Networking Research at the University of Kentucky:

VIP Lanes and NetSecOps*

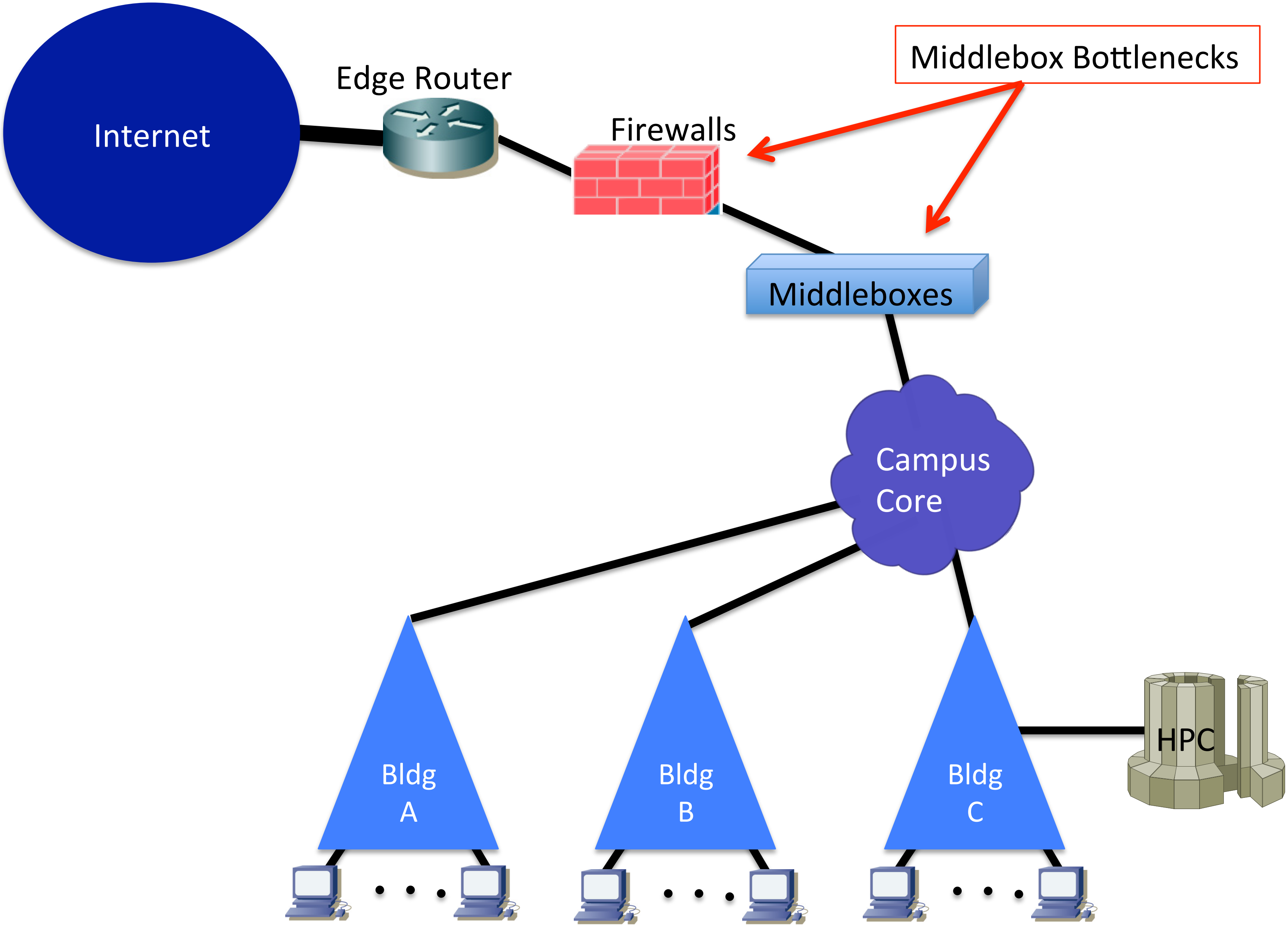
James Griffioen,
Laboratory for Advanced Networking
University of Kentucky

GENI Regional Workshop
May 14, 2018

UNIVERSITY OF KENTUCKY

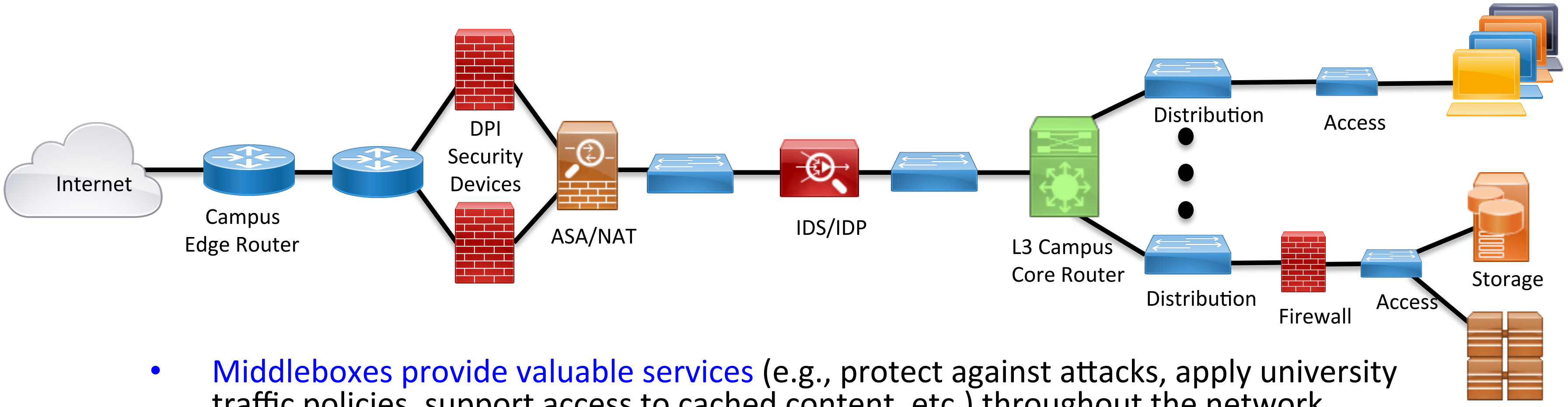
*NetSecOps is a collaborative project between the University of Kentucky and the University of Utah

Typical Campus Network



The Middlebox Problem

(Middleboxes in an example campus network)

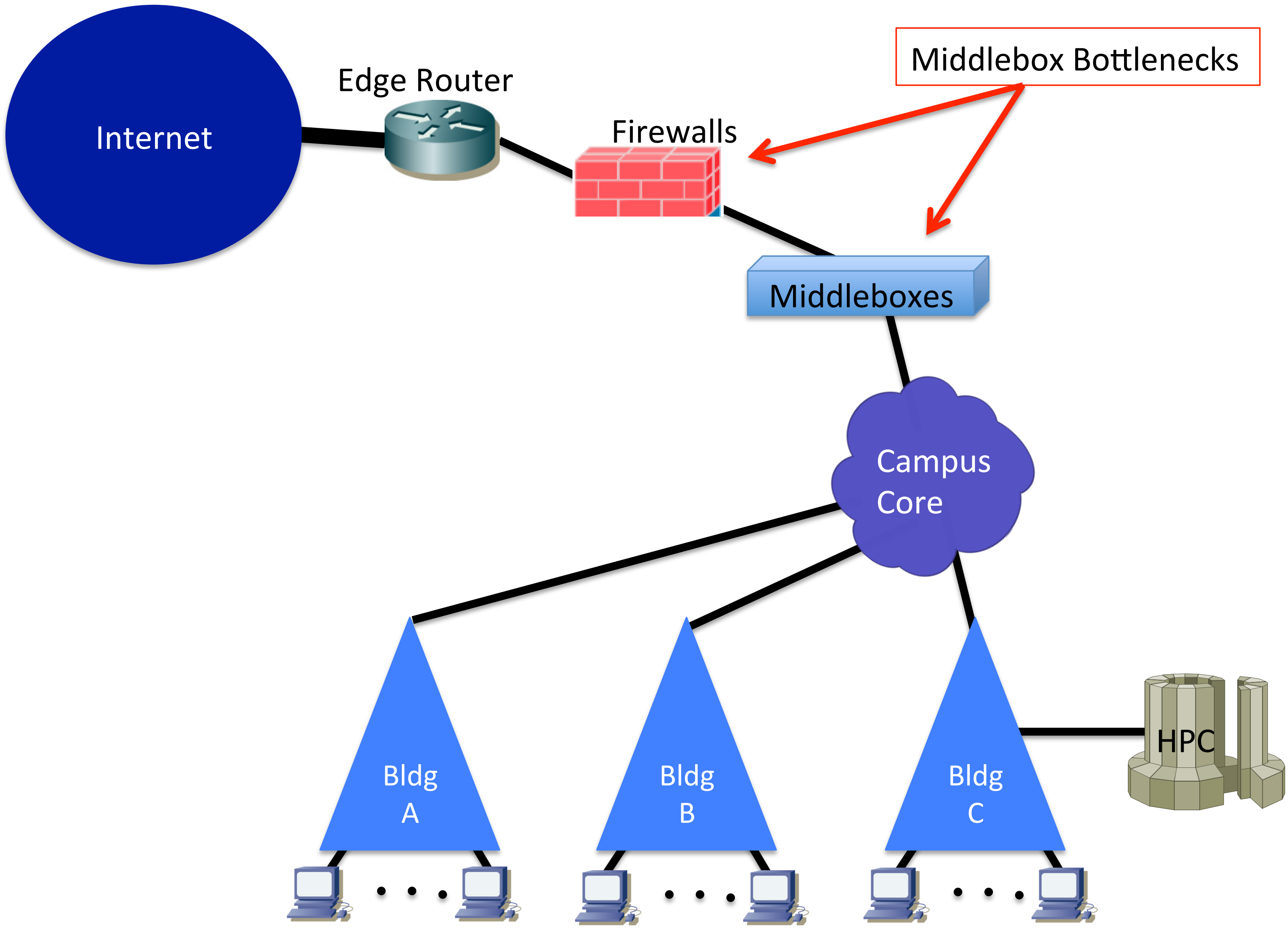


- Middleboxes provide valuable services (e.g., protect against attacks, apply university traffic policies, support access to cached content, etc.) throughout the network.
- Example middleboxes include
  - Firewalls
  - IDS/IDP
  - NAT boxes
  - Load balancers
  - VPN gateways
  - Caching servers/Proxies
  - Wireless gateways
- Middleboxes pose a bottleneck to network performance
  - Add delay
  - Limit throughput (particularly DPI-based services)
  - And upgrading speeds/feeds often does not yield the expected benefits

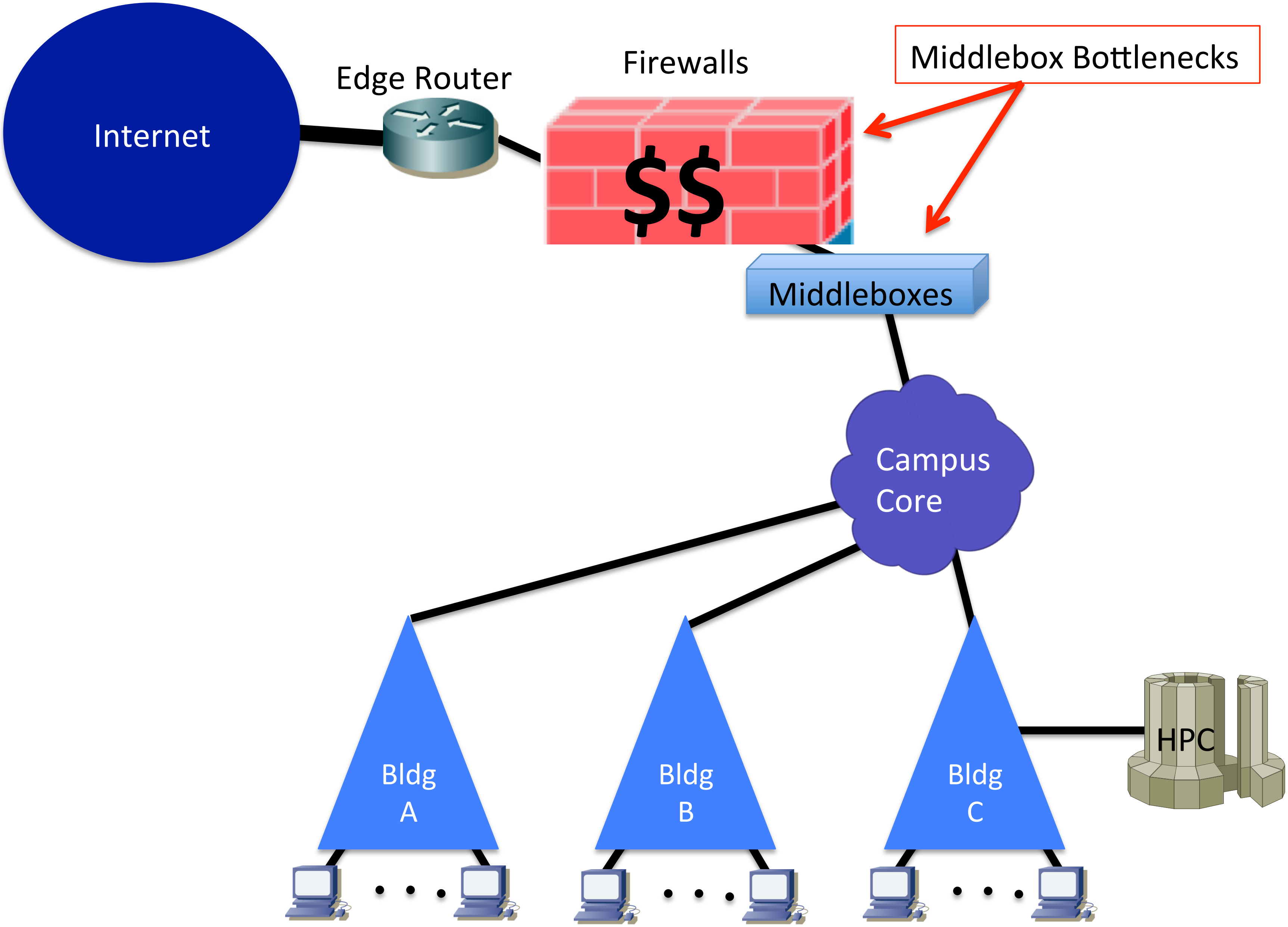
University data-driven research (i.e., big data) is being hampered by middleboxes that permeate the network, creating choke points that increase latency and sometimes break flows altogether.

UNIVERSITY OF KENTUCKY

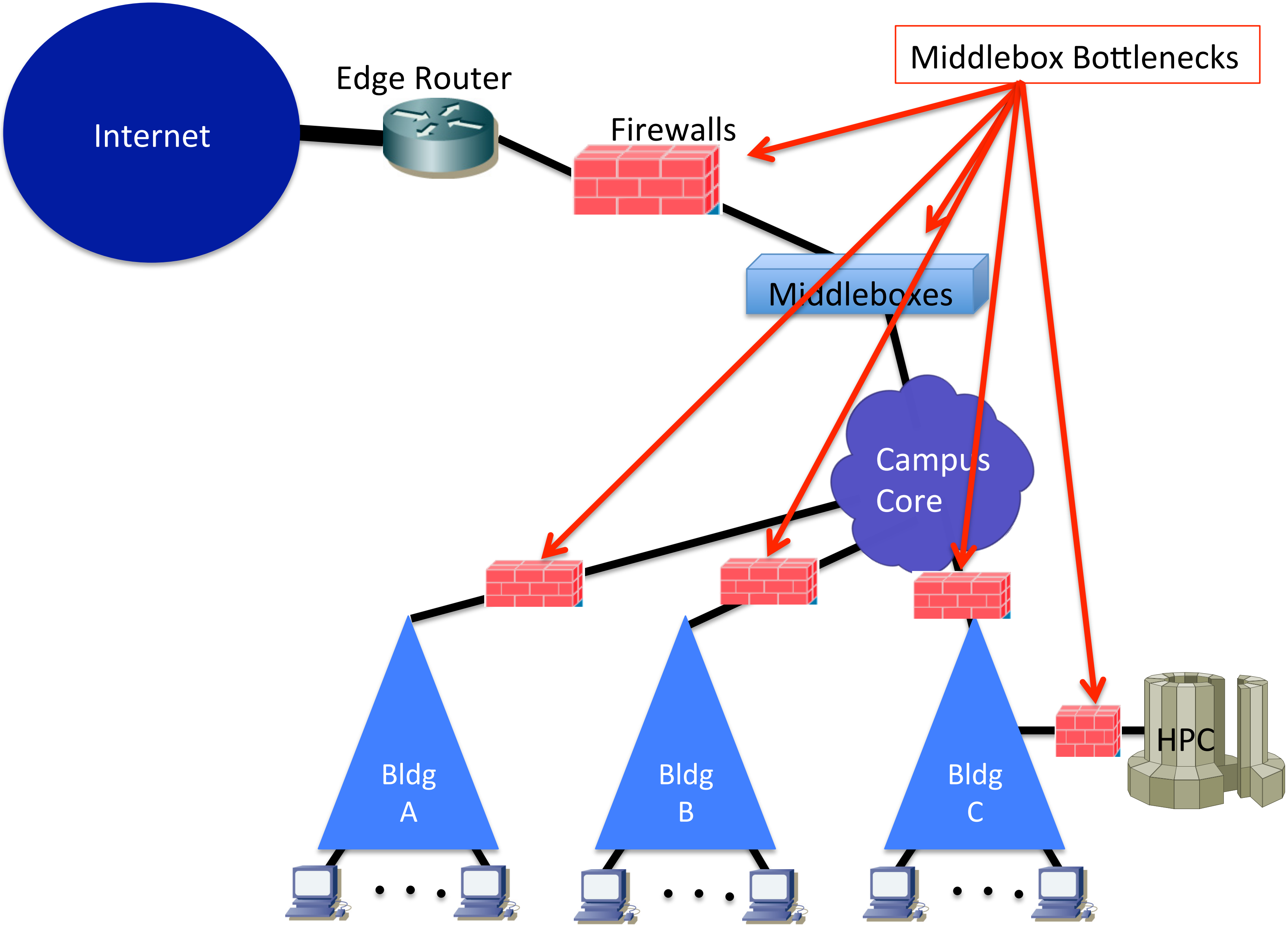
Typical Campus Network



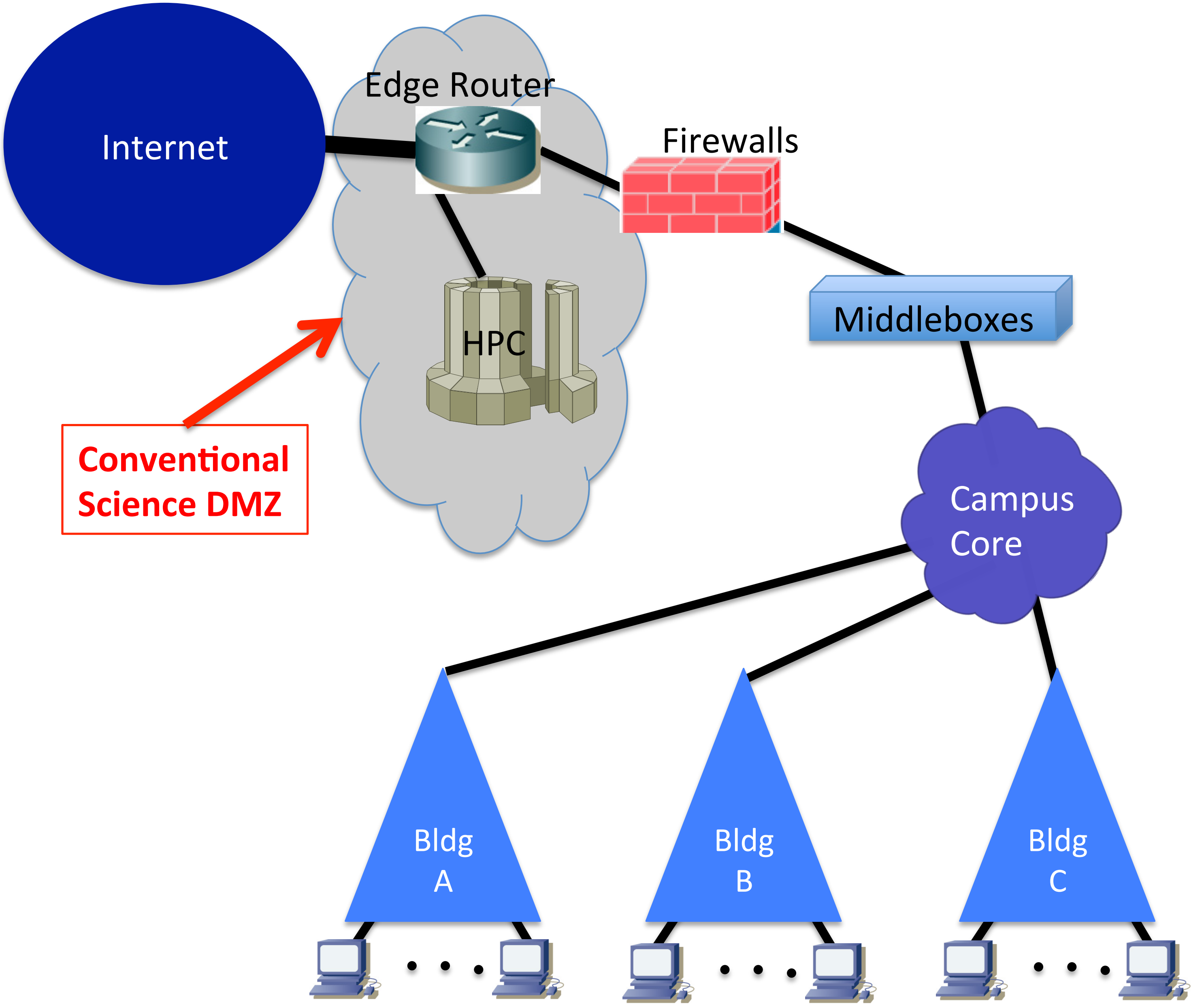
Typical Campus Network



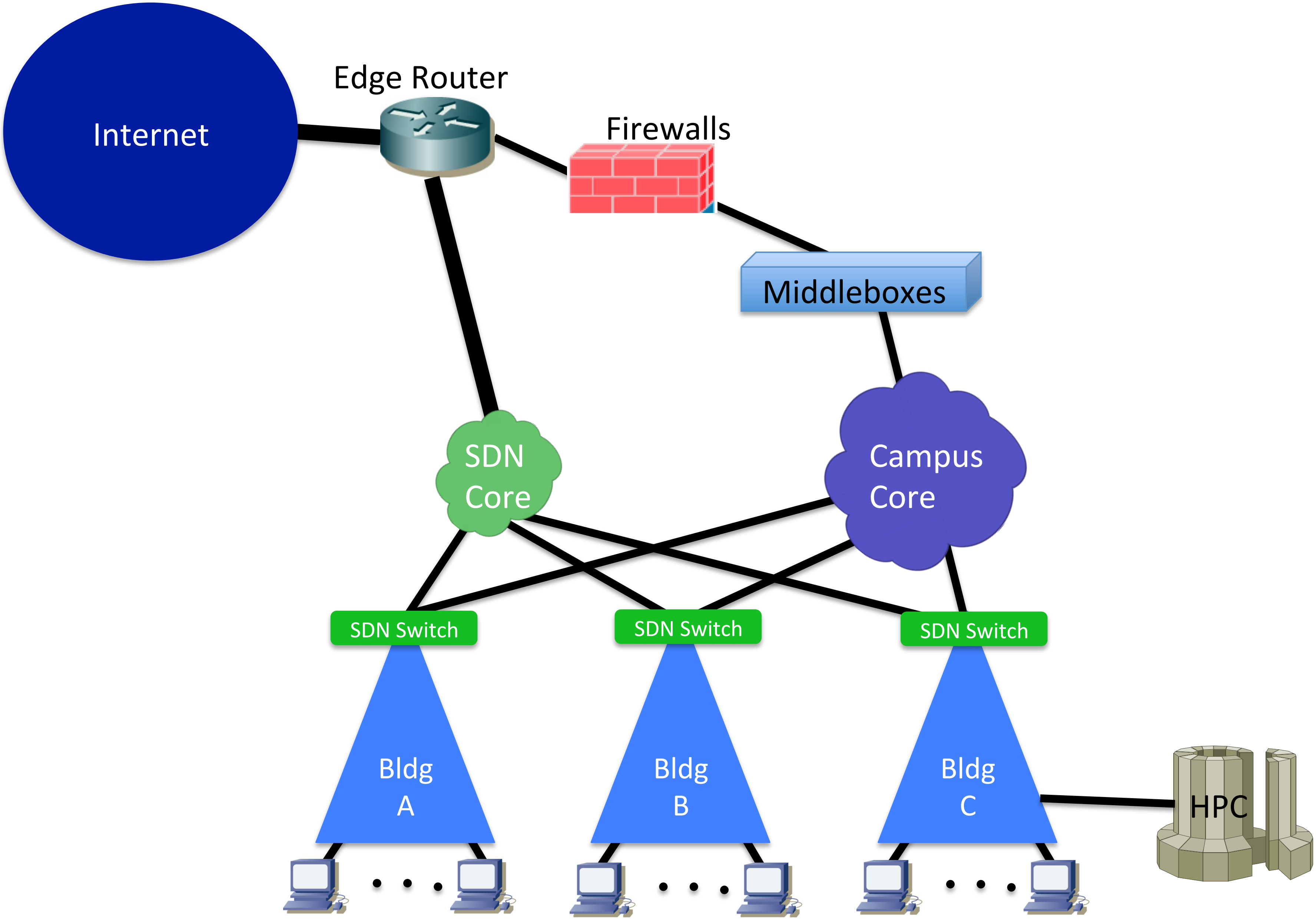
Typical Campus Network



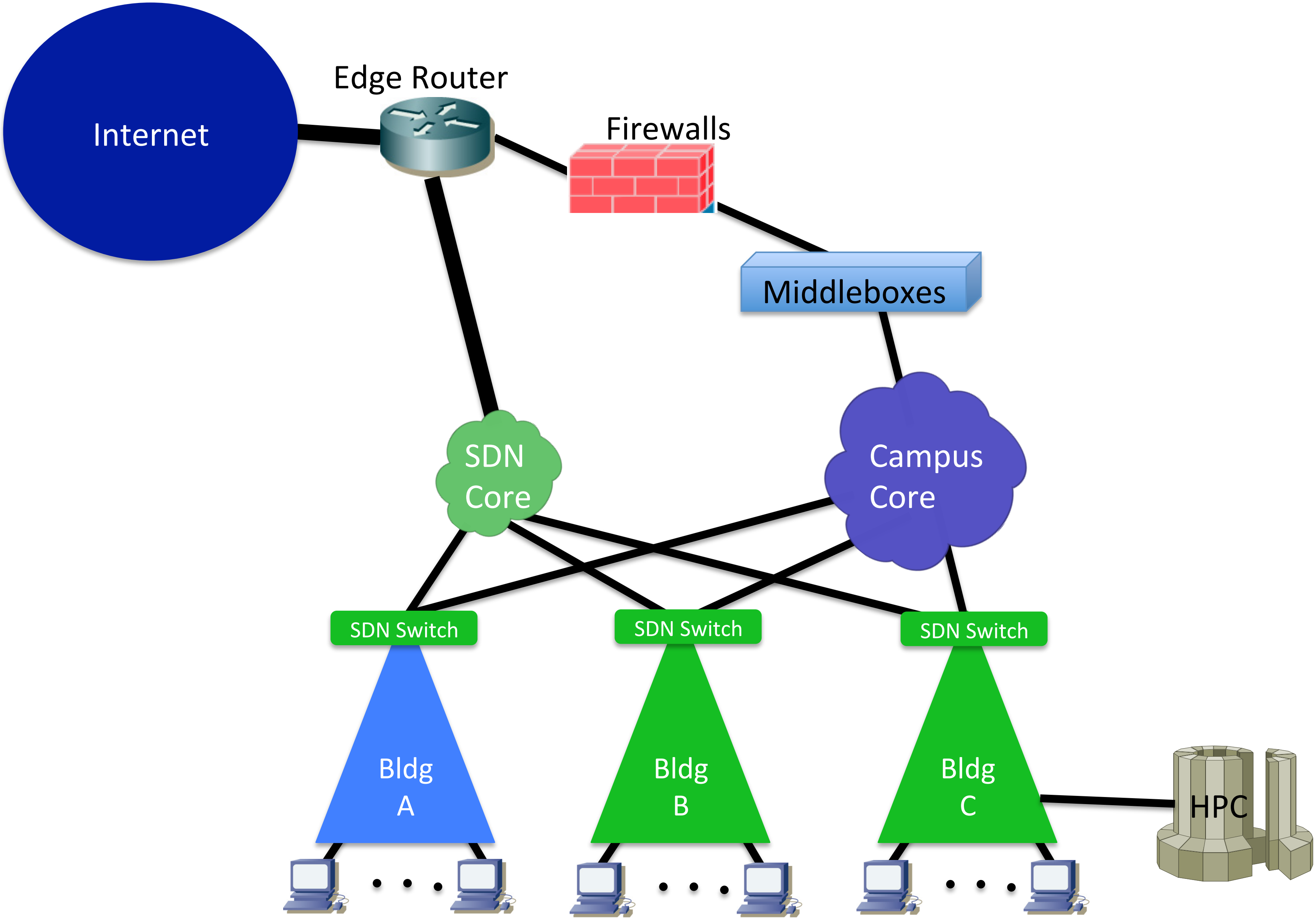
Science DMZ


Internet
Edge Router
Firewalls
HPC
Middleboxes
Conventional Science DMZ
Campus Core
Bldg A
Bldg B
Bldg C

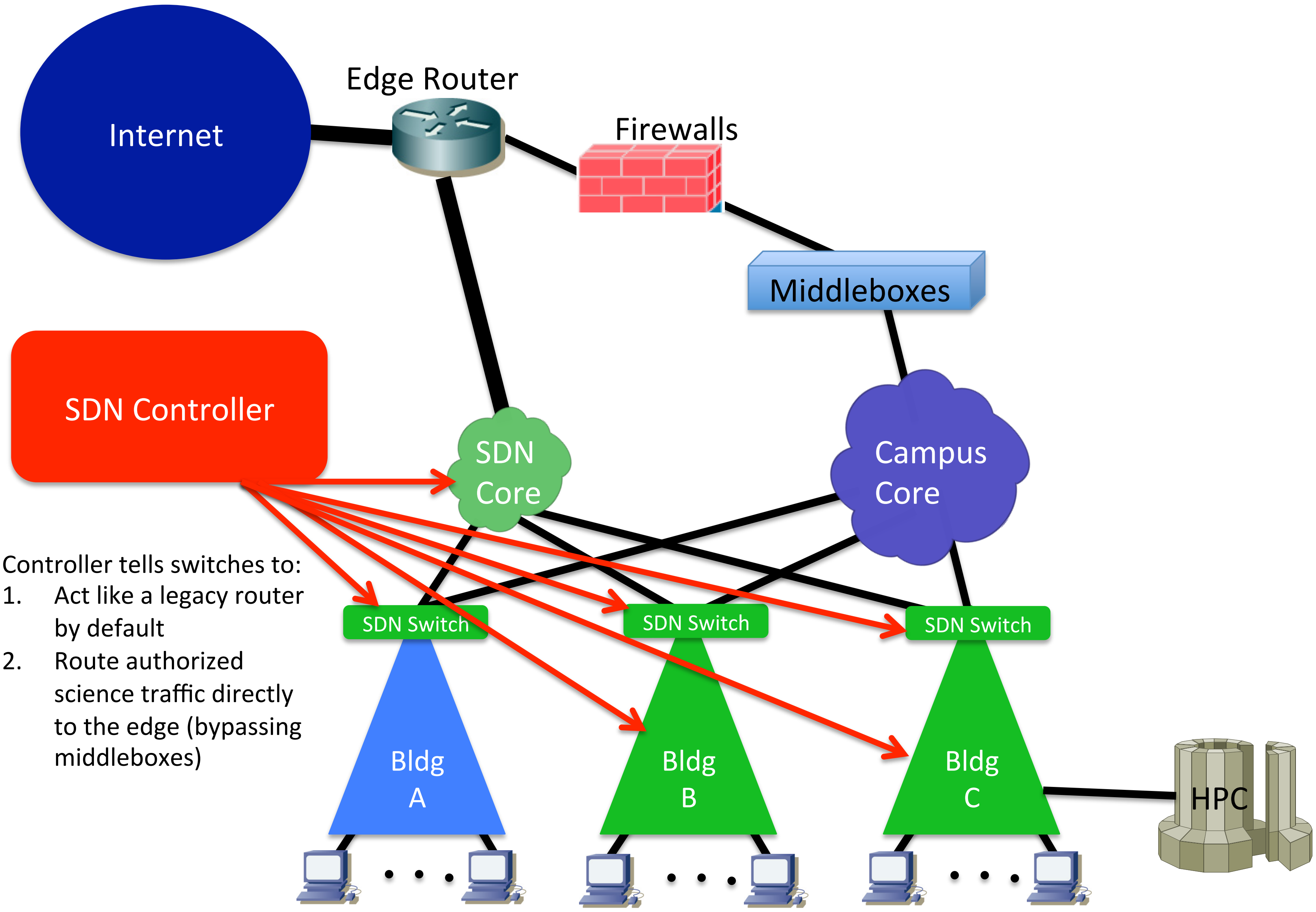
UKY SDN Core


Internet
Edge Router
Firewalls
Middleboxes
SDN Core
Campus Core
SDN Switch
SDN Switch
SDN Switch
Bldg A
Bldg B
Bldg C
HPC

UKY SDN Network



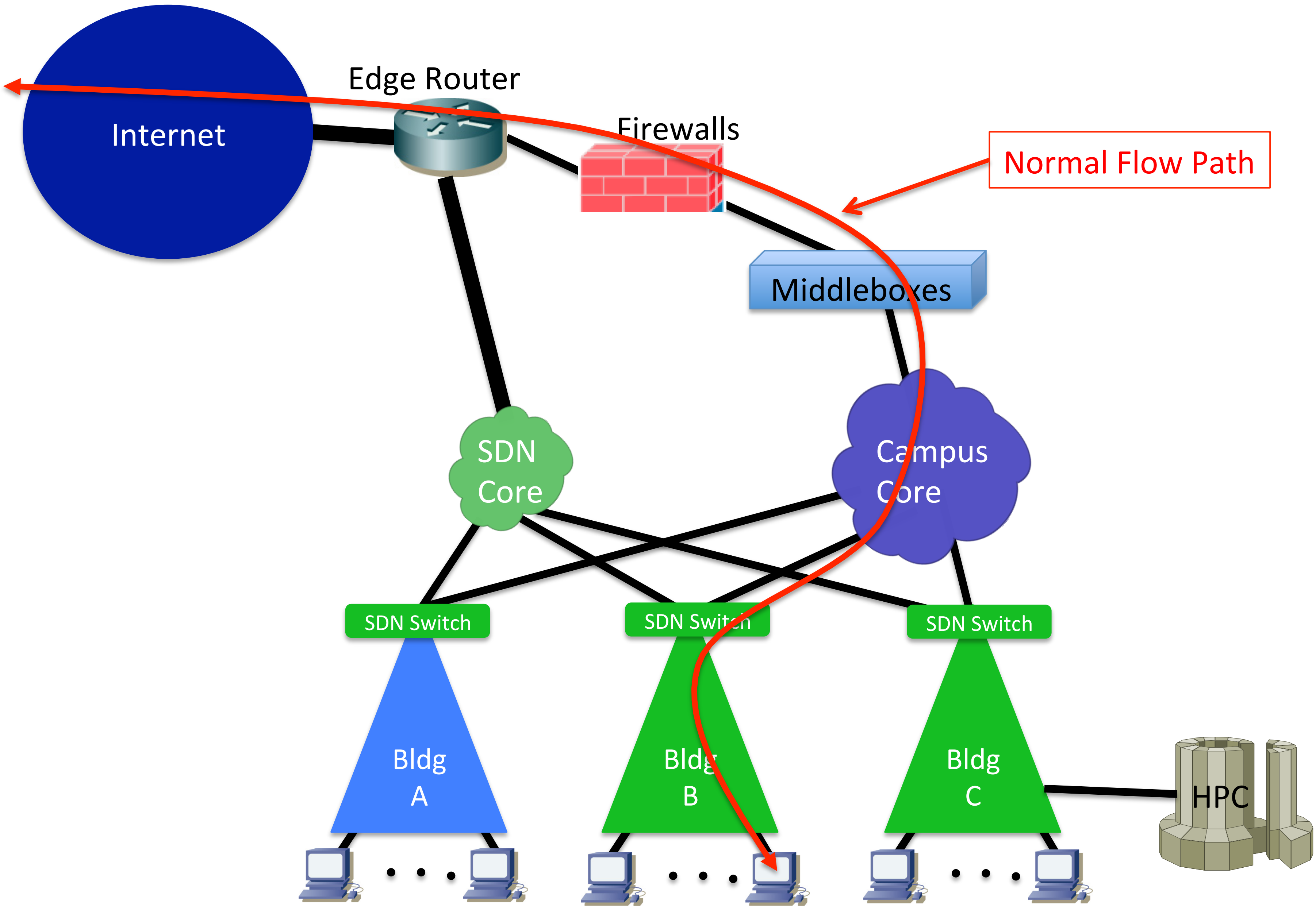
UKY SDN Network



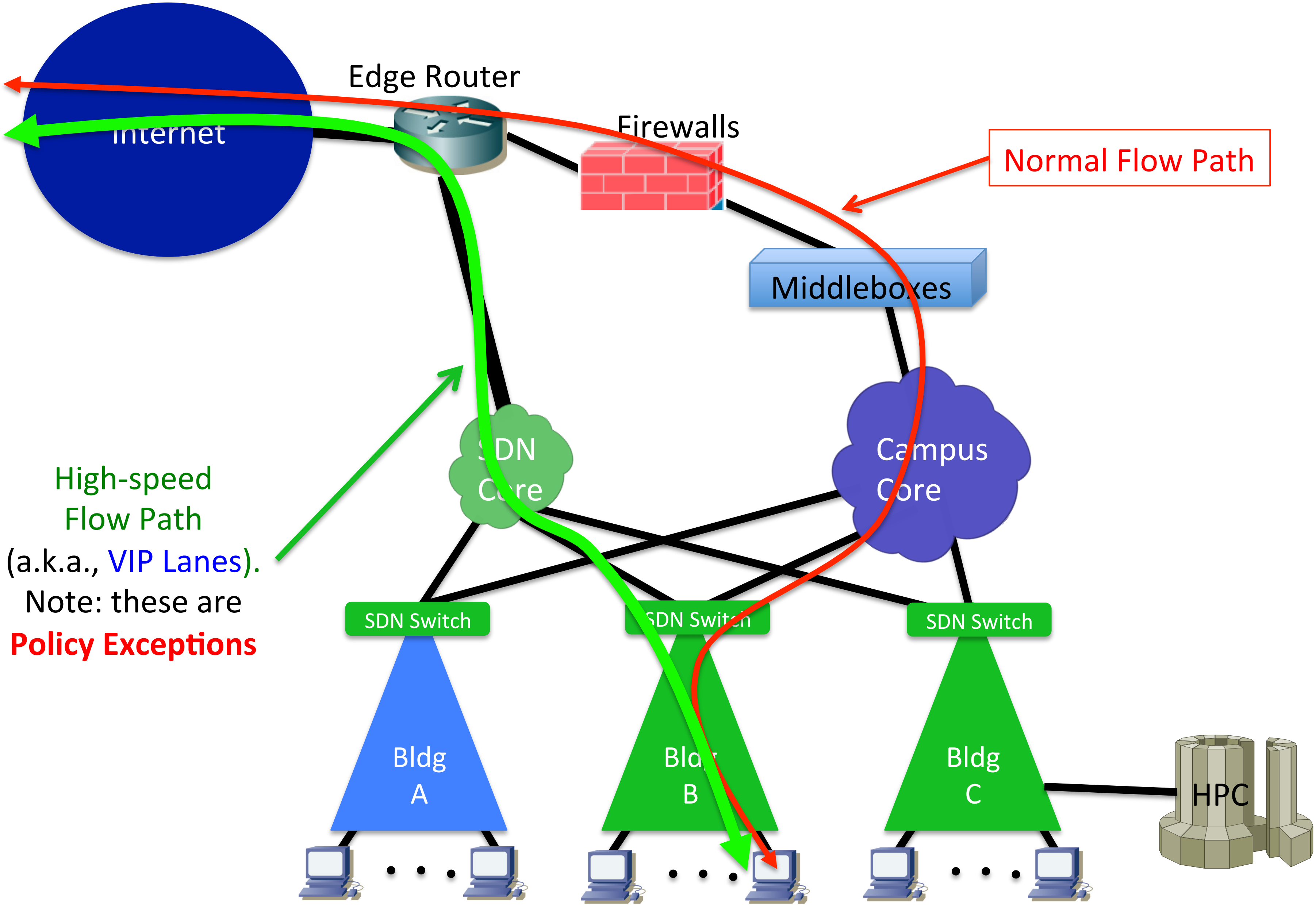
Controller tells switches to:

1. Act like a legacy router by default
2. Route authorized science traffic directly to the edge (bypassing middleboxes)

UKY SDN Network



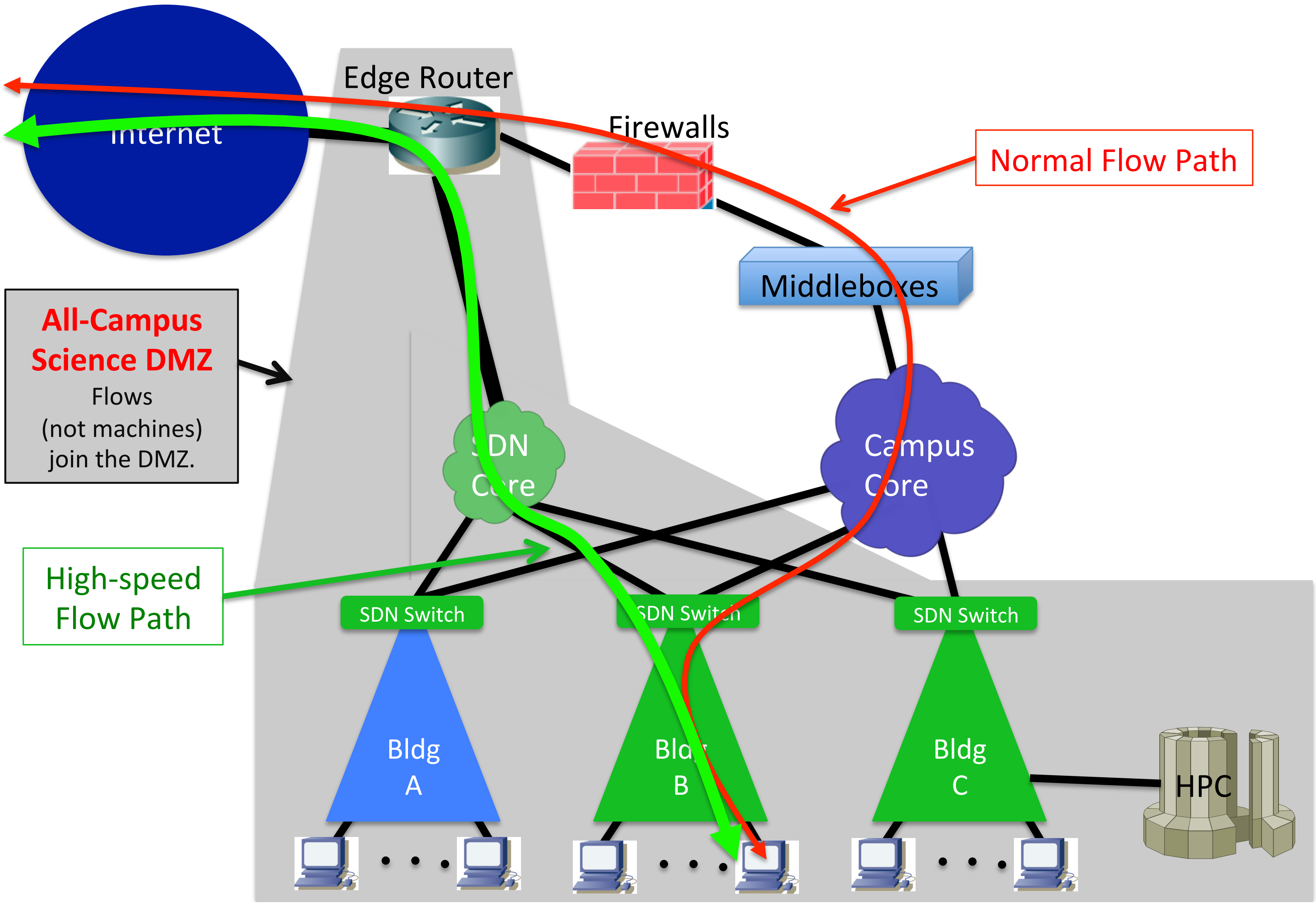
UKY SDN Network



Normal Flow Path

High-speed Flow Path (a.k.a., VIP Lanes). Note: these are **Policy Exceptions**

UKY All-Campus Science DMZ



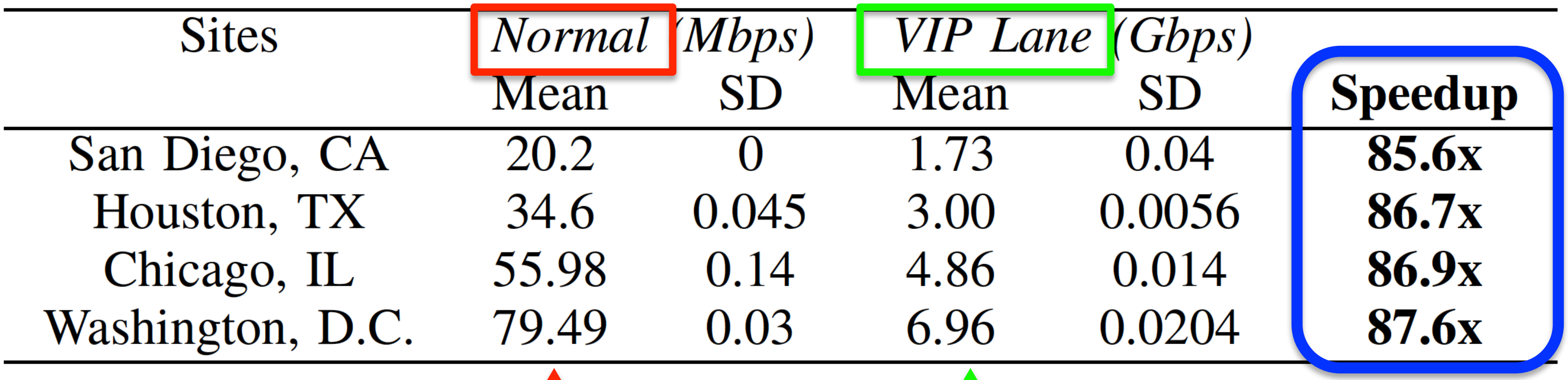
All-Campus Science DMZ

Flows
(not machines)
join the DMZ.

Normal Flow Path

High-speed Flow Path

Internet Performance Results



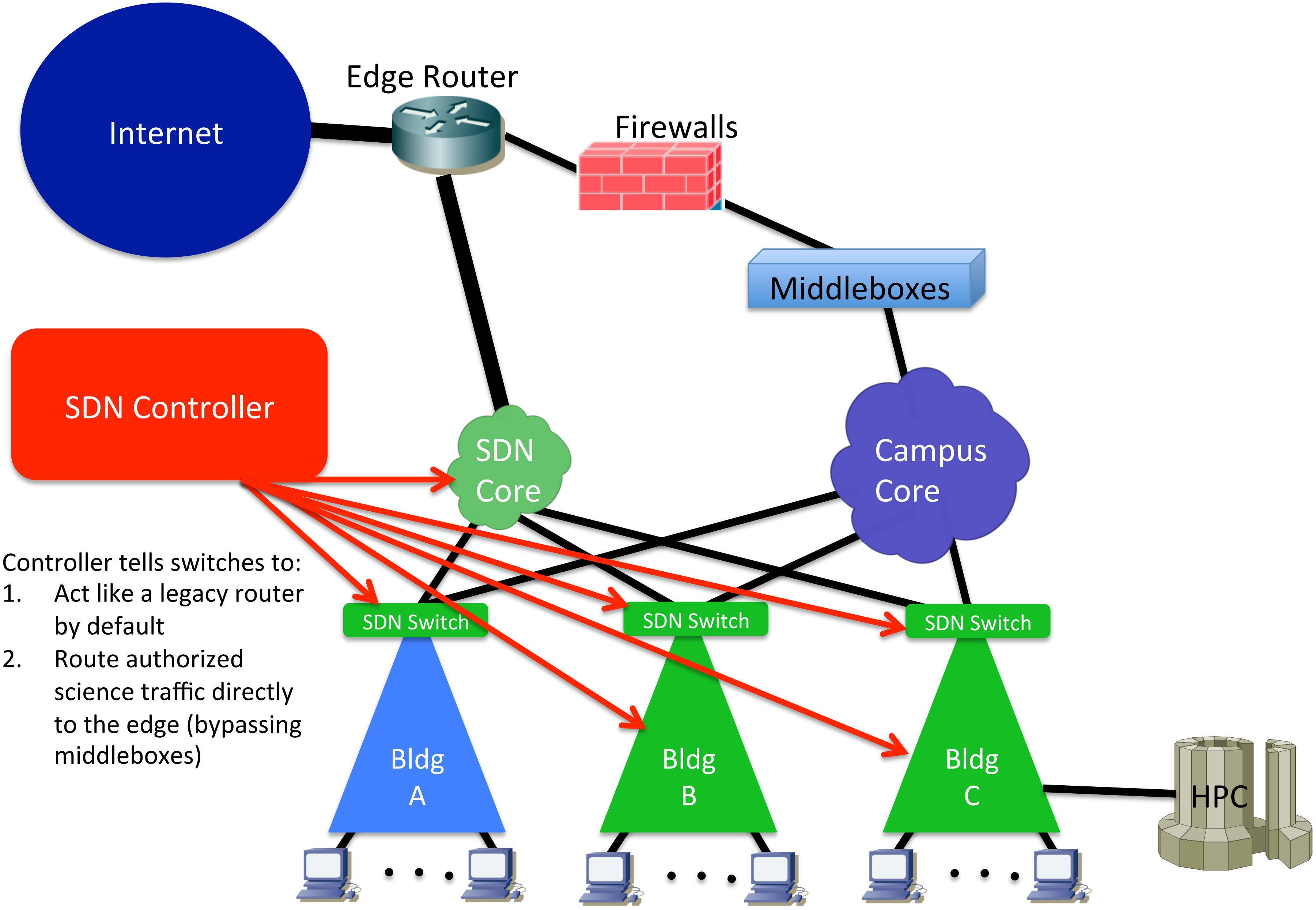
Sites	*Normal (Mbps)*		*VIP Lane (Gbps)*		
	Mean	SD	Mean	SD	**Speedup**
San Diego, CA	20.2	0	1.73	0.04	**85.6x**
Houston, TX	34.6	0.045	3.00	0.0056	**86.7x**
Chicago, IL	55.98	0.14	4.86	0.014	**86.9x**
Washington, D.C.	79.49	0.03	6.96	0.0204	**87.6x**

Mbps

Gbps

See ICCCN 2017 VIP Lanes Paper

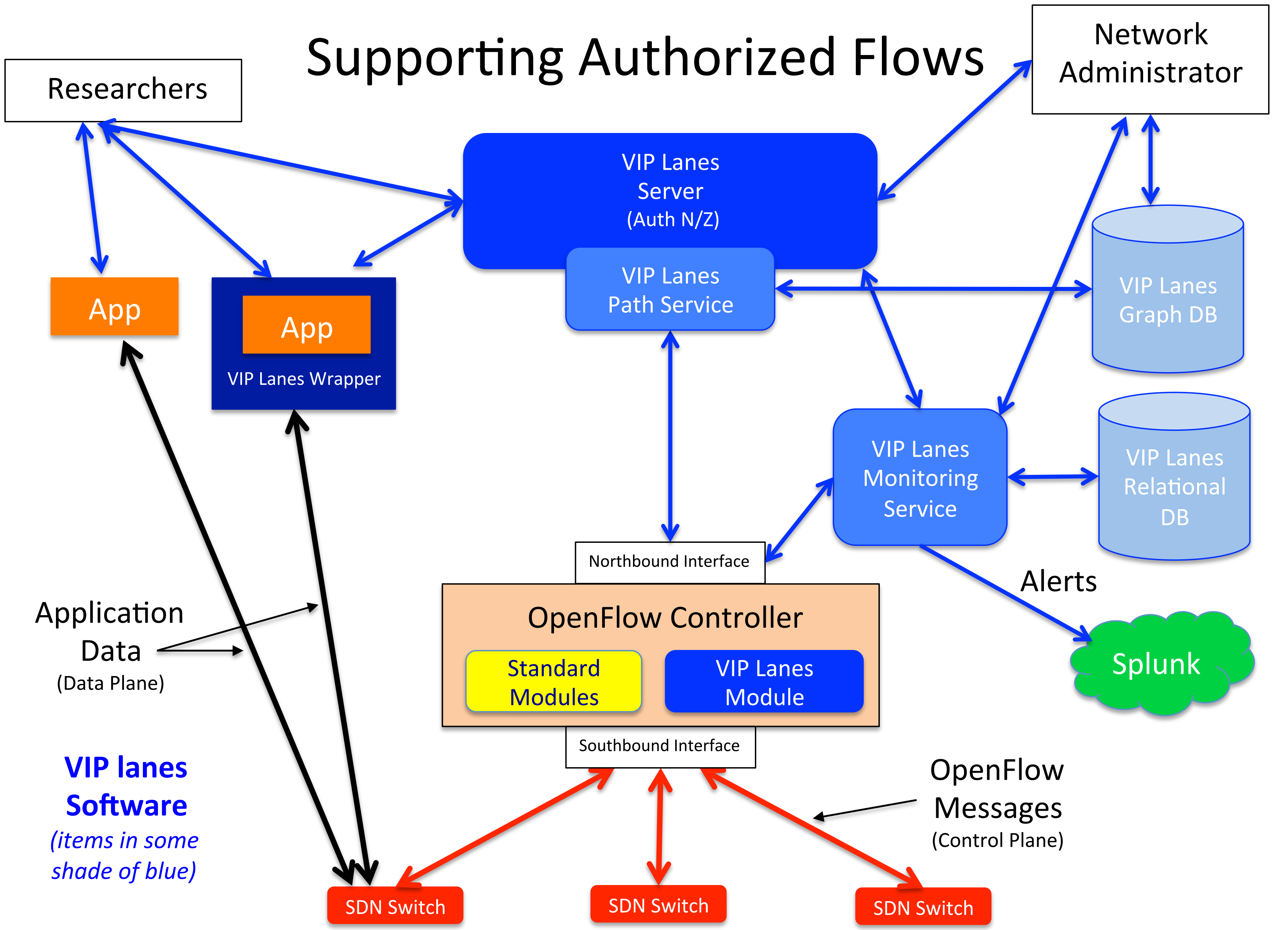
SDN Controller Software



Controller tells switches to:

1. Act like a legacy router by default
2. Route authorized science traffic directly to the edge (bypassing middleboxes)

Supporting Authorized Flows



Researchers

Network Administrator

VIP Lanes Server (Auth N/Z)

VIP Lanes Path Service

VIP Lanes Graph DB

App

App

VIP Lanes Wrapper

VIP Lanes Monitoring Service

VIP Lanes Relational DB

Alerts

Splunk

Northbound Interface

OpenFlow Controller

Standard Modules

VIP Lanes Module

Southbound Interface

Application Data (Data Plane)

OpenFlow Messages (Control Plane)

SDN Switch

SDN Switch

SDN Switch

VIP lanes Software

(items in some shade of blue)

See ICCCN 2017 VIP Lanes Paper for details

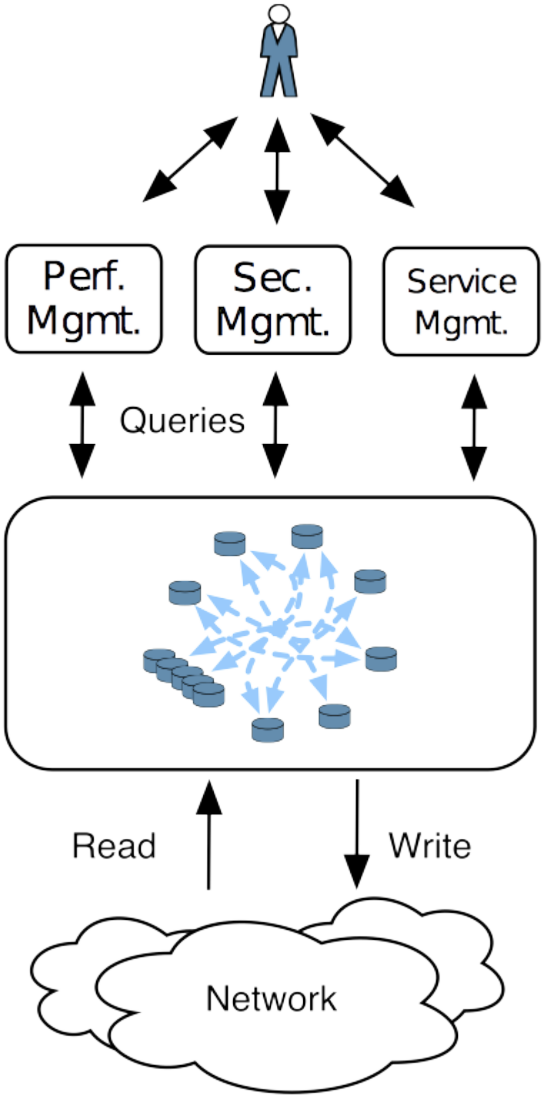
Securing an All-Campus Science DMZ

- Scaling the Science DMZ to the entire campus
  - The number of machines is much larger
  - The number of potential users is much larger
  - The number of policies is much larger
    - policies are per flow, not per machine
- Scaling the decision-making processes
  - Defining policies
  - Authorizing Users
  - Defining Trust relationships

UK

UNIVERSITY OF KENTUCKY

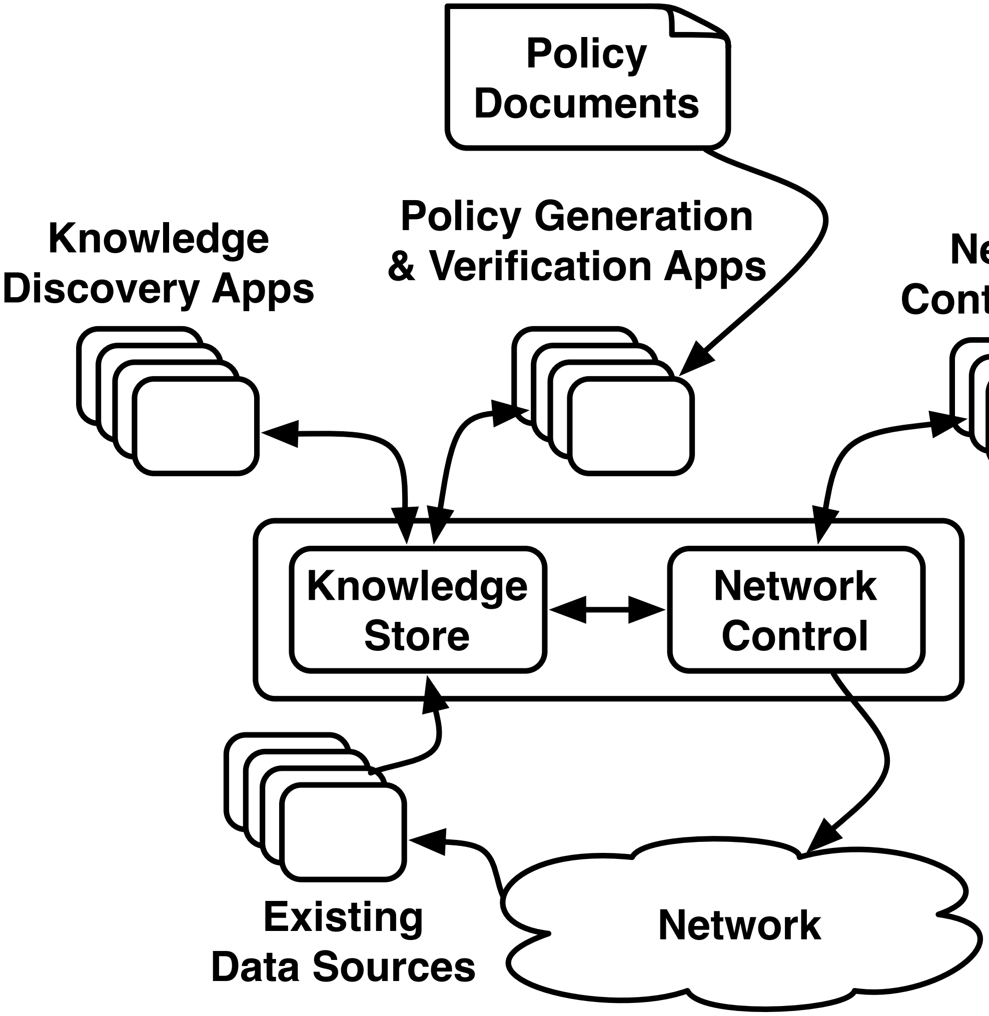
NetSecOps
(Network Security Operations)



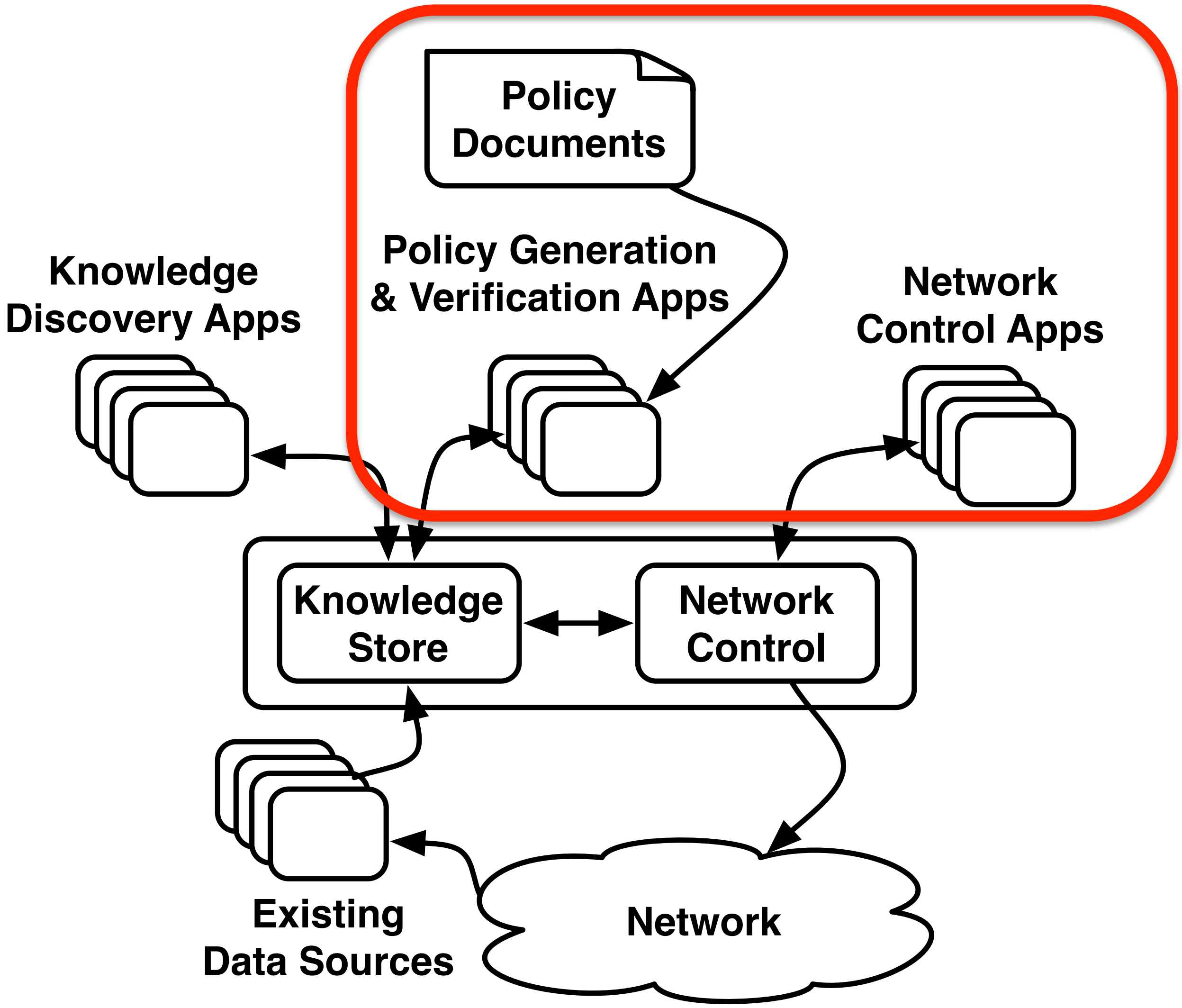
Basic Goal:

Assist IT security teams by automating network security operational steps that are tedious and error-prone.

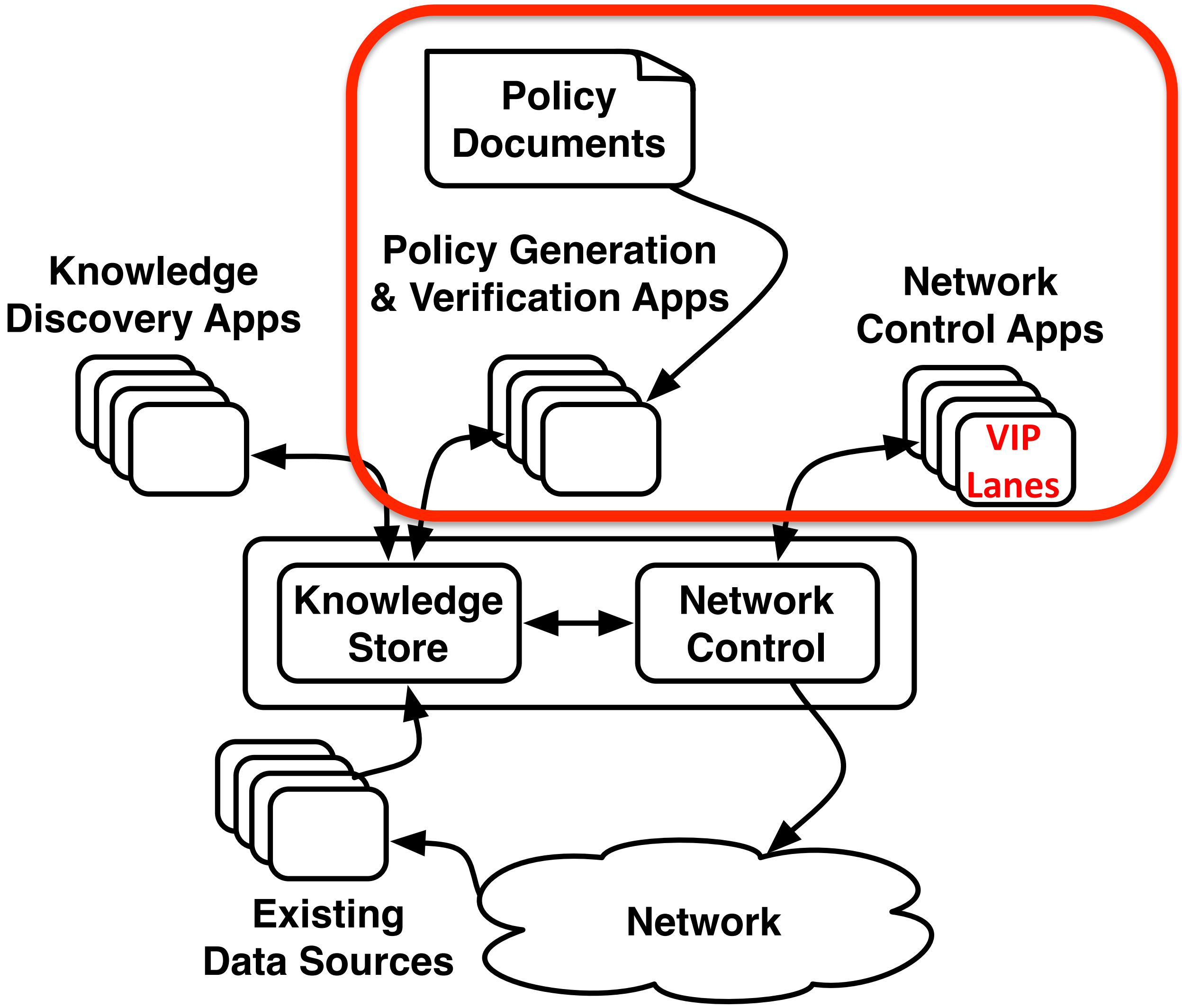
NetSecOps Architecture



NetSecOps Architecture



NetSecOps Architecture



Authorization/Policy Questions

- Who can authorize a VIP Lane(s)?
  - A single authority? Multiple authorities?
  - What is the authorization process?
- When does authorization occur? When does instantiation occur?
  - Instantaneously? Pre-authorized?,
- What is the lifetime of a VIP Lane(s)?
  - Months, days, hours, minutes?
- Etc …

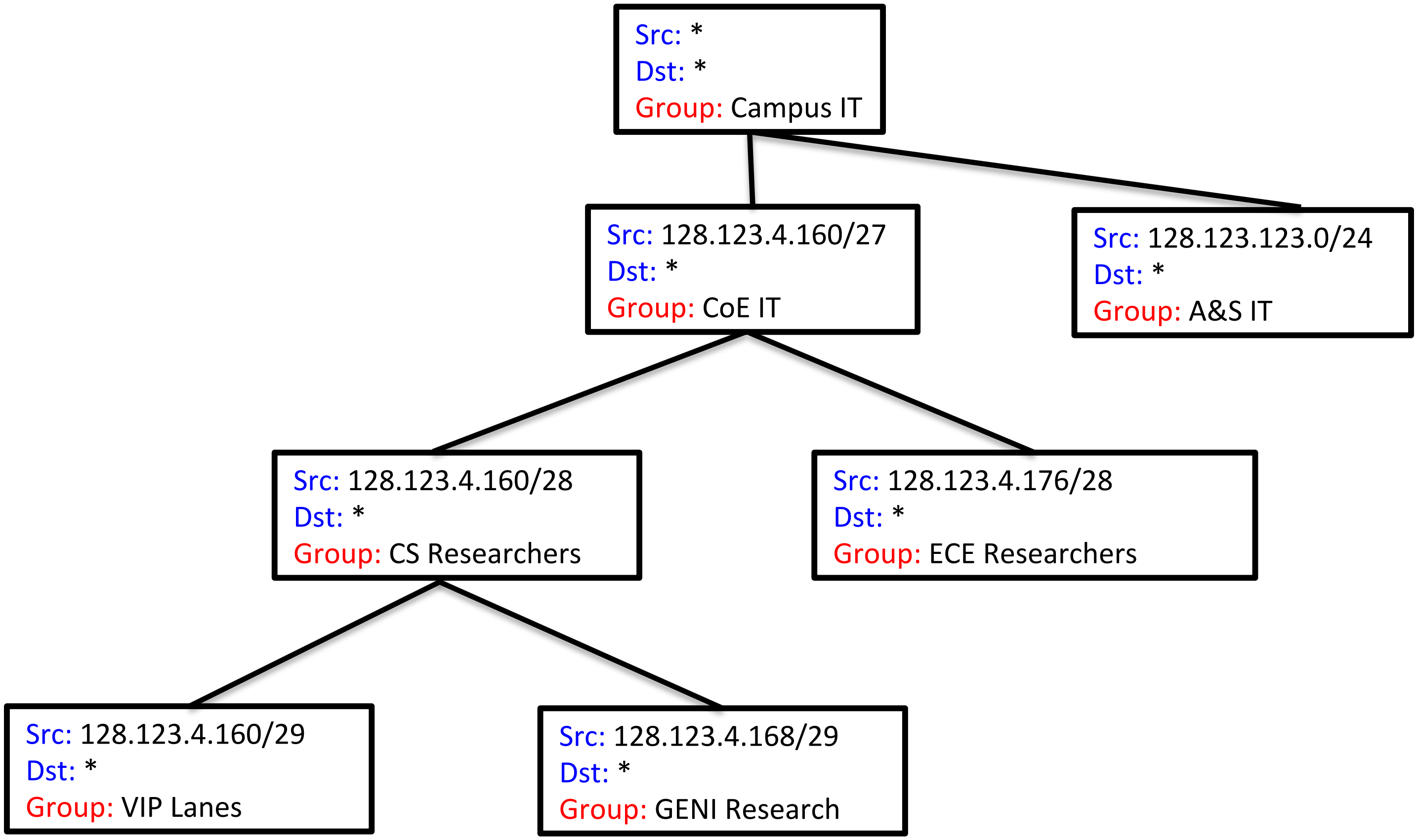
UNIVERSITY OF KENTUCKY

NetSecOps Policy

- Default policy is to route normally
- NetSecOps defines who can declare a Policy Exception and on which flows (i.e., Policy Exception = VIP Lane) and verifies exceptions match written policy requirements.
- Flows space is arranged into a hierarchy
  - Root = all flows
  - Subnodes = strict subset of parent's flows
  - Flows defined by tuple (e.g., src IP, dst IP, dst port)
- Trusted Users assigned to manage portions of the hierarchy
  - Can instantiate a flow (i.e., create a policy exception)
  - Can delegate control to other Trusted User
  - Delegation defines a hierarchy of responsibility

See ICCCN 2017 VIP Lanes Paper

Example Policy Exception Tree



Src: *
Dst: *
Group: Campus IT

Src: 128.123.4.160/27
Dst: *
Group: CoE IT

Src: 128.123.123.0/24
Dst: *
Group: A&S IT

Src: 128.123.4.160/28
Dst: *
Group: CS Researchers

Src: 128.123.4.176/28
Dst: *
Group: ECE Researchers

Src: 128.123.4.160/29
Dst: *
Group: VIP Lanes

Src: 128.123.4.168/29
Dst: *
Group: GENI Research

Policy tree is created by users in a distributed way (through a web server that maintains the policy tree).

Demo

Thank You

Questions?

UNIVERSITY OF KENTUCKY

This work is supported, in part, by the National Science Foundation under NSF grants ACI-1642134, ACI-1642158, ACI-1541426 and ACI-1541380