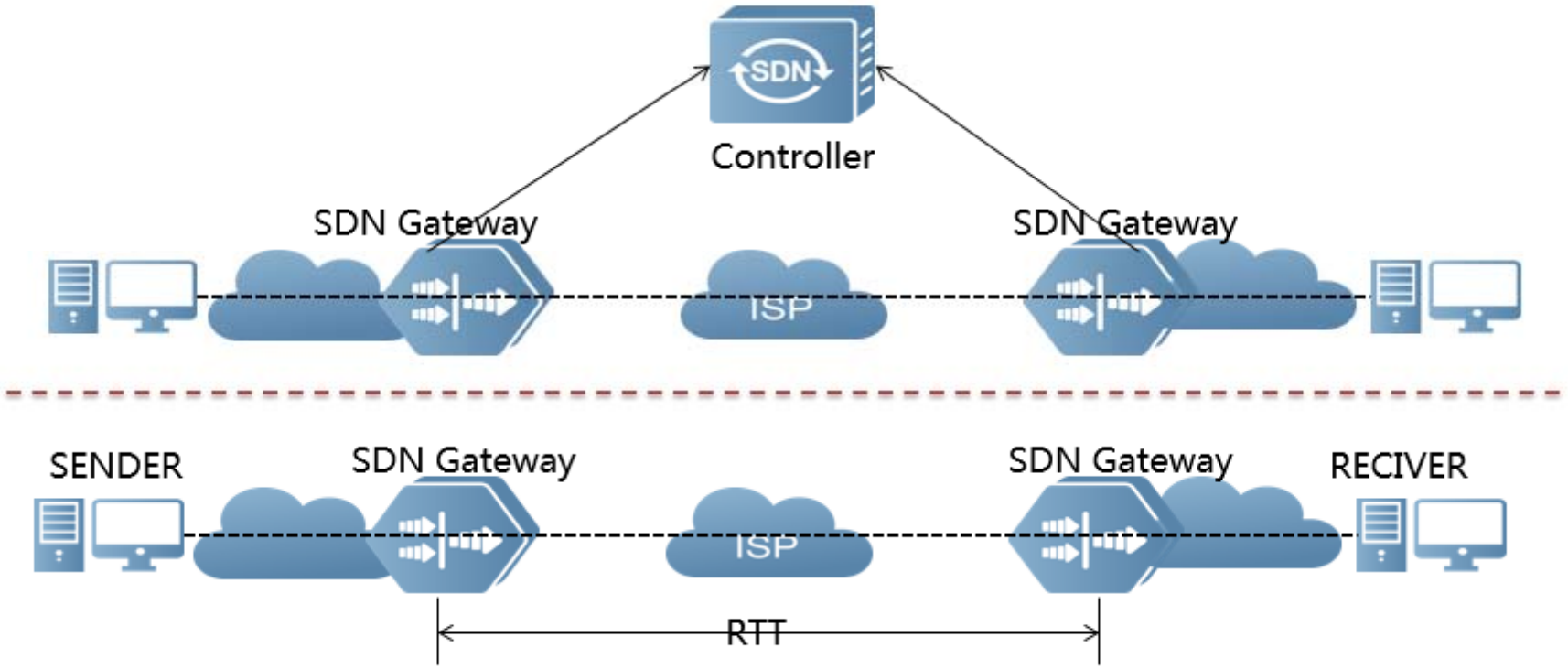
SDN-WAN & vWAN

- vWAN :virtual WAN , which is considered a part of SD-WAN.
- vWANs are used to replace private WAN services with regular broadband connectivity.
- vWANs are used to secure the connection and encrypt the traffic across public networks providing an additional layer of security through secure socket layer offload.
- vWAN also aggregates WAN links, making multiple dedicated or public network links function as a single large link. This helps with applications.
- vWAN also is used for load balancing across various communications channels because they can selectively route flows and packets based upon link performance.

Different path with different flow



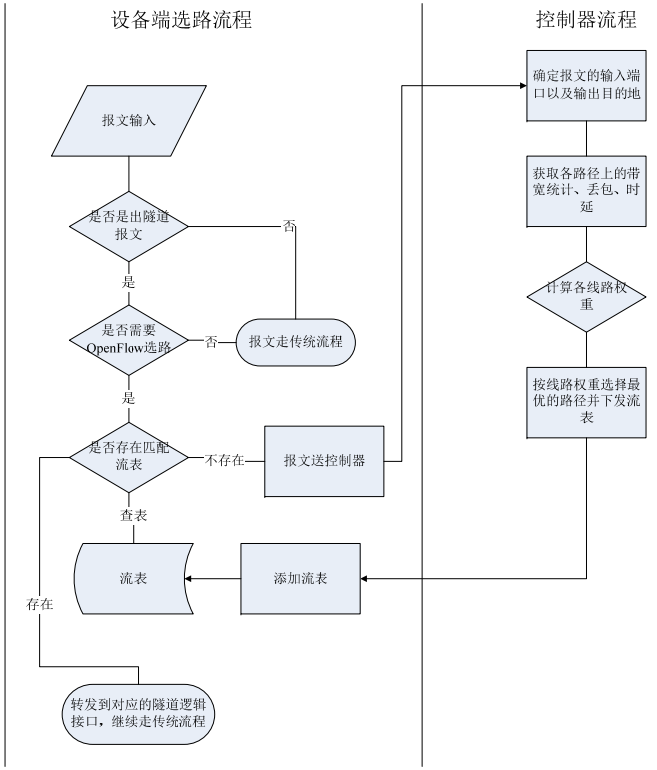
SDN Gateway

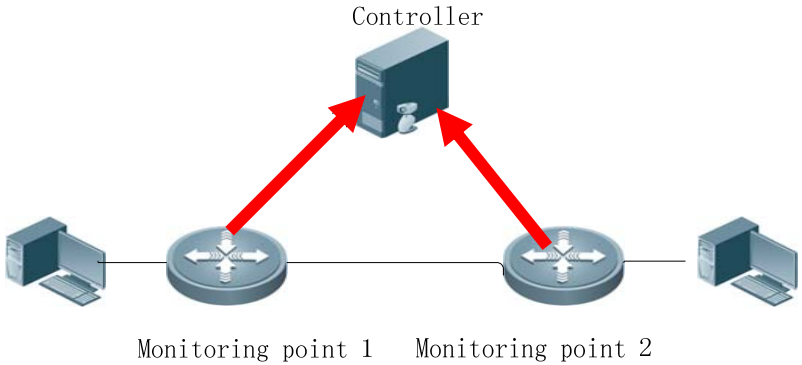


- **Gateway: All-in-one device**
- VPN: Virtual link/IPv4 Over IPv6
- Network performance monitoring (Packet loss,RTT,Throughput)
- Active network performance measurement: iperf

The Key Technology

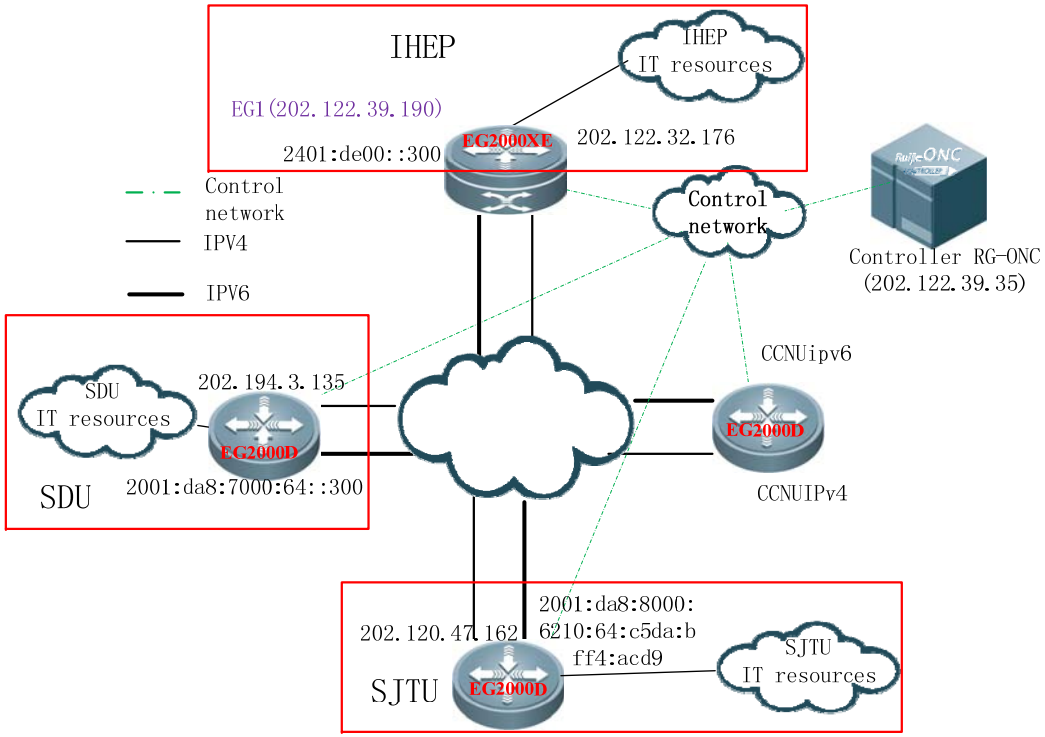
- Dynamic path selection base on
  - Packet loss
  - Latency
  - Link Bandwidth
  - Traffic throughput
  - Historical data statistics
  - →Available performance





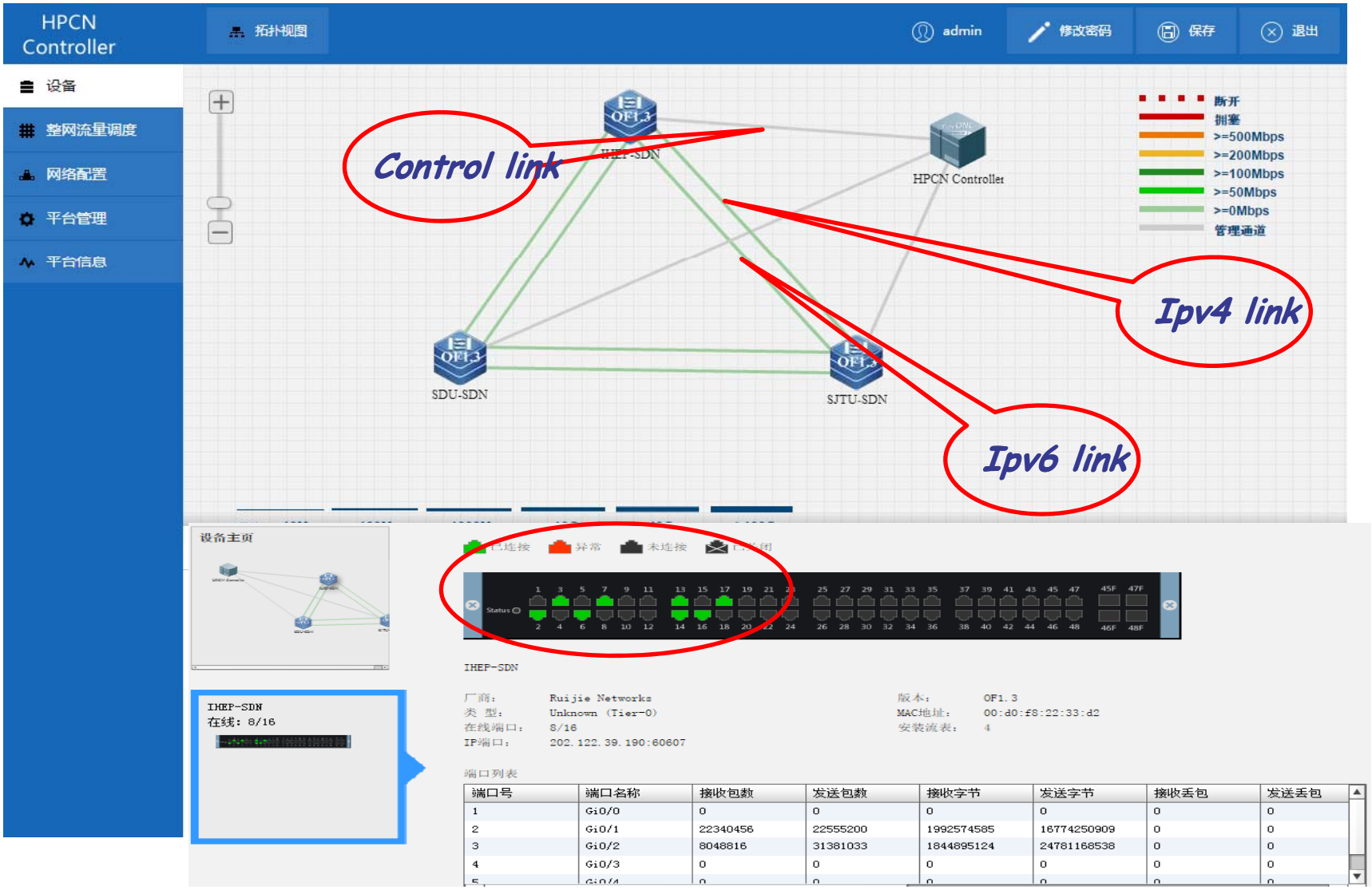
path	Packet loss	latency	Available bandwidth
Site A->site B(ipv4)			
Site A->site B(ipv6)			
Site A->site C->site B (ipv4)			
Site A->site C->site B (ipv6)			
Site A->(ipv4)site C-> (ipv6)site B			
Site A->(ipv6)site C-> (ipv4)site B			

Deployment status

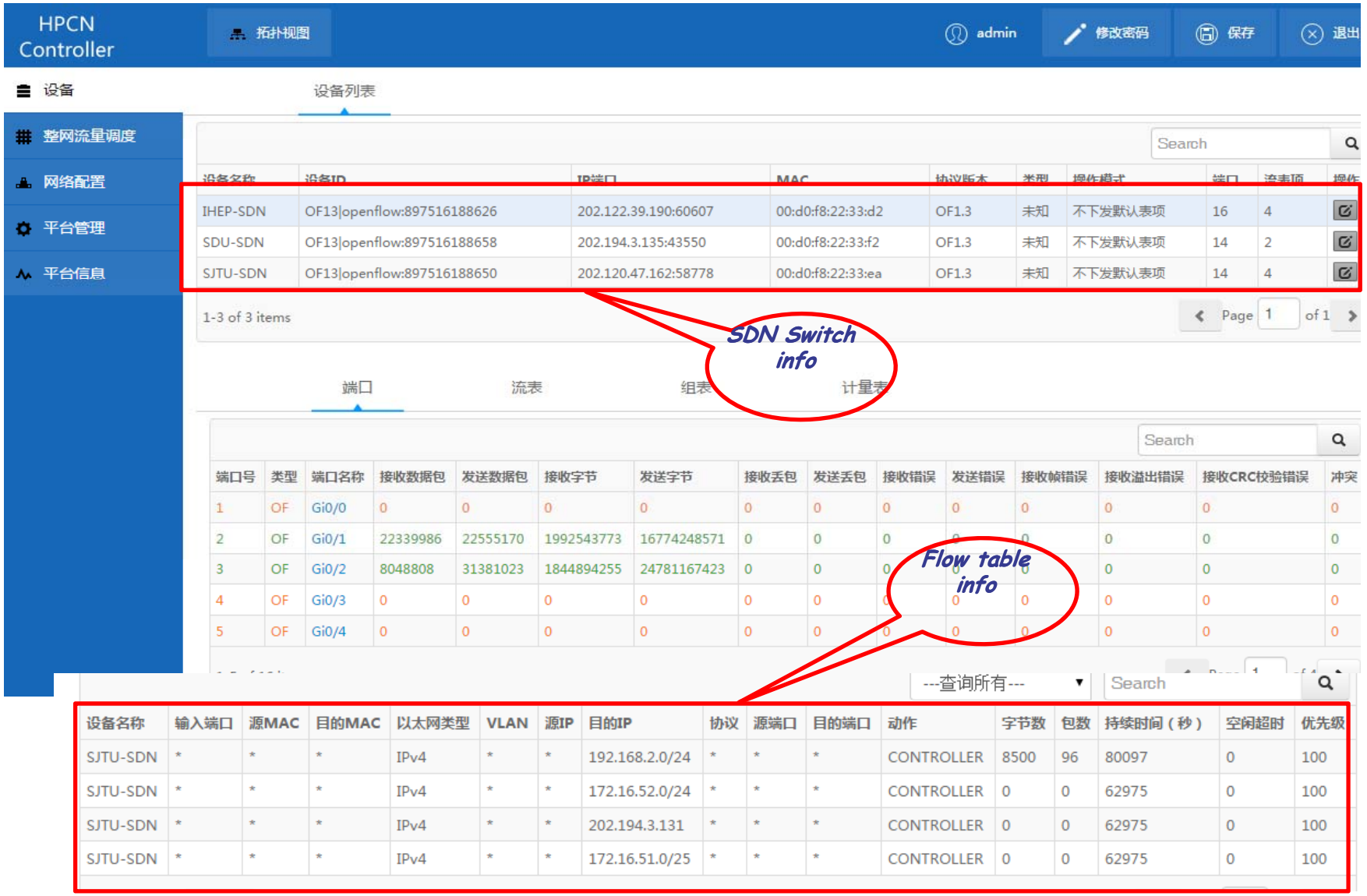


- Network topology
  - SJTU (Shanghai Jiao Tong University), SDU (Shandong University), CCNU (Central China Normal University), IHEP
  - IPv4 & IPv6

Controller dashboard – network & devices status



Controller dashboard



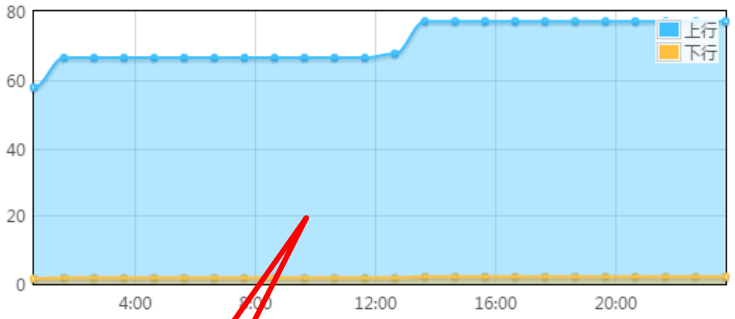
Controller dashboard – link performance statistics

链路质量统计

Tu2(14)@IHEP-SDN(202.122.39.190:34268)---------->Tu2(12)@SJTU-SDN(202.120.47.162:54019)

视图类型： 天 有效带宽 查询

单位：Mbps



上行1天内平均/最大有效带宽：71.04/77.08 Mbps

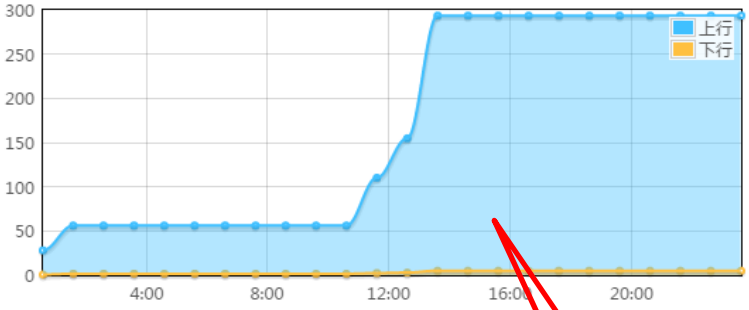
下行1天内平均/最大有效带宽：1.93/2.11 Mbps

链路质量统计

Tu26(17)@IHEP-SDN(202.122.39.190:34268)---------->Tu26(15)@SJTU-SDN(202.120.47.162:54019)

视图类型： 天 有效带宽 查询

单位：Mbps



上行1天内平均/最大有效带宽：170.26/293.68 Mbps

下行1天内平均/最大有效带宽：3.26/5.09 Mbps

Available bandwidth (ipv4)

Available bandwidth (ipv6)

业务监测

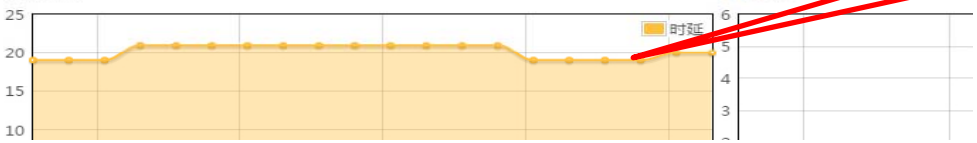
链接起点	链接终点
Tu16(12)@SJTU-SDN(202.120.47.162:36713)	Tu36(14)@SDU-SDN(202.194.3.135:46489)
Tu36(14)@SDU-SDN(202.194.3.135:46489)	Tu16(12)@SJTU-SDN(202.120.47.162:36713)
Tu1(9)@SJTU-SDN(202.120.47.162:36713)	Tu3(11)@SDU-SDN(202.194.3.135:46489)
Tu3(11)@SDU-SDN(202.194.3.135:46489)	Tu1(9)@SJTU-SDN(202.120.47.162:36713)

1-4 of 4 items

业务流统计

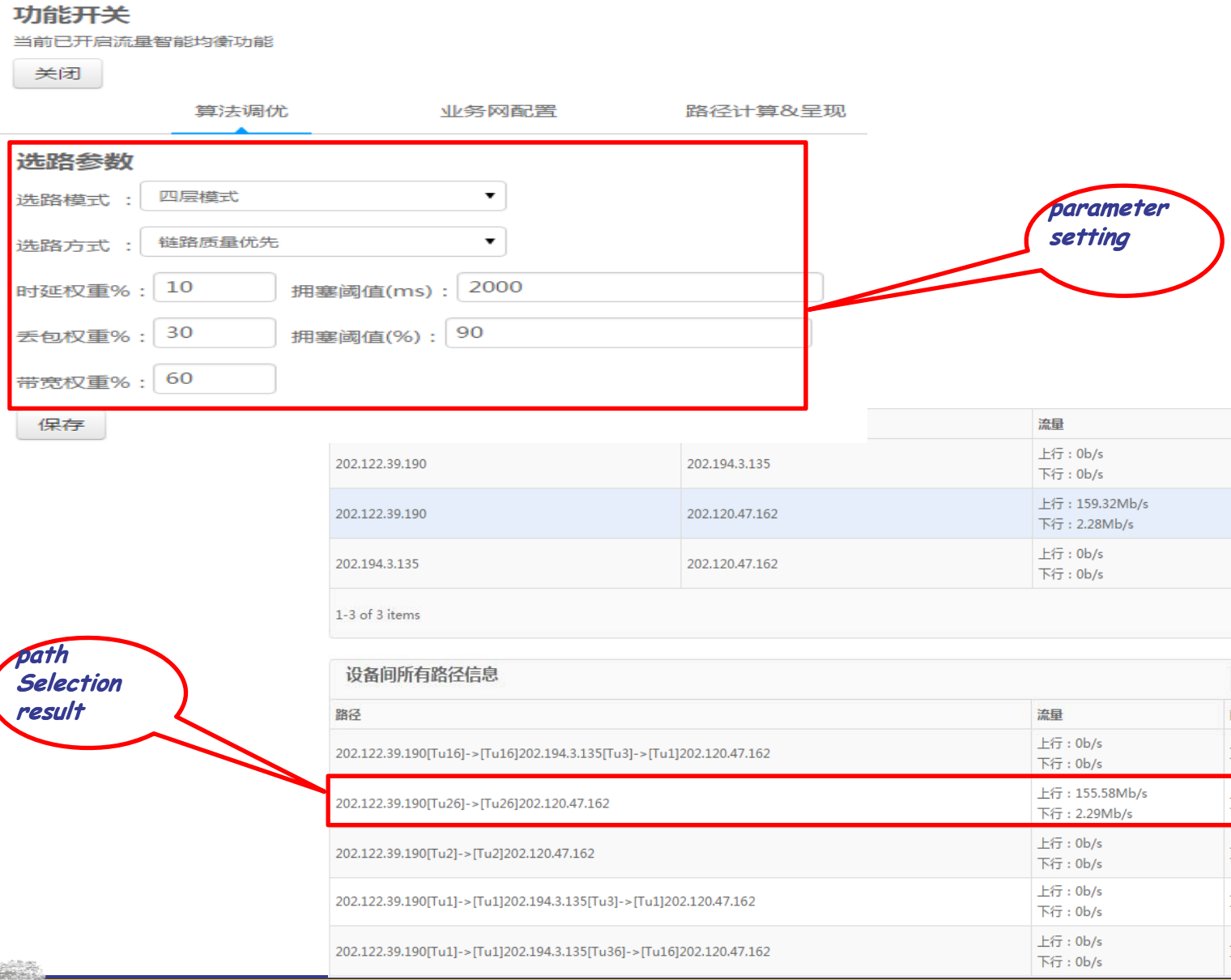
分

单位：ms 单位：%

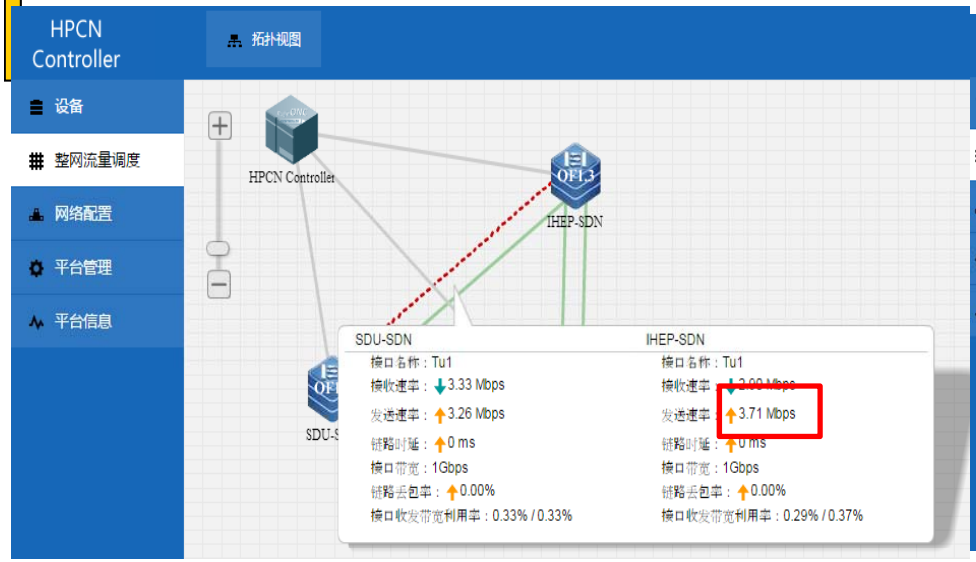


latency (ipv6)

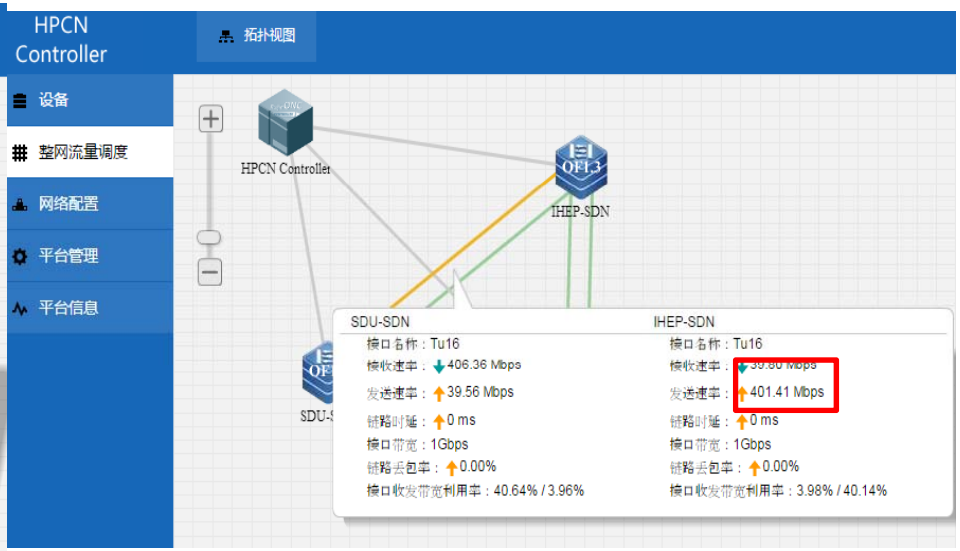
Controller dashboard- Path selection



IHEP<->SDU Results (Girdftp)



IHEP<->SDU:IPv4



IHEP<->SDU:IPv6

- IPv6 is much better than IPv4, 10~100 times increased

Agenda

- About SDN
- SDN for HEP Data Transfer
- SDN for Security
- Summary

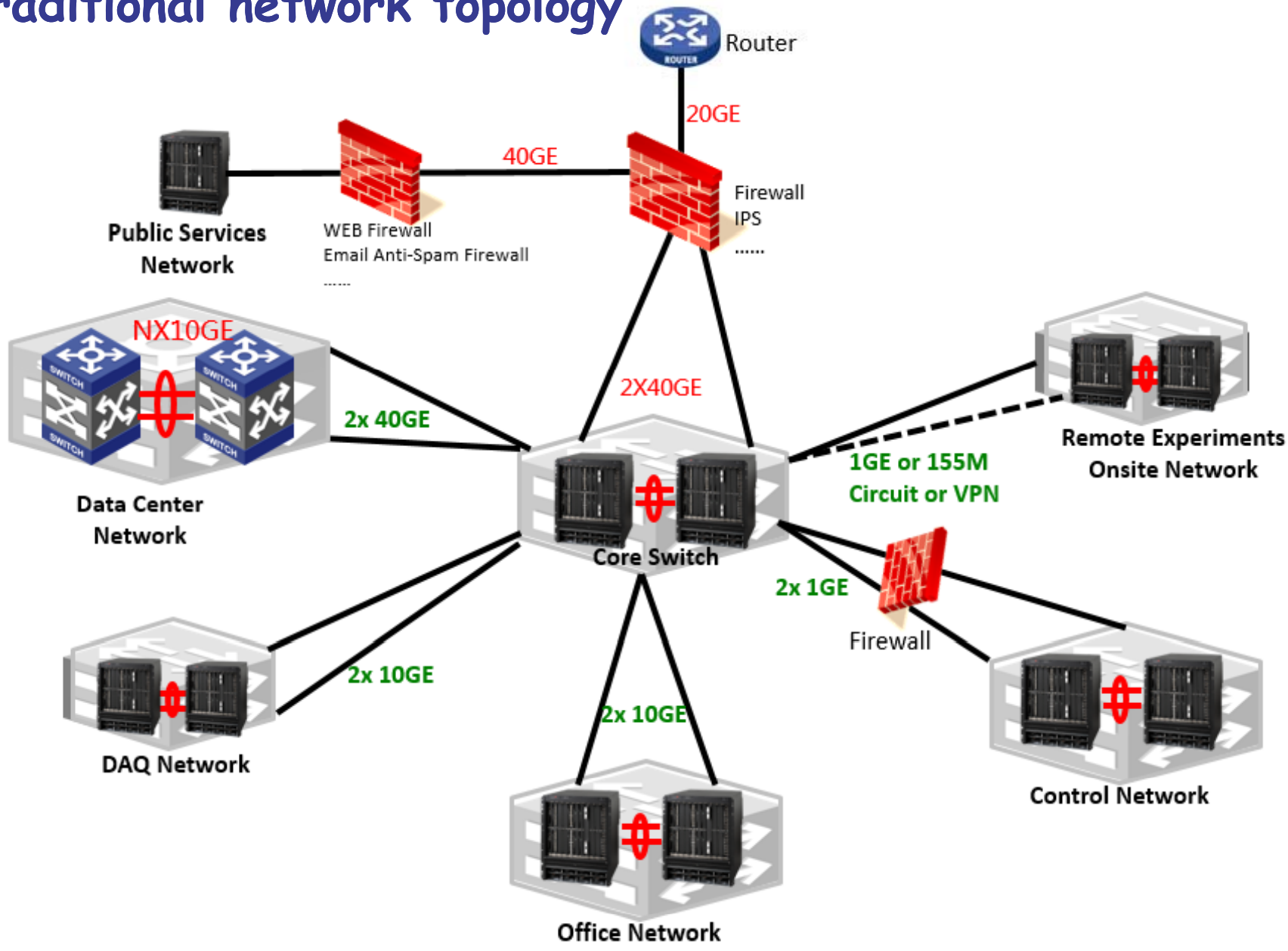
Why

- The underlying network becomes increasingly critical for supporting end user applications and services
- Network traffic management, service complexity, and security become more taxing.
- Network managers face network performance and reliability challenges, including security-related attacks and breaches, resulting in service disruptions that can occur at any moment
- It is important to deploy security devices and policies without applications disruptions / smoothly

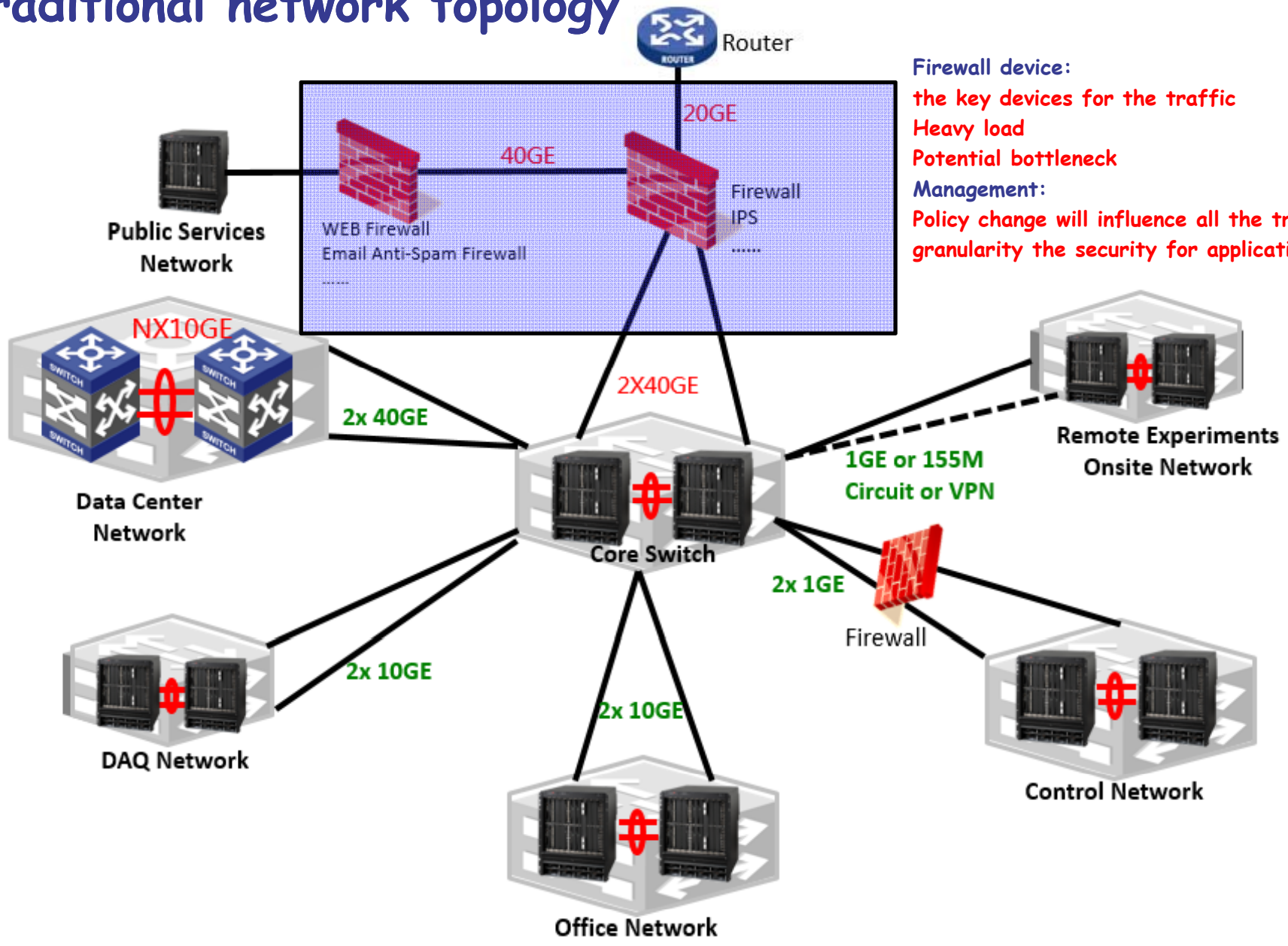
What we should do

- Threat Management: Detect and mitigate threats in the network quickly and efficiently
  - Detection: using the available tools/IDS, system log analysis …
  - Mitigation: Real-time programmability of the network base on the detection results
  - Integration detection and mitigation: with third-party security and analytics platforms, such as IDS, Log analysis system, vulnerability scanner……
  - Interface
    - User: web-based Graphical User Interface (GUI) that provides simple profile configurations and a detailed view of the dashboard and associated settings
    - Controller to detection: Rest APIs
    - Controller to network devices : Openflow

Traditional network topology

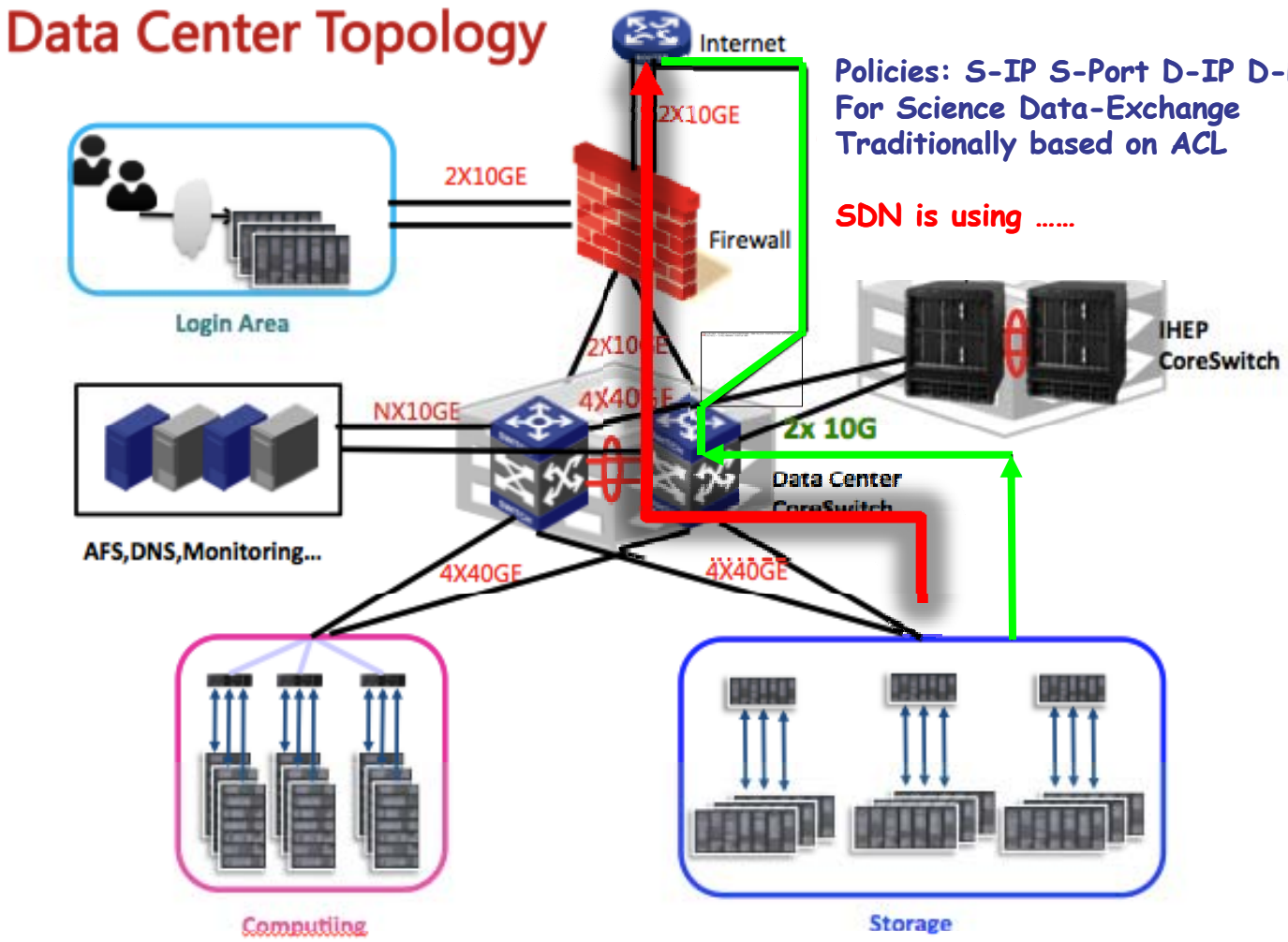


Traditional network topology

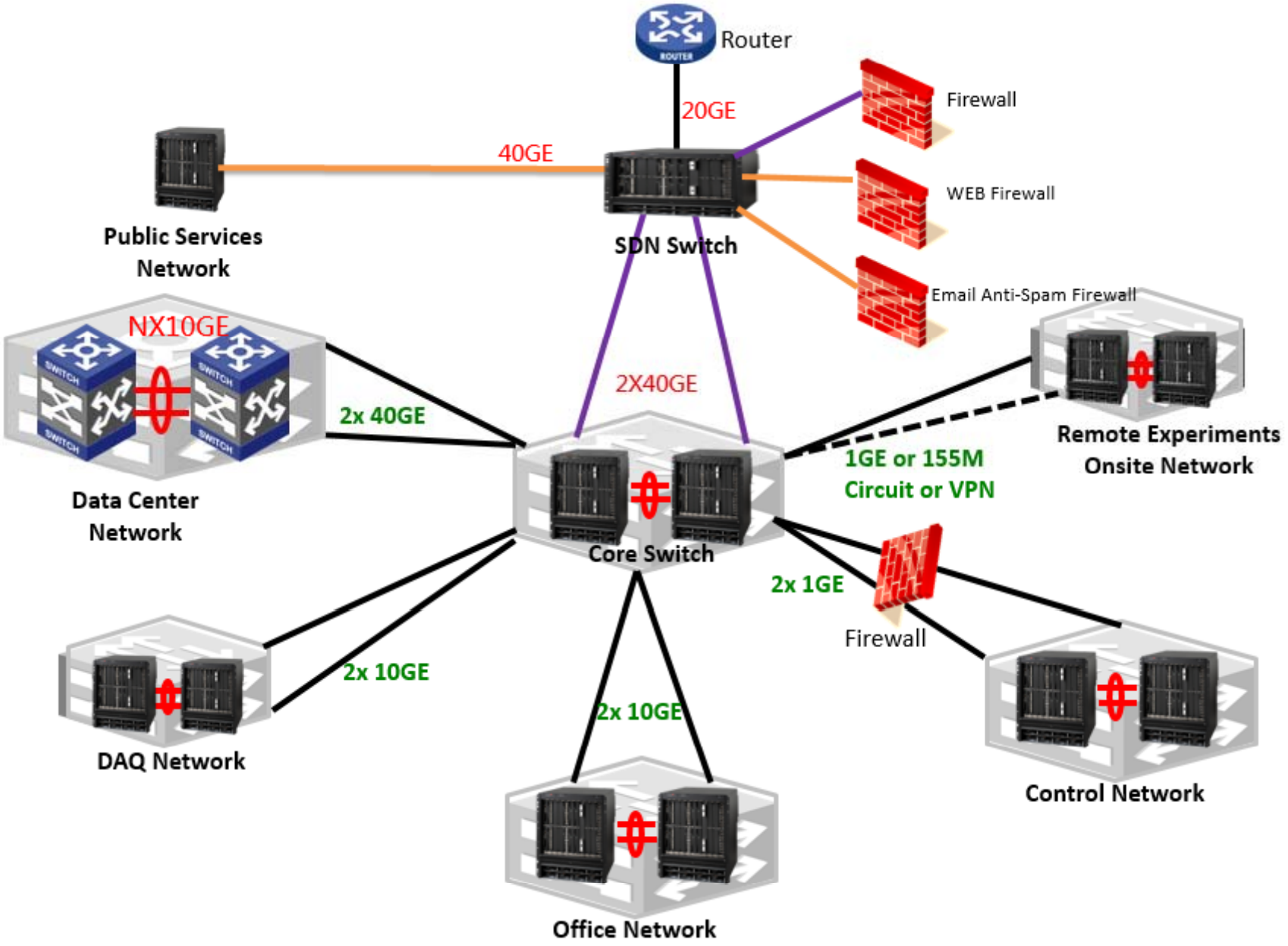


Firewall device:
the key devices for the traffic
Heavy load
Potential bottleneck
Management:
Policy change will influence all the traffic
granularity the security for applications

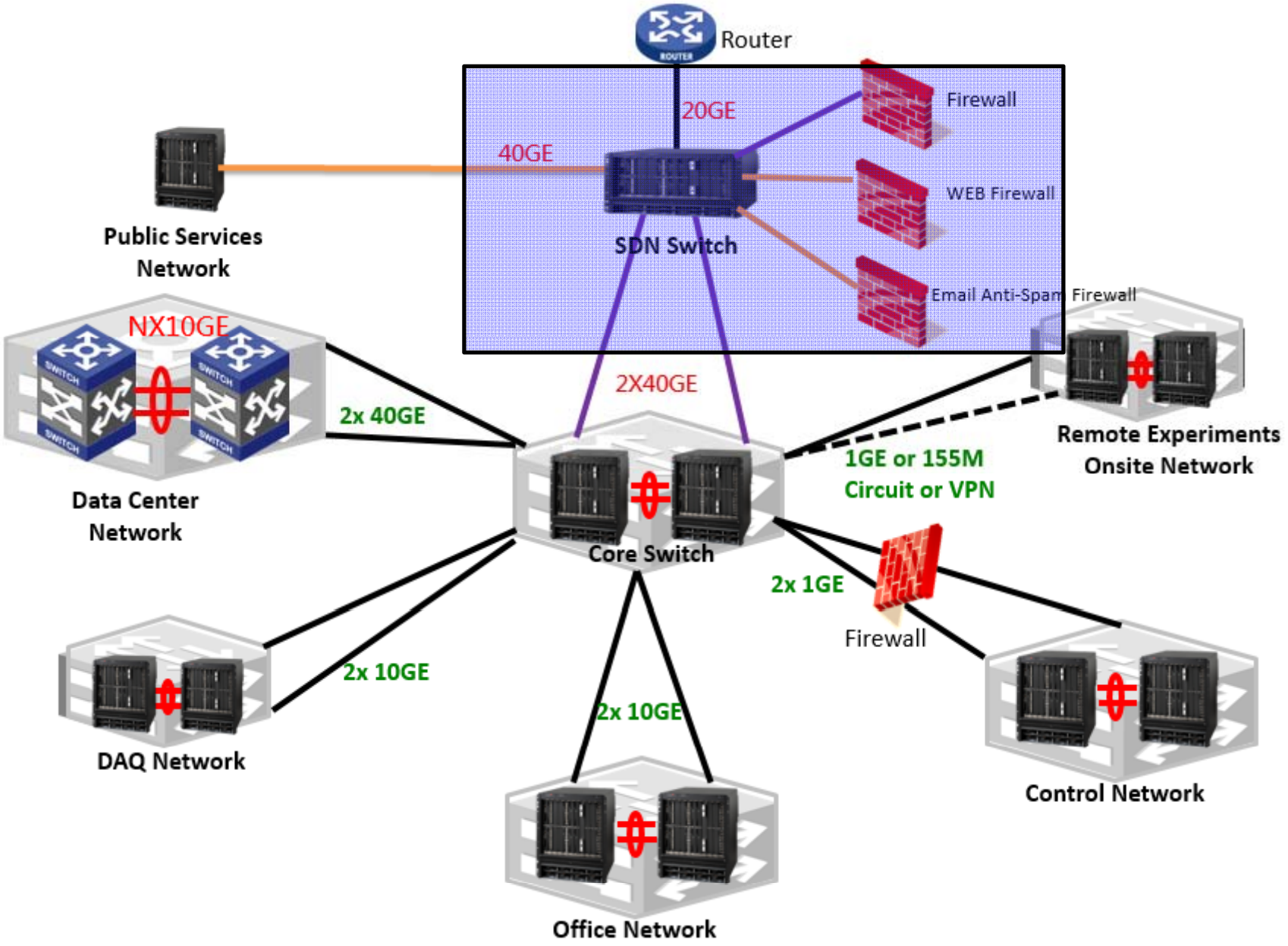
Science DMZ for traditional network



Network topology upgrade

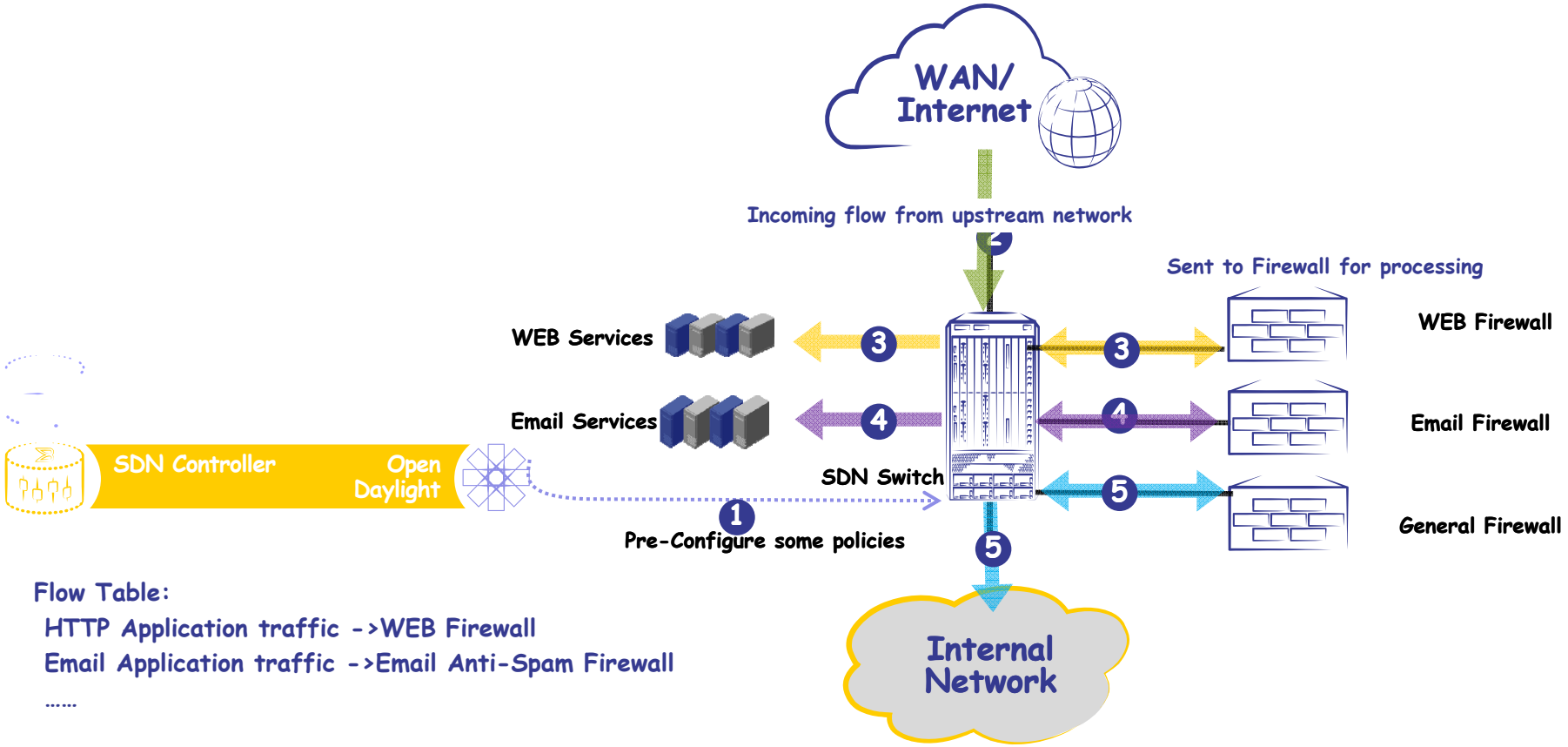


Network topology upgrade



Case 1: Service Chain

Send different applications traffic to different firewall



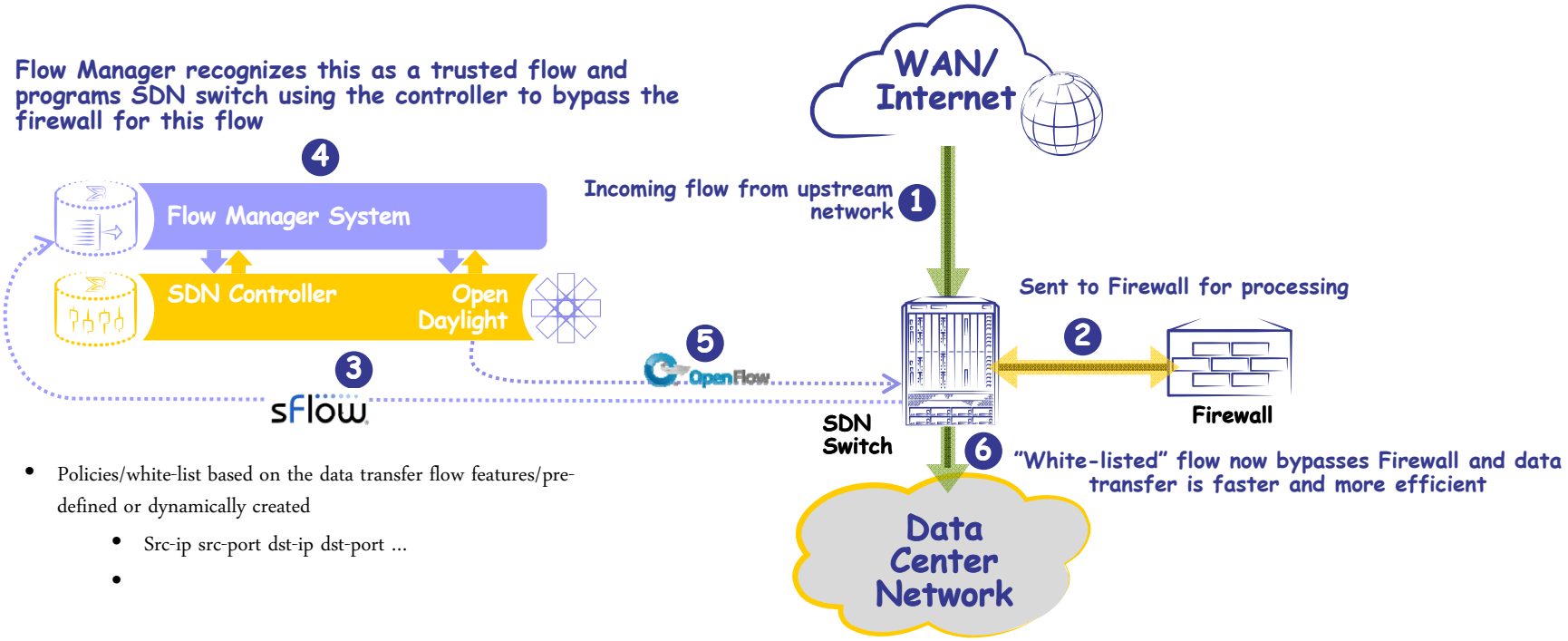
Flow Table:

HTTP Application traffic ->WEB Firewall

Email Application traffic ->Email Anti-Spam Firewall

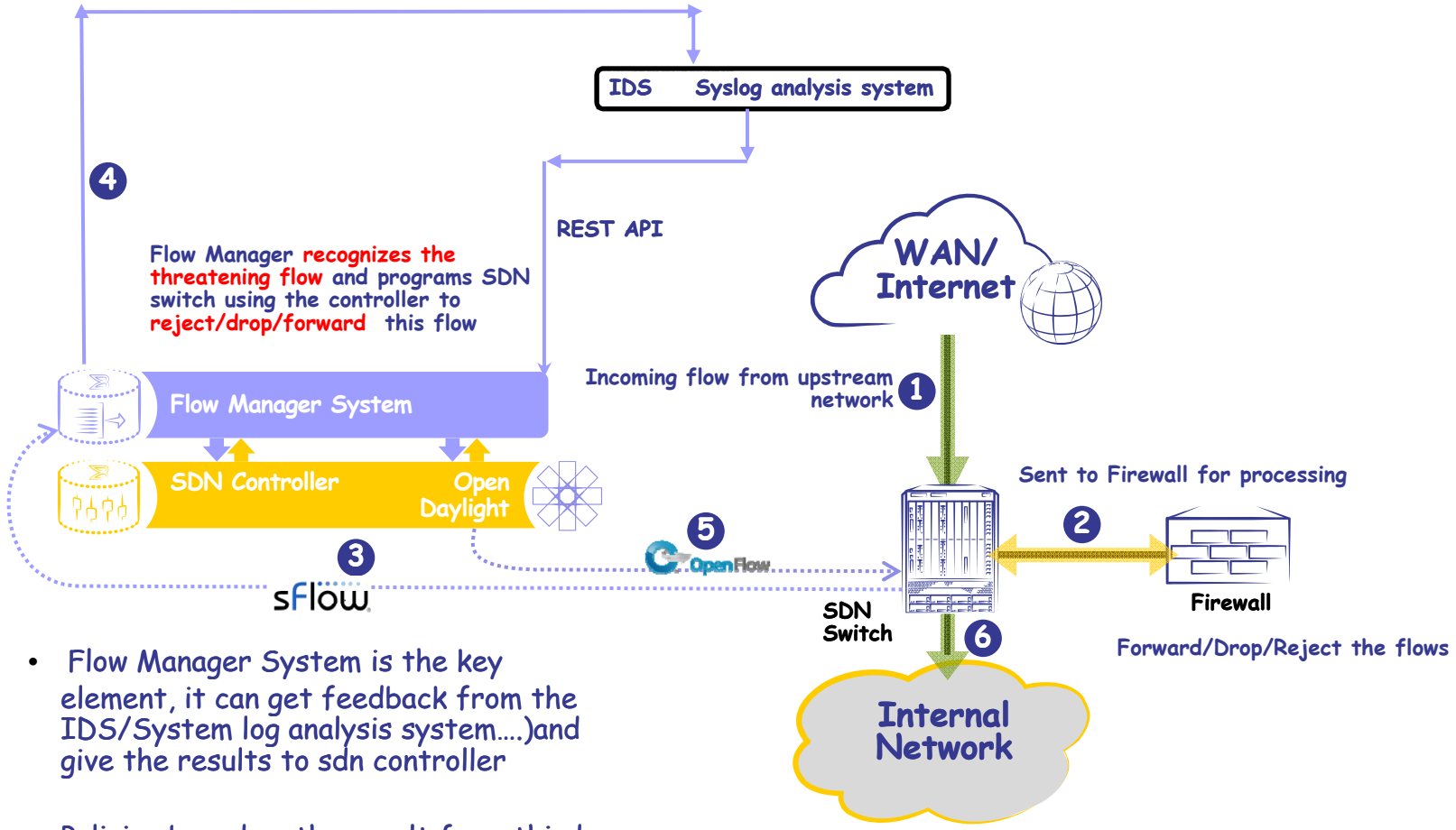
……

Case 2: Firewall Bypass for Science-DMZ



- Policies/white-list based on the data transfer flow features/pre-defined or dynamically created
  - Src-ip src-port dst-ip dst-port ...
  -

Case 3: Dynamic security policies

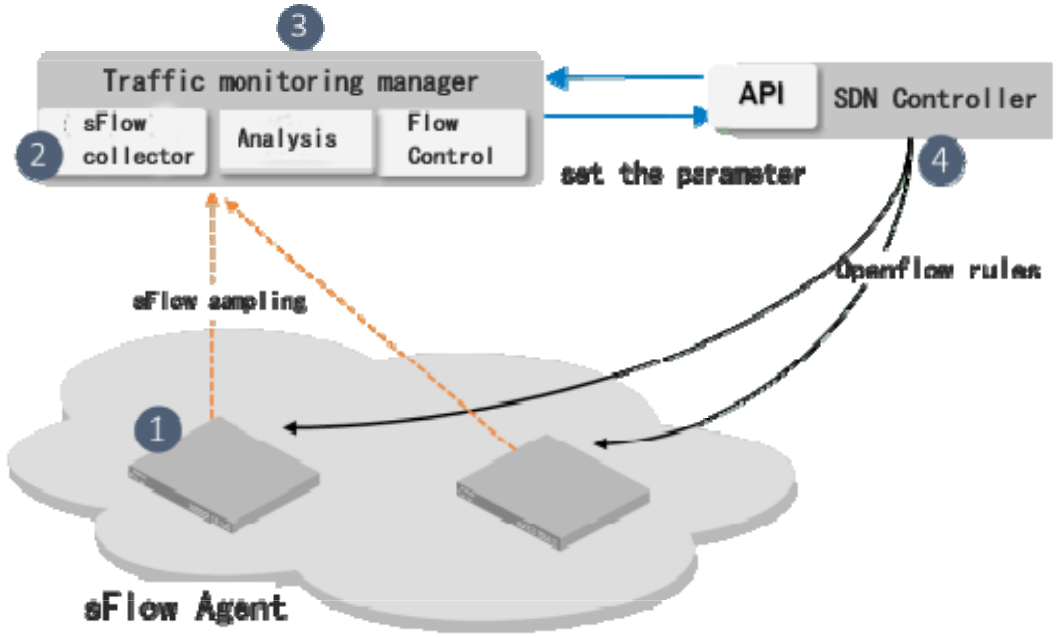


- Flow Manager System is the key element, it can get feedback from the IDS/System log analysis system….)and give the results to sdn controller
- Policies based on the result from third-party system
  - IDS
  - Syslog analysis system
  - ,,,,,,

SDN + Detection

Key technology: Traffic Analysis

- Capture the traffic: Sflow/Netflow
- Analyze the traffic(using the available open source or commercial tools) and transfer the results to SDN controller through REST API
- Based on the early built feature library, SDN controller established the openflow rules and set up in the network switches



Summary and outlook

- SDN is one choice to make the network (security) management easily/efficiently
- Data transfer application is in production and 4 sites have been involved and running well , other 2 sites will join soon…
- Security application has been launched in IHEP network, and more functions will be developed and released
- Still many things to do……

Thanks