

The SDN Applications for Data Transfer & Network Security @ IHEP

Fazhi Qi
CC, IHEP

9th Mar, 2017



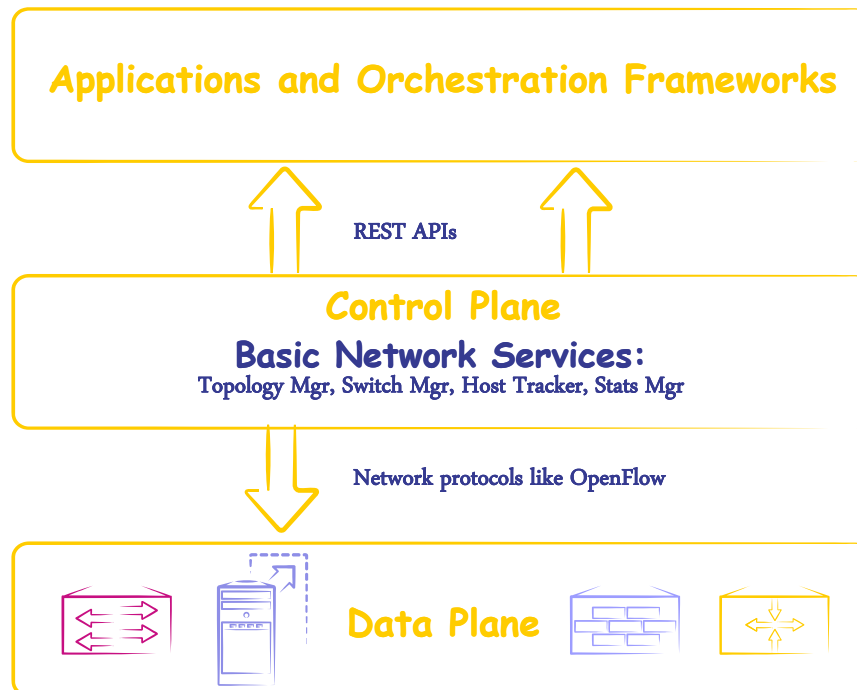
Agenda

- 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

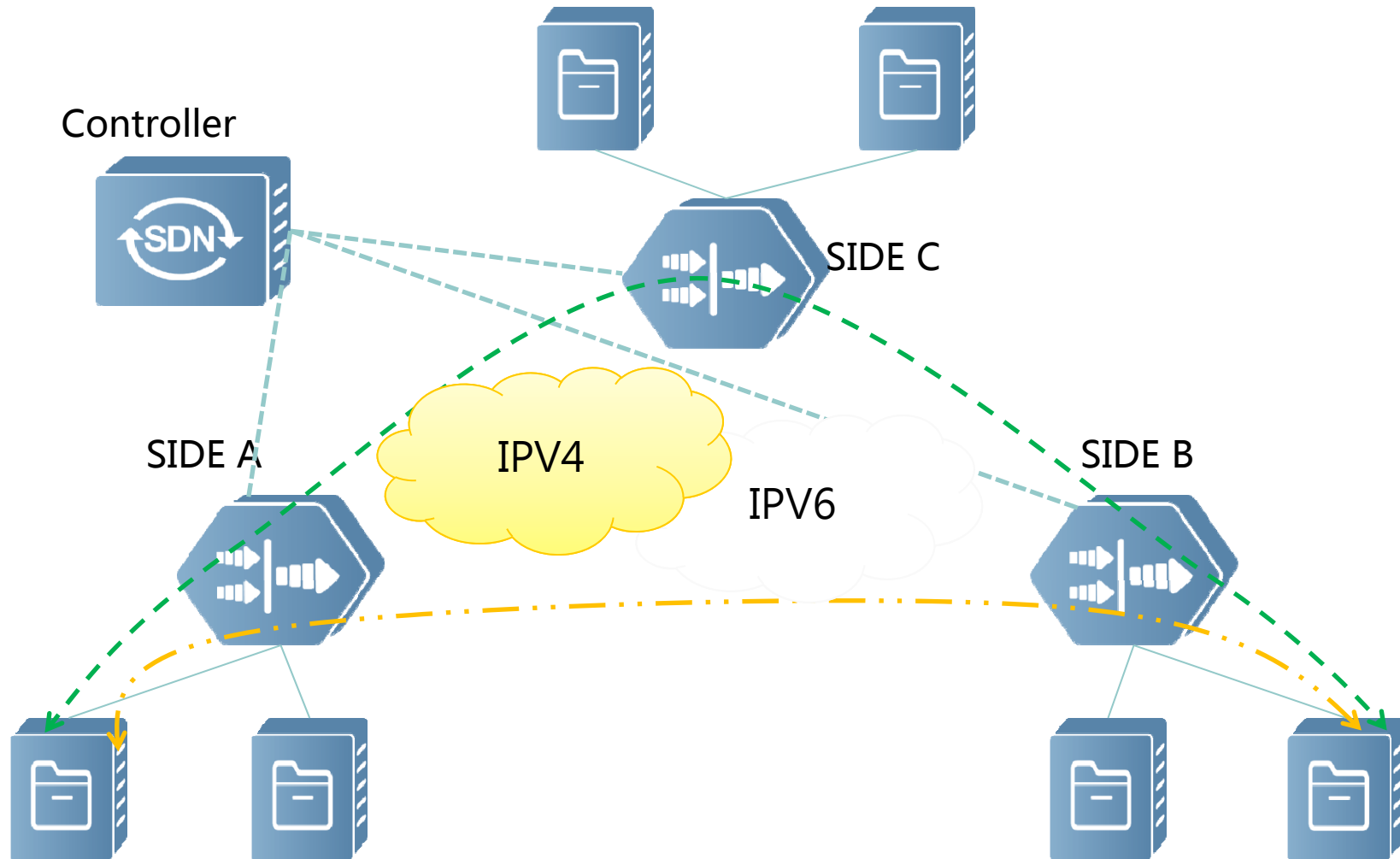


SDN-WAN & vWAN

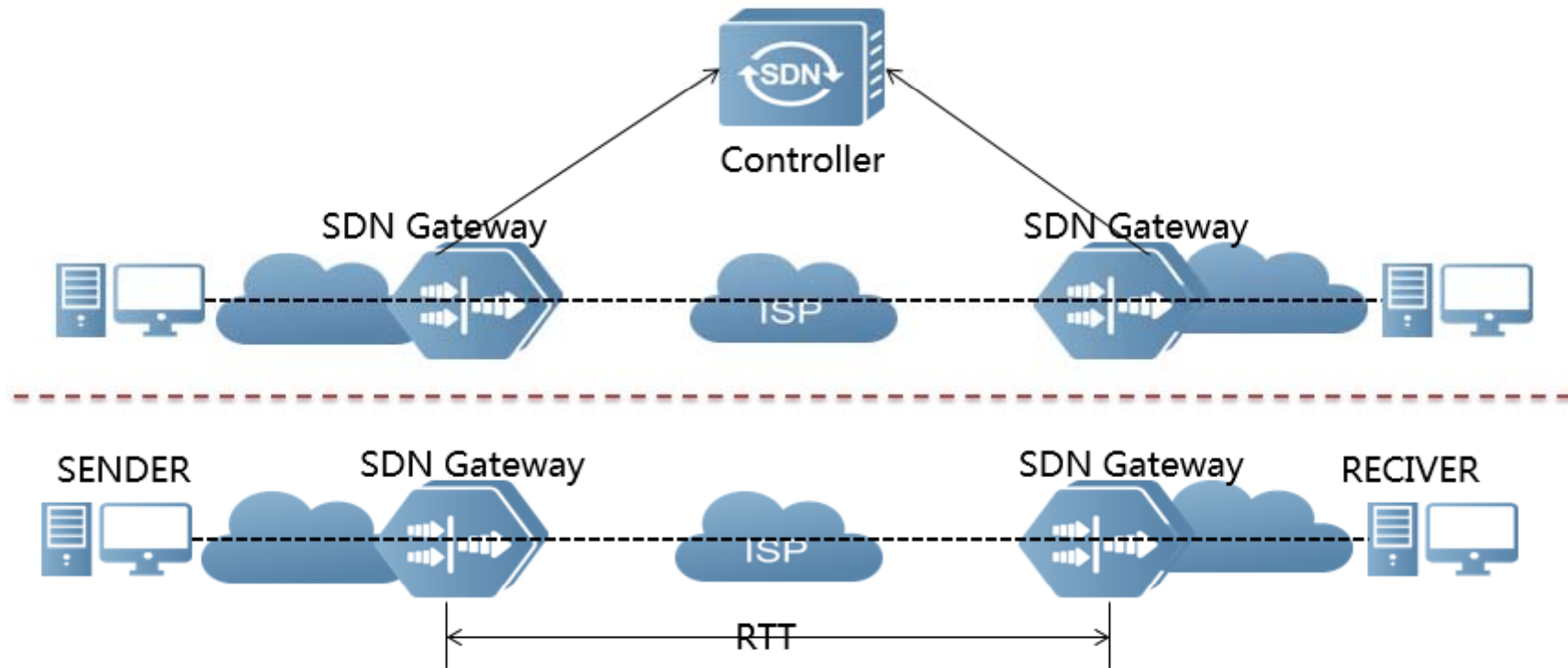
- vWAN :virtual WAN , which is considered a part of SD-WAN.
- vWANs are used to replace private WAN services with regular broadband connectivity.
- vWANs are used to secure the connection and encrypt the traffic across public networks providing an additional layer of security through secure socket layer 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



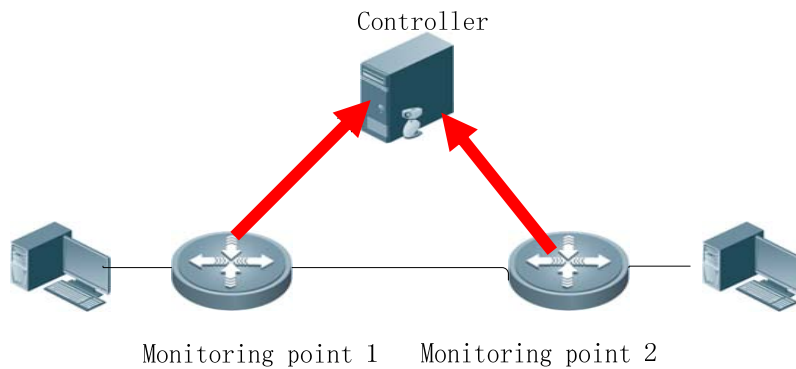
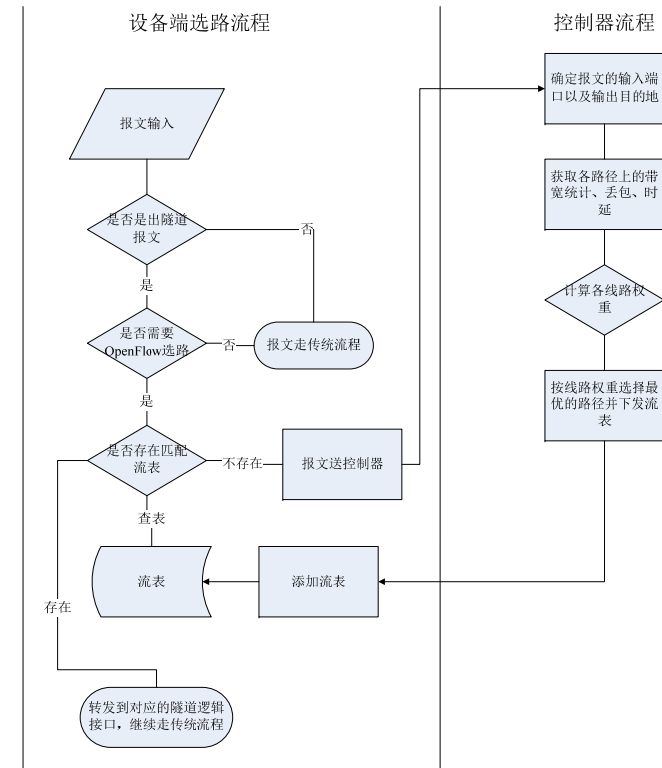
- **Gateway: All-in-one device**
- VPN: Virtual link/IPv4 Over IPv6
- Network performance monitoring (Packet loss,RTT,Throughput)
- Active network performance measurement: iperf



The Key Technology

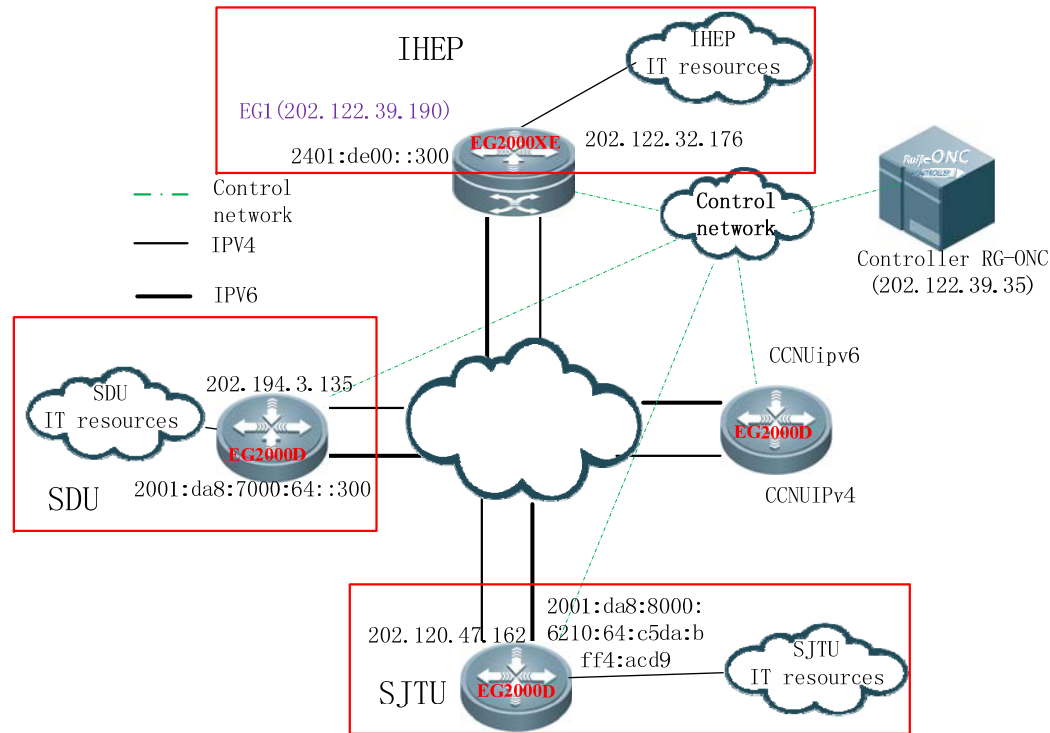
❖ Dynamic path selection base on

- 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

HPCN Controller
admin 修改密码 保存 退出

设备
整网流量调度
网络配置
平台管理
平台信息

- 断开
- 拥塞
- >=500Mbps
- >=200Mbps
- >=100Mbps
- >=50Mbps
- >=0Mbps
- 管理通道

设备主页

■ 已连接 ■ 异常 ■ 未连接 ■ 已关闭

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52

IHEP-SDN

厂商: Ruijie Networks 版本: OF1.3

类型: Unknown (Tlx-0) MAC地址: 00:d0:f8:22:33:d2

在线端口: 8/16 安装流表: 4

IP端口: 202.122.39.190:60607

端口列表

端口号	端口名称	接收包数	发送包数	接收字节	发送字节	接收丢包	发送丢包
1	Gi0/0	0	0	0	0	0	0
2	Gi0/1	22340456	22555200	1992574585	16774250909	0	0
3	Gi0/2	8048816	31381033	1844895124	24781168538	0	0
4	Gi0/3	0	0	0	0	0	0
5	Gi0/4	0	0	0	0	0	0



Controller dashboard

HPCN Controller
拓扑视图
admin
修改密码
保存
退出

设备
设备列表

整网流量调度
网络配置
平台管理
平台信息

设备名称	设备ID	IP地址	MAC	协议版本	类型	操作模式	端口	流表项	操作
IHEP-SDN	OF13 openflow:897516188626	202.122.39.190:60607	00:d0:f8:22:33:d2	OF1.3	未知	不下发默认表项	16	4	
SDU-SDN	OF13 openflow:897516188658	202.194.3.135:43550	00:d0:f8:22:33:f2	OF1.3	未知	不下发默认表项	14	2	
SJTU-SDN	OF13 openflow:897516188650	202.120.47.162:58778	00:d0:f8:22:33:ea	OF1.3	未知	不下发默认表项	14	4	

1-3 of 3 items

Page 1 of 1

端口
流表
组表
计量表

端口号	类型	端口名称	接收数据包	发送数据包	接收字节	发送字节	接收丢包	发送丢包	接收错误	发送错误	接收帧错误	接收溢出错误	接收CRC校验错误	冲突
1	OF	Gi0/0	0	0	0	0	0	0	0	0	0	0	0	0
2	OF	Gi0/1	22339986	22555170	1992543773	16774248571	0	0	0	0	0	0	0	0
3	OF	Gi0/2	8048808	31381023	1844894255	24781167423	0	0	0	0	0	0	0	0
4	OF	Gi0/3	0	0	0	0	0	0	0	0	0	0	0	0
5	OF	Gi0/4	0	0	0	0	0	0	0	0	0	0	0	0

---查询所有---

设备名称	输入端口	源MAC	目的MAC	以太网类型	VLAN	源IP	目的IP	协议	源端口	目的端口	动作	字节数	包数	持续时间 (秒)	空闲超时	优先级
SJTU-SDN	*	*	*	IPv4	*	*	192.168.2.0/24	*	*	*	CONTROLLER	8500	96	80097	0	100
SJTU-SDN	*	*	*	IPv4	*	*	172.16.52.0/24	*	*	*	CONTROLLER	0	0	62975	0	100
SJTU-SDN	*	*	*	IPv4	*	*	202.194.3.131	*	*	*	CONTROLLER	0	0	62975	0	100
SJTU-SDN	*	*	*	IPv4	*	*	172.16.51.0/25	*	*	*	CONTROLLER	0	0	62975	0	100

SDN Switch info

Flow table info



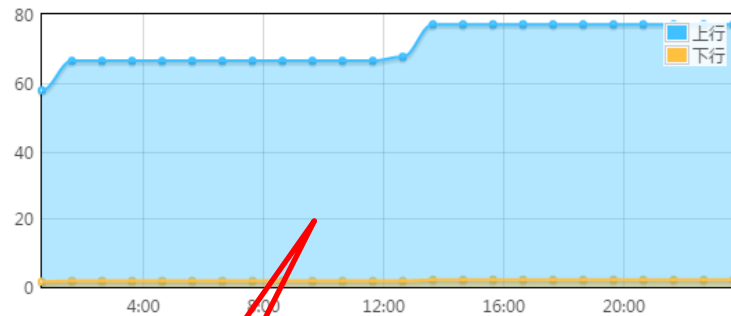
Controller dashboard - link performance statistics

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

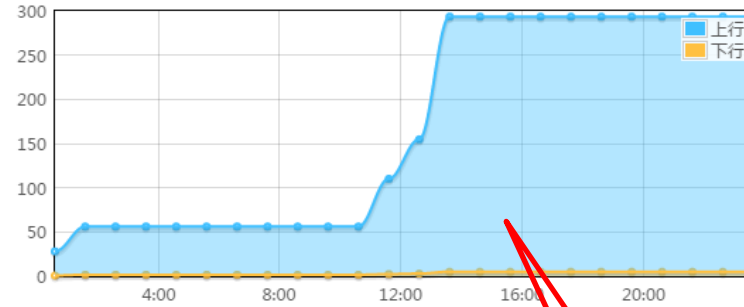
Available bandwidth (ipv4)

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 (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)

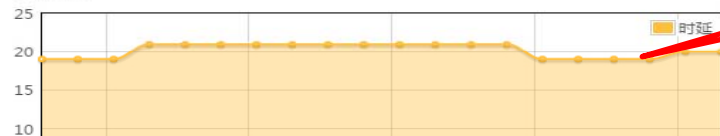
1-4 of 4 items

latency (ipv6)

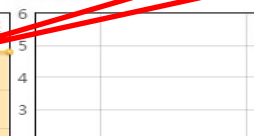
业务流统计

分

单位: ms



单位: %



Controller dashboard- Path selection

功能开关

当前已开启流量智能均衡功能

关闭

算法调优

业务网配置

路径计算&呈现

选路参数

选路模式 : 四层模式

选路方式 : 链路质量优先

时延权重% : 10 拥塞阈值(ms) : 2000

丢包权重% : 30 拥塞阈值(%) : 90

带宽权重% : 60

保存

parameter setting

		流量
202.122.39.190	202.194.3.135	上行 : 0b/s 下行 : 0b/s
202.122.39.190	202.120.47.162	上行 : 159.32Mb/s 下行 : 2.28Mb/s
202.194.3.135	202.120.47.162	上行 : 0b/s 下行 : 0b/s

1-3 of 3 items

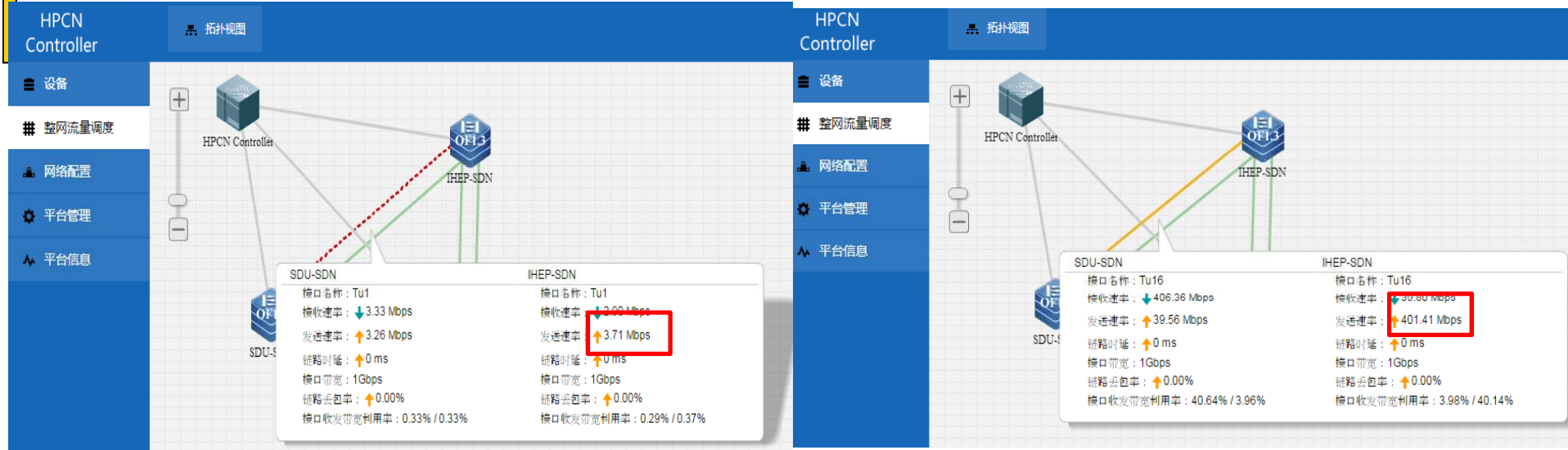
Page 1 of 1

path Selection result

设备间所有路径信息				Search
路径	流量	时延	丢包率	
202.122.39.190[Tu16]->[Tu16]202.194.3.135[Tu3]->[Tu1]202.120.47.162	上行 : 0b/s 下行 : 0b/s	上行 : 0ms 下行 : 0ms	上行 : 0% 下行 : 0%	
202.122.39.190[Tu26]->[Tu26]202.120.47.162	上行 : 155.58Mb/s 下行 : 2.29Mb/s	上行 : 0ms 下行 : 0ms	上行 : 0% 下行 : 0%	
202.122.39.190[Tu2]->[Tu2]202.120.47.162	上行 : 0b/s 下行 : 0b/s	上行 : 0ms 下行 : 0ms	上行 : 0% 下行 : 0%	
202.122.39.190[Tu1]->[Tu1]202.194.3.135[Tu3]->[Tu1]202.120.47.162	上行 : 0b/s 下行 : 0b/s	上行 : 0ms 下行 : 0ms	上行 : 0% 下行 : 0%	
202.122.39.190[Tu1]->[Tu1]202.194.3.135[Tu36]->[Tu16]202.120.47.162	上行 : 0b/s 下行 : 0b/s	上行 : 0ms 下行 : 0ms	上行 : 0% 下行 : 0%	



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

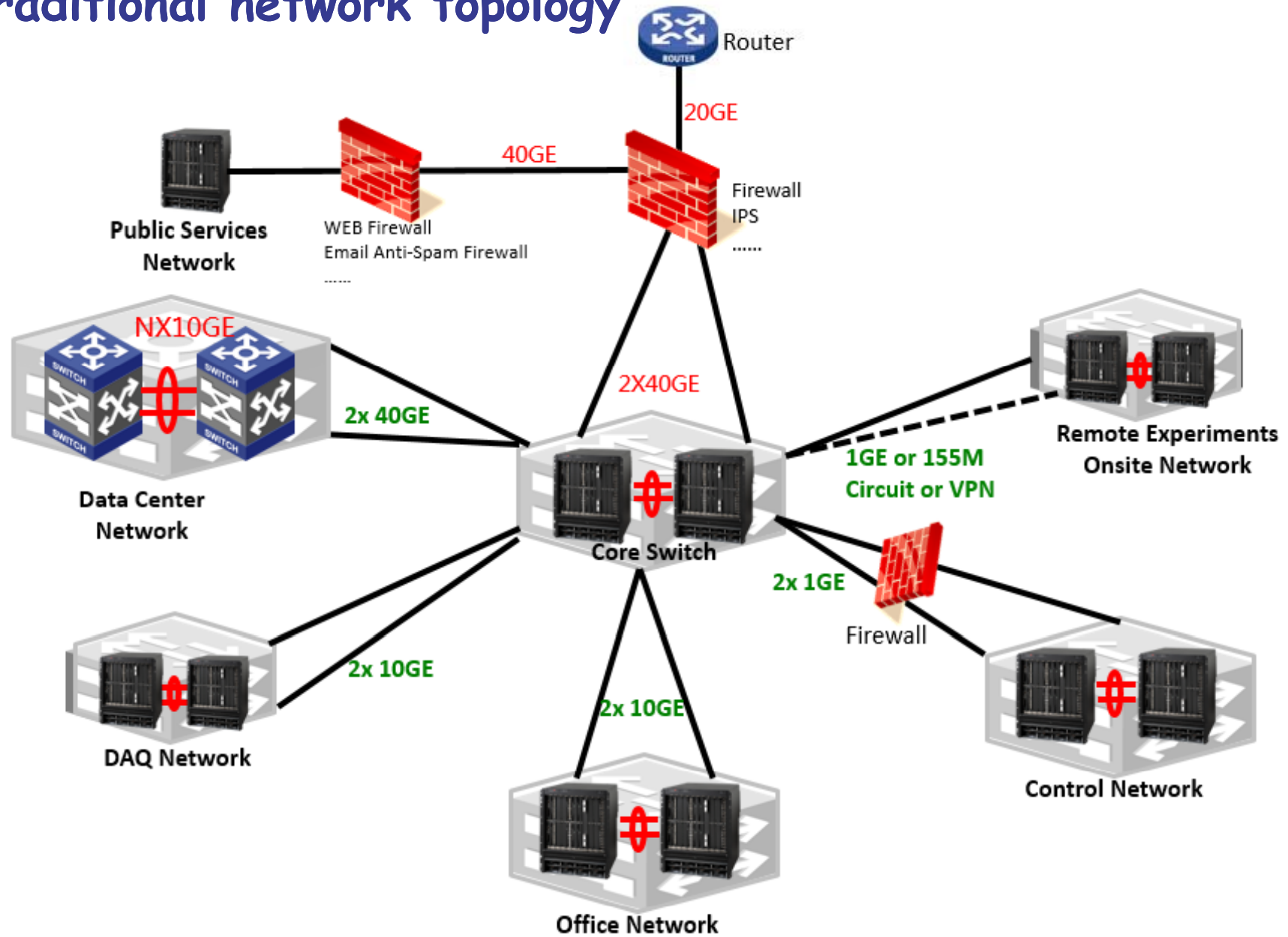


What we should do

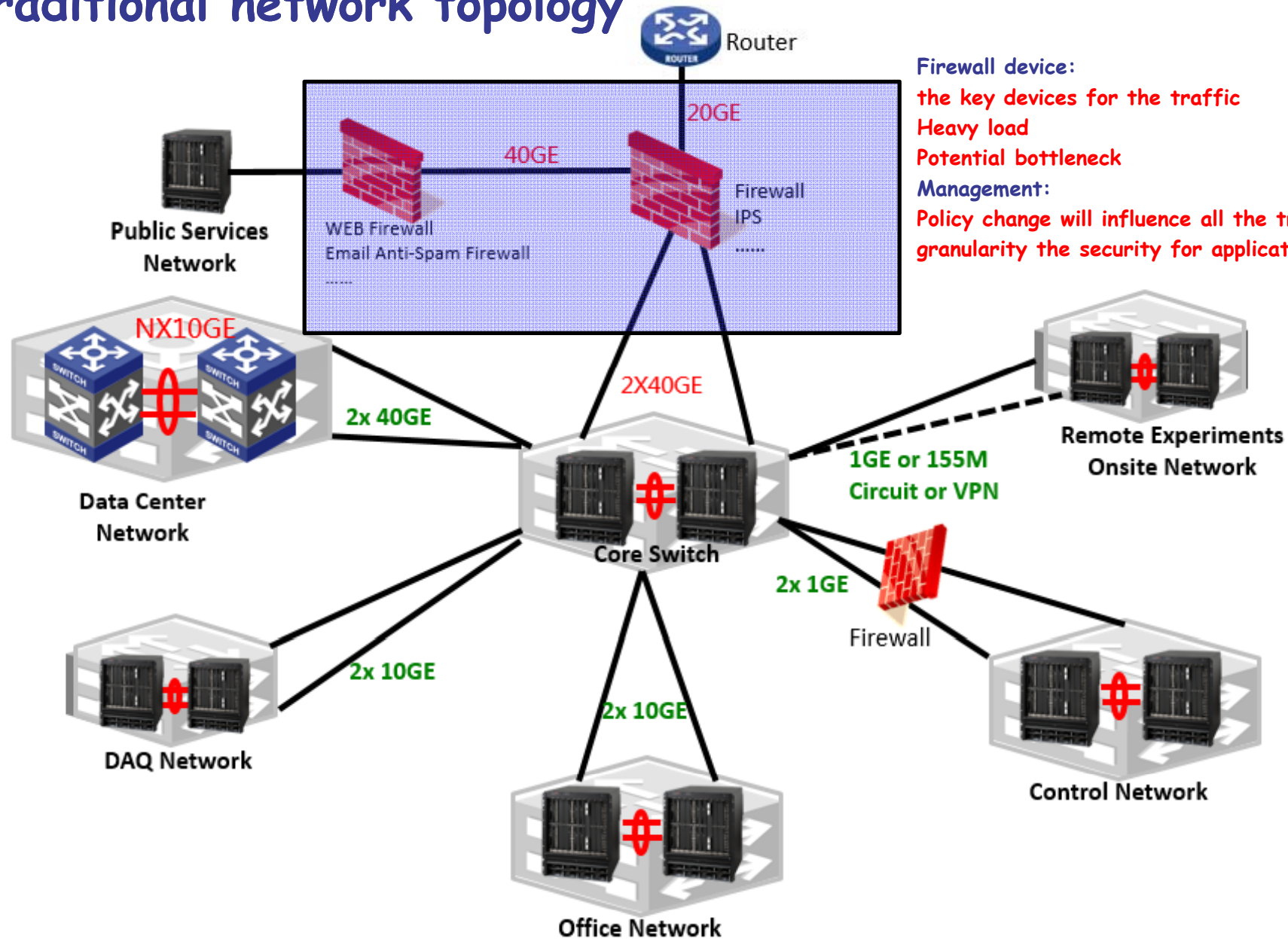
- Threat Management: Detect and mitigate threats in the network quickly and efficiently
 - Detection: using the available tools/IDS, system log analysis ...
 - Mitigation: Real-time programmability of the network base on the detection results
 - Integration detection and mitigation: with third-party 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



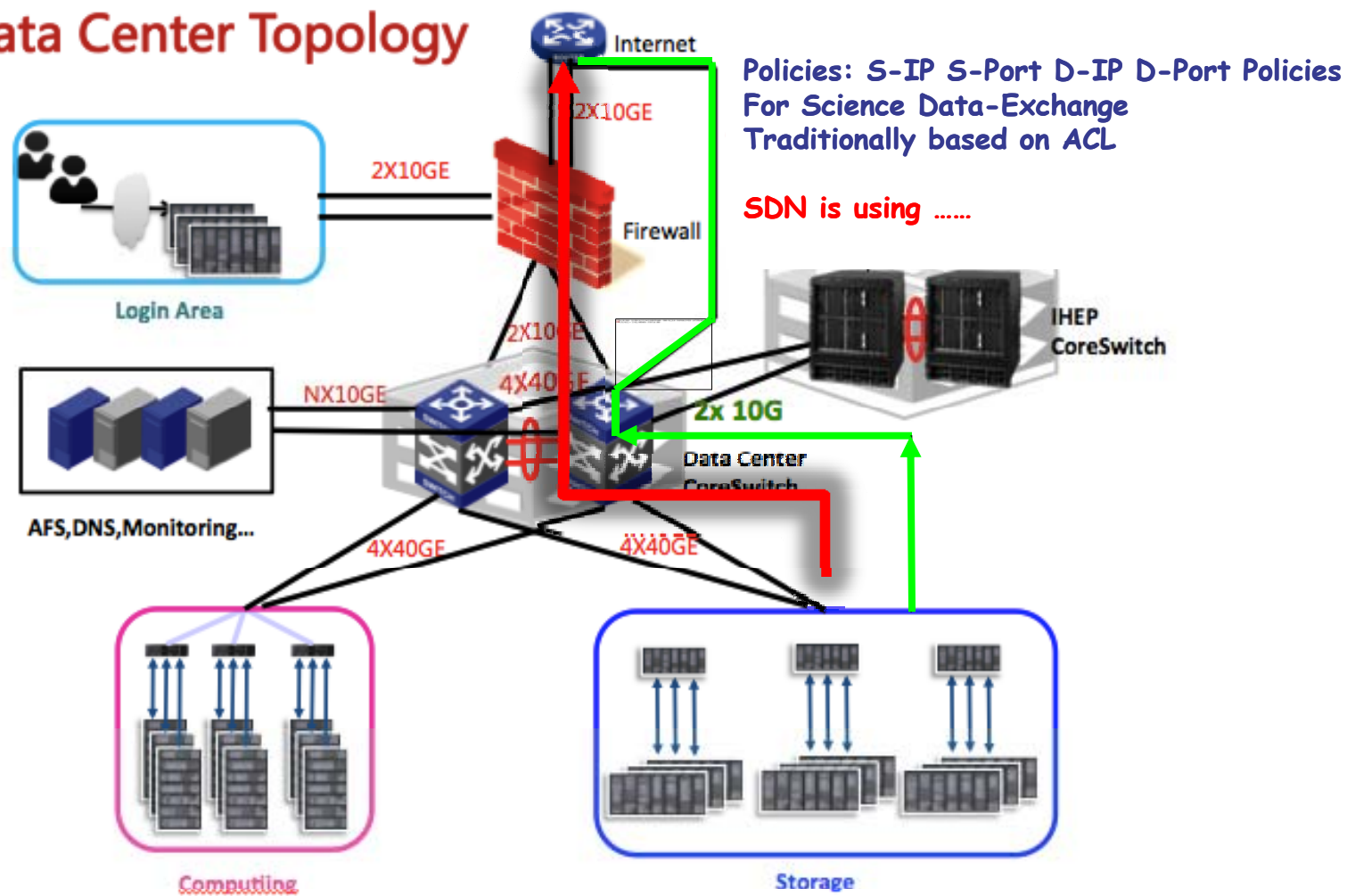
Firewall device:
the key devices for the traffic
Heavy load
Potential bottleneck

Management:
Policy change will influence all the traffic
granularity the security for applications

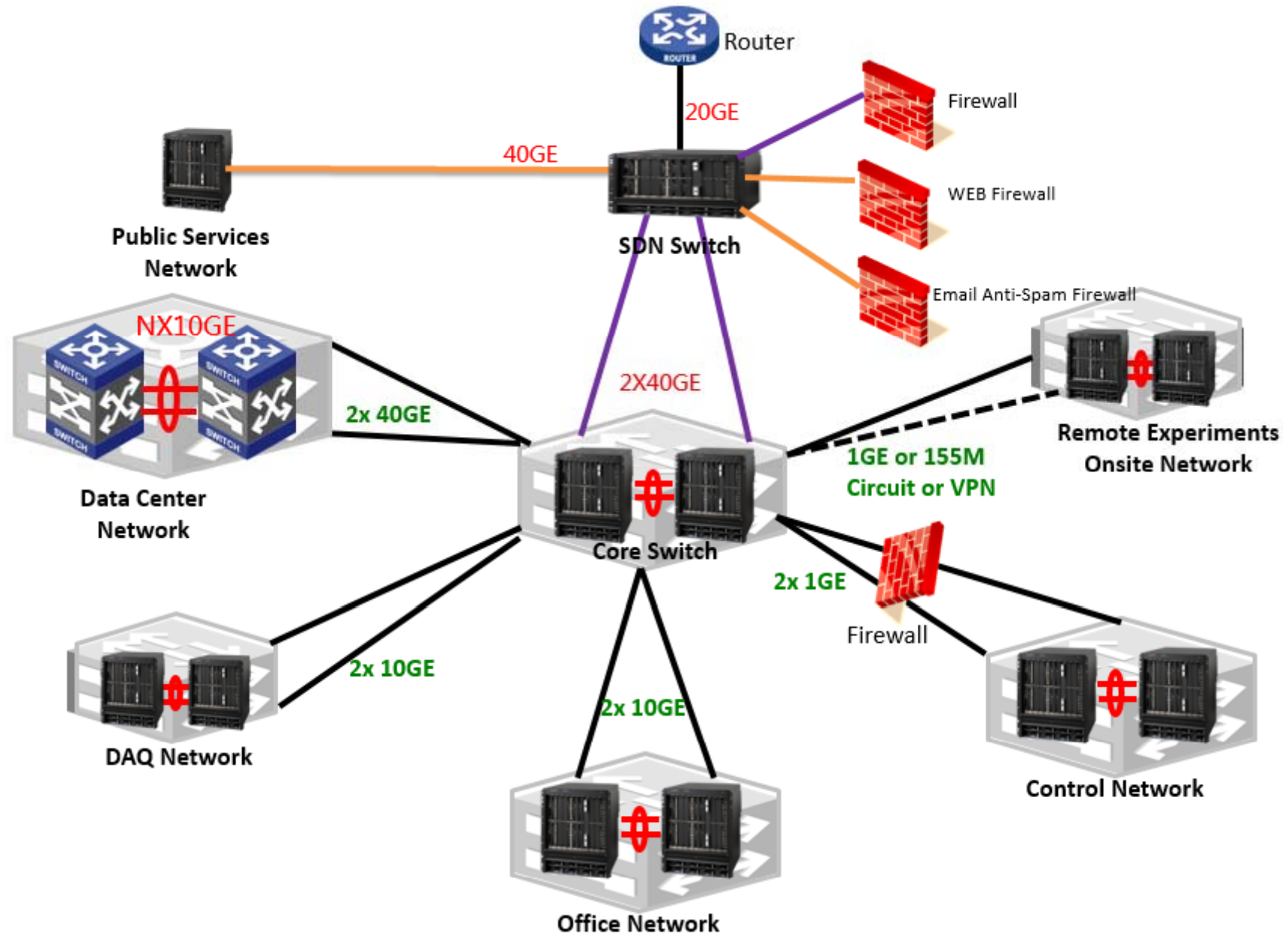


Science DMZ for traditional network

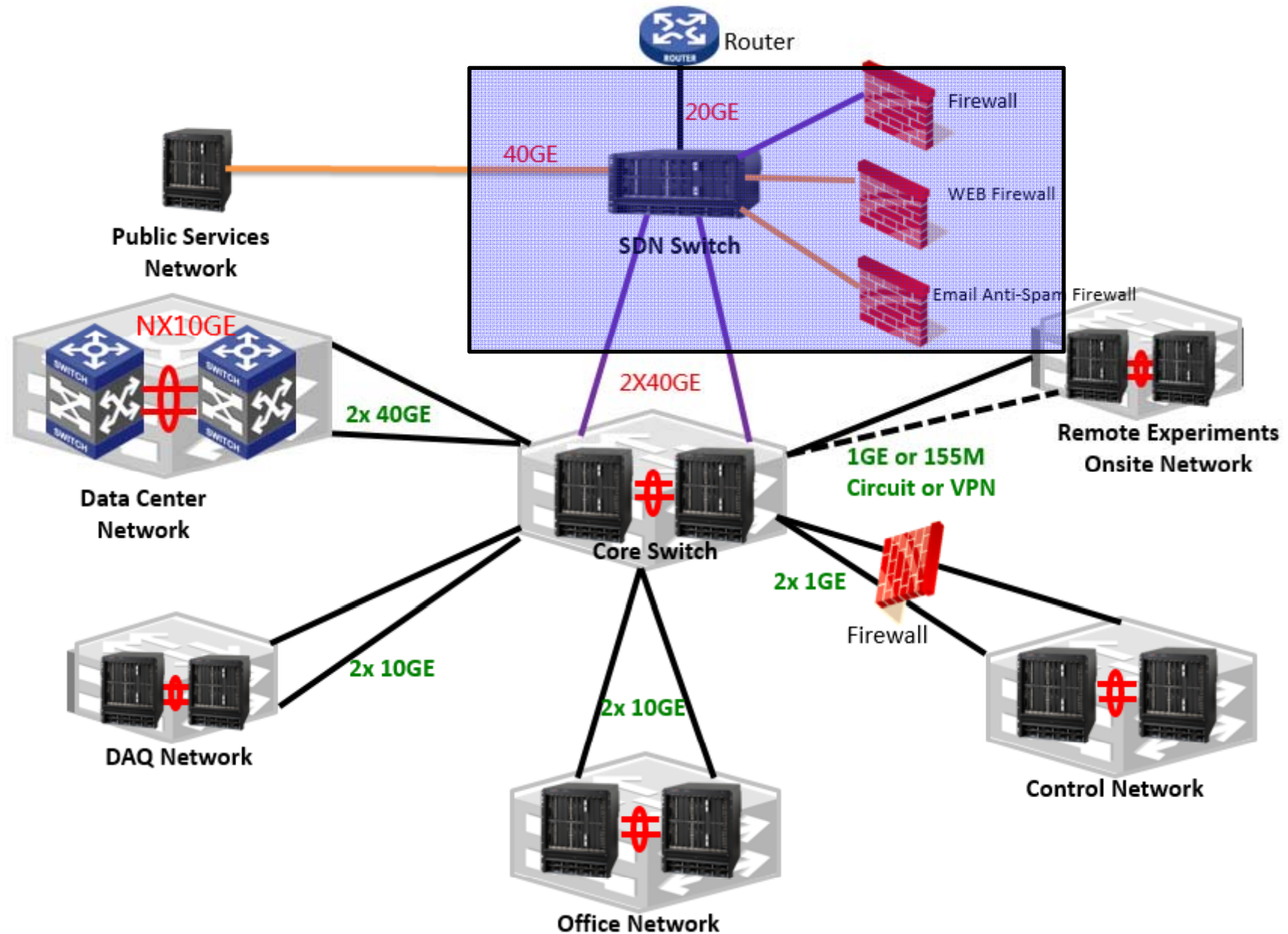
Data Center Topology



Network topology upgrade

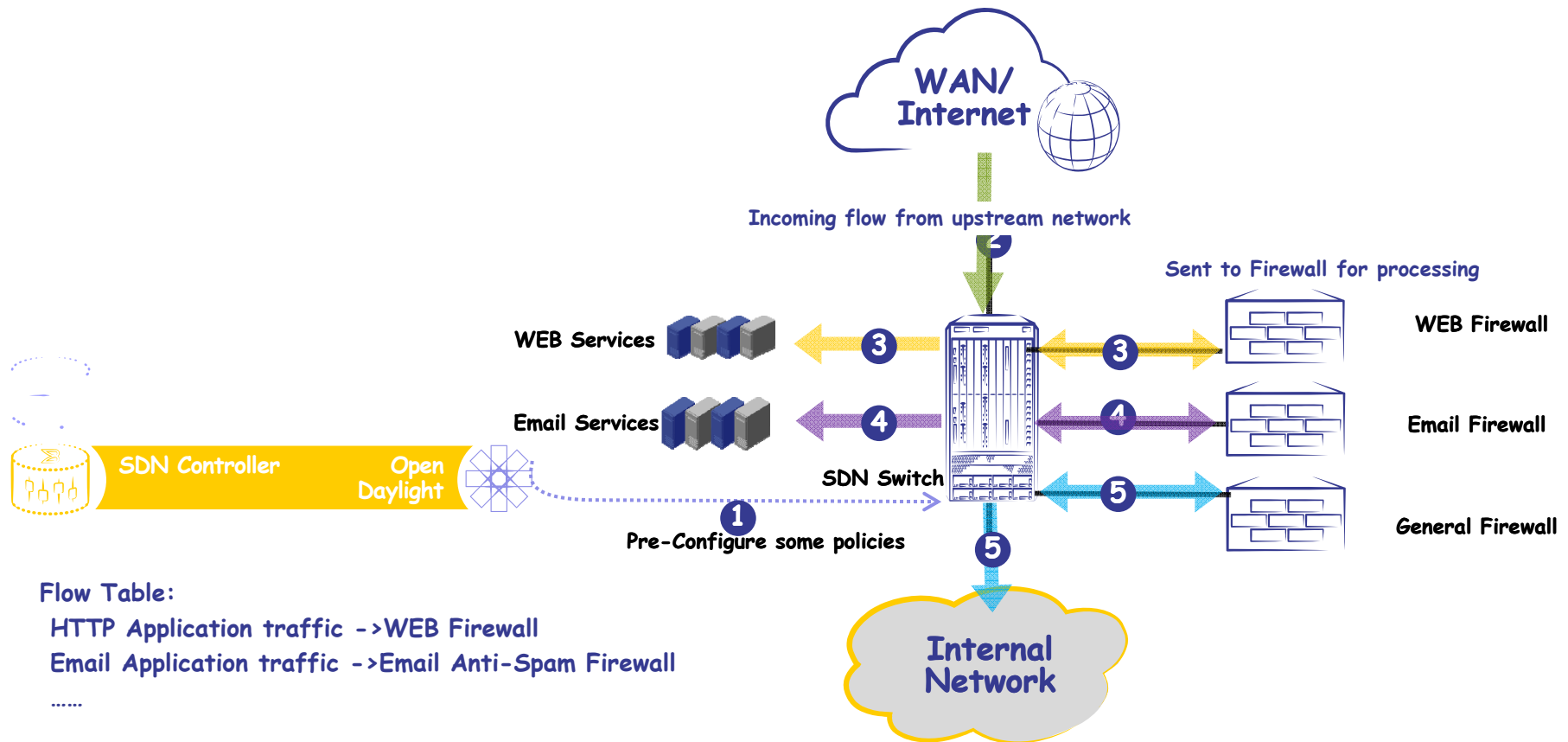


Network topology upgrade



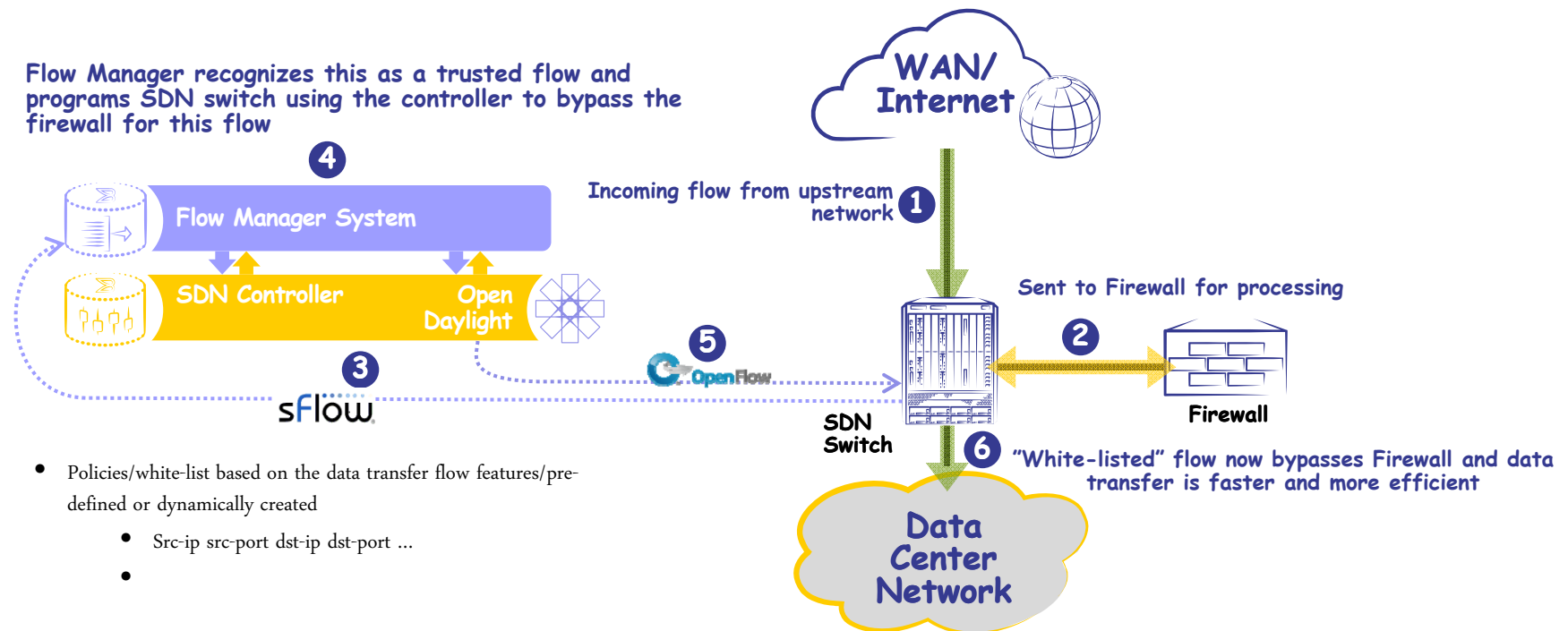
Case 1: Service Chain

Send different applications traffic to different firewall

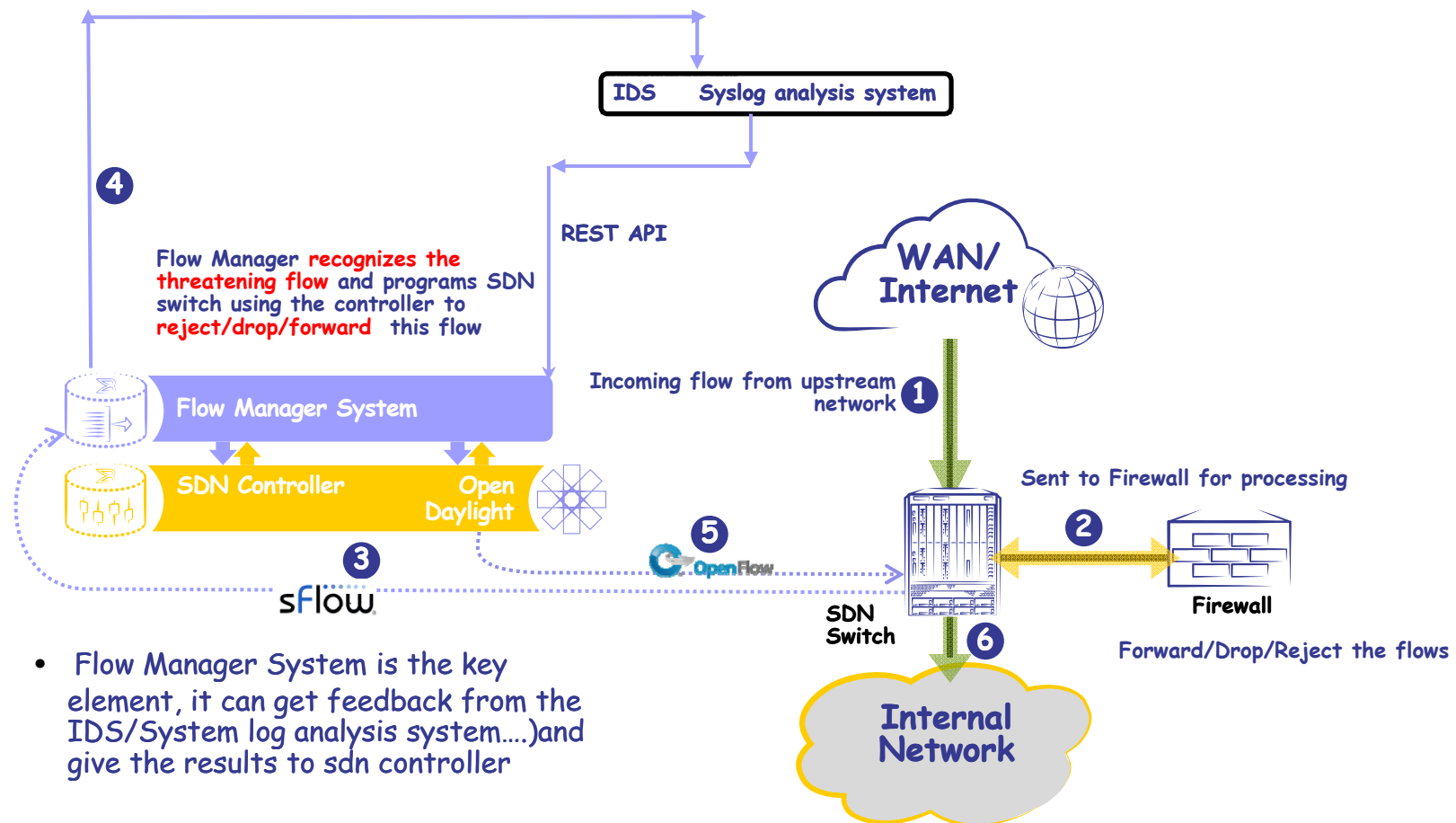


Case 2: Firewall Bypass for Science-DMZ

Flow Manager recognizes this as a trusted flow and programs SDN switch using the controller to bypass the firewall for this flow



Case 3: Dynamic security policies

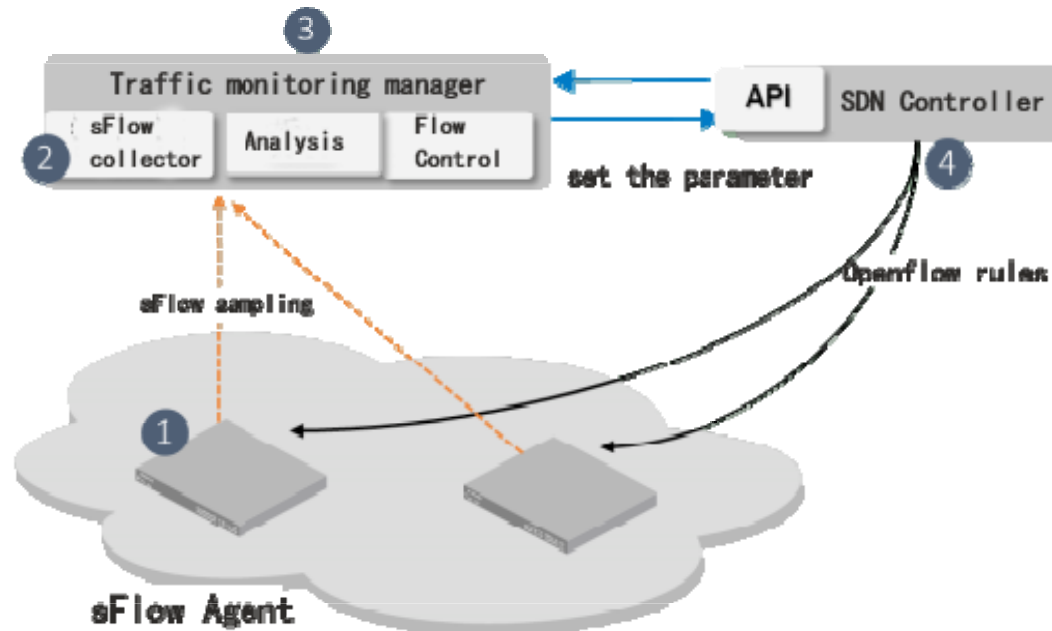


- Flow Manager System is the key element, it can get feedback from the IDS/System log analysis system...and give the results to sdn controller
- Policies based on the result from third-party system
 - IDS
 - Syslog analysis system
 -

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

