Jobber
Automating Inter-Tenant Trust in The Cloud

Andy Sayler
Eric Keller
Dirk Grunwald

University of Colorado **Boulder**

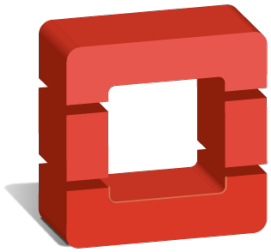
How can we make
the Data Center...

more efficient?

more secure?

more manageable?

Windows Azure™



openstack™

cloudstack

Google app engine

Over 50%

Enterprise Companies Use Cloud Infrastructure*

* Cohen, Reuven. *The Cloud Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*. Forbes. April 16th, 2013.

10% to 40%

of all Data Center Traffic is Inter-Tenant Traffic*

* BALLANI, H., JANG, K., AND KARAGIANNIS, T. Chatty Tenants and the Cloud Network Sharing Problem. Proc. of NSDI (2013).

Ad Network ↔ Web Host

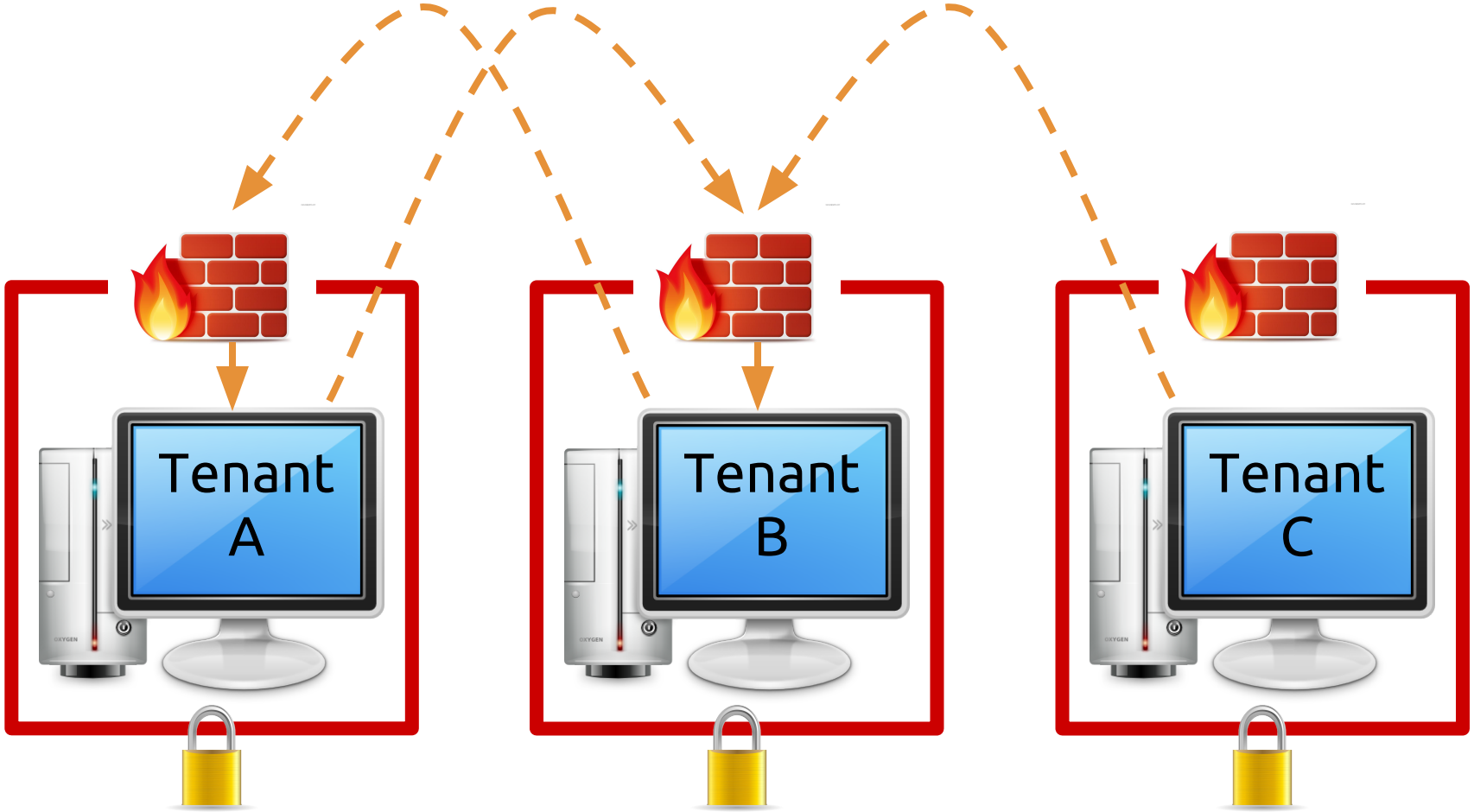
CDN ↔ ISP

NSA ↔ Google, Yahoo, Etc

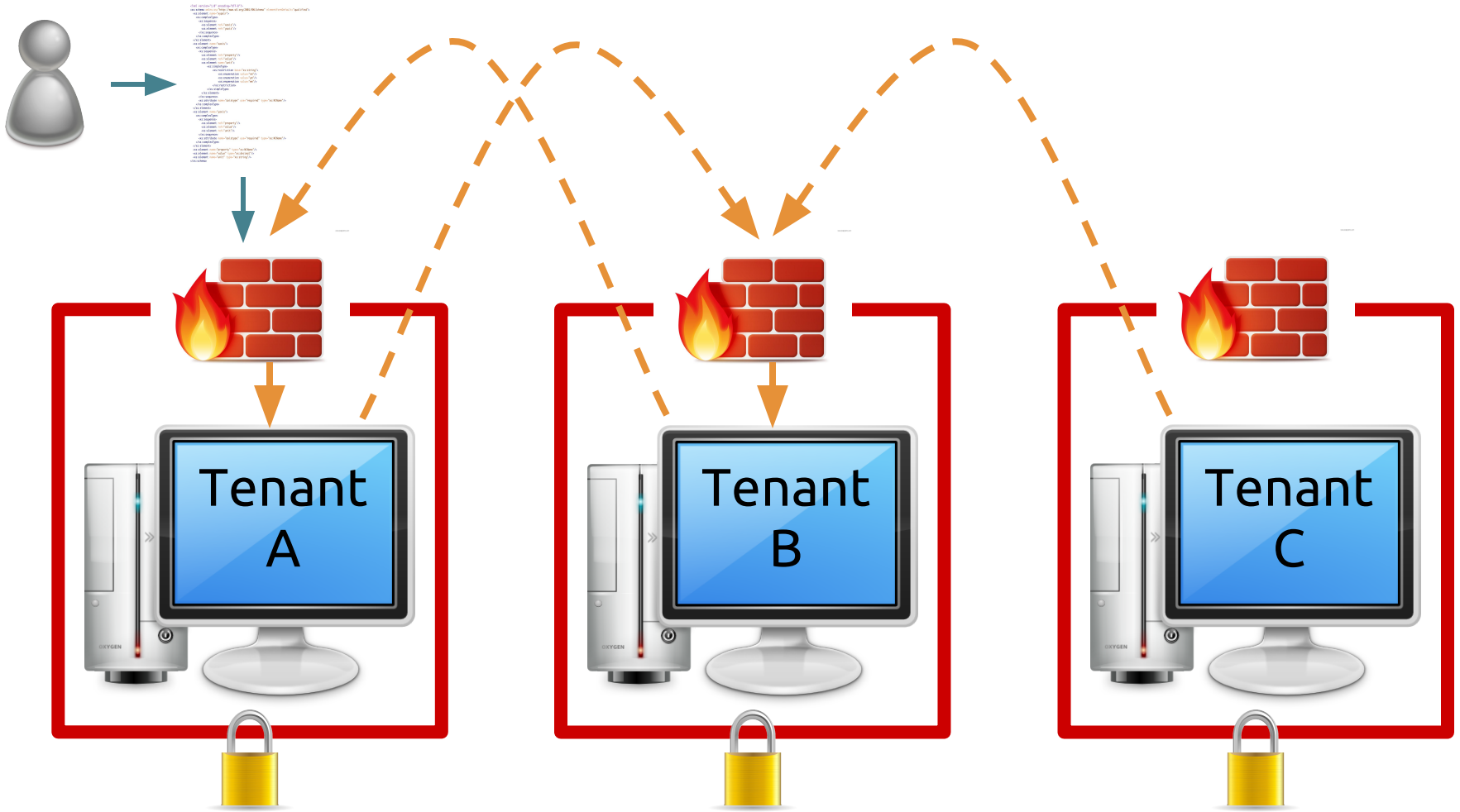
emphasis is on isolation

hindering inter-tenant traffic

all traffic is untrusted

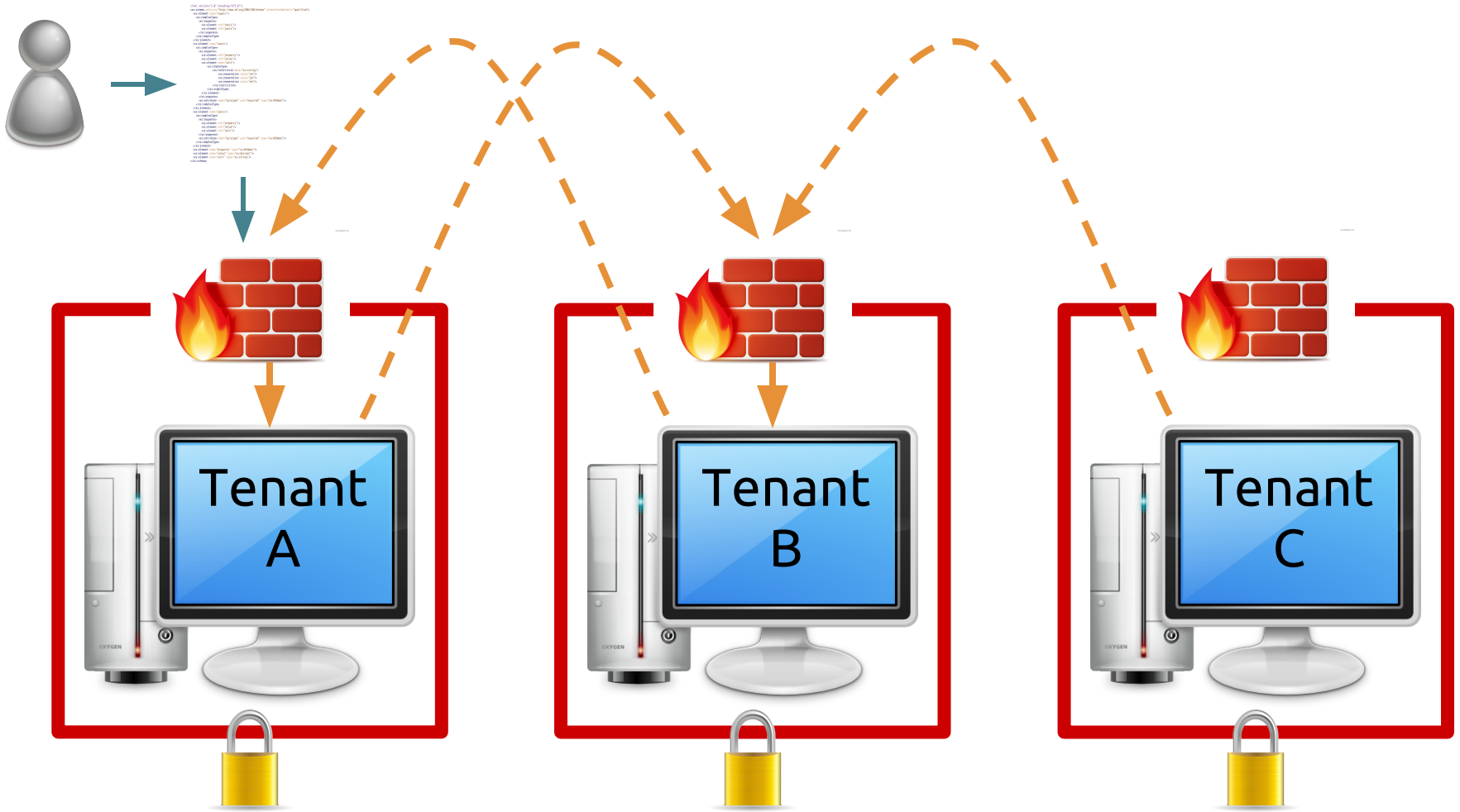


manual static configuration



misconfiguration

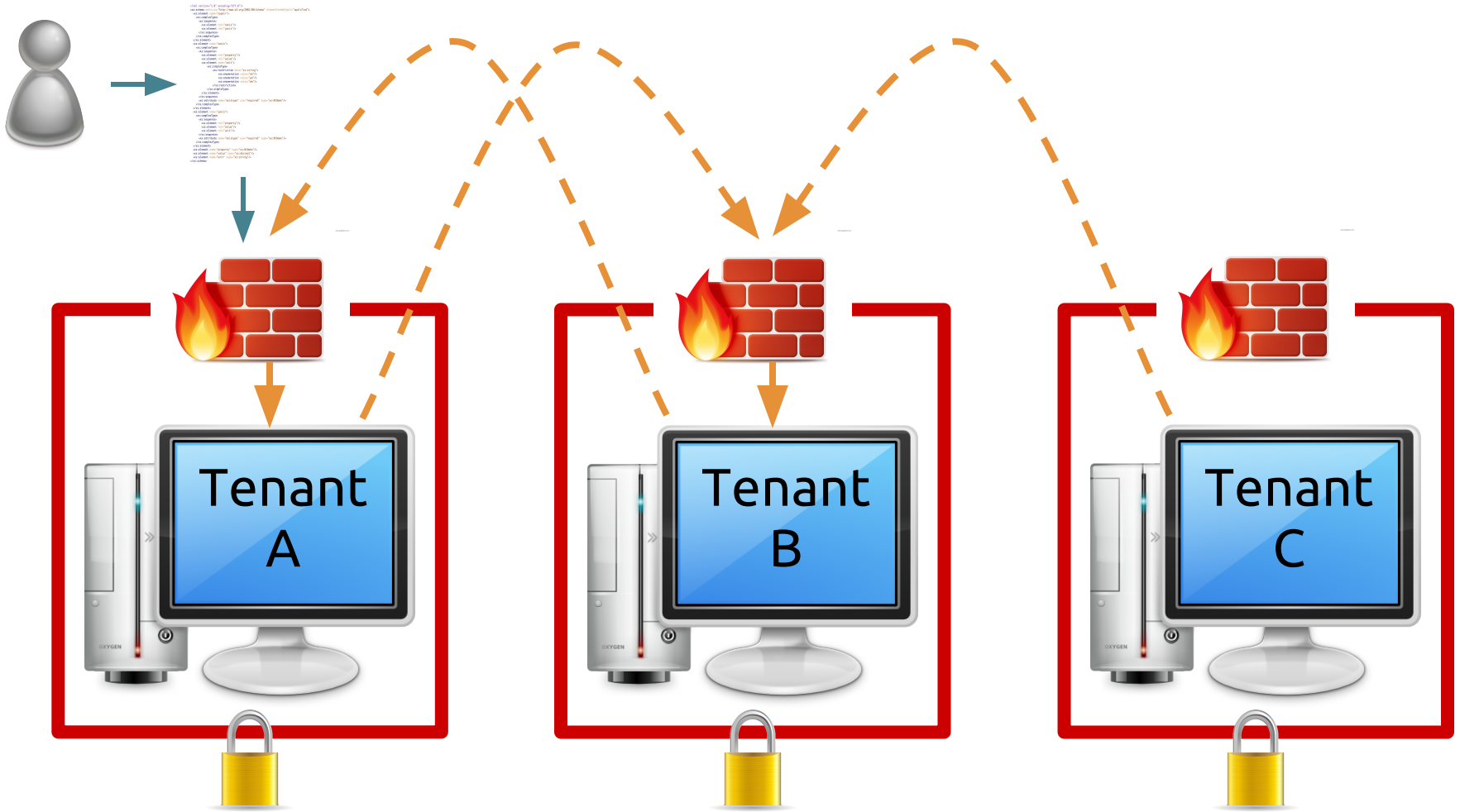
is a major security problem



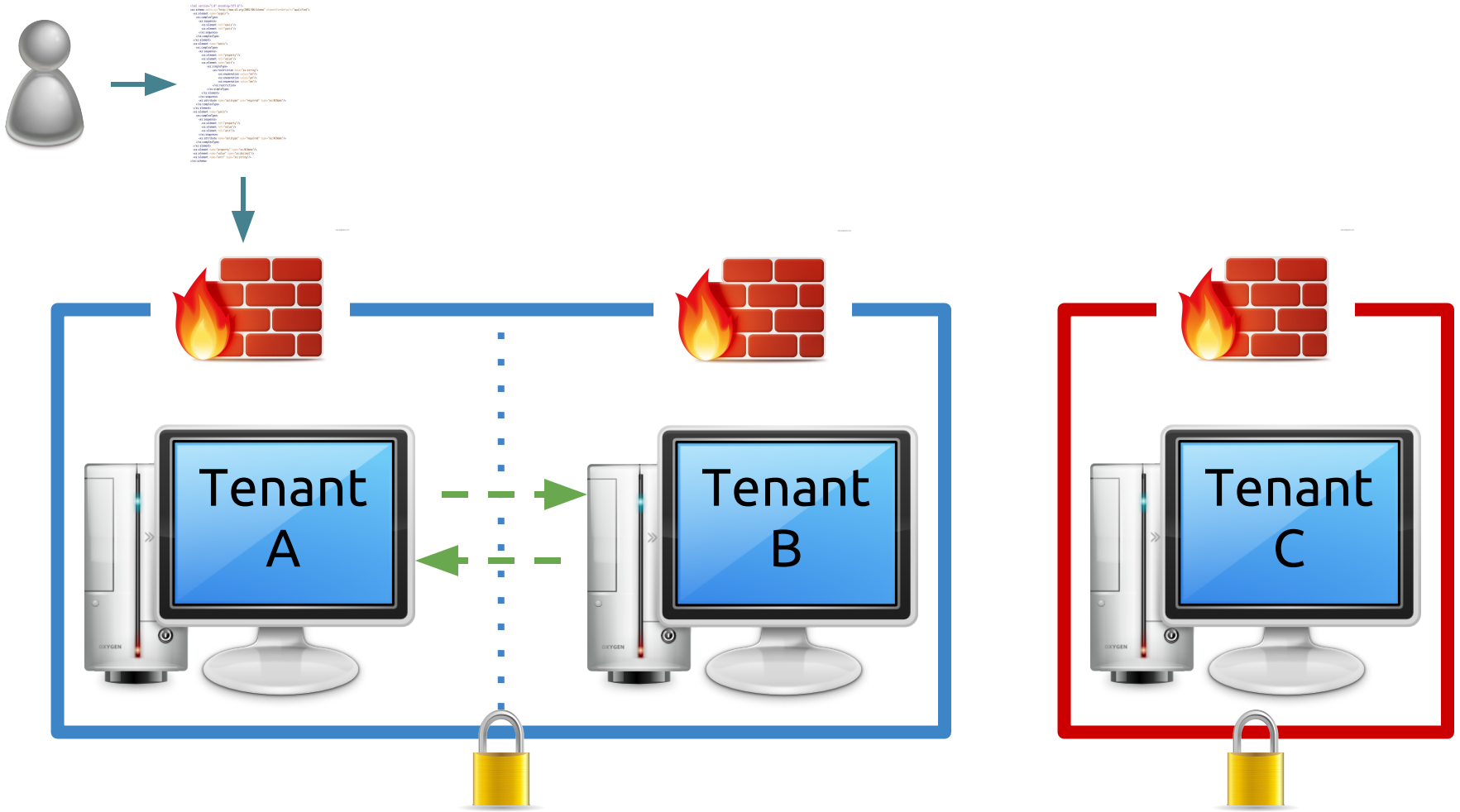
extra overhead

prone to error

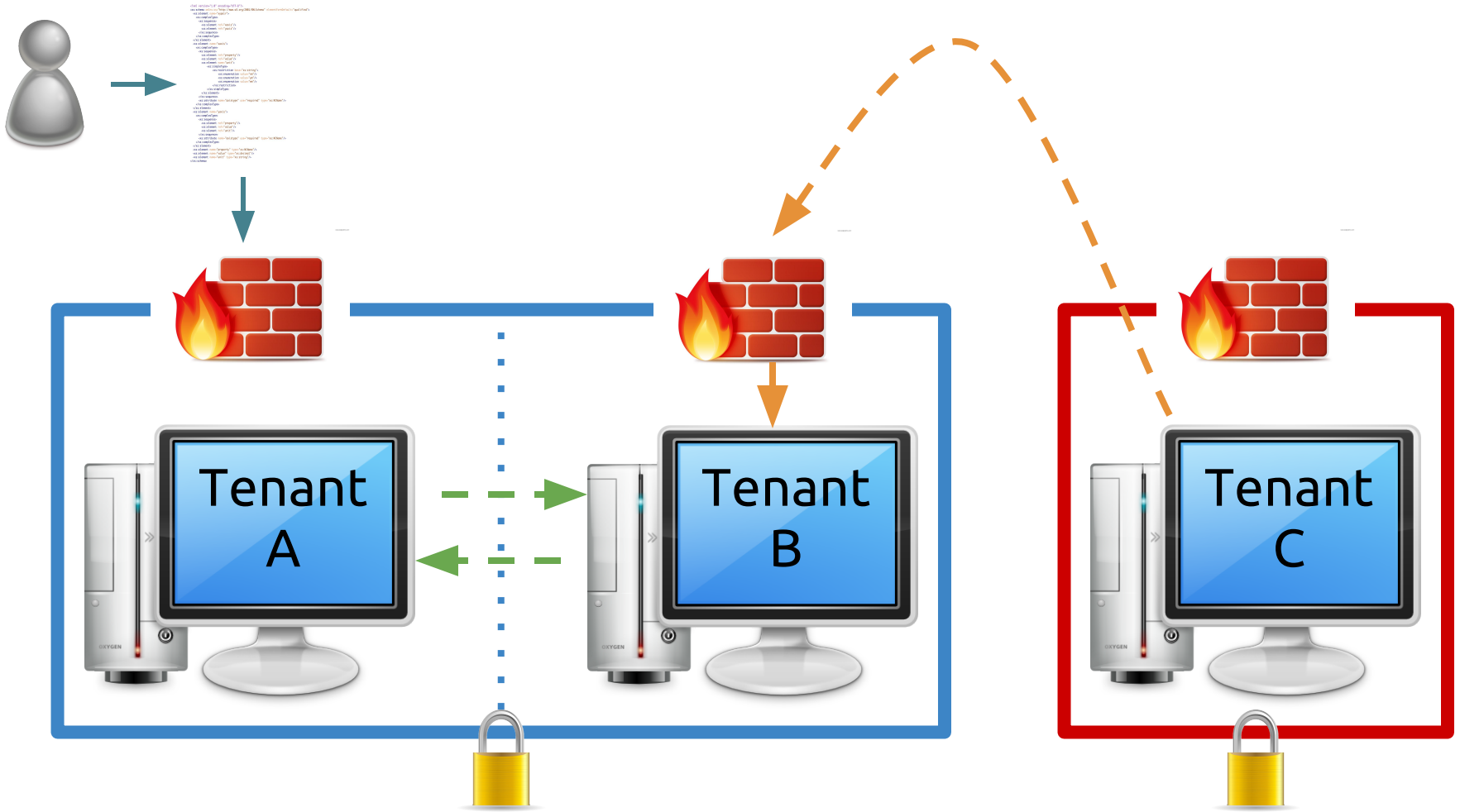
untapped potential



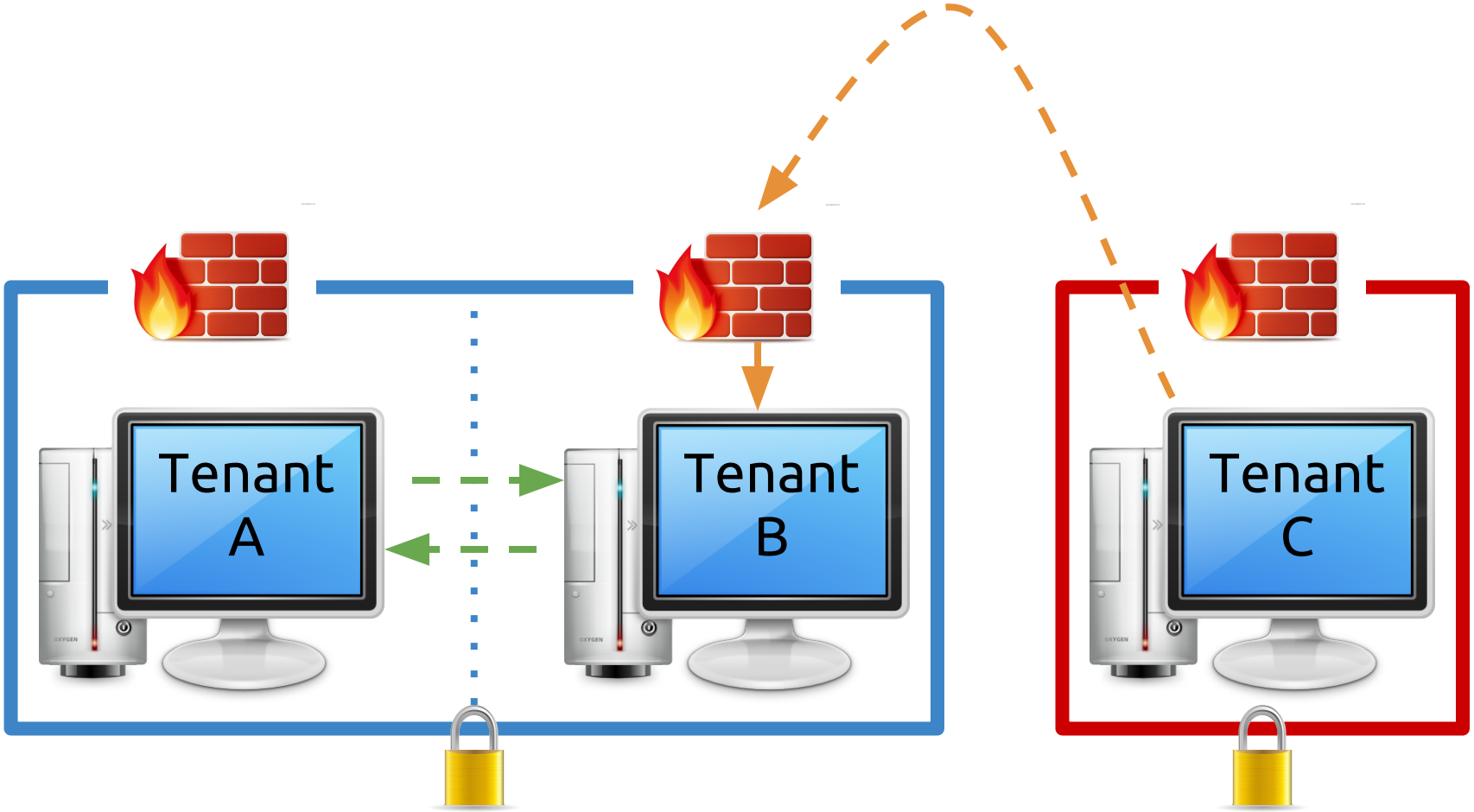
optimize trusted traffic



optimize trusted traffic while filtering untrusted traffic



automatically



Jobber

a **dynamic network security architecture**

designed to handle the

volatile nature of the cloud

and the desire for

optimized inter-tenant communication

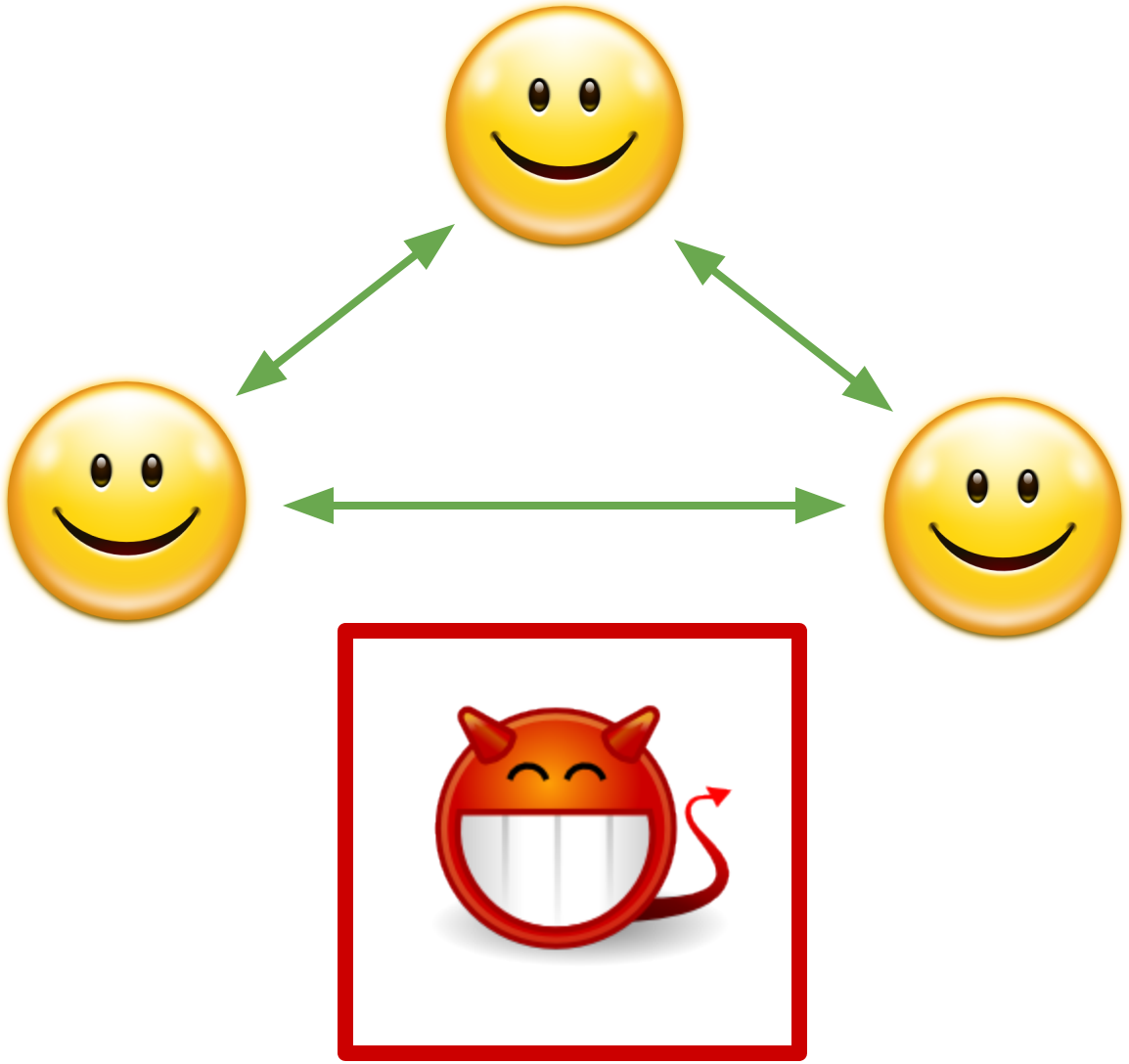
Jobber Components

How can we

securely

designate trusted and untrusted traffic?

trust networks



Introduction Based Routing*

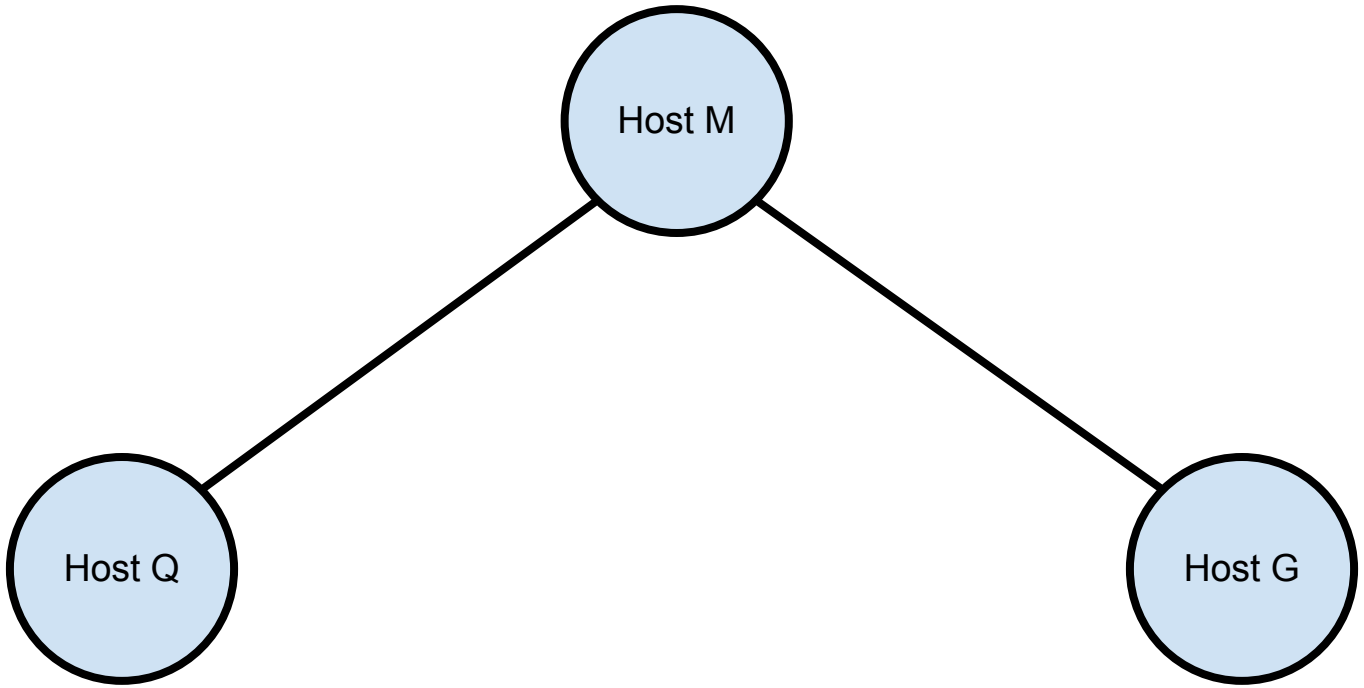
Social Relationships

Behavioral Reputation

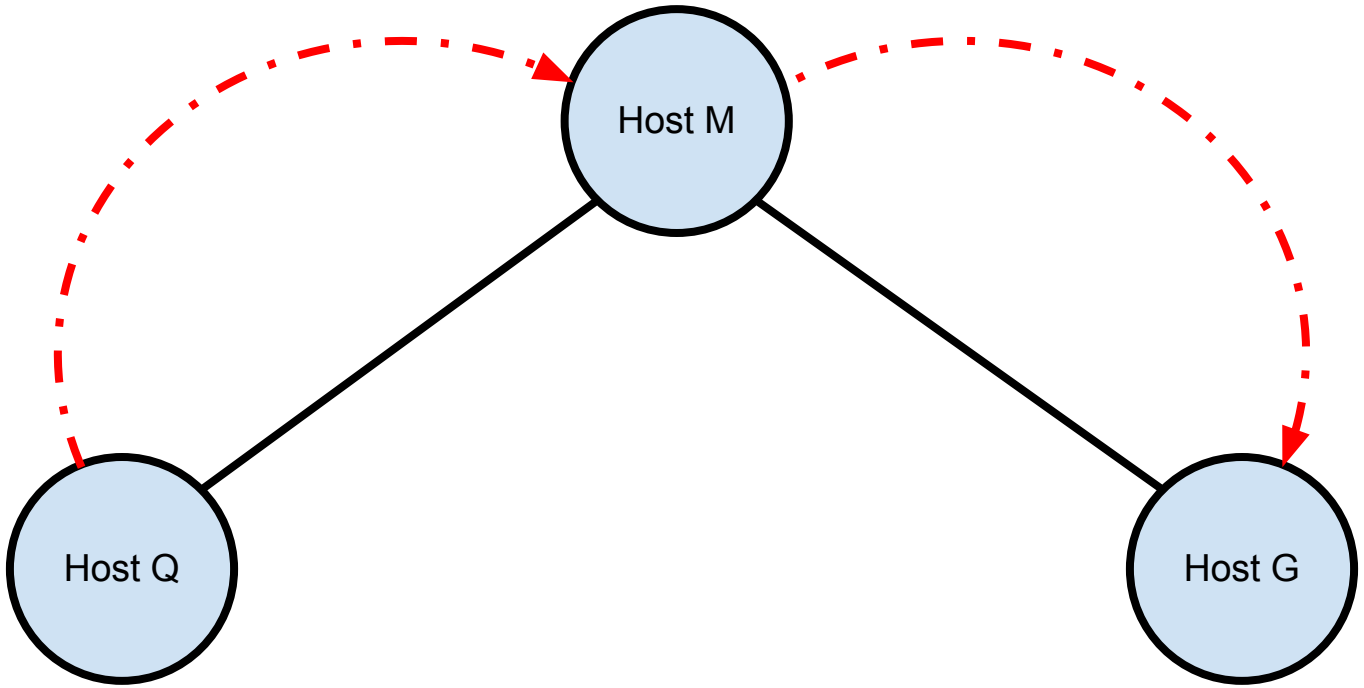
...

* FRAZIER, G., DUONG, Q., WELLMAN, M., AND PETERSEN, E. Incentivizing responsible networking via introduction-based routing. Trust and Trustworthy Computing 6740 (2011).

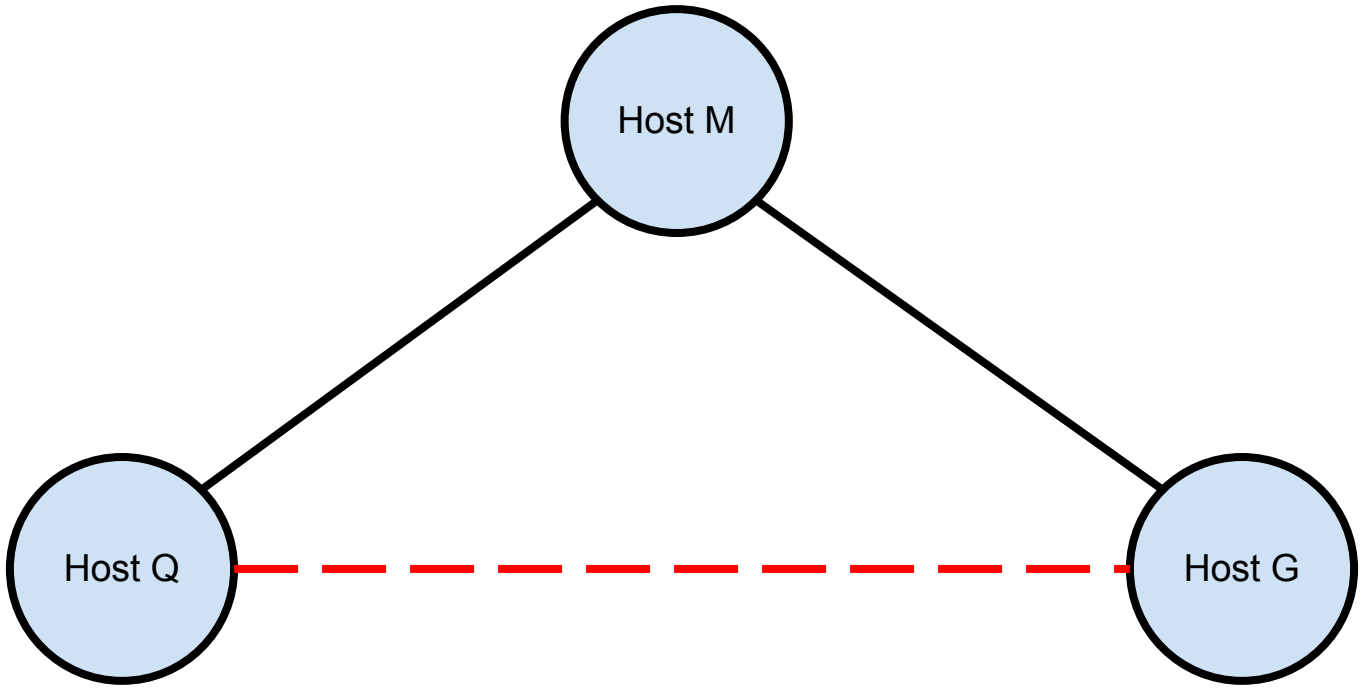
Introduction Based Routing



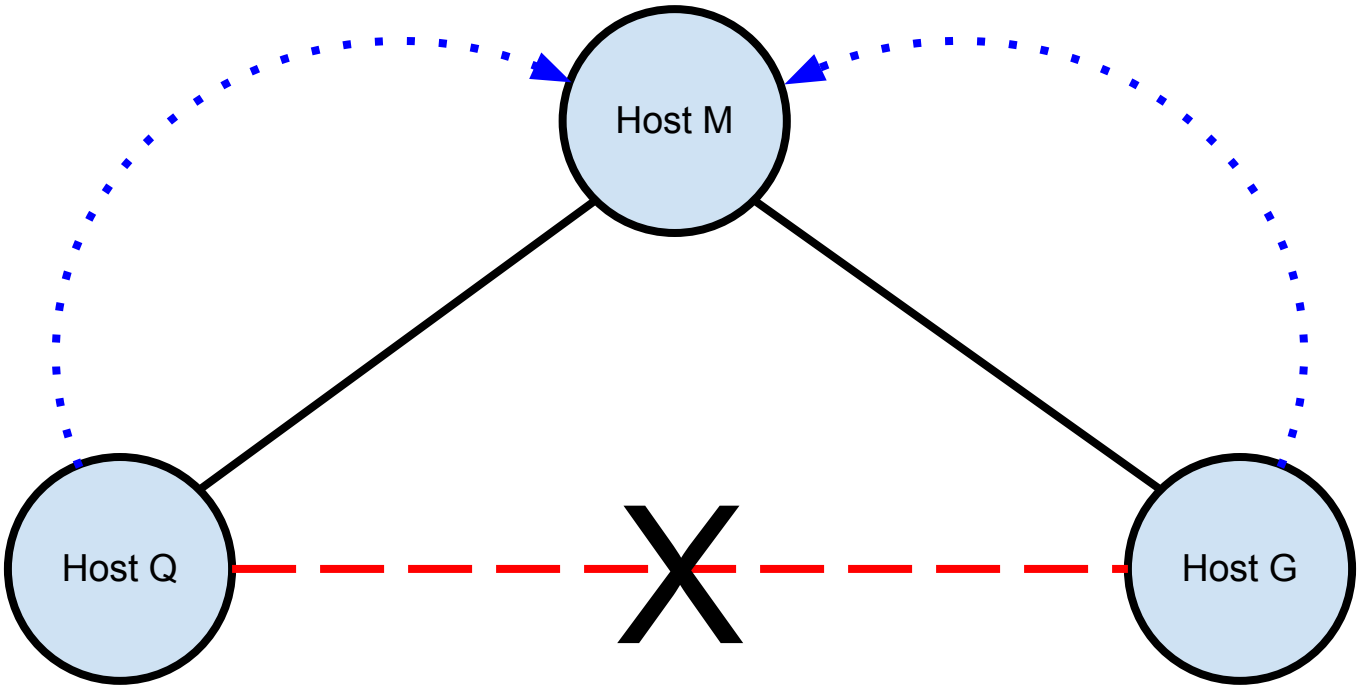
Introduction Based Routing



Introduction Based Routing



Introduction Based Routing

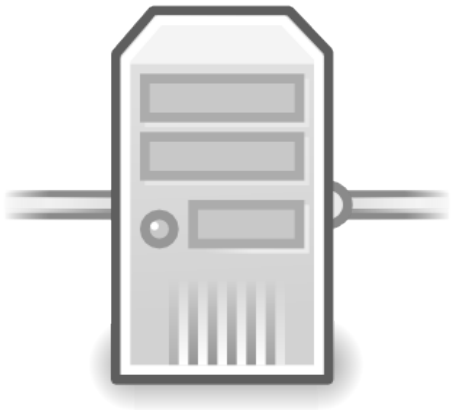


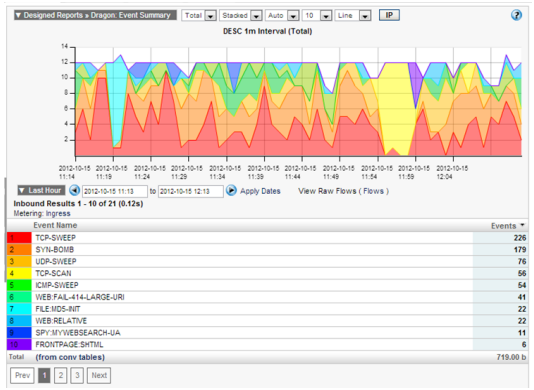
How can we

automatically

ascertain and track reputation?

sensor frameworks

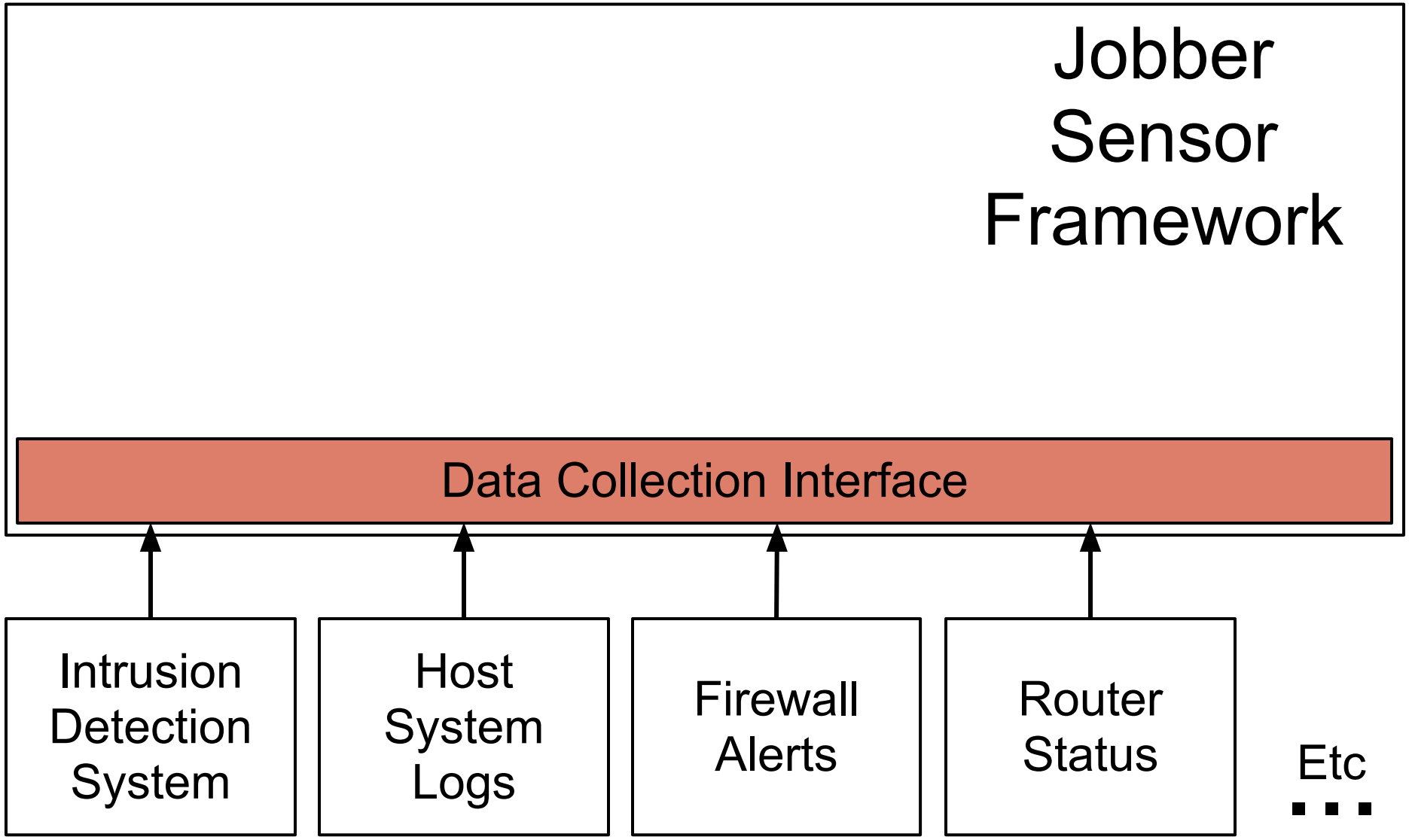


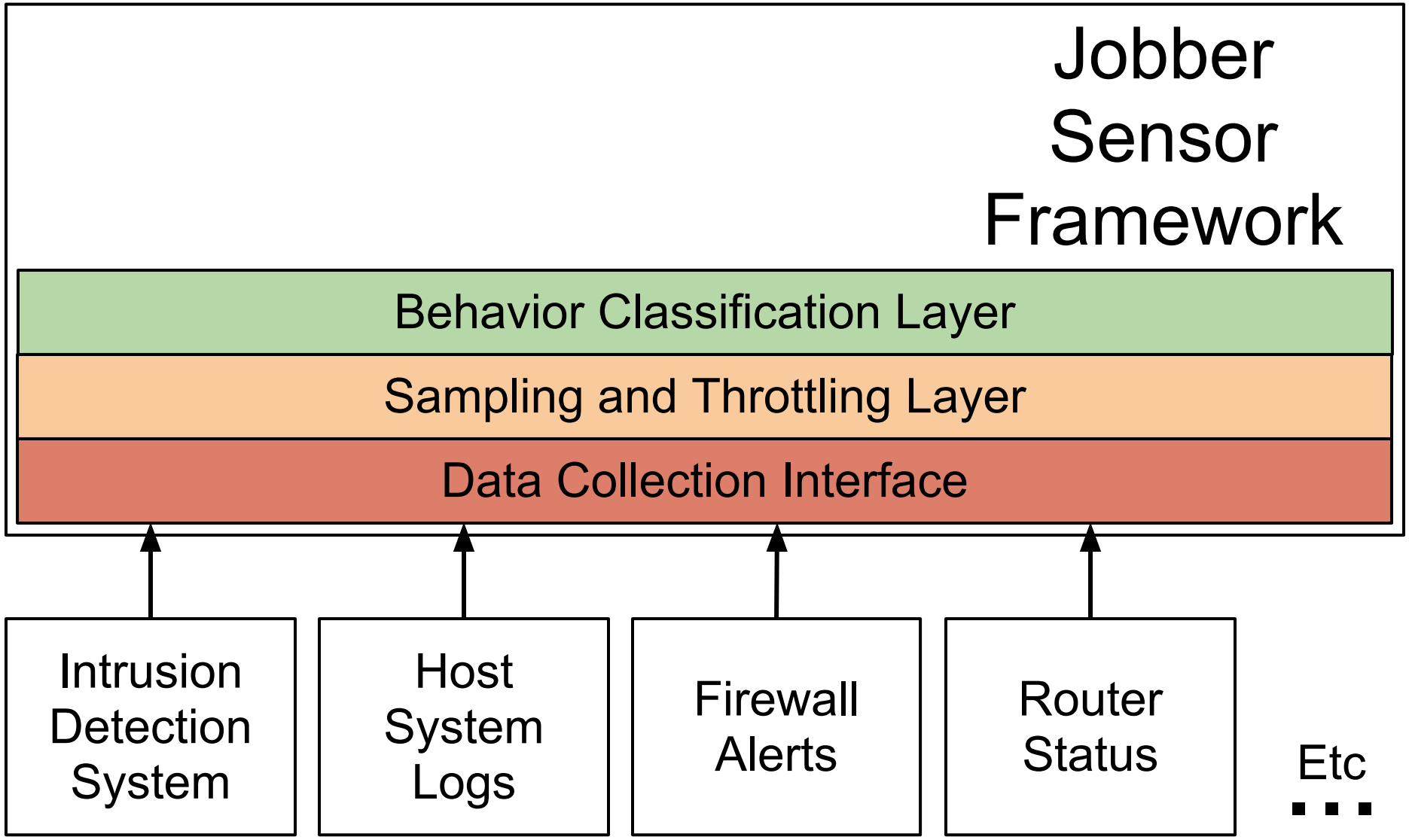


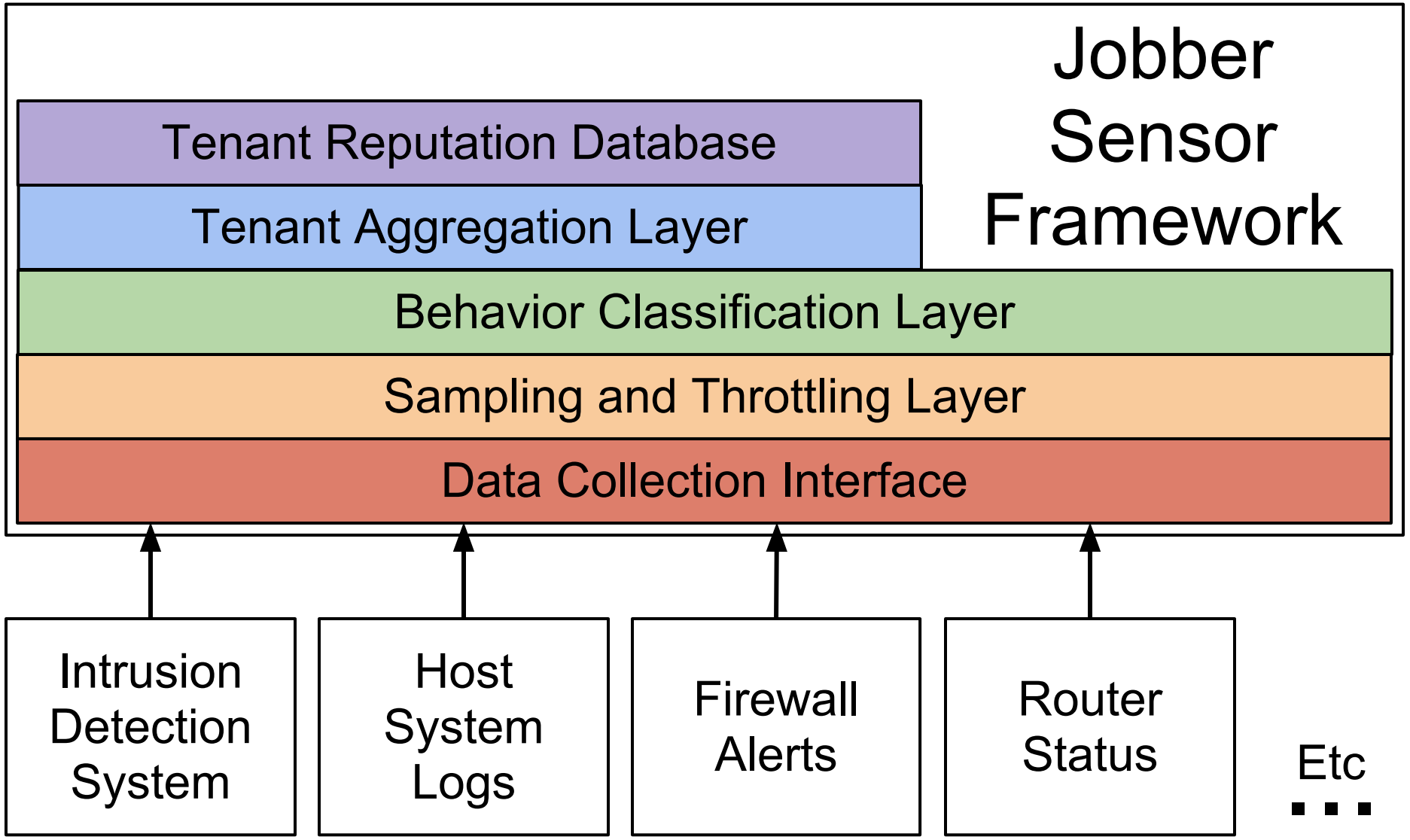
Open Source Frameworks
(nagios, ...)

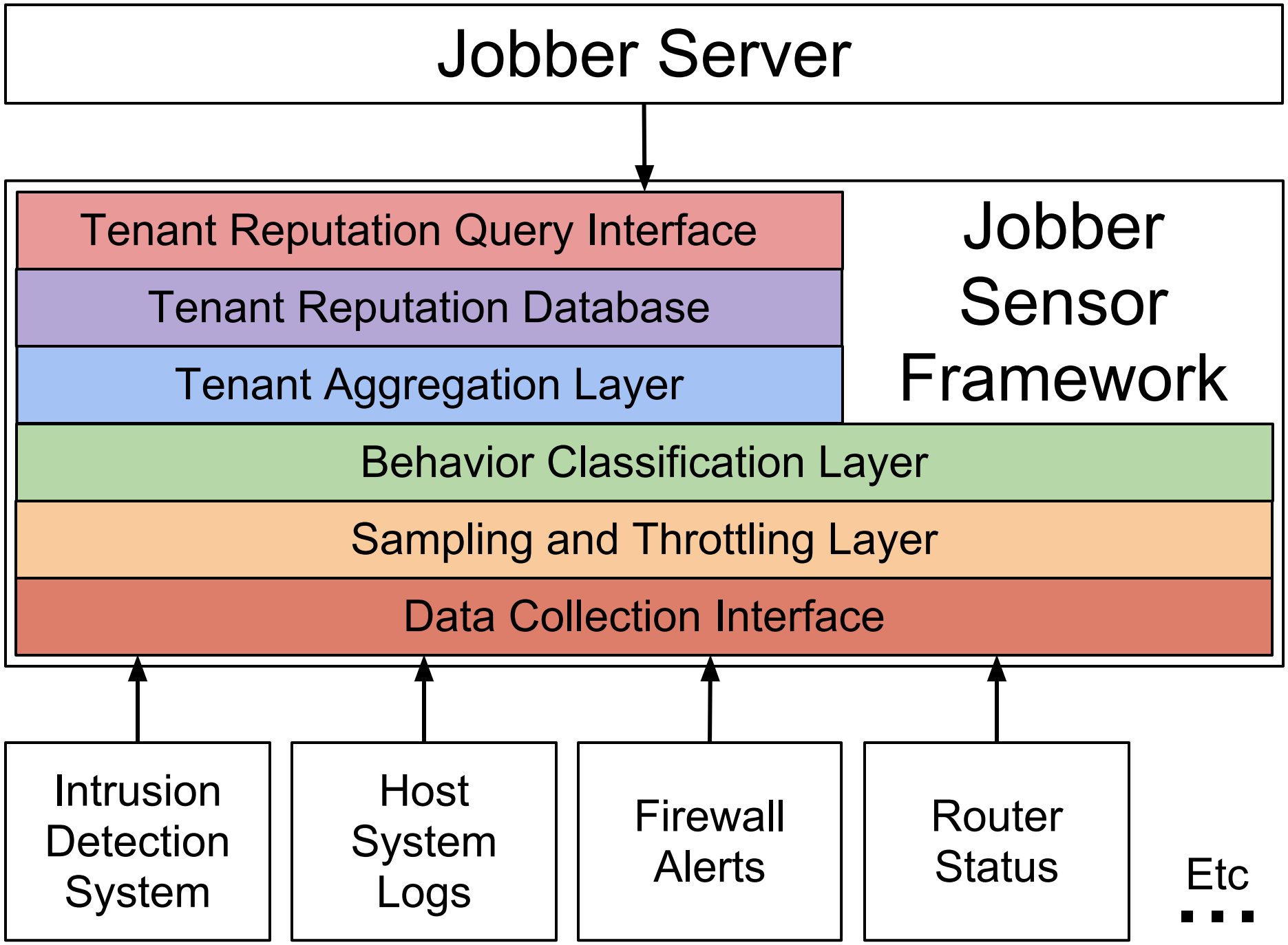
Platform-Specific Frameworks
(Amazon CloudWatch, ...)

Custom Solutions
(Big Data analytic tools, ..)


Jobber
Sensor
Framework
Data Collection Interface
Intrusion
Detection
System
Host
System
Logs
Firewall
Alerts
Router
Status
Etc


Jobber
Sensor
Framework
Behavior Classification Layer
Sampling and Throttling Layer
Data Collection Interface
Intrusion
Detection
System
Host
System
Logs
Firewall
Alerts
Router
Status
Etc
...


Jobber
Sensor
Framework
Tenant Reputation Database
Tenant Aggregation Layer
Behavior Classification Layer
Sampling and Throttling Layer
Data Collection Interface
Intrusion Detection System
Host System Logs
Firewall Alerts
Router Status
Etc
...

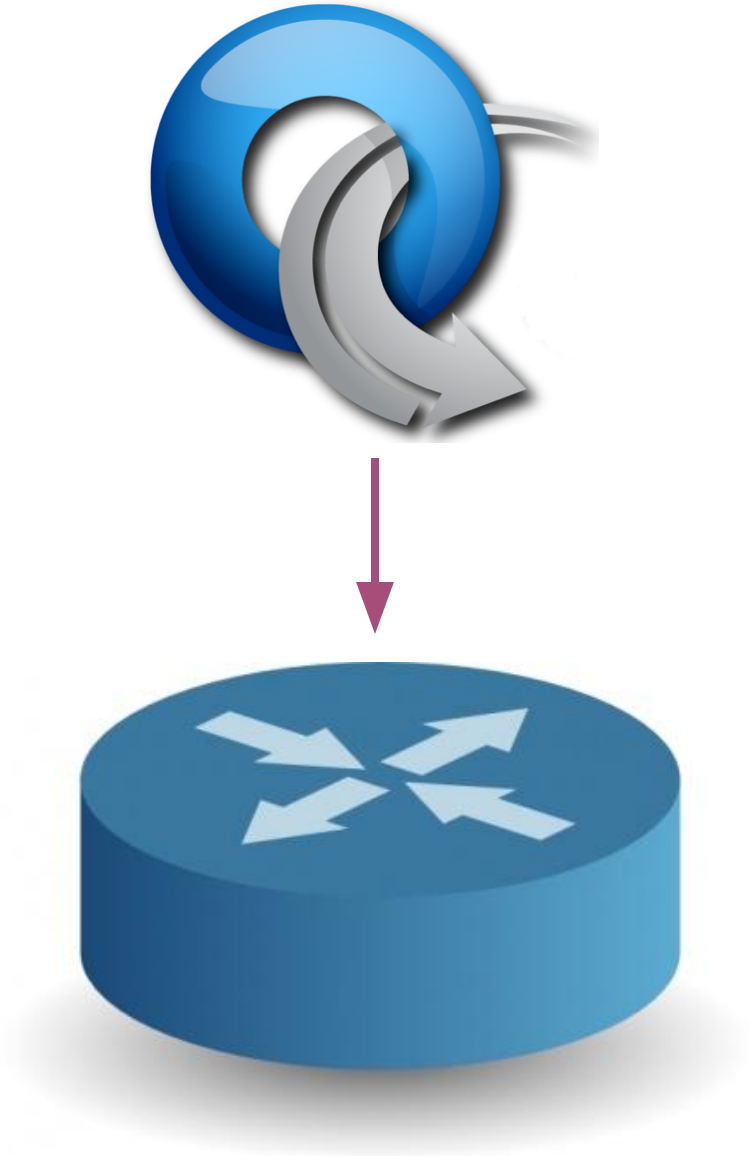

Jobber Server
Tenant Reputation Query Interface
Tenant Reputation Database
Tenant Aggregation Layer
Jobber Sensor Framework
Behavior Classification Layer
Sampling and Throttling Layer
Data Collection Interface
Intrusion Detection System
Host System Logs
Firewall Alerts
Router Status
Etc

How can we

control

network and resource access?

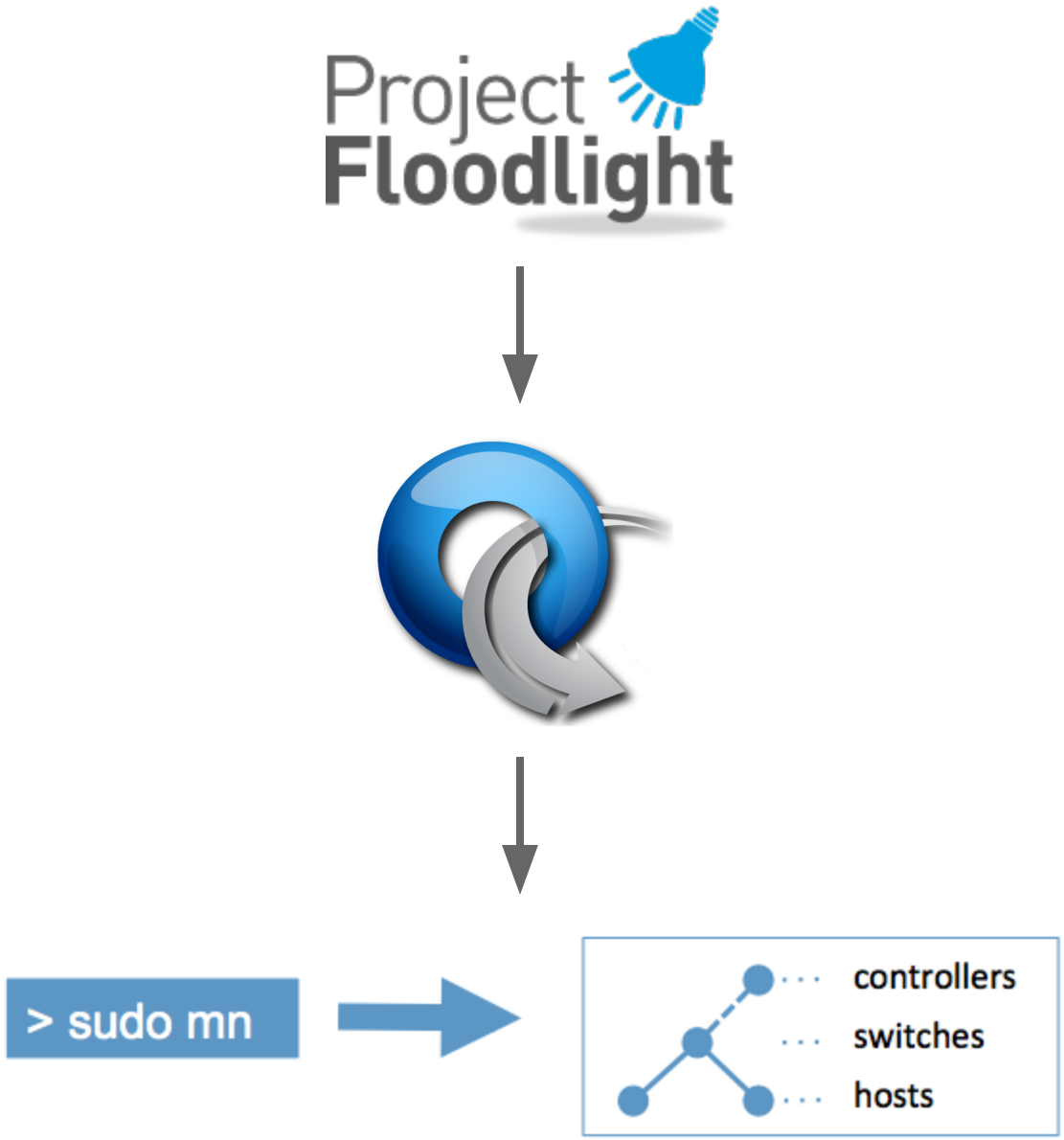
programmable routing



Standardized Interfaces
(OpenFlow, MPLS, GRE, ...)

Cloud Platforms
(EC2, OpenStack, ...)

Vendor Systems
(Cisco, HP, ...)


Project
Floodlight
> sudo mn
controllers
switches
hosts

Jobber Architectures

Data Center

Legacy vs Future

Host

Modified vs Unmodified

Jobber Routing

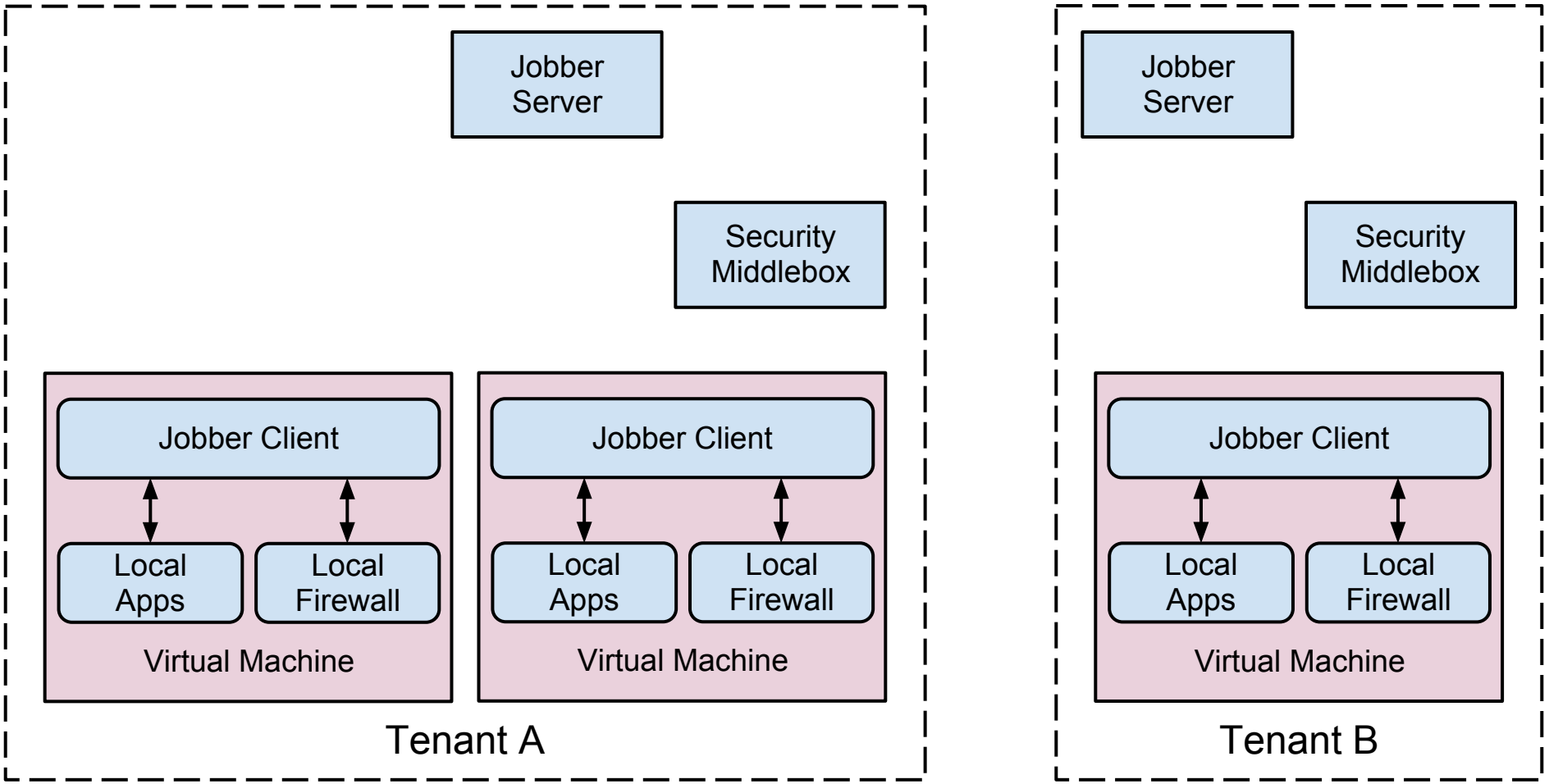
Active vs Passive

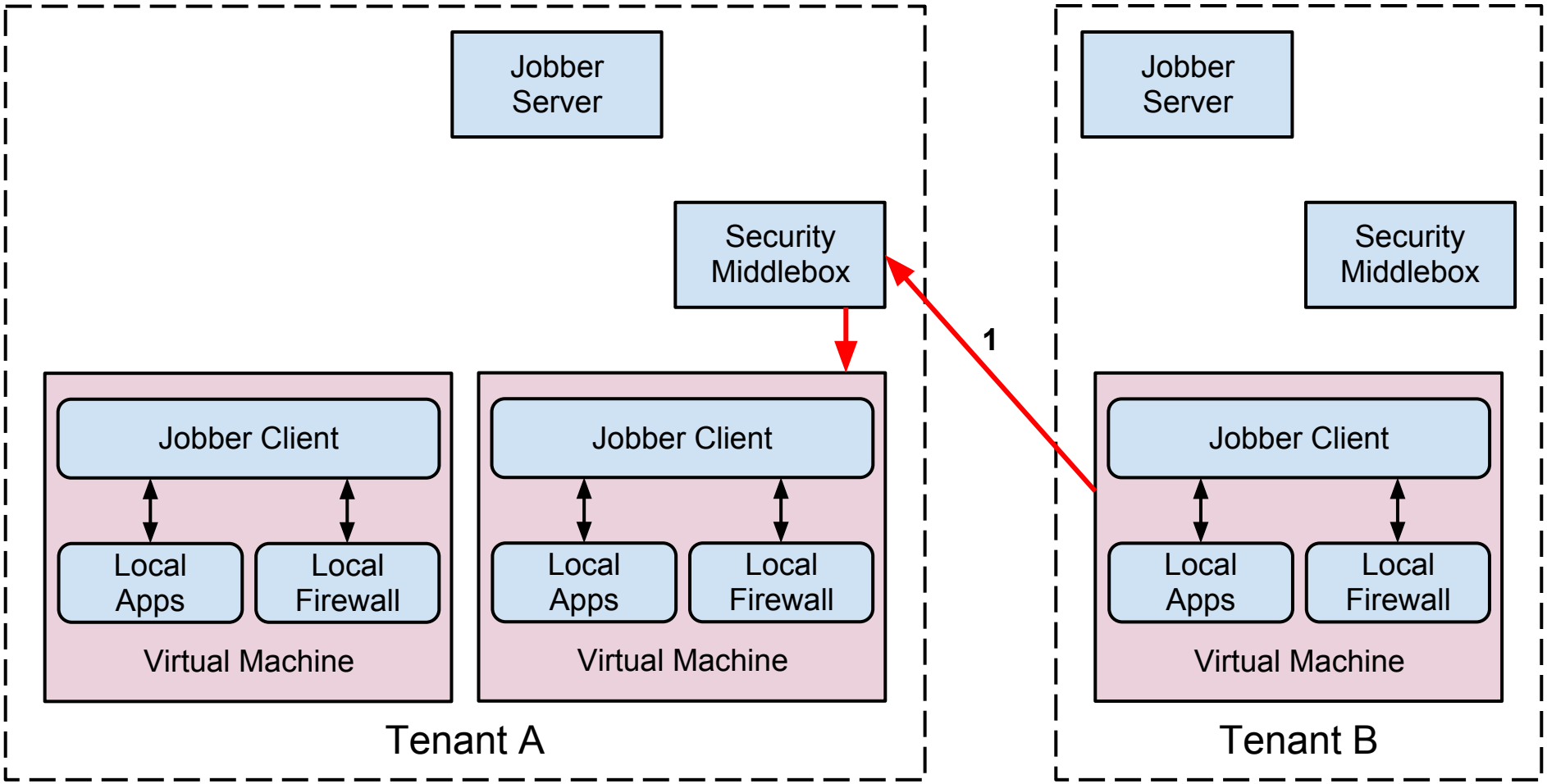
IBR

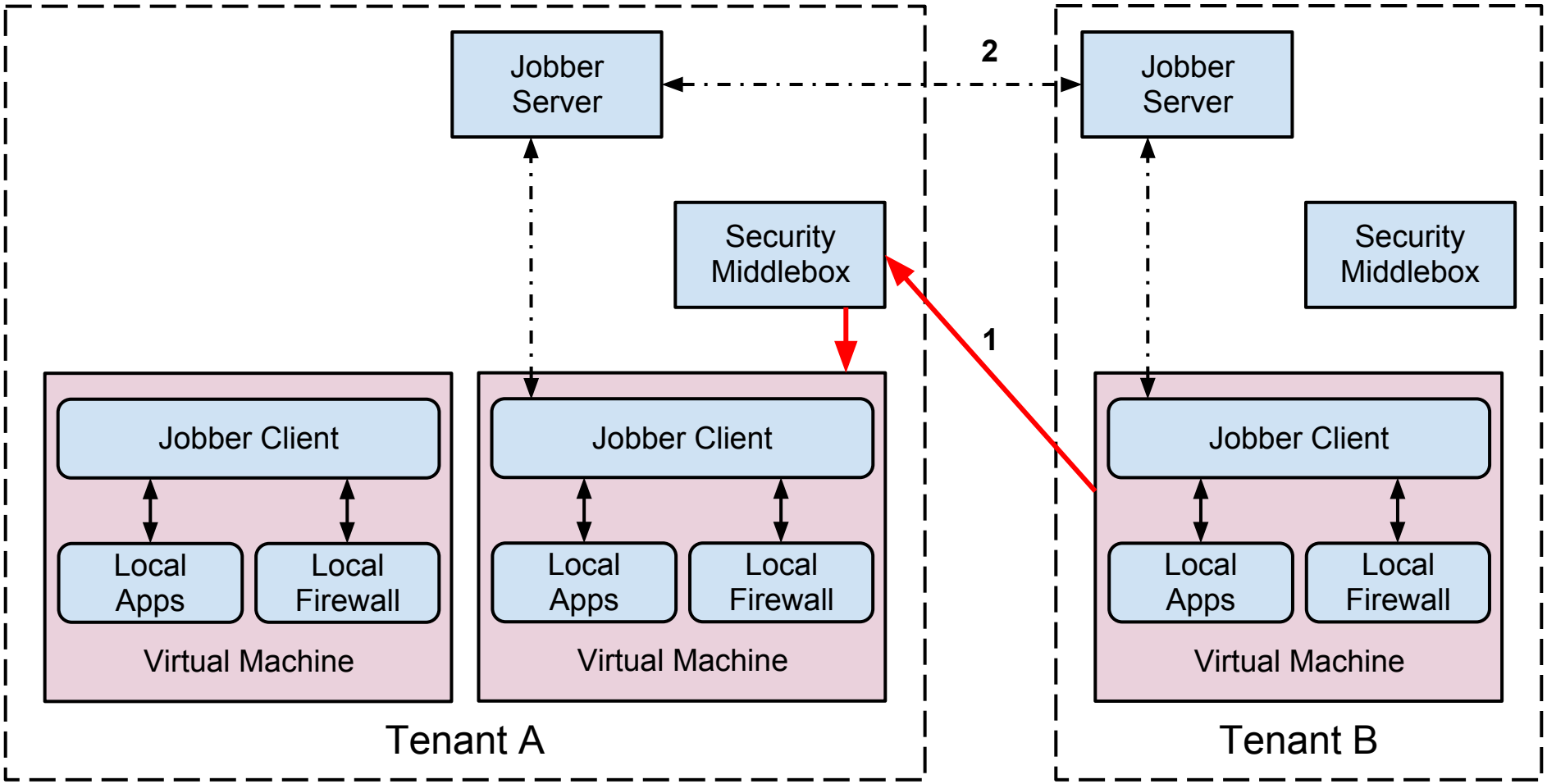
Distributed vs Centralized

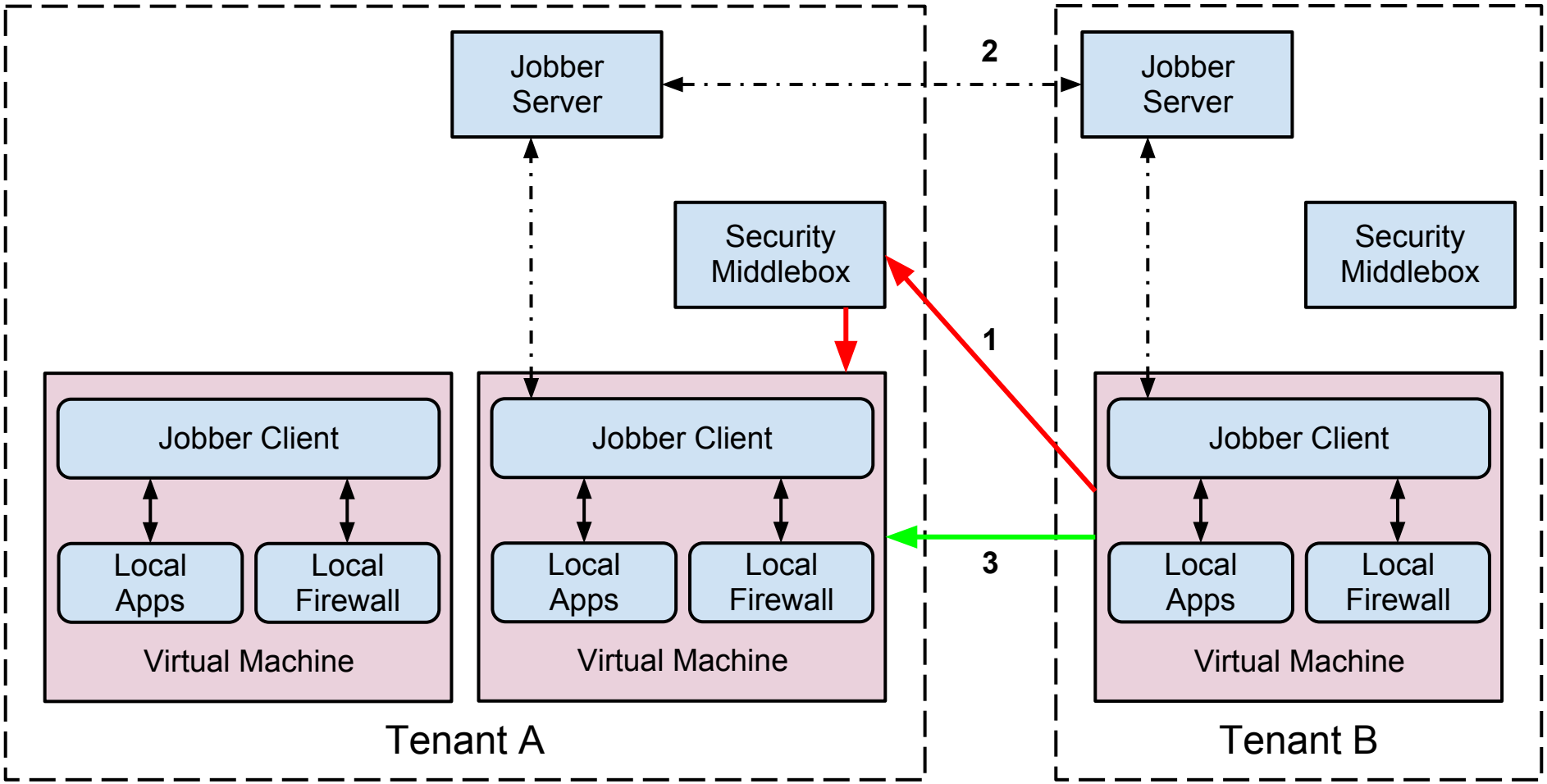
Legacy Data Center

Host Aware


Jobber Server
Security Middlebox
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Tenant A
Jobber Server
Security Middlebox
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Tenant B


Jobber Server
Security Middlebox
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Tenant A
1
Jobber Server
Security Middlebox
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Tenant B

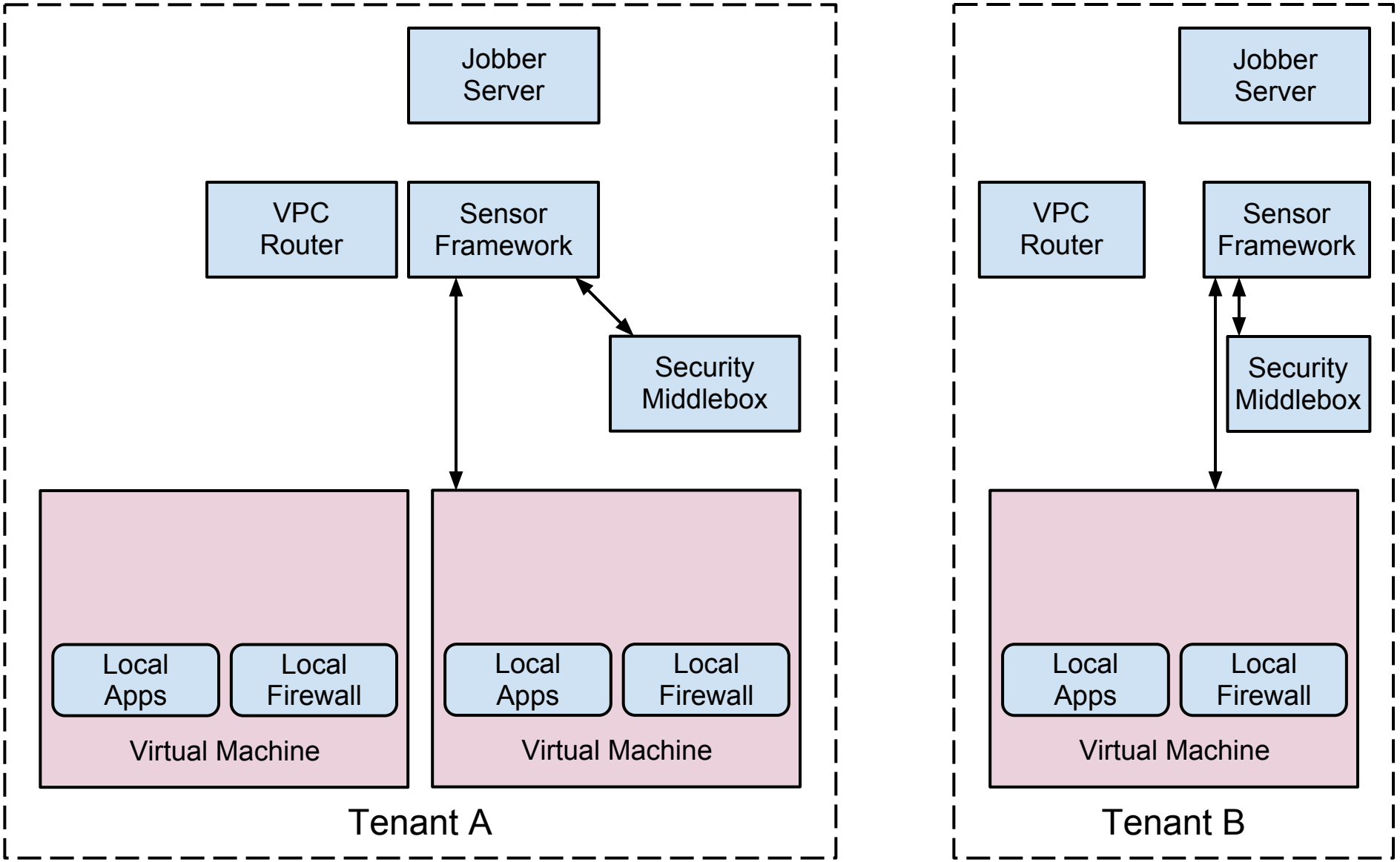

Jobber Server
2
Jobber Server
Security Middlebox
Security Middlebox
1
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Jobber Client
Local Apps
Local Firewall
Virtual Machine
Tenant A
Tenant B

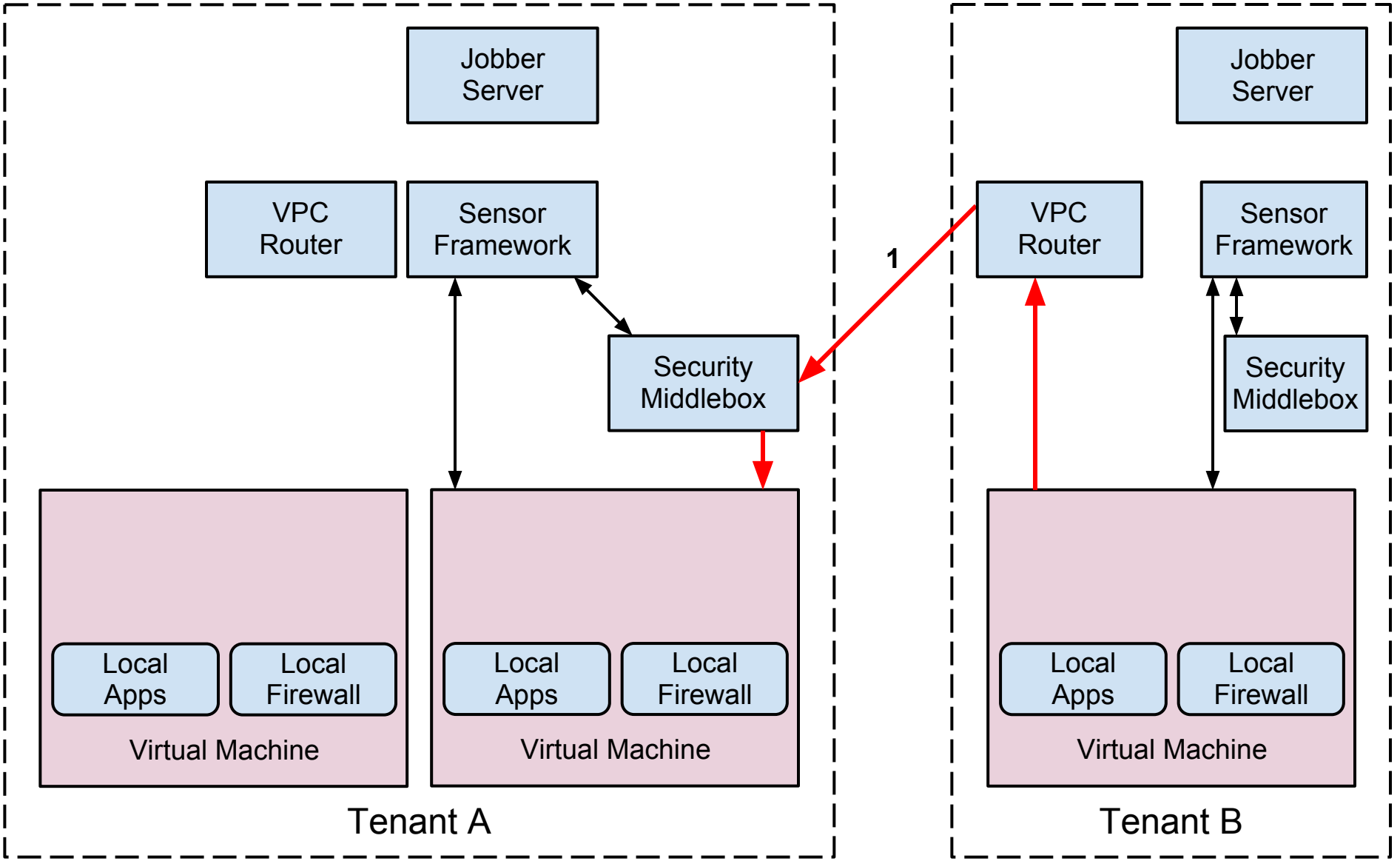

Jobber Server
2
Jobber Server
Security Middlebox
Security Middlebox
1
Jobber Client
Jobber Client
Jobber Client
Local Apps
Local Firewall
Local Apps
Local Firewall
3
Local Apps
Local Firewall
Virtual Machine
Virtual Machine
Virtual Machine
Tenant A
Tenant B

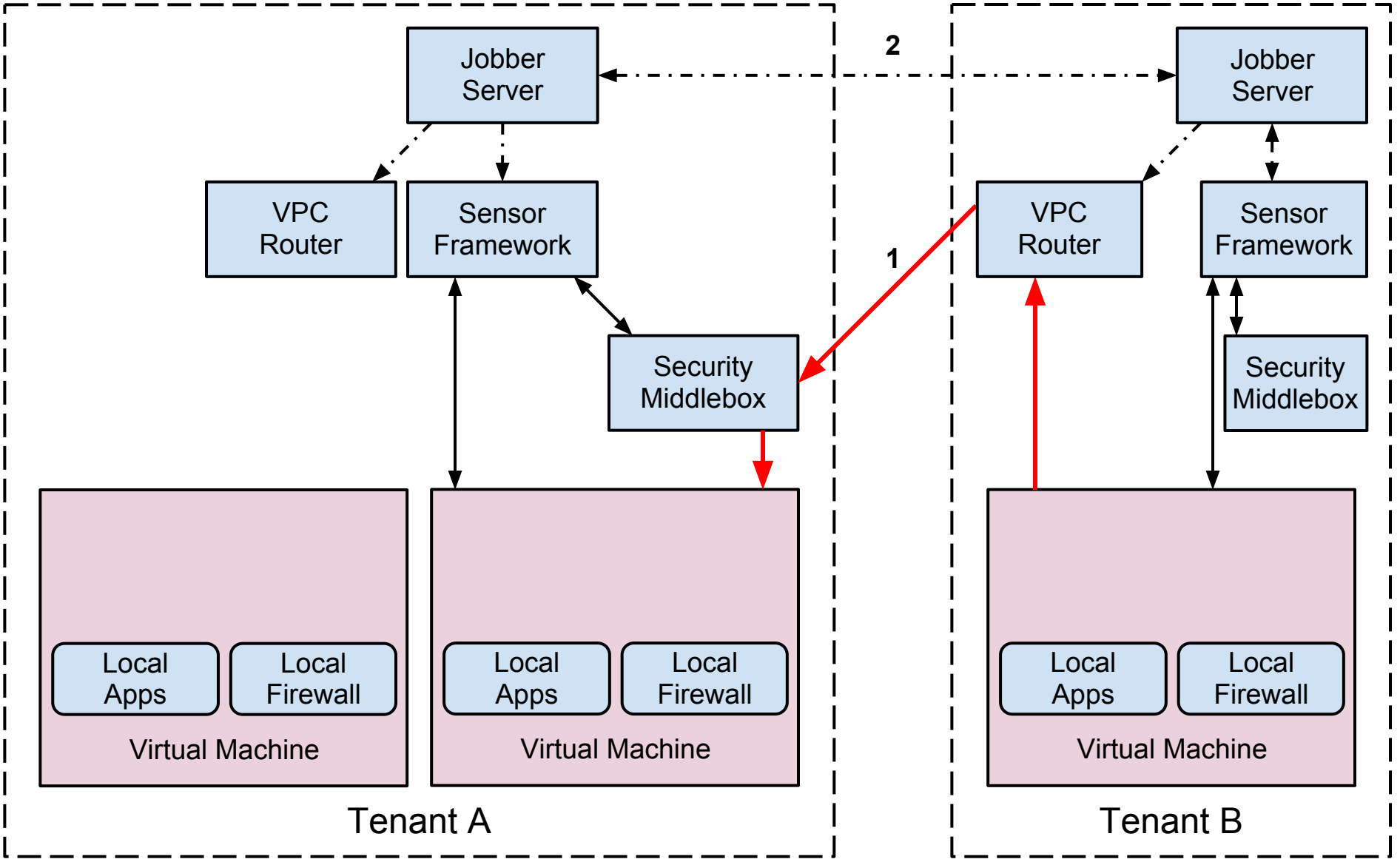
	Legacy *Aware*	Legacy *Agnostic*	SDN *Agnostic*
Deployable Today	Yes		
Unmodified Host	No		
Passive Routing	No		
Central IBR Coordination	No		

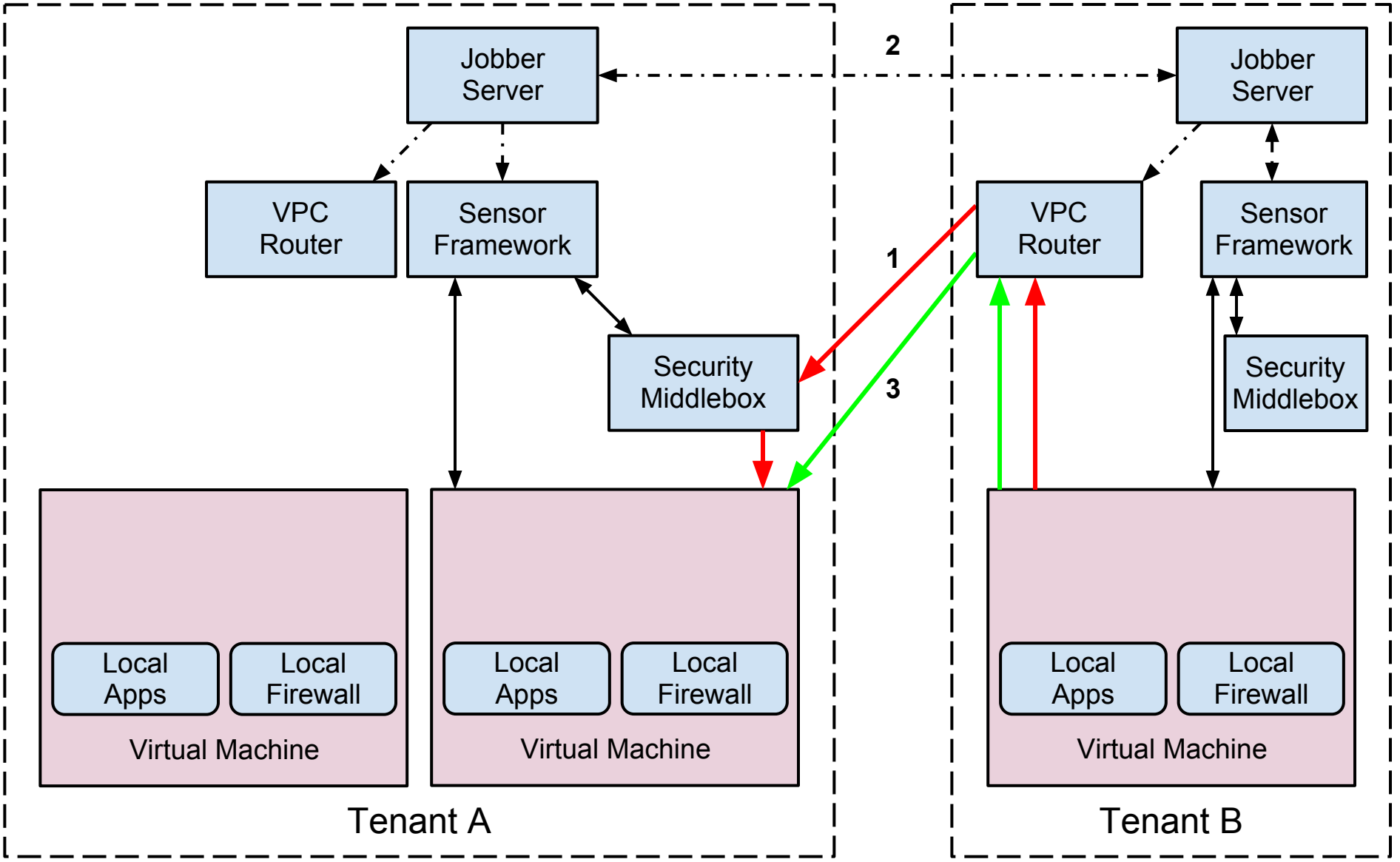
Legacy Data Center

Host Unaware


Jobber Server
VPC Router
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Jobber Server
VPC Router
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Tenant B


Jobber Server
VPC Router
Sensor Framework
Security Middlebox
1
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Jobber Server
VPC Router
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Tenant B

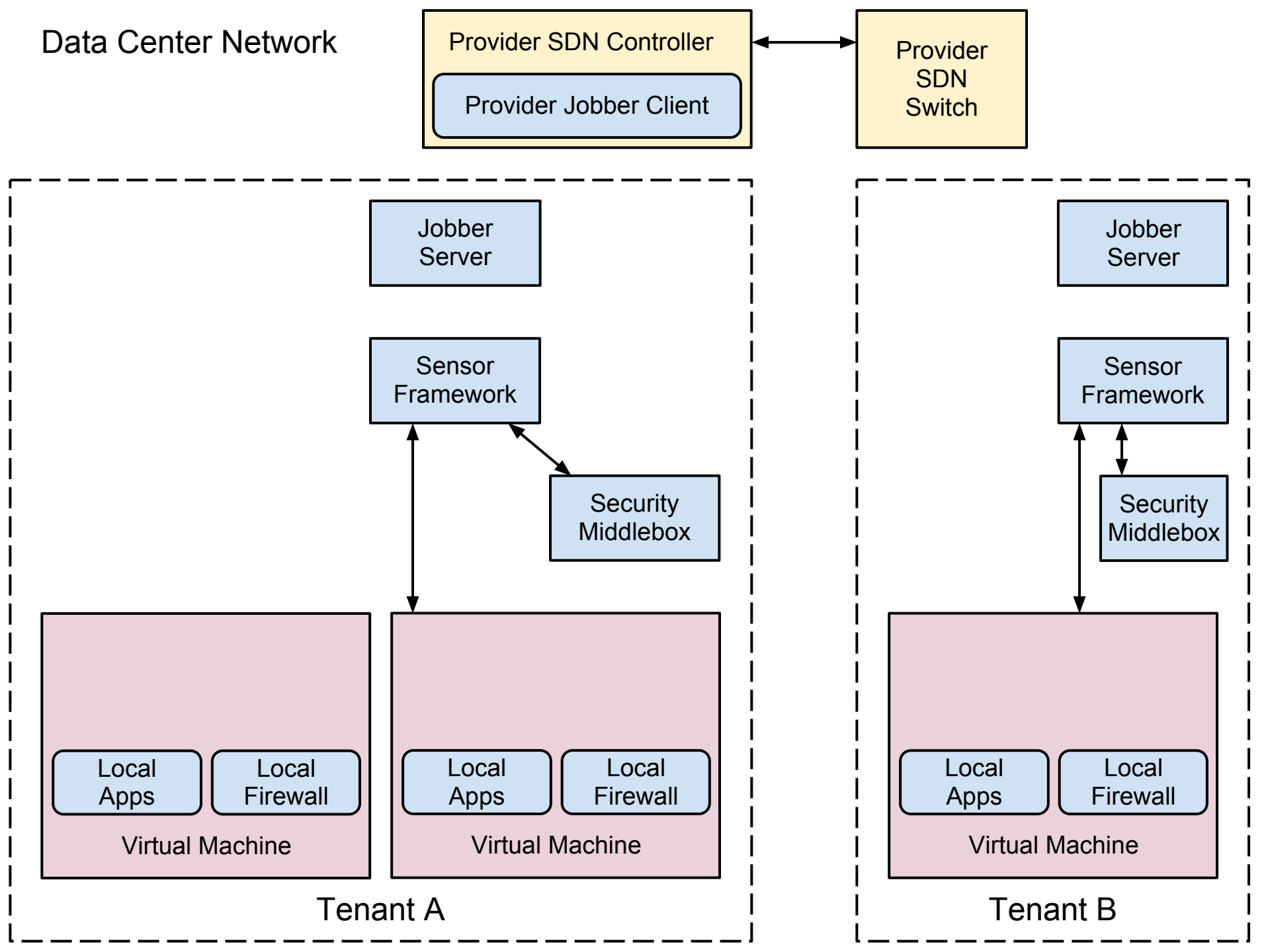

Jobber Server
2
Jobber Server
VPC Router
Sensor Framework
1
VPC Router
Sensor Framework
Security Middlebox
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Tenant B

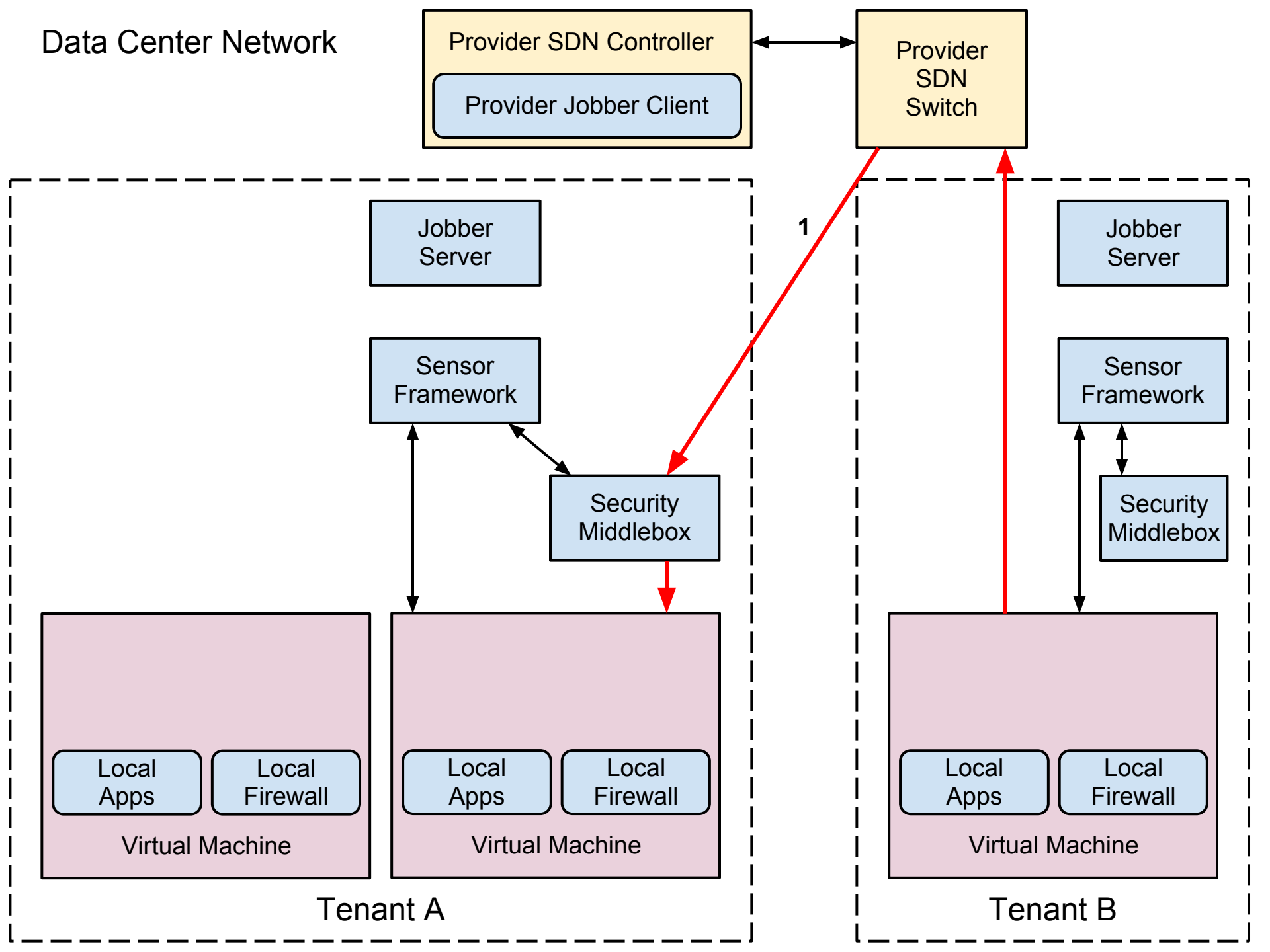

Jobber Server
2
Jobber Server
VPC Router
Sensor Framework
1
VPC Router
Sensor Framework
Security Middlebox
3
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Tenant B

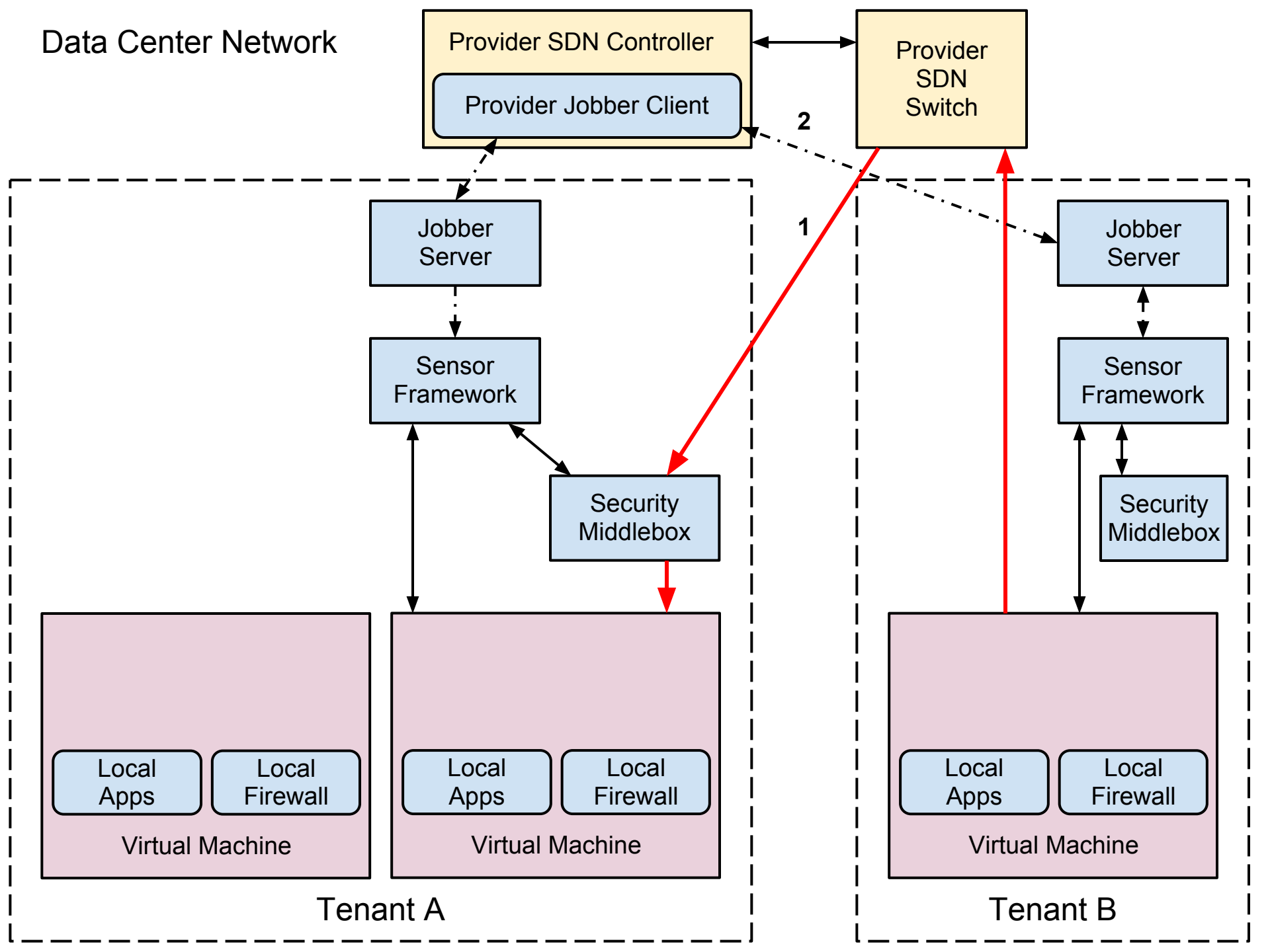
	Legacy *Aware*	Legacy *Agnostic*	SDN *Agnostic*
Deployable Today	Yes	Yes	
Unmodified Host	No	Yes	
Passive Routing	No	No	
Central IBR Coordination	No	No	

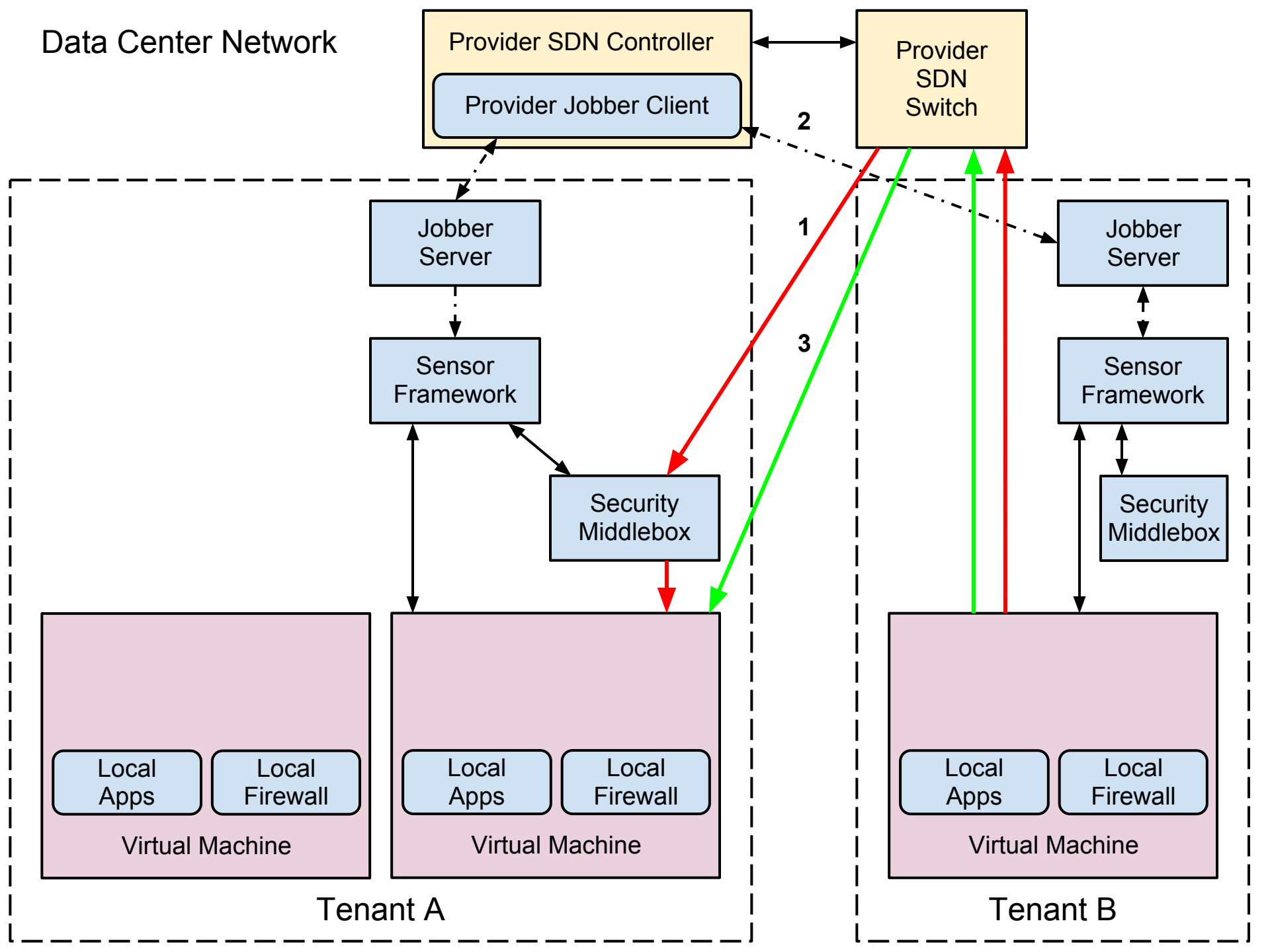
SDN Data Center

Host Unaware


Data Center Network
Provider SDN Controller
Provider Jobber Client
Provider SDN Switch
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Tenant B


Data Center Network
Provider SDN Controller
Provider Jobber Client
Provider SDN Switch
1
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Tenant B


Data Center Network
Provider SDN Controller
Provider Jobber Client
Provider SDN Switch
2
1
Jobber Server
Sensor Framework
Security Middlebox
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Tenant B


Data Center Network
Provider SDN Controller
Provider Jobber Client
Provider SDN Switch
2
1
3
Jobber Server
Sensor Framework
Security Middlebox
Jobber Server
Sensor Framework
Security Middlebox
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Local Apps
Local Firewall
Virtual Machine
Tenant A
Tenant B

	Legacy *Aware*	Legacy *Agnostic*	SDN *Agnostic*
Deployable Today	Yes	Yes	No
Unmodified Host	No	Yes	Yes
Passive Routing	No	No	Yes
Central IBR Coordination	No	No	Yes

Current Status

Complete

Multi-Architecture Design

Proof-of-concept Prototype

In Progress

Full-system Prototype for SDN Arch.

Partial Prototypes for Legacy Archs.

To Do

Performance Analysis & Evaluation

Usability Analysis & Evaluation

How can we make the datacenter...

more efficient?

more secure?

more manageable?

Jobber Provides...

efficiency

via direct inter-tenant communication

security

via introduction-based-routing

manageability

via automatic network control

Questions

Graduated or Binary Trust Designations?

Acceptable Overhead?
Performance Requirements?

Best Architecture?

Jobber as a Service?

Economics of IBR?