A Proposal of Access Control Mechanism Towards User-dedicated PRAGMA-ENT for IoT Era

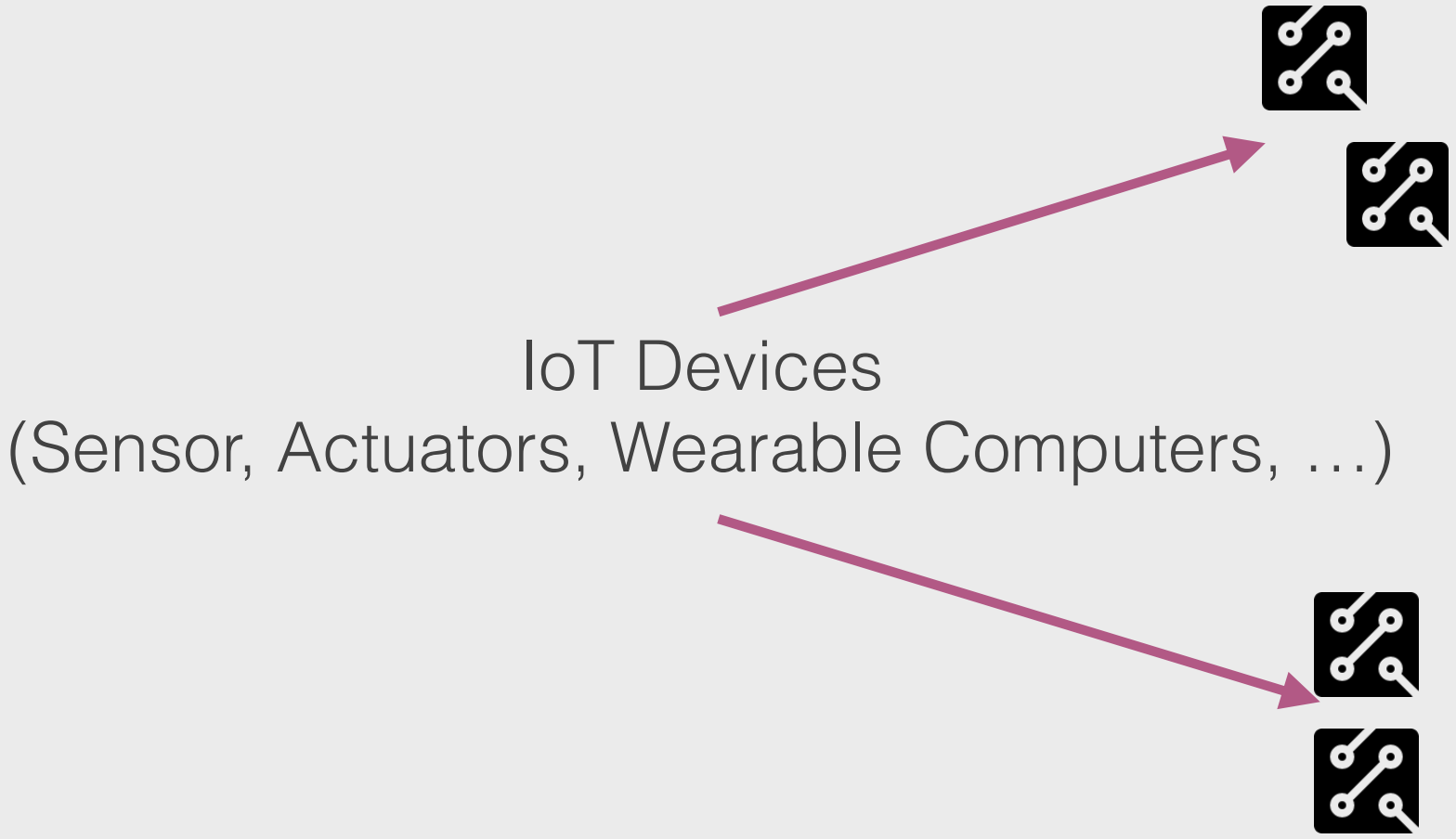
Takuya Yamada[1], Keichi Takahashi[1], Masaya Muraki[2],
Yoshiyuki Kido[3], Susumu Date[3], Shinji Shimojo[3]
[1]Graduate School of Information Science and Technology, Osaka University, Japan
[2]TIS Inc., Japan
[3]Cybermedia Center, Osaka University, Japan

IoT Era

The IoT Era has arrived.

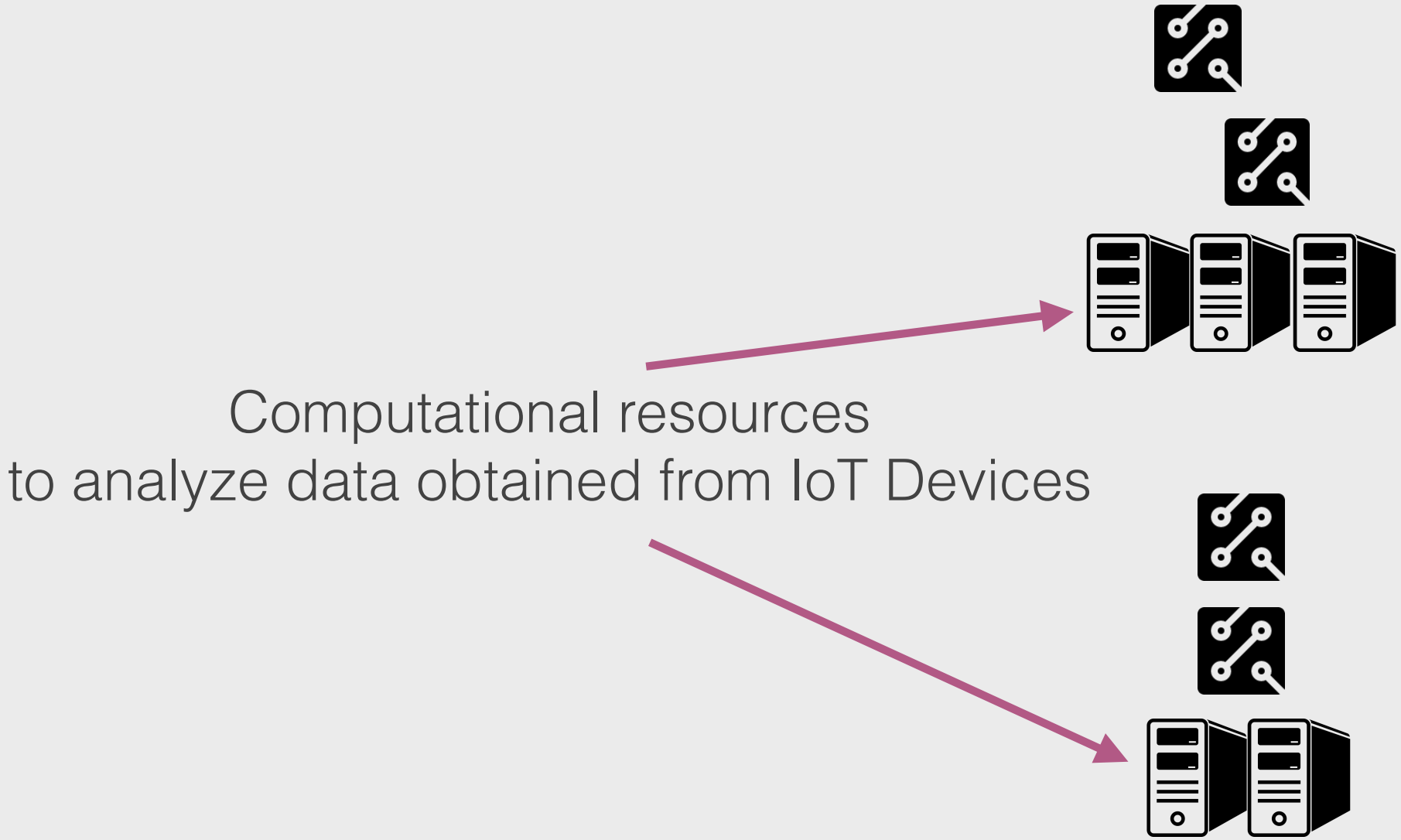
IoT Era

The IoT Era has arrived.



IoT Era

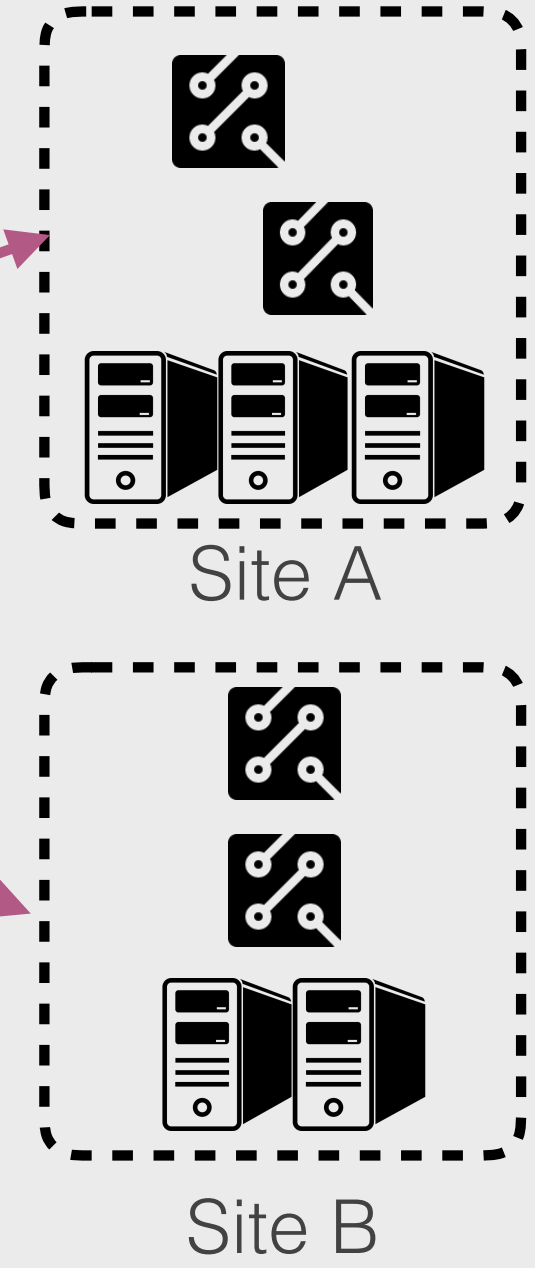
The IoT Era has arrived.



IoT Era

The IoT Era has arrived.

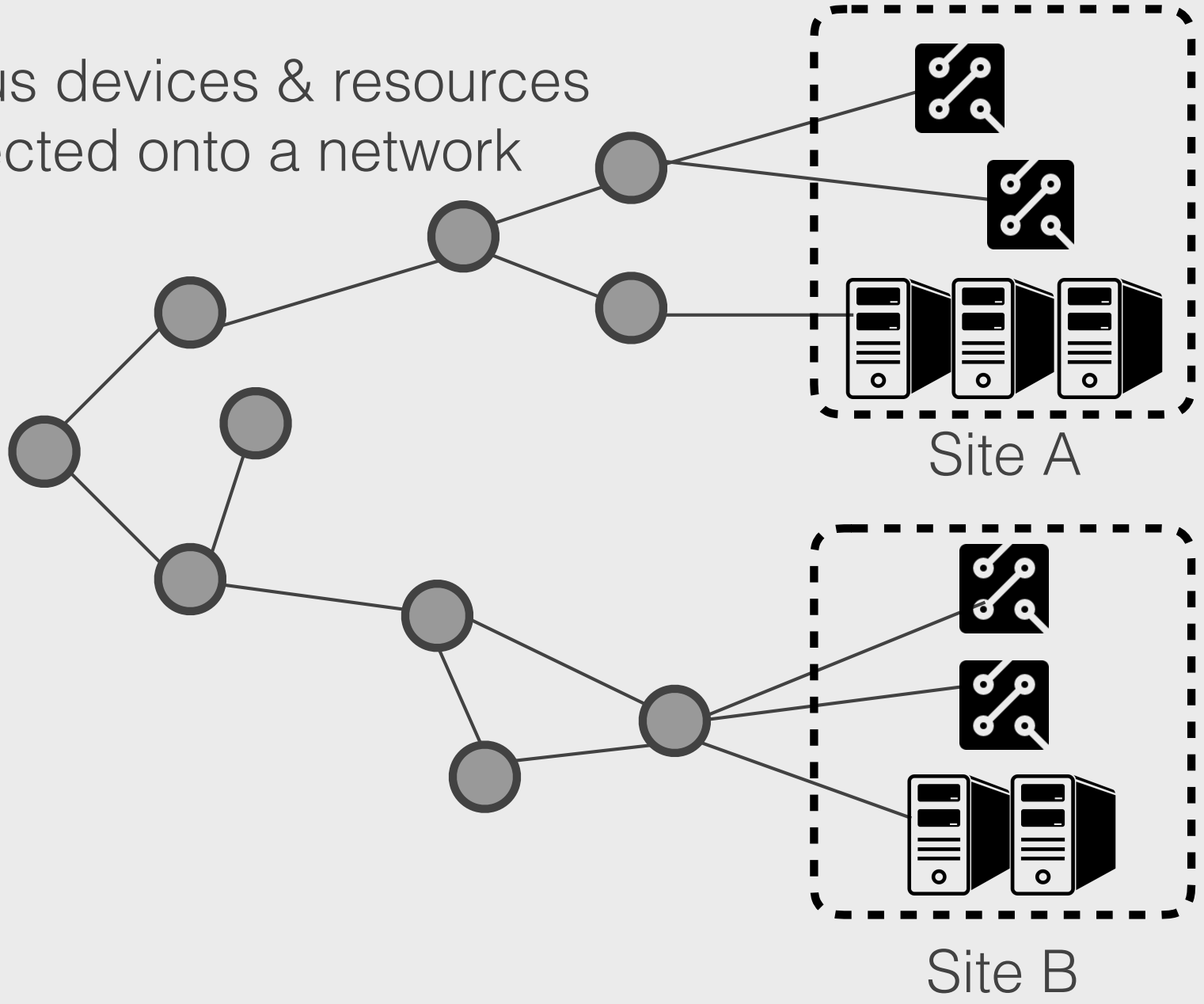
These devices & resources
are distributed spatially to multi-site



IoT Era

The IoT Era has arrived.

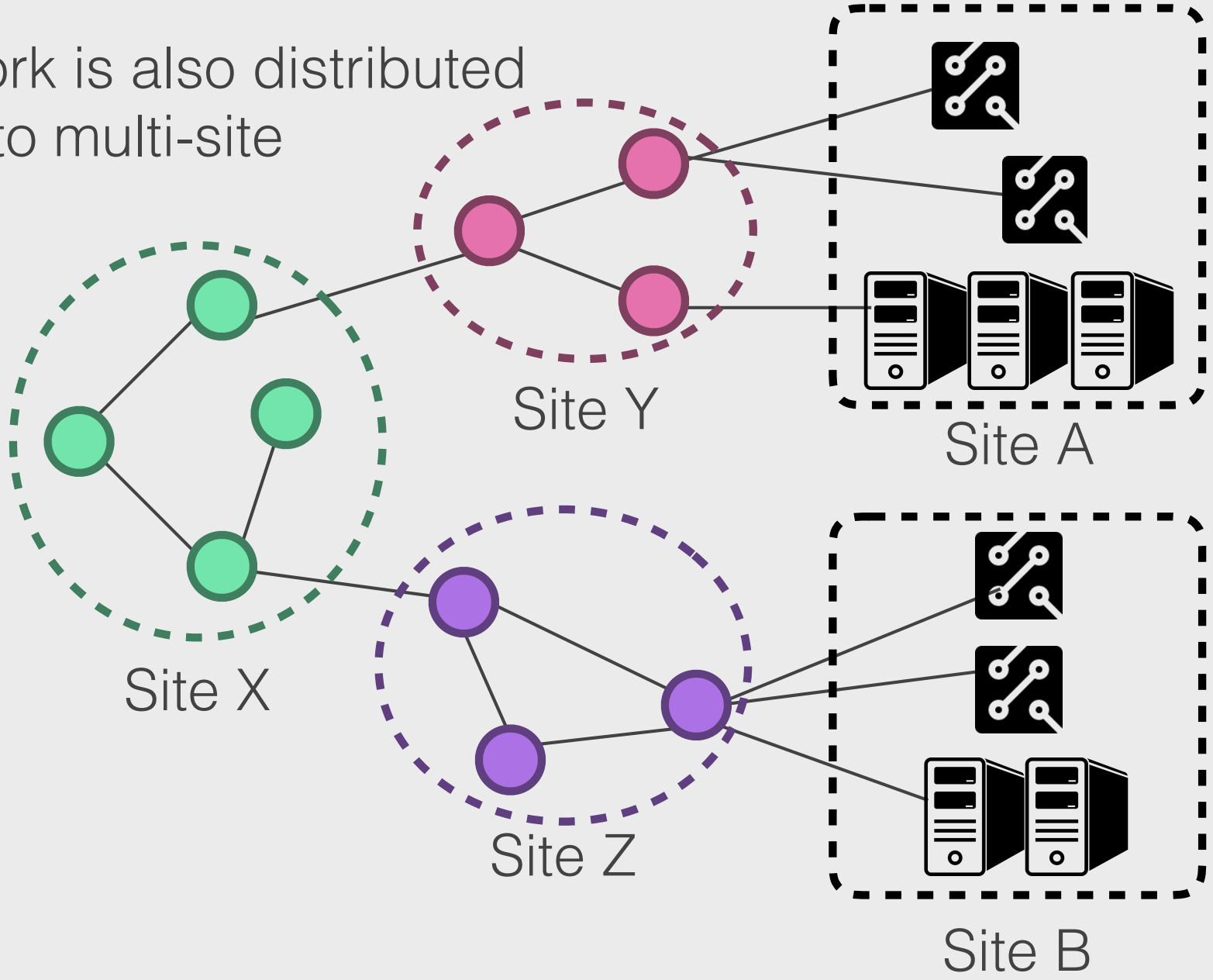
These various devices & resources are connected onto a network



IoT Era

The IoT Era has arrived.

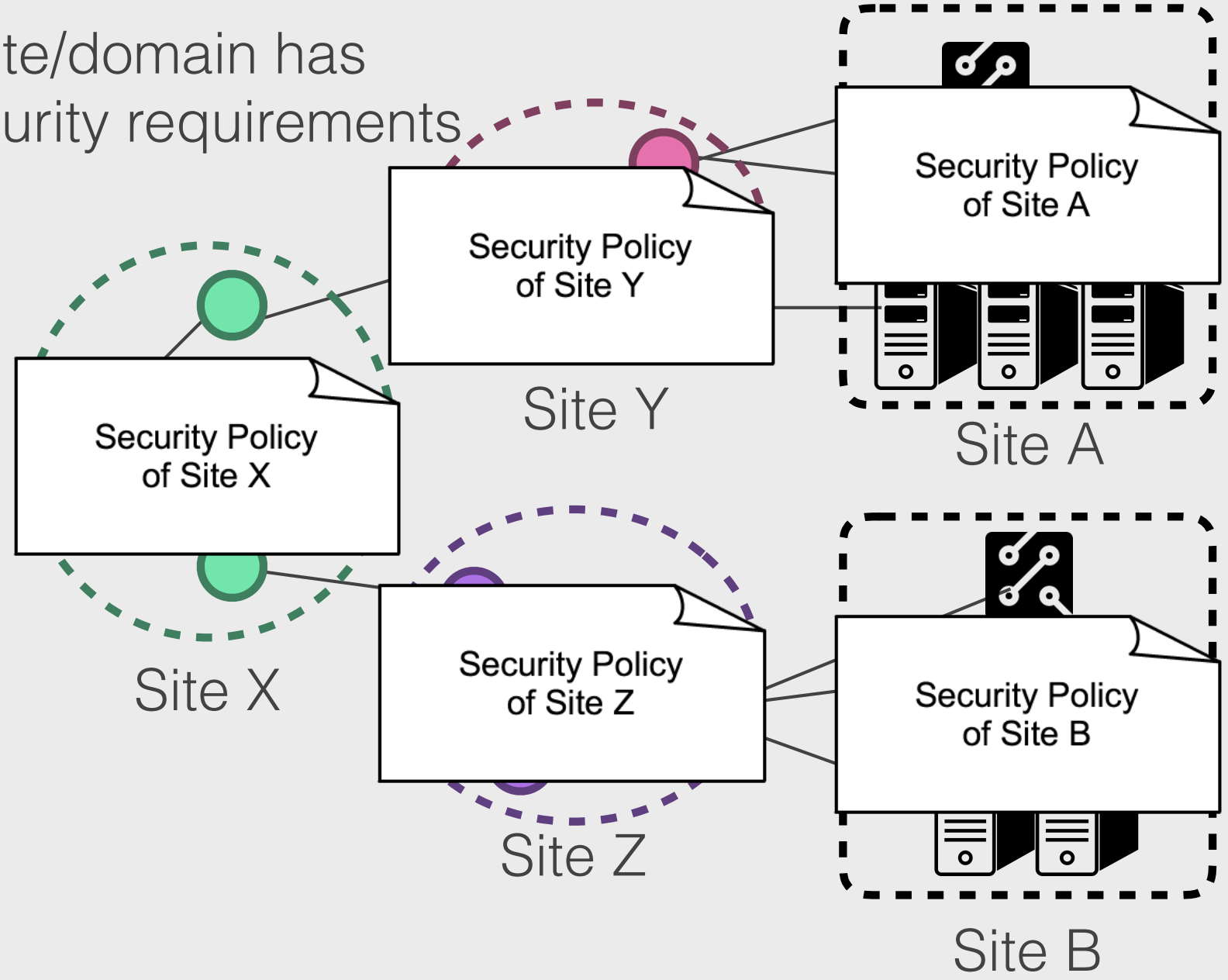
The network is also distributed to multi-site



IoT Era

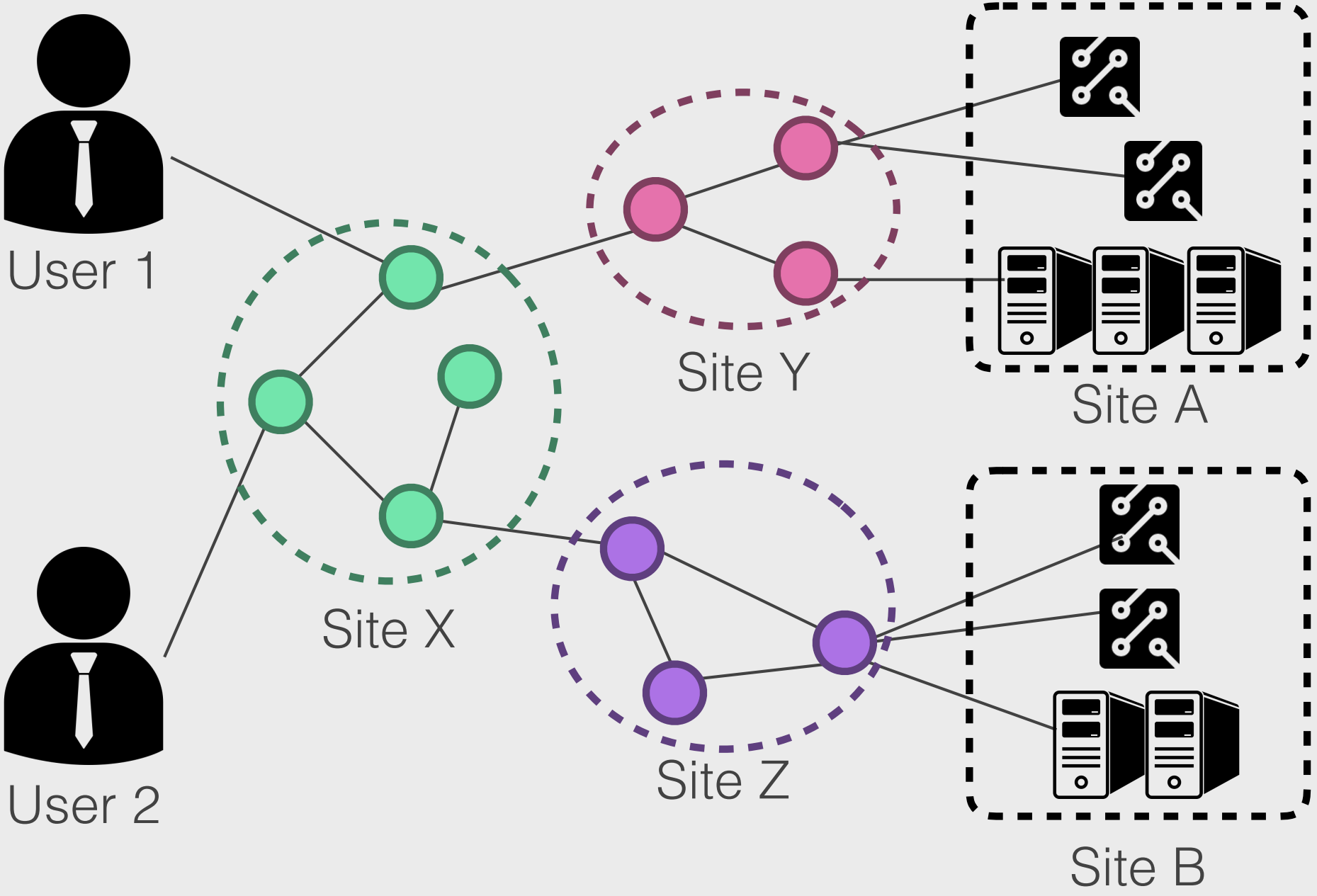
The IoT Era has arrived.

Each site/domain has
unique security requirements



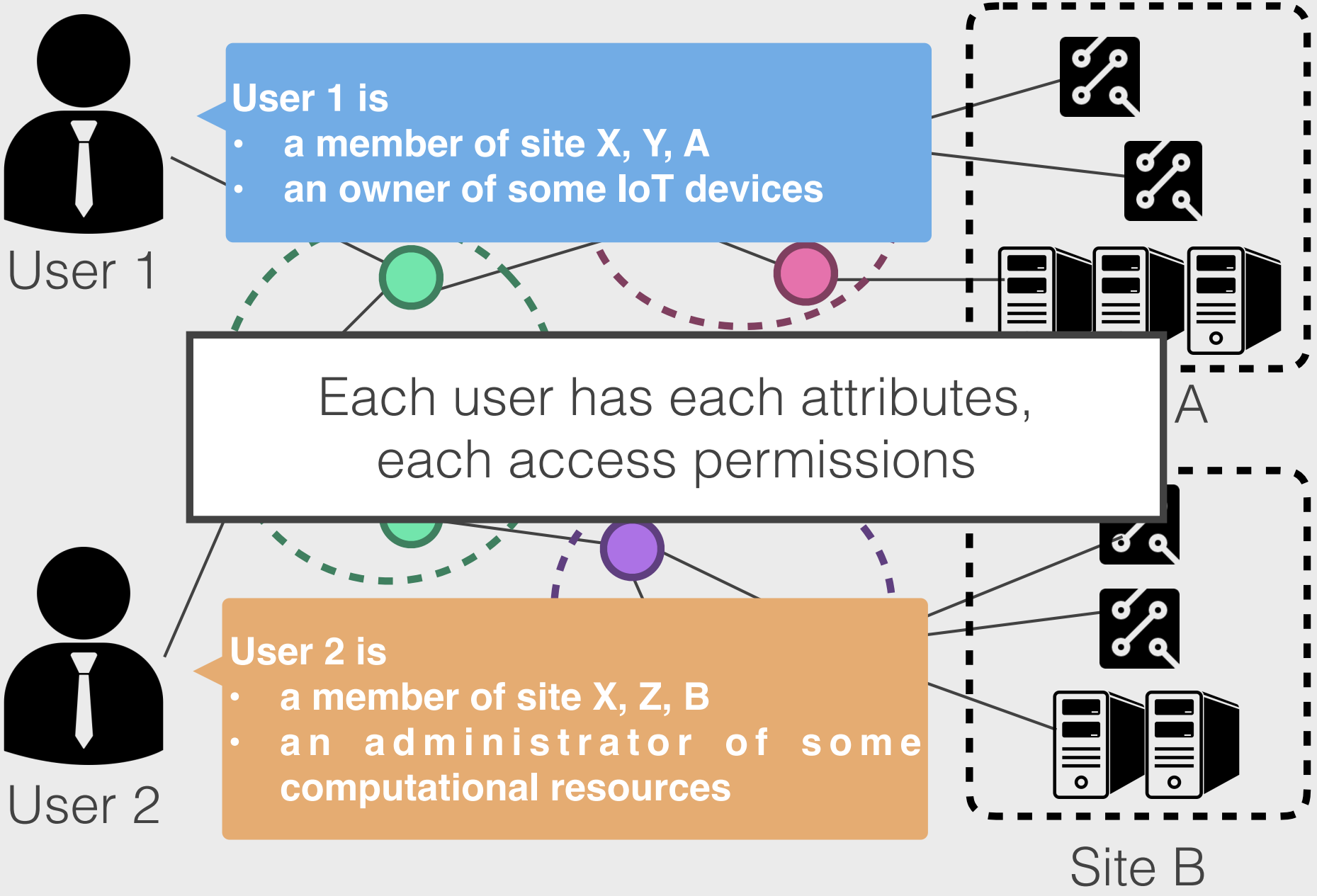
IoT Era

The IoT Era has arrived.



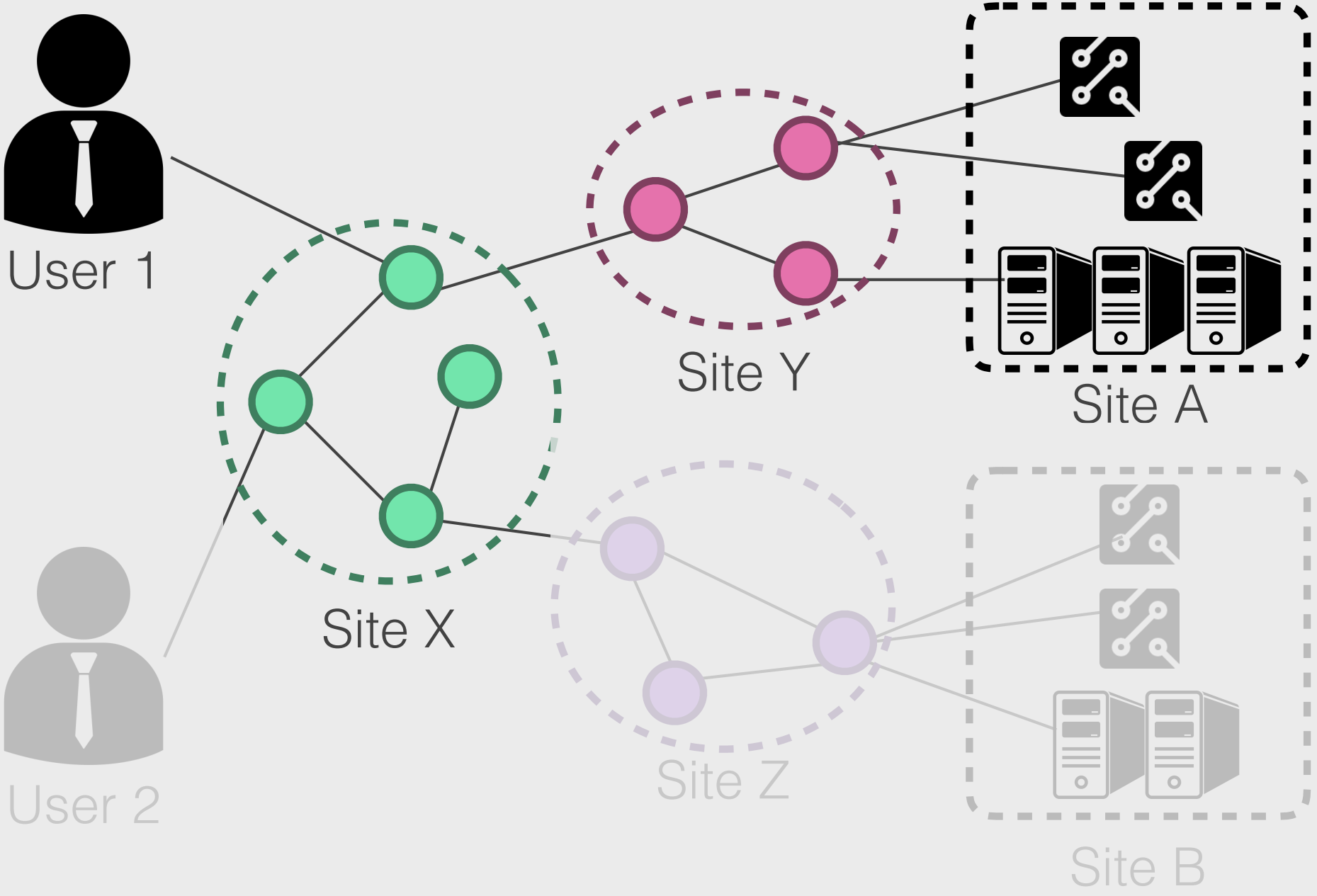
IoT Era

The IoT Era has arrived.



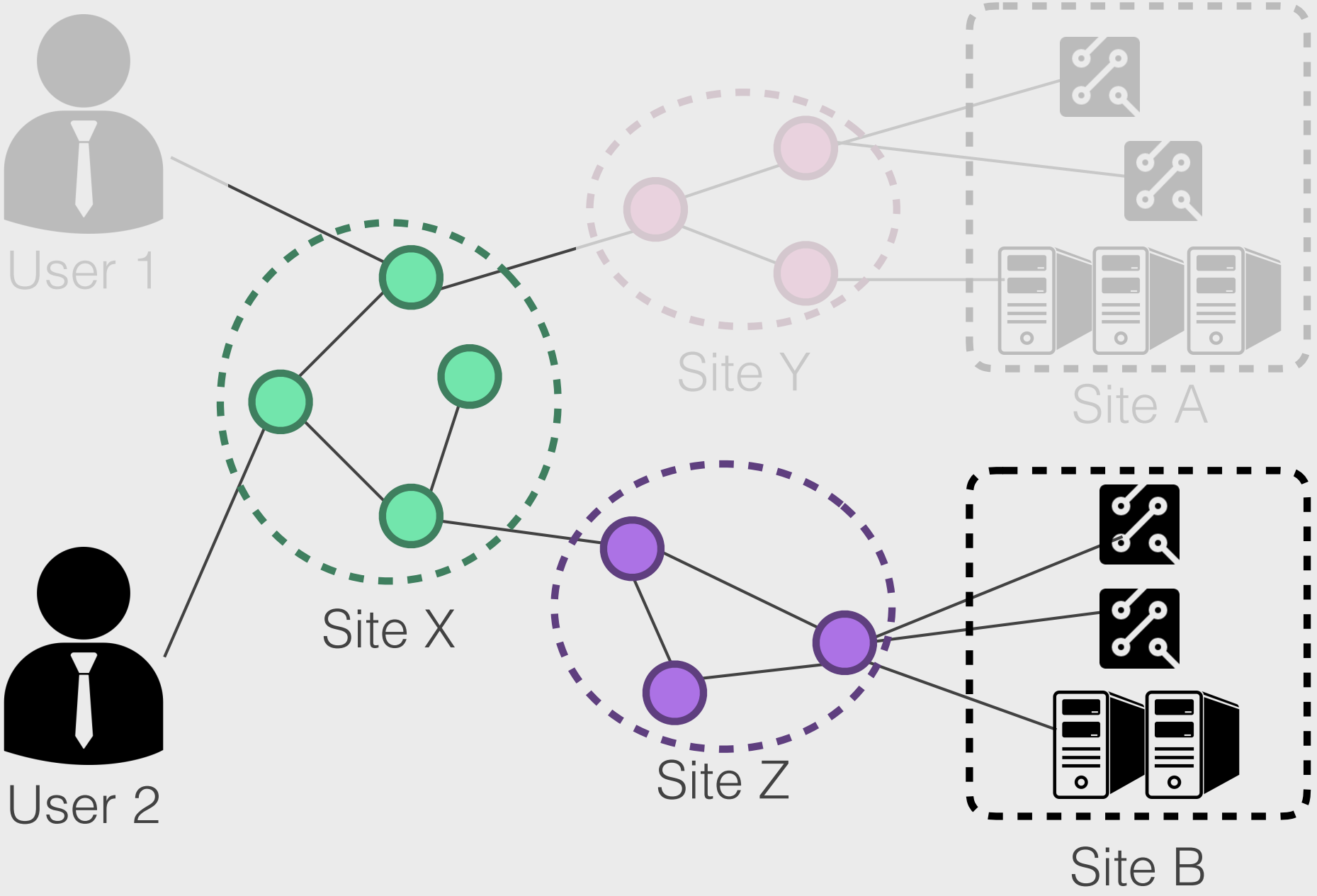
IoT Era

The IoT Era has arrived.



IoT Era

The IoT Era has arrived.

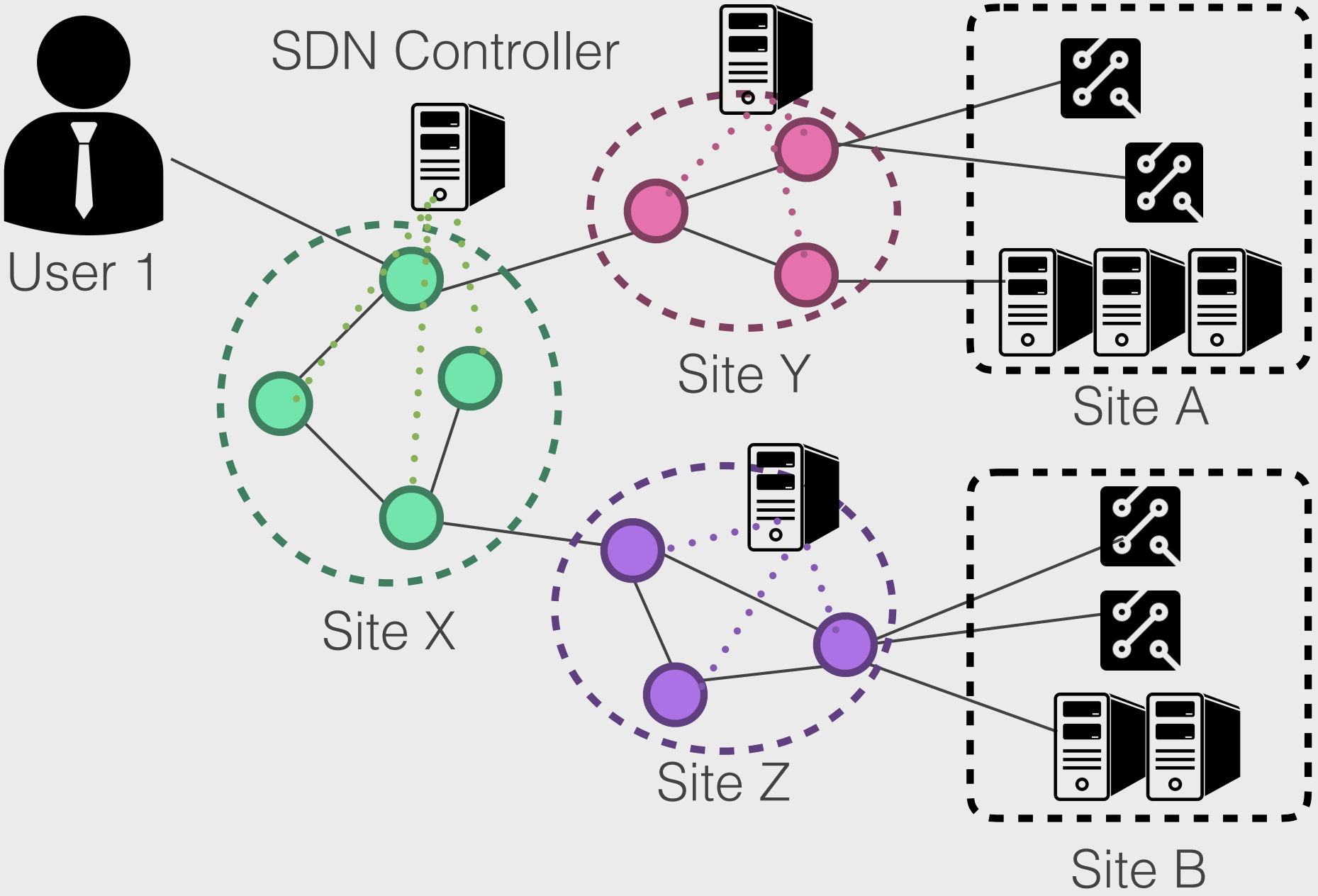


Access Control

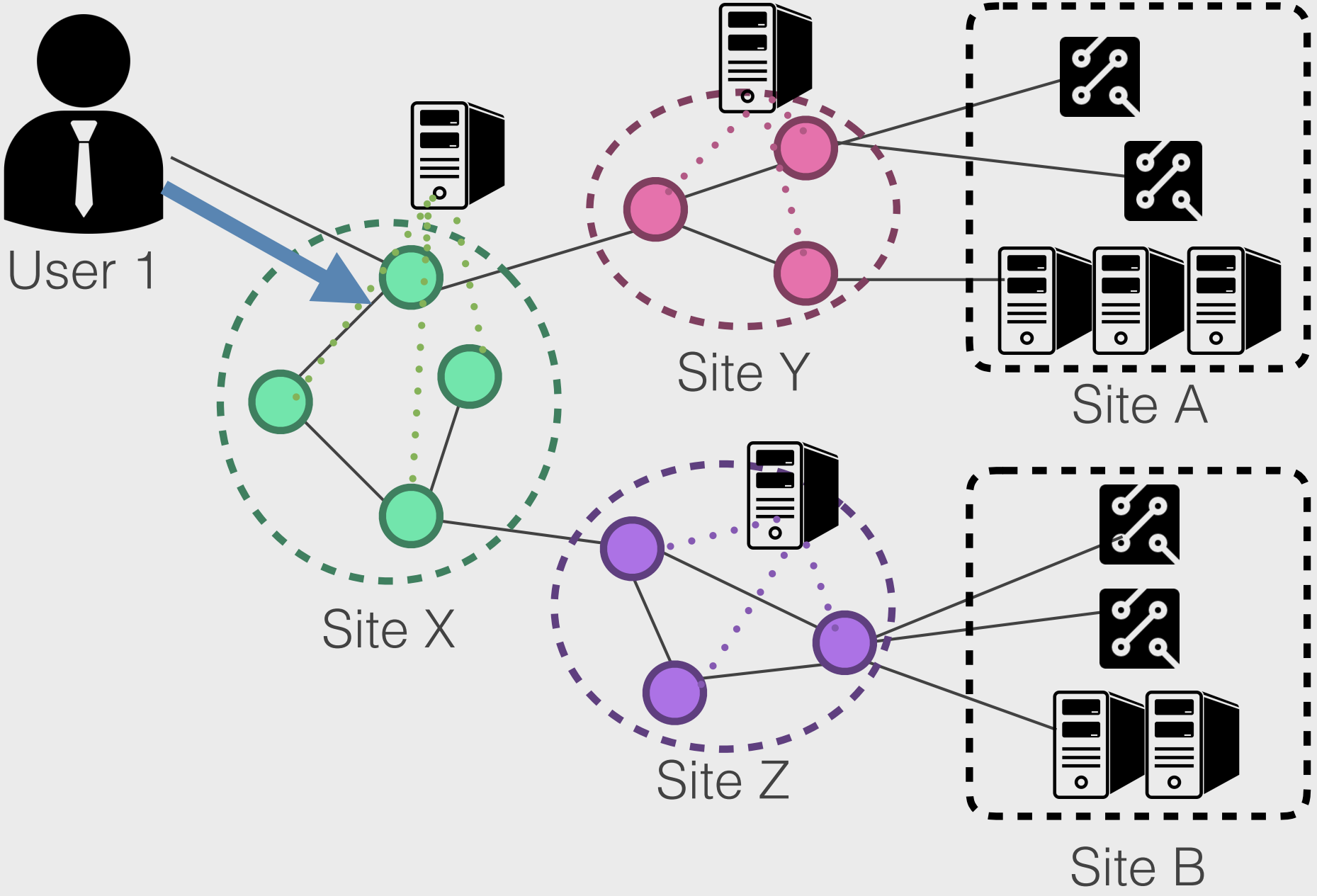
Access control becomes an important problem.

- To date, various security technologies have been proposed. (e.g. GSI, Shibboleth, VOMS, …)
- However, these technologies have targeted only computational resources, not targeted network resources as access-controlled resources.
- **We proposed an access control mechanism that targets network resources as access-controlled resources**.
  - We have adopted **SDN** & **RBAC (Role Based Access Control)** to develop the mechanism.

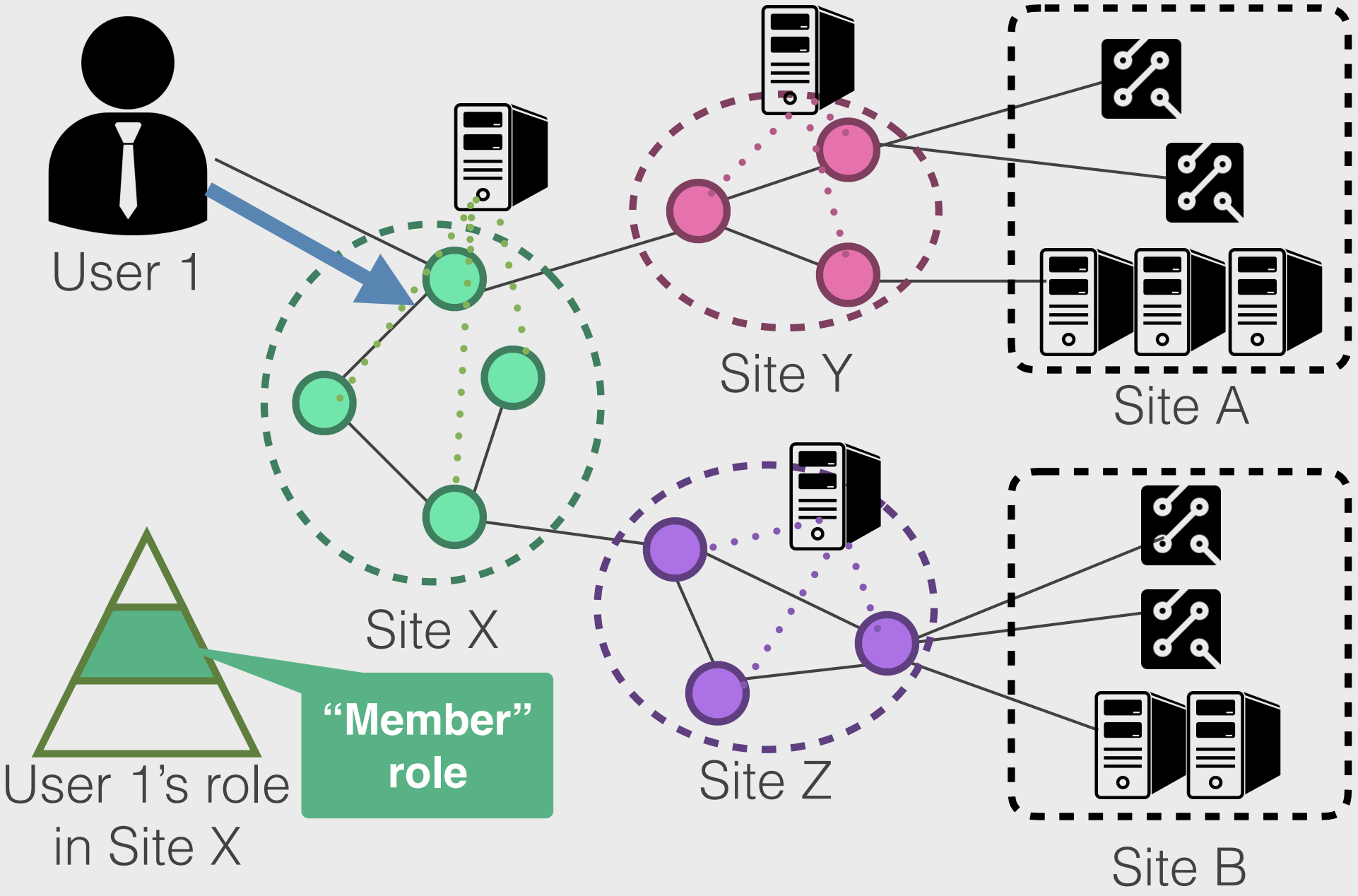
Proposed Mechanism



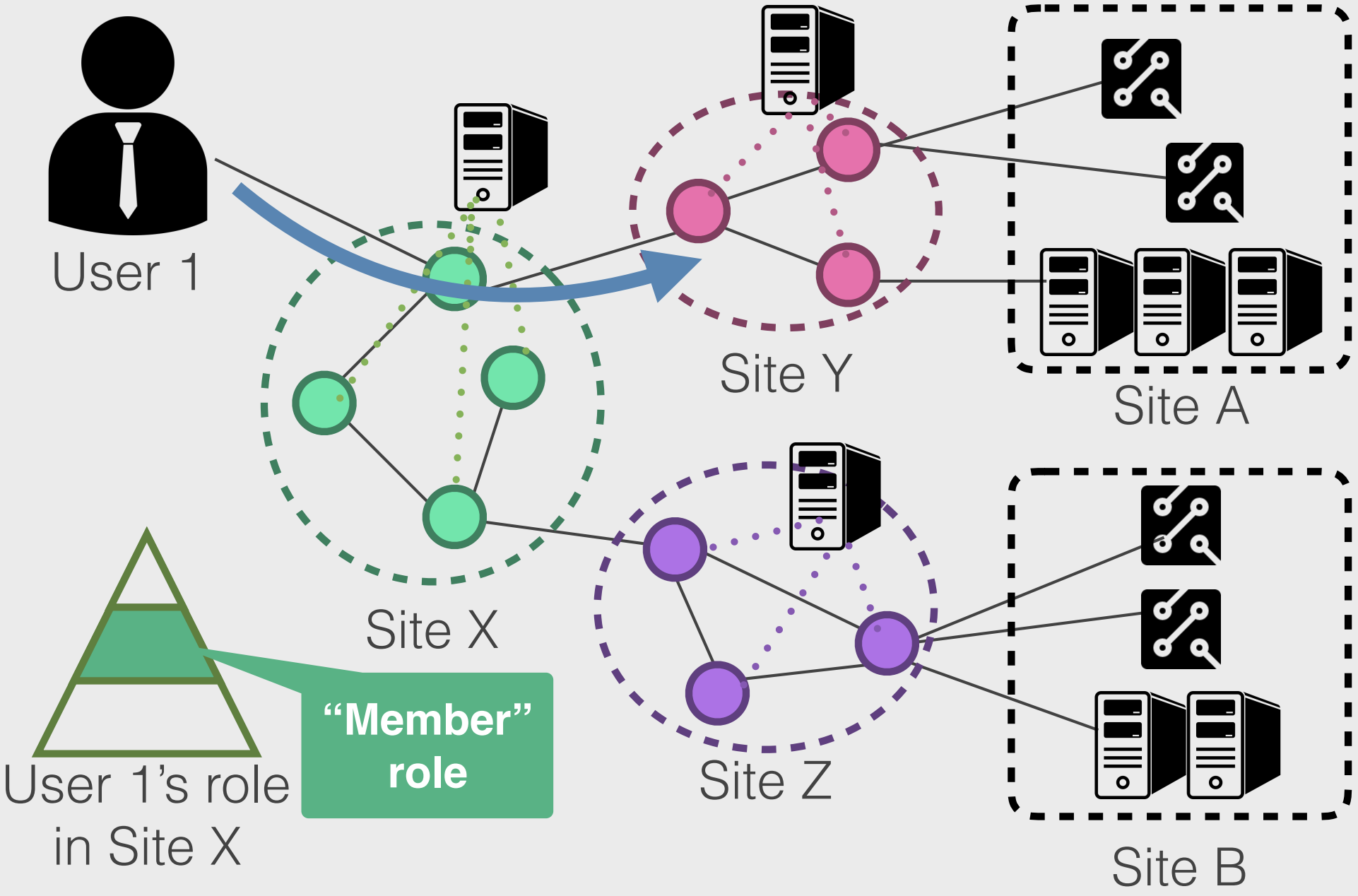
Proposed Mechanism



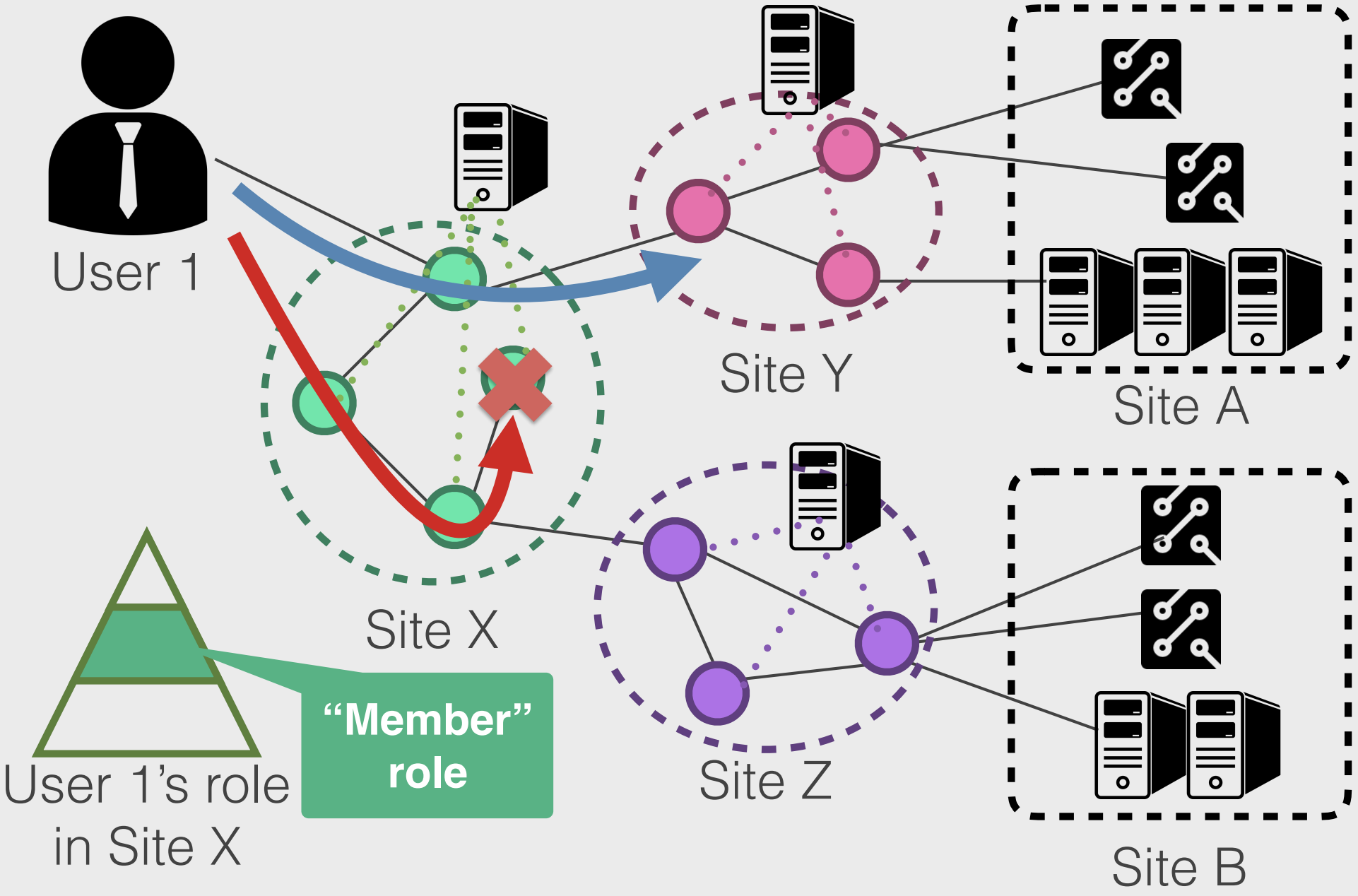
Proposed Mechanism



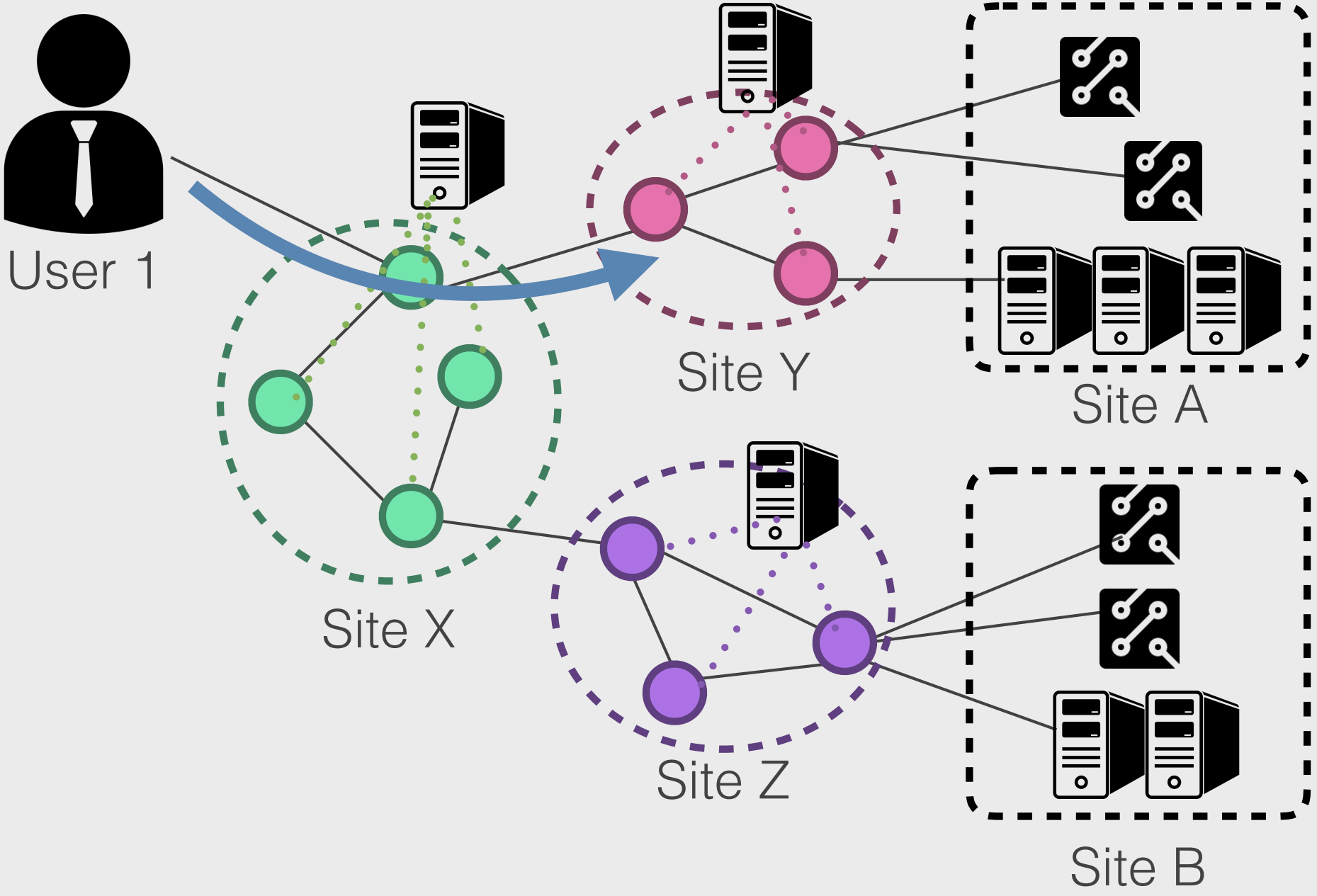
Proposed Mechanism



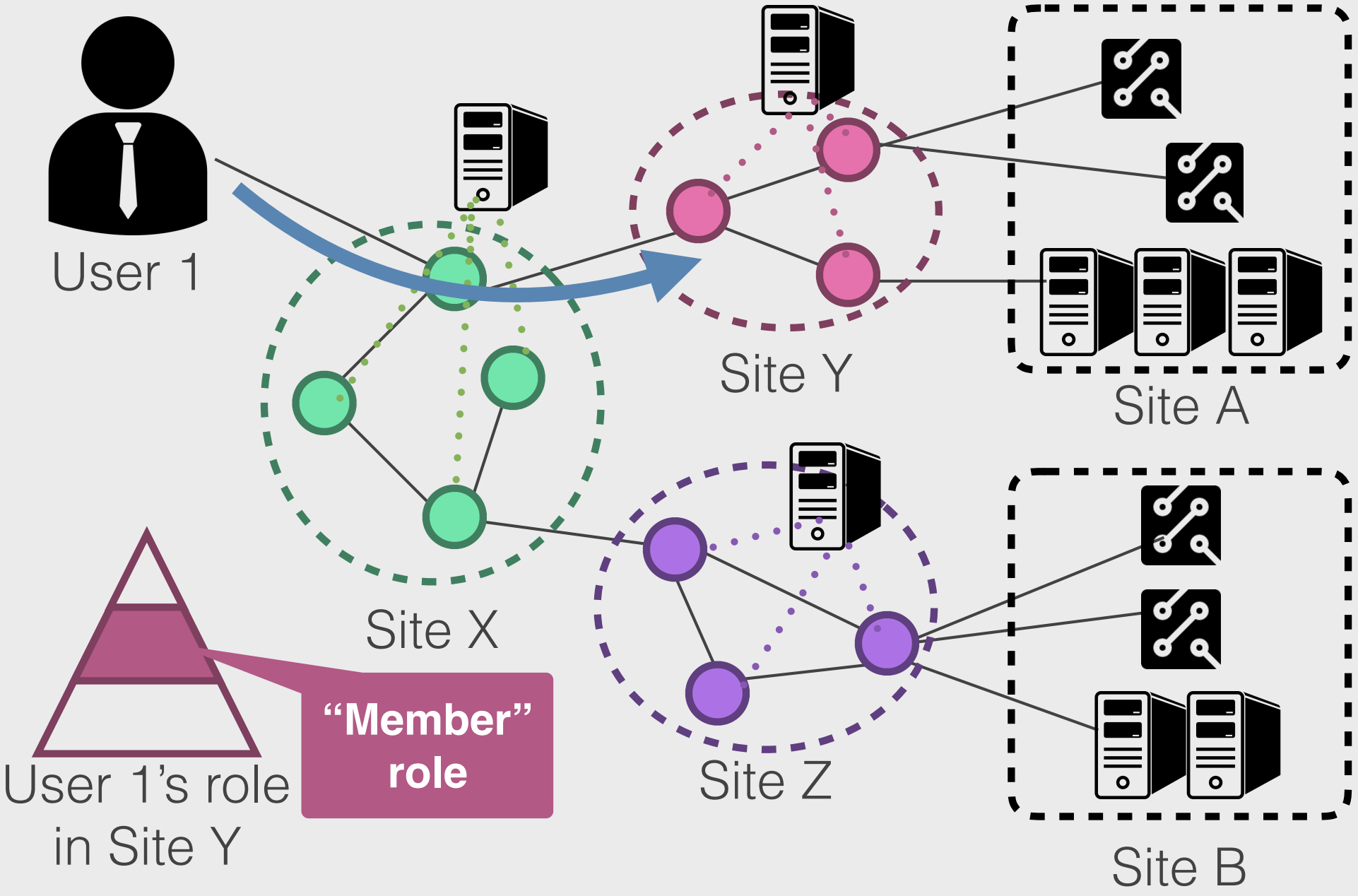
Proposed Mechanism



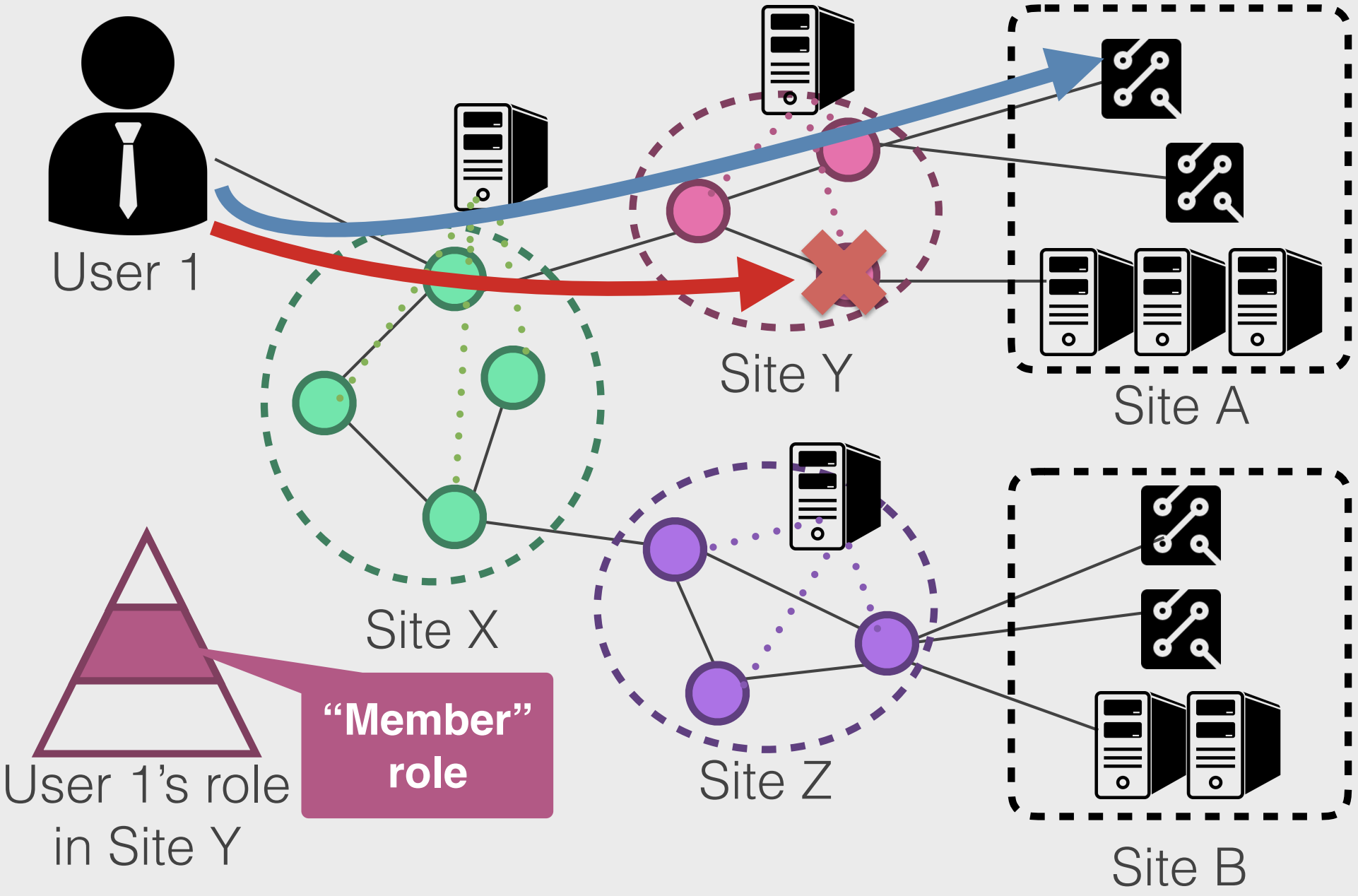
Proposed Mechanism



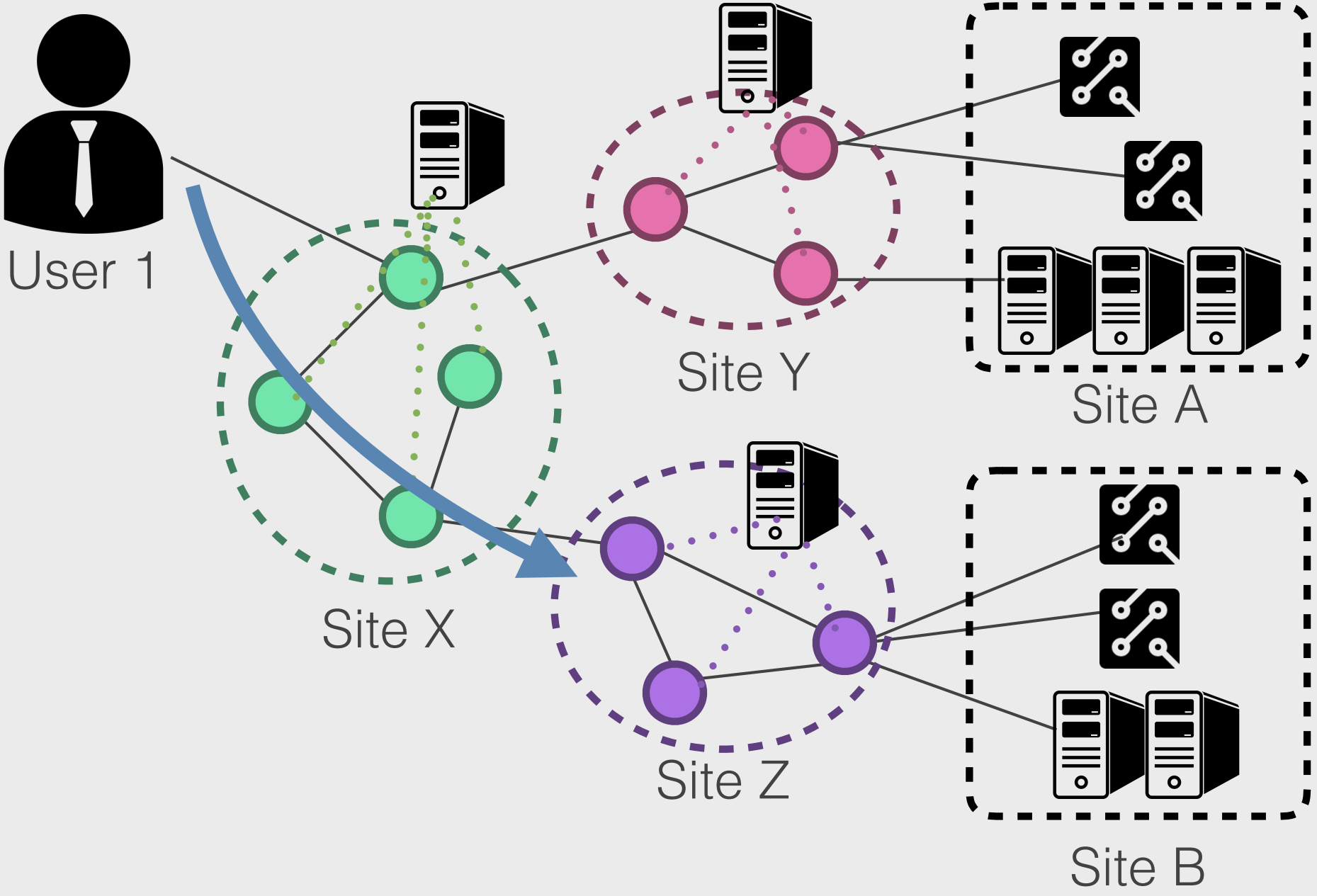
Proposed Mechanism



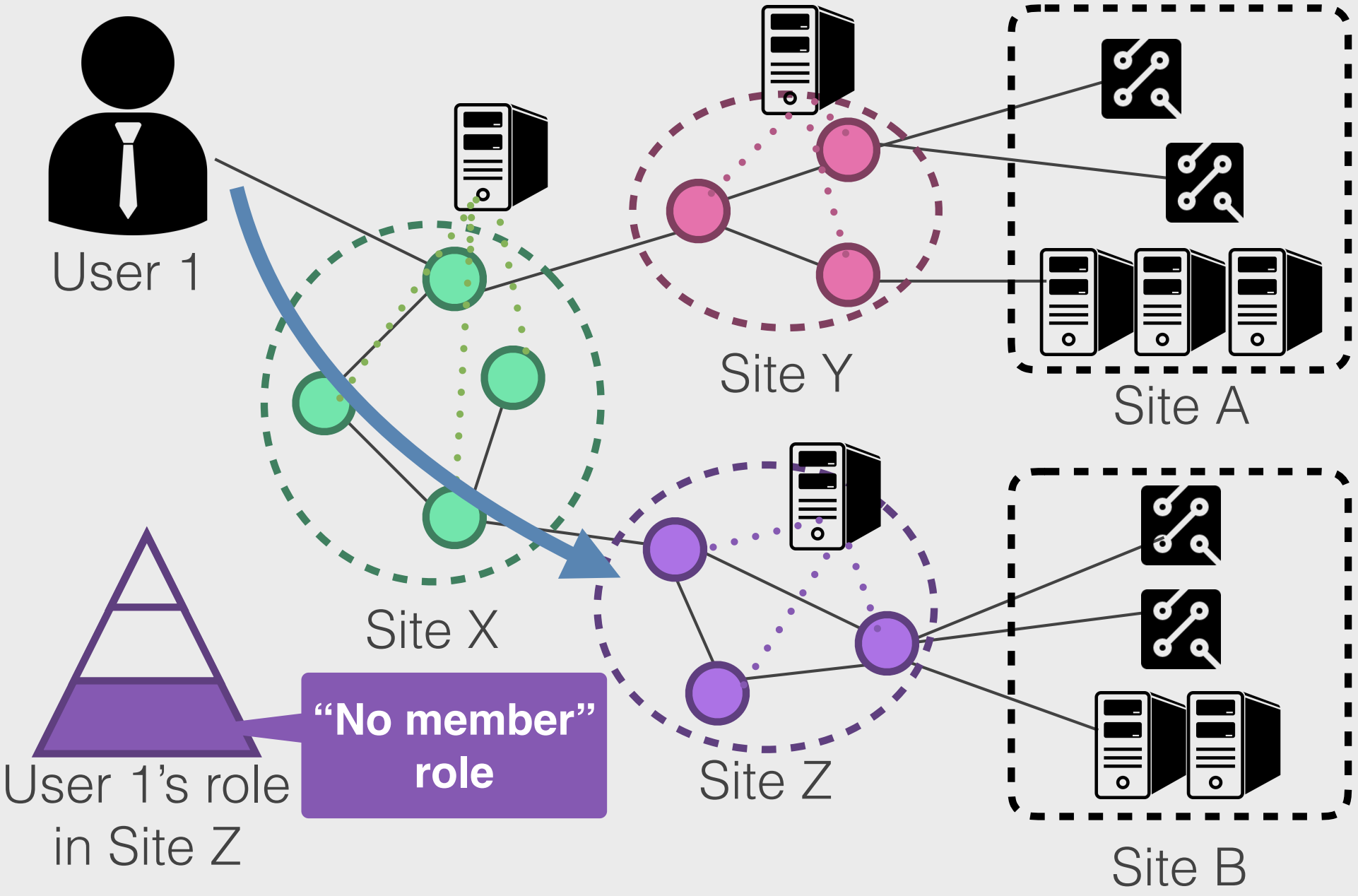
Proposed Mechanism



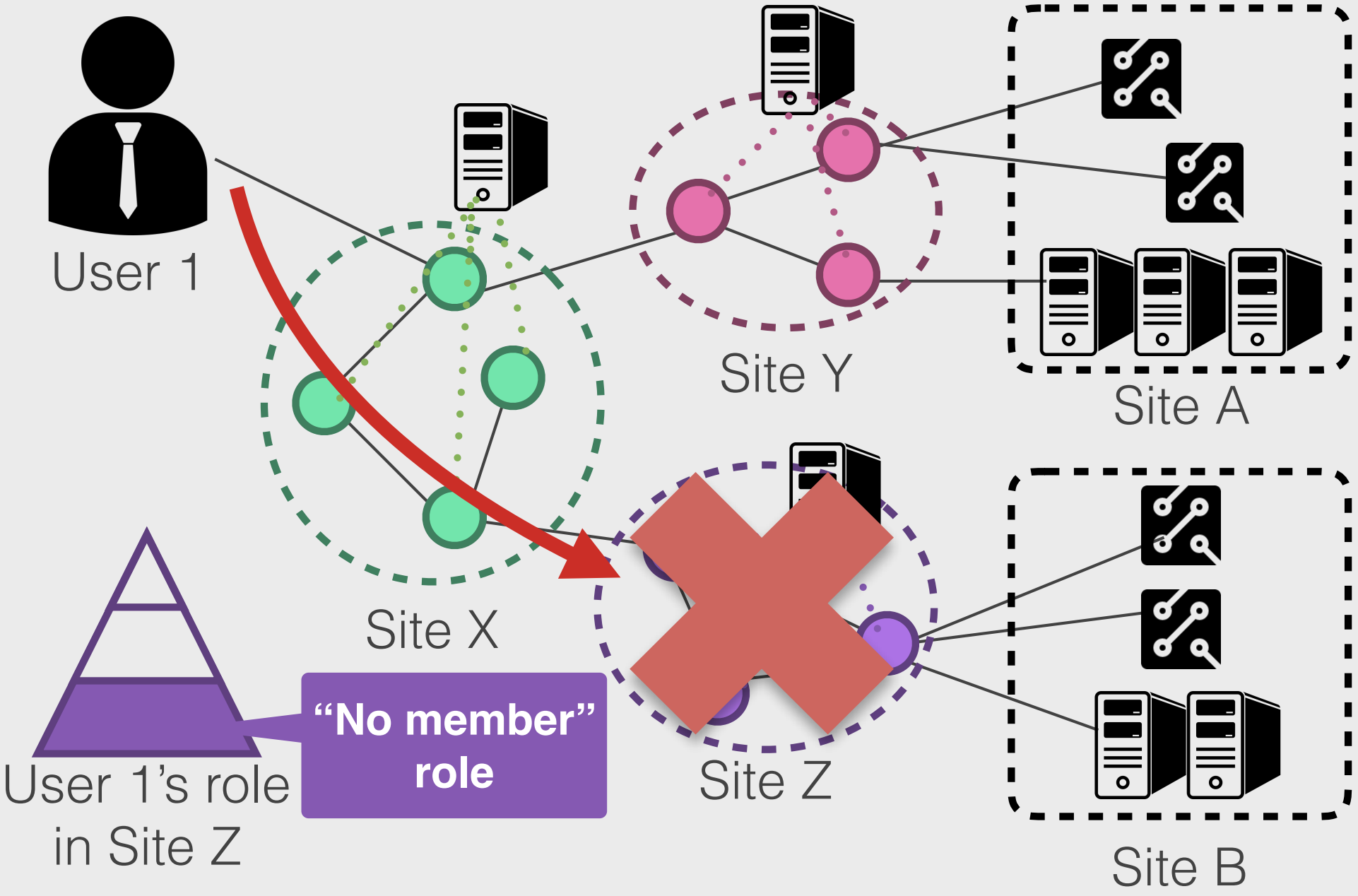
Proposed Mechanism



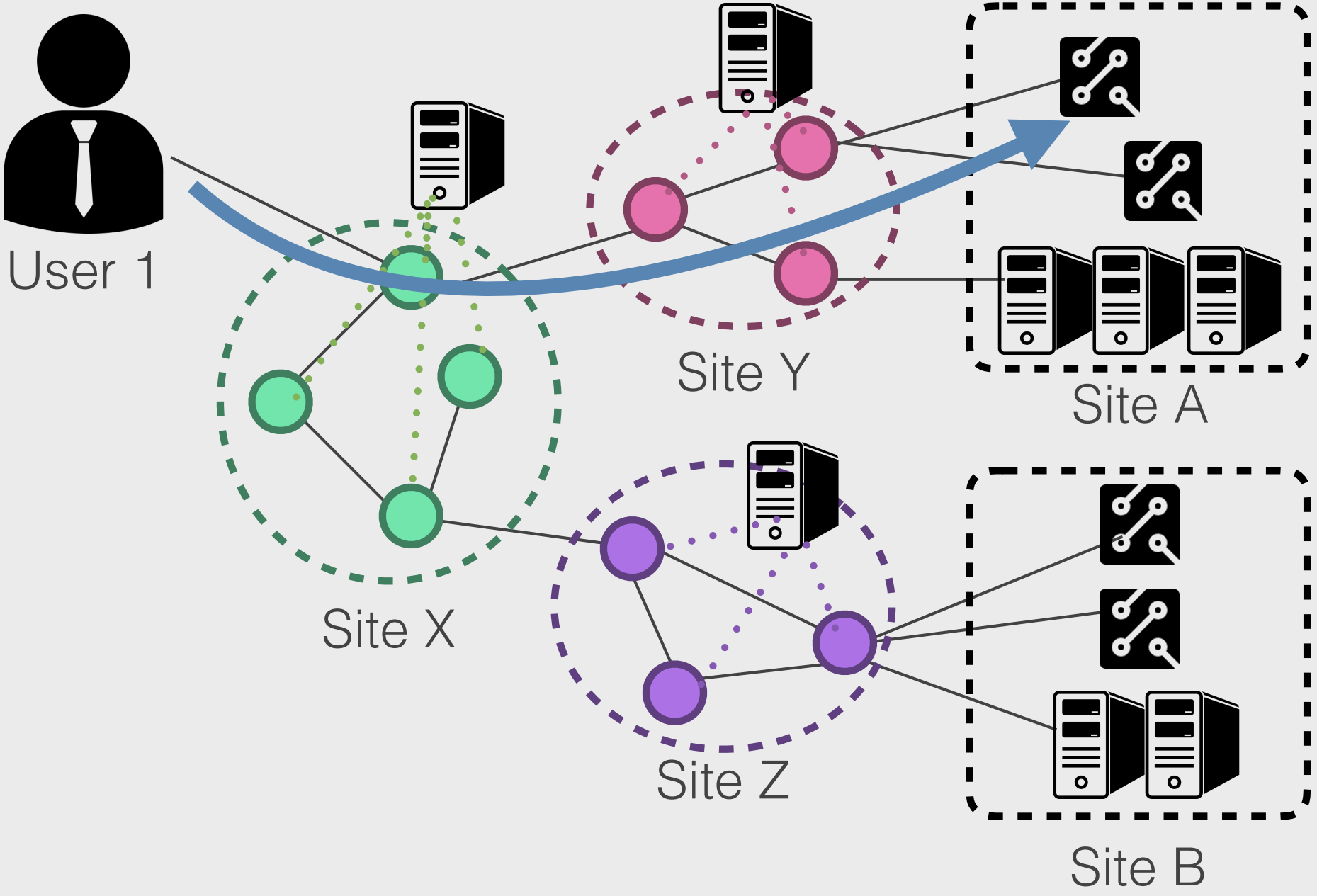
Proposed Mechanism



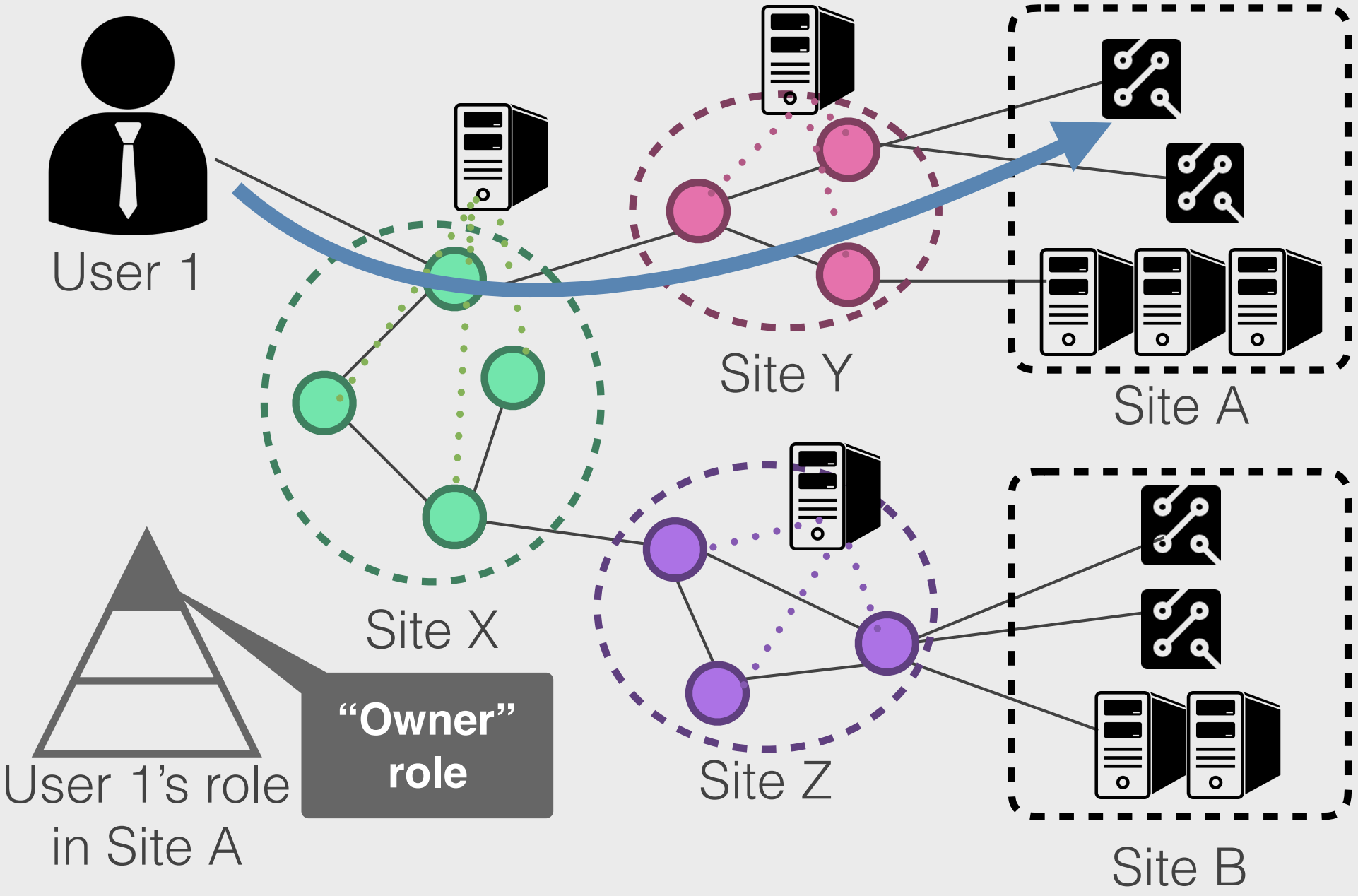
Proposed Mechanism



Proposed Mechanism



Proposed Mechanism

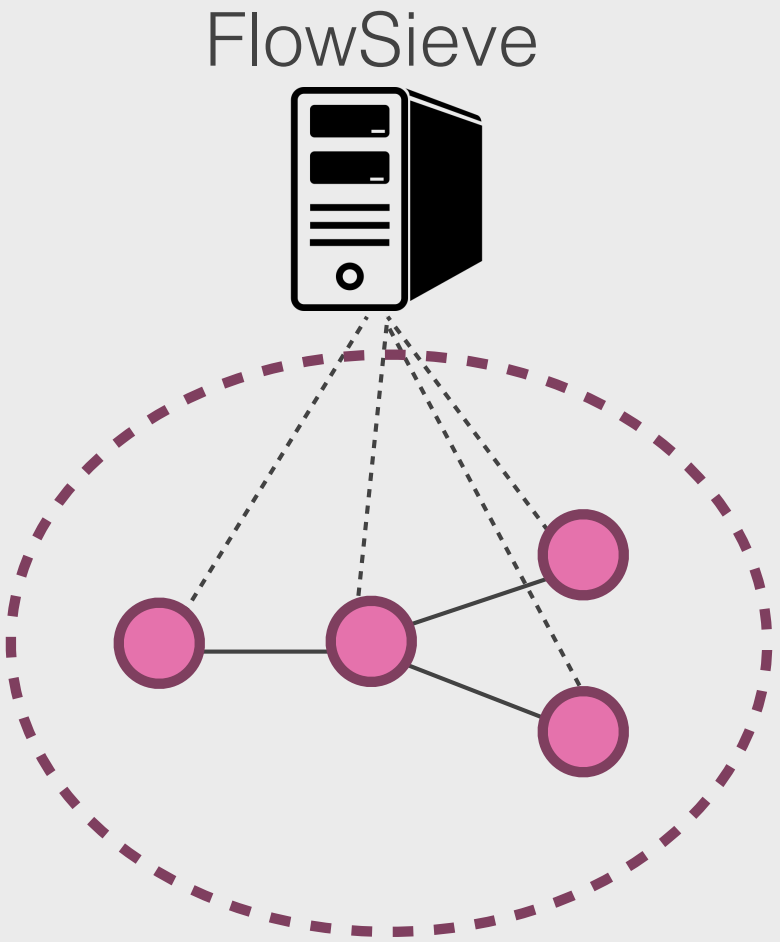


FlowSieve

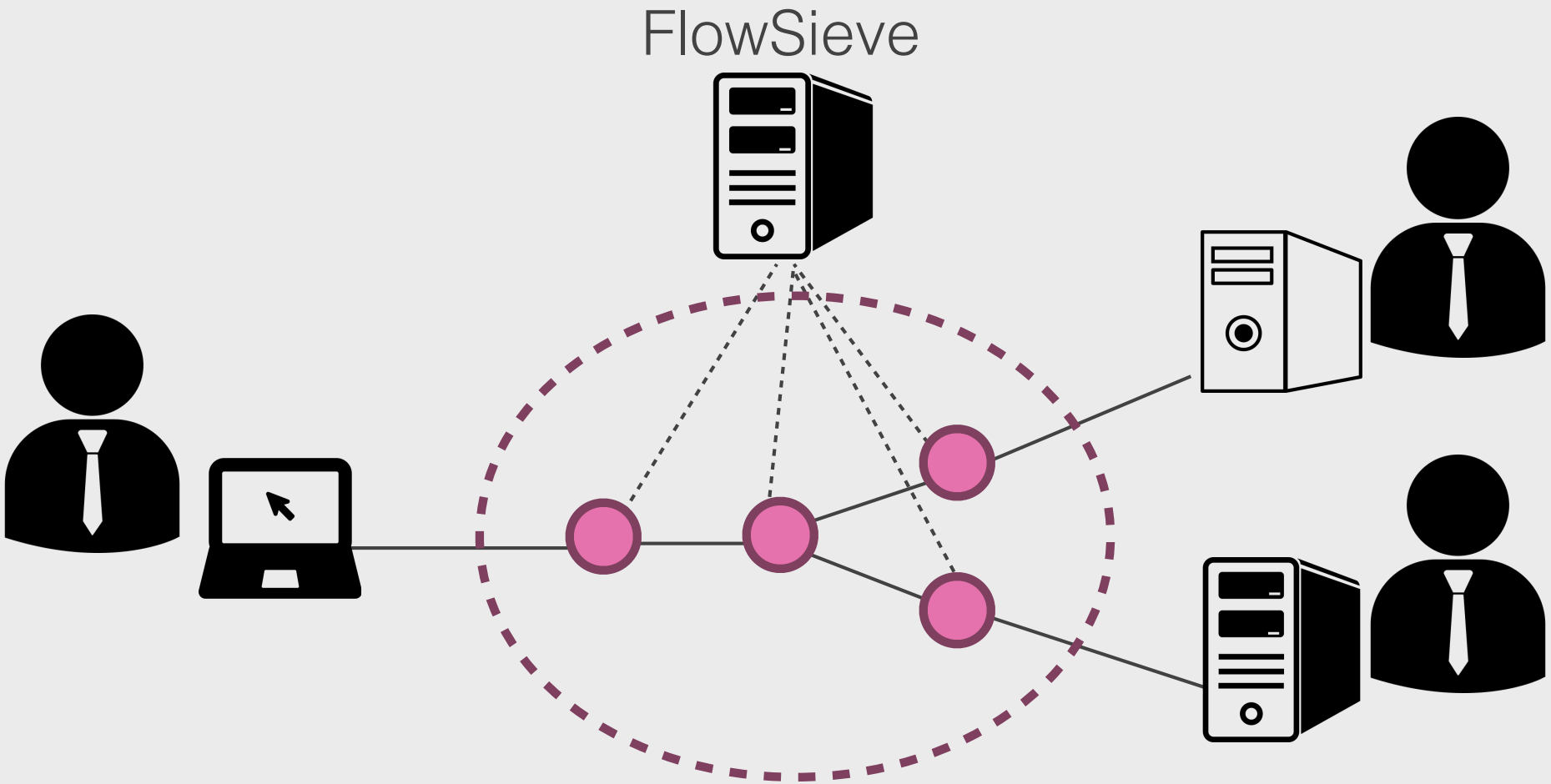
FlowSieve is a preliminary implementation of the access control mechanism.

- FlowSieve is implemented as an OpenFlow controller program.
- FlowSieve authenticates users (based on IEEE 802.1X standard), and authorizes access from users to network resources in an OpenFlow network.

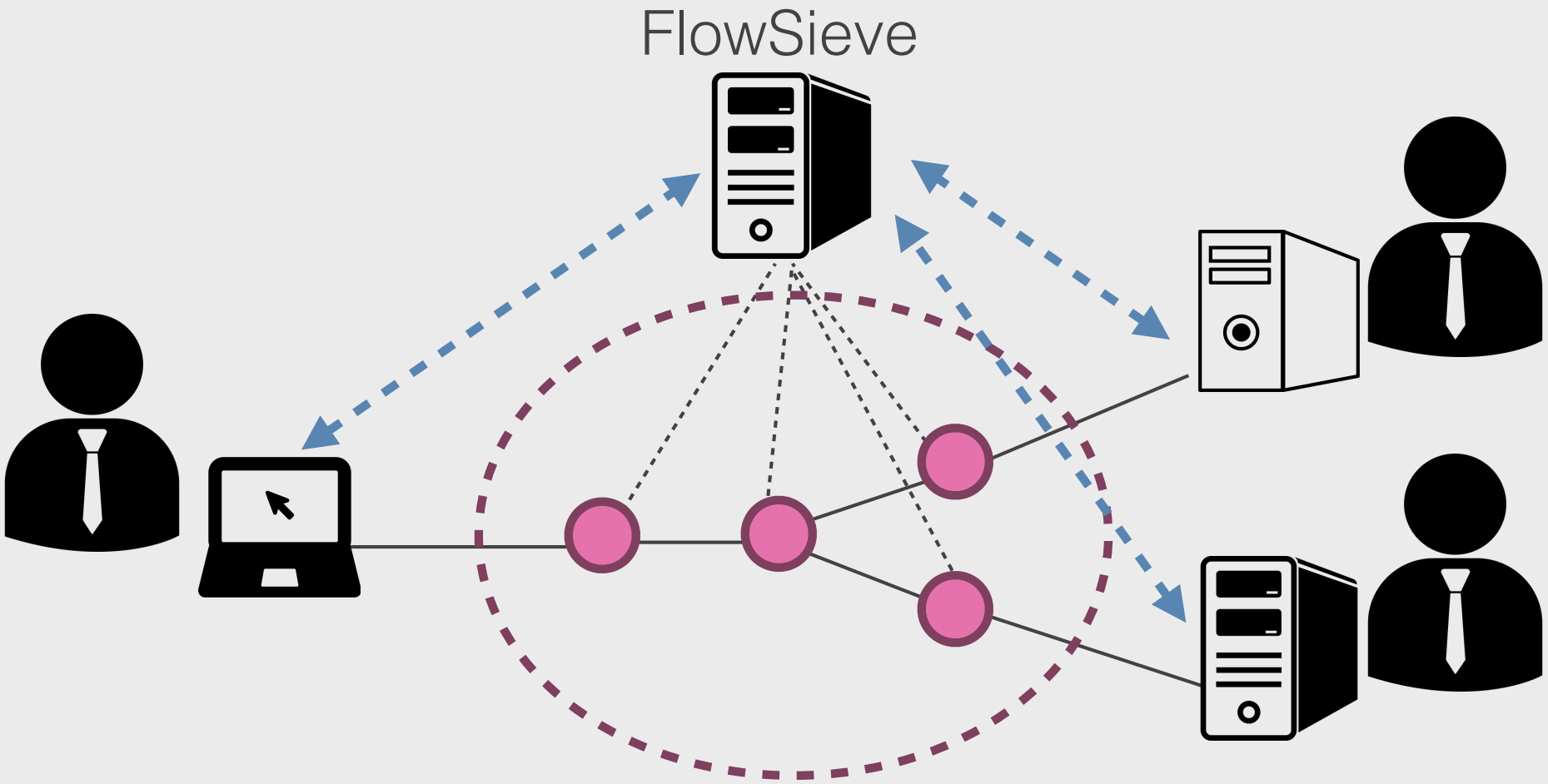
FlowSieve in Action



FlowSieve in Action

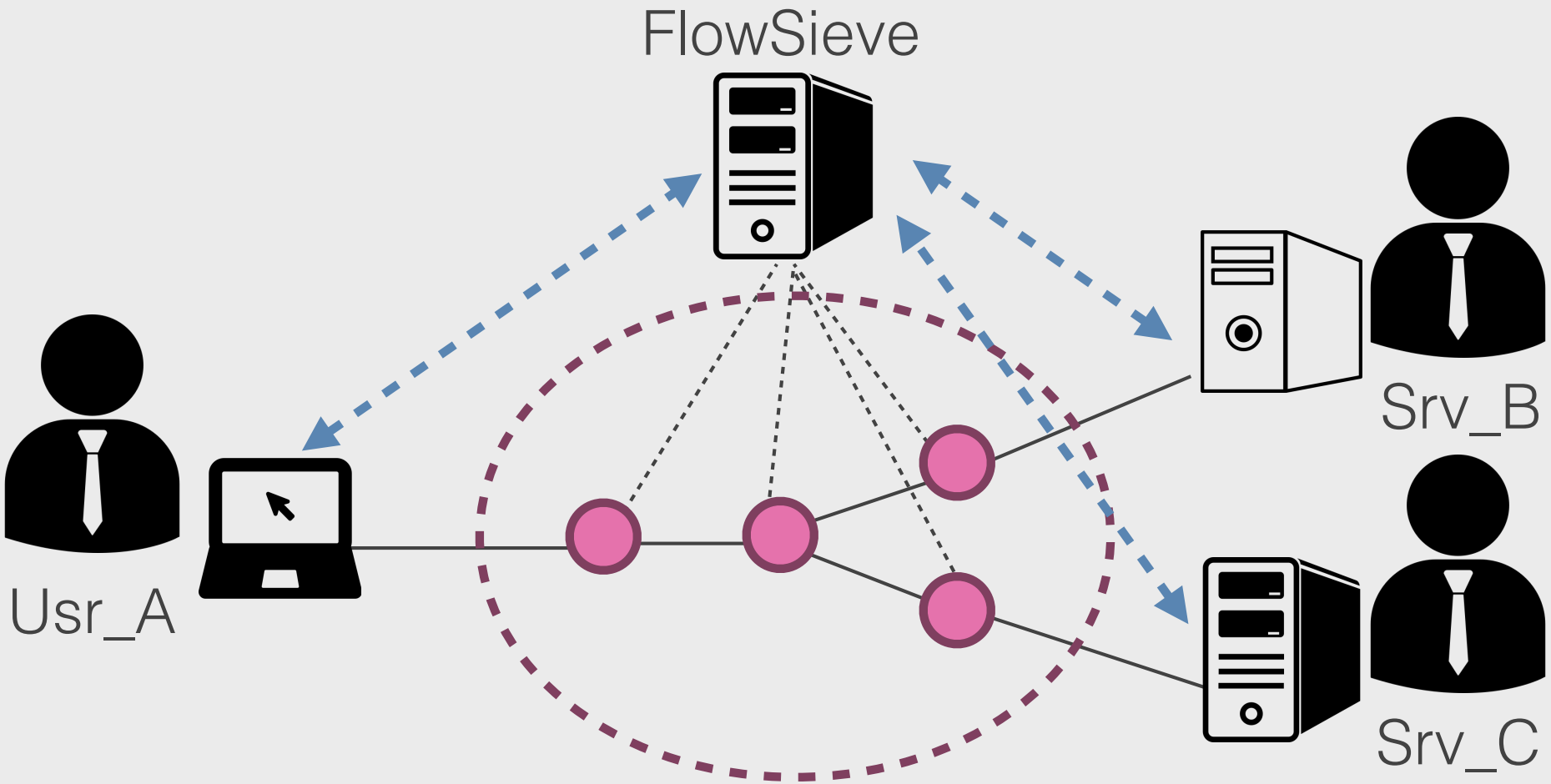


FlowSieve in Action



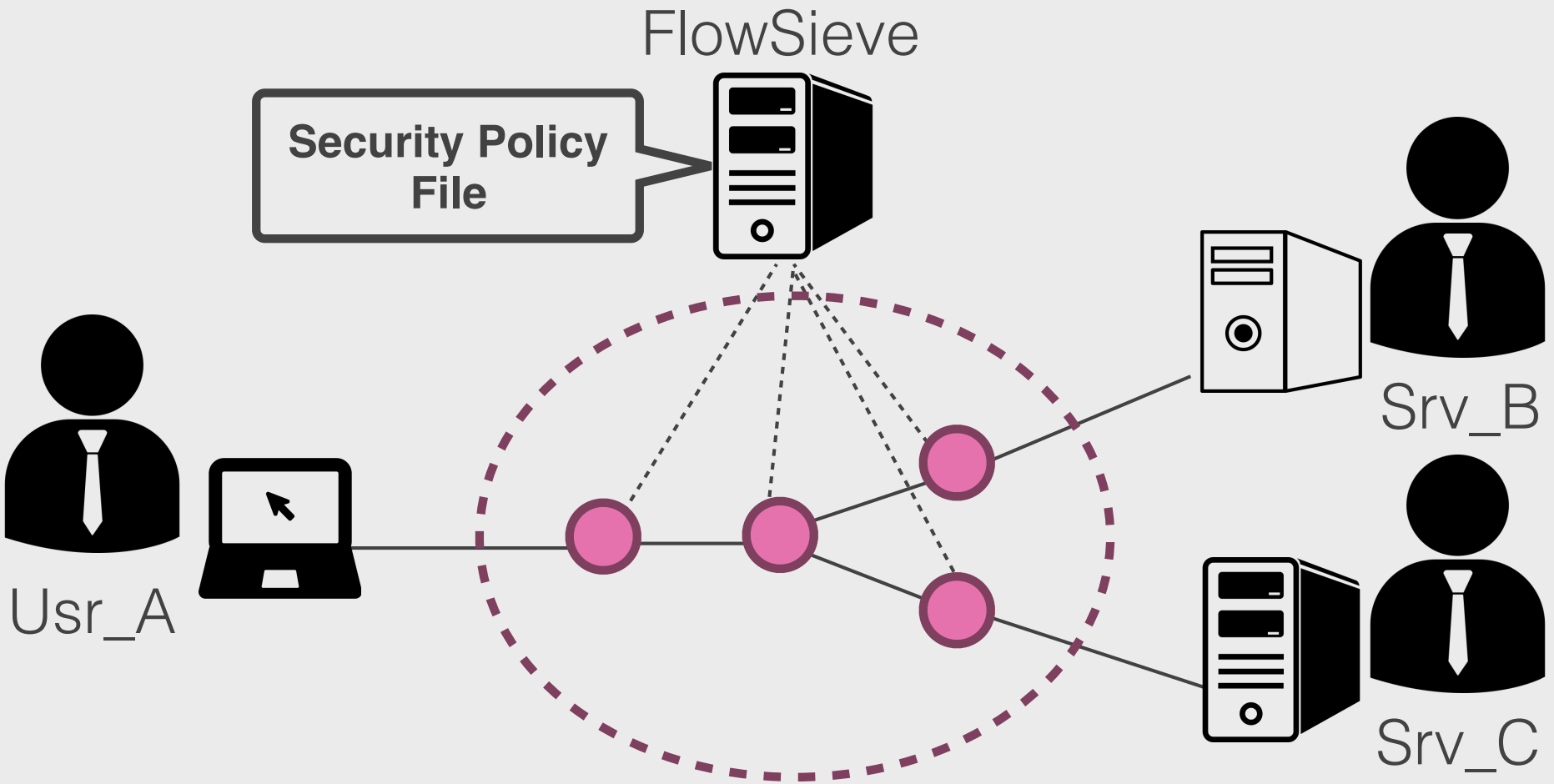
FlowSieve works as 802.1X authentication Server, authenticates every user

FlowSieve in Action

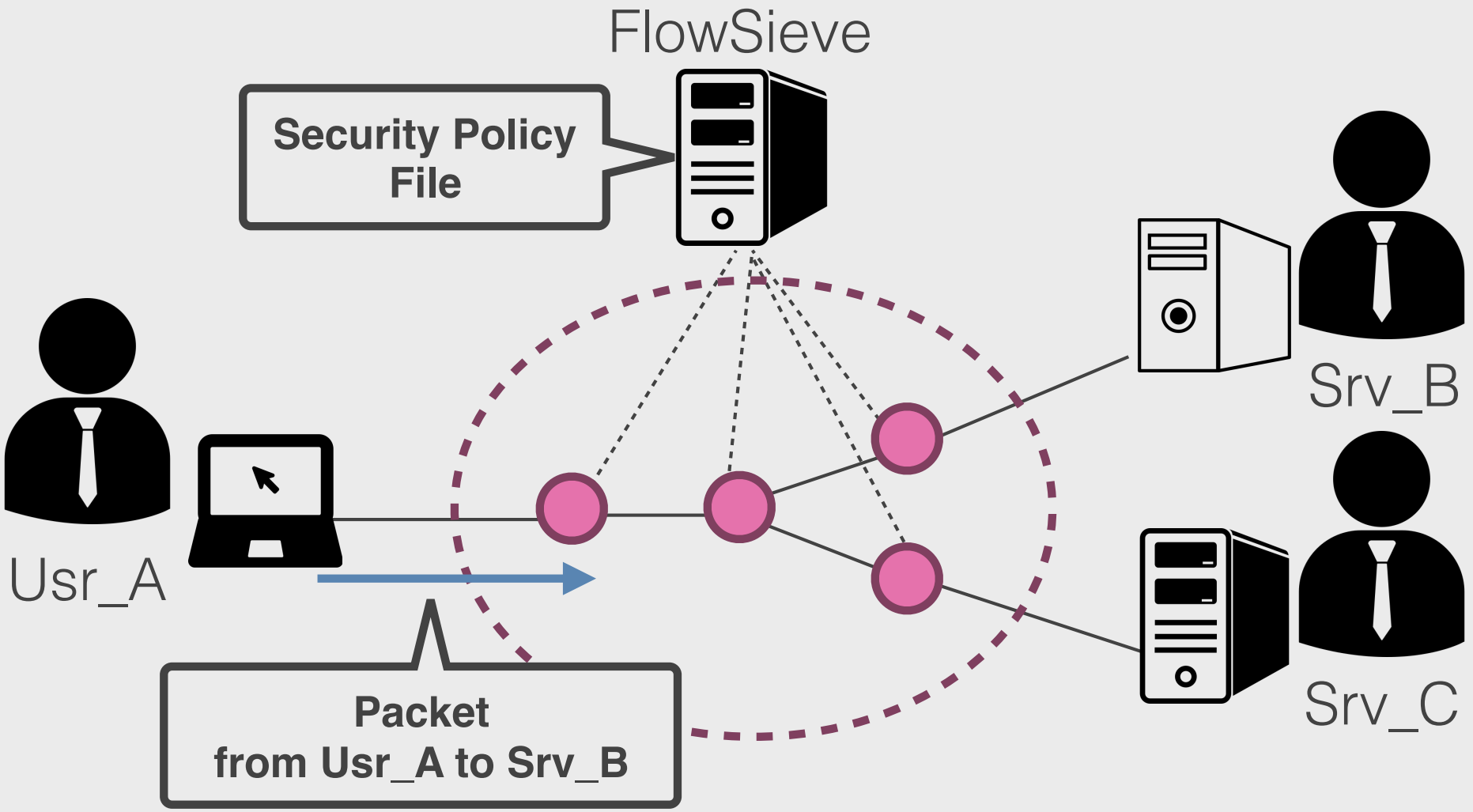


FlowSieve works as 802.1X authentication Server, authenticates every user

FlowSieve in Action

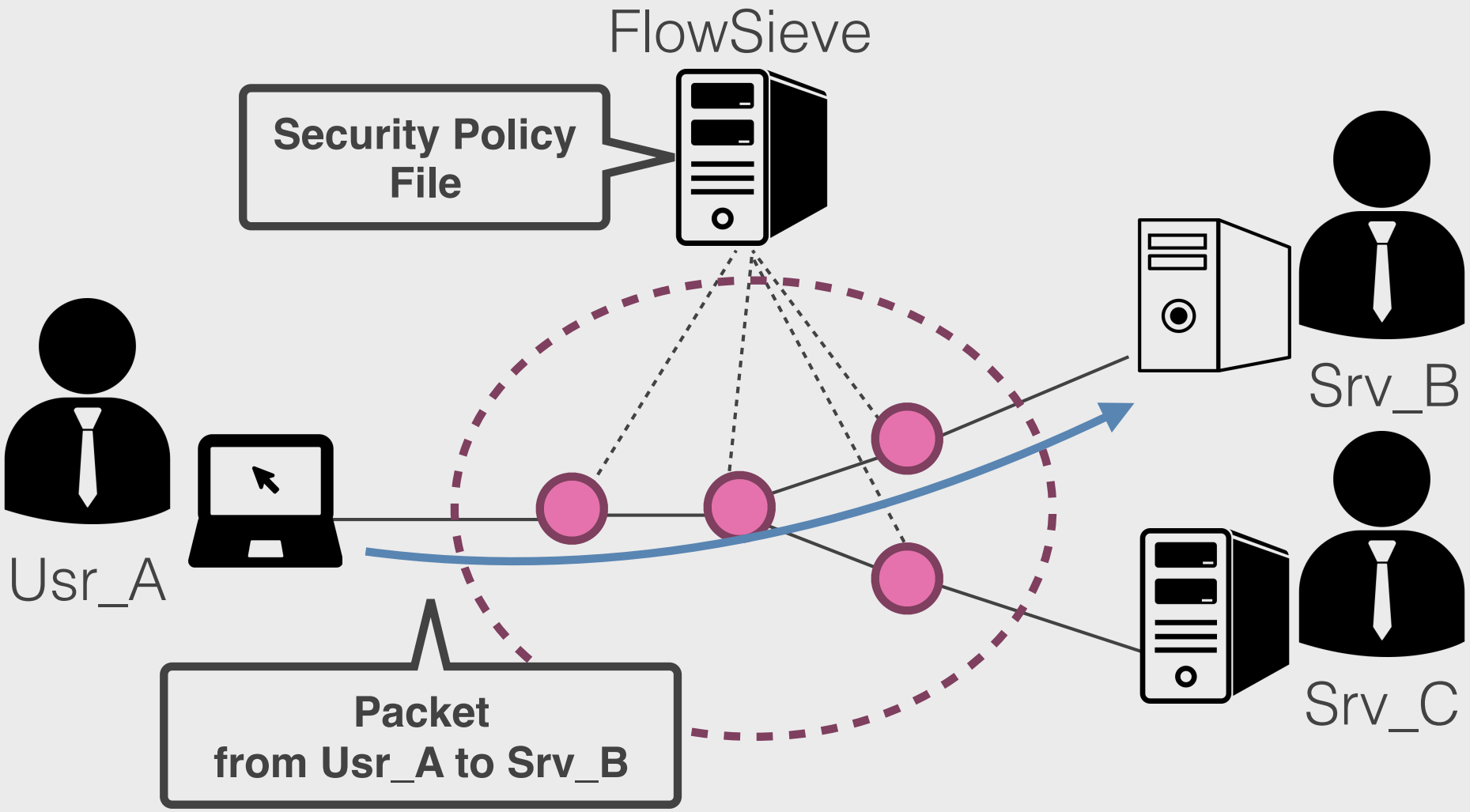


FlowSieve in Action



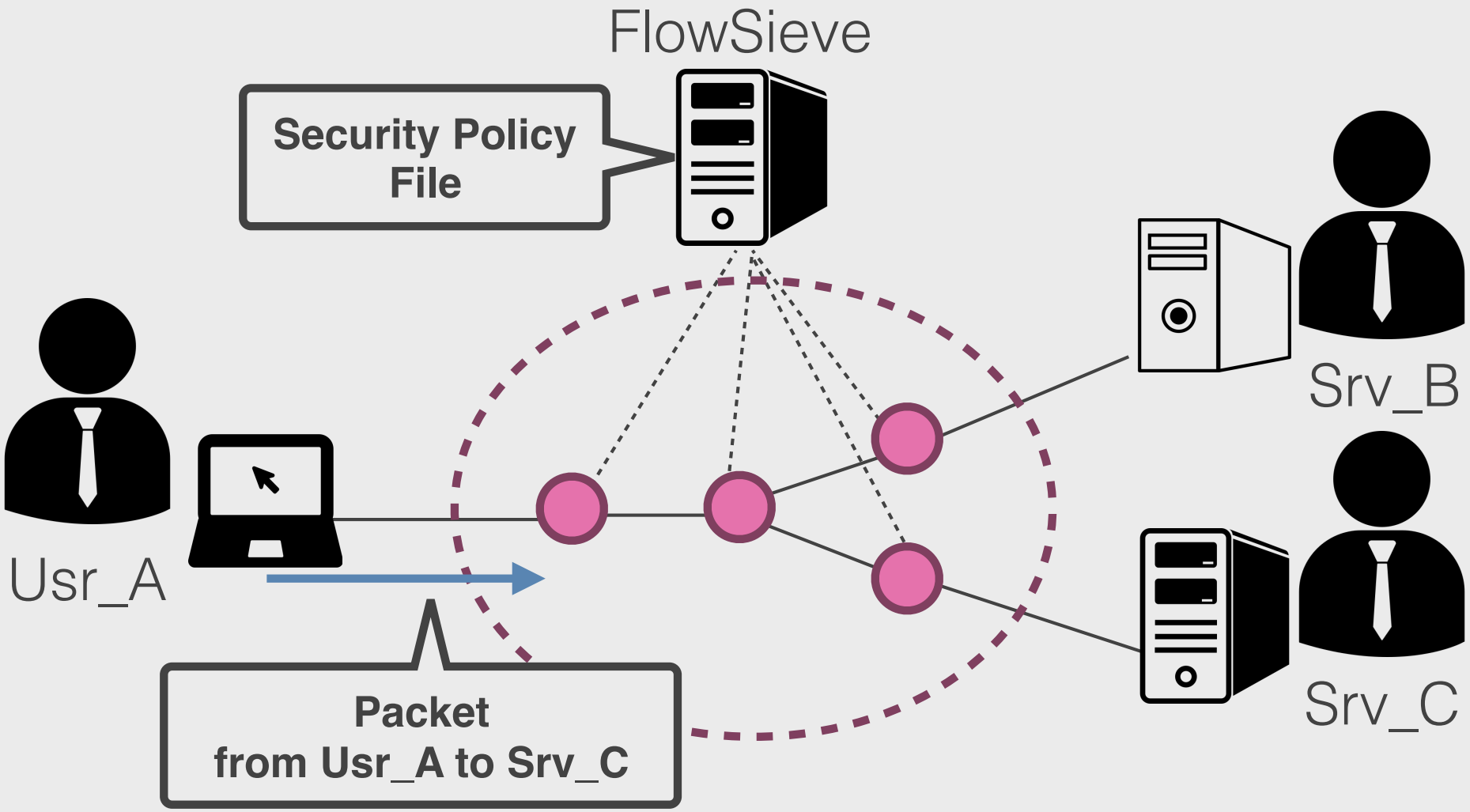
When a user sends a packet,
FlowSieve judge this access is allowed or not.

FlowSieve in Action



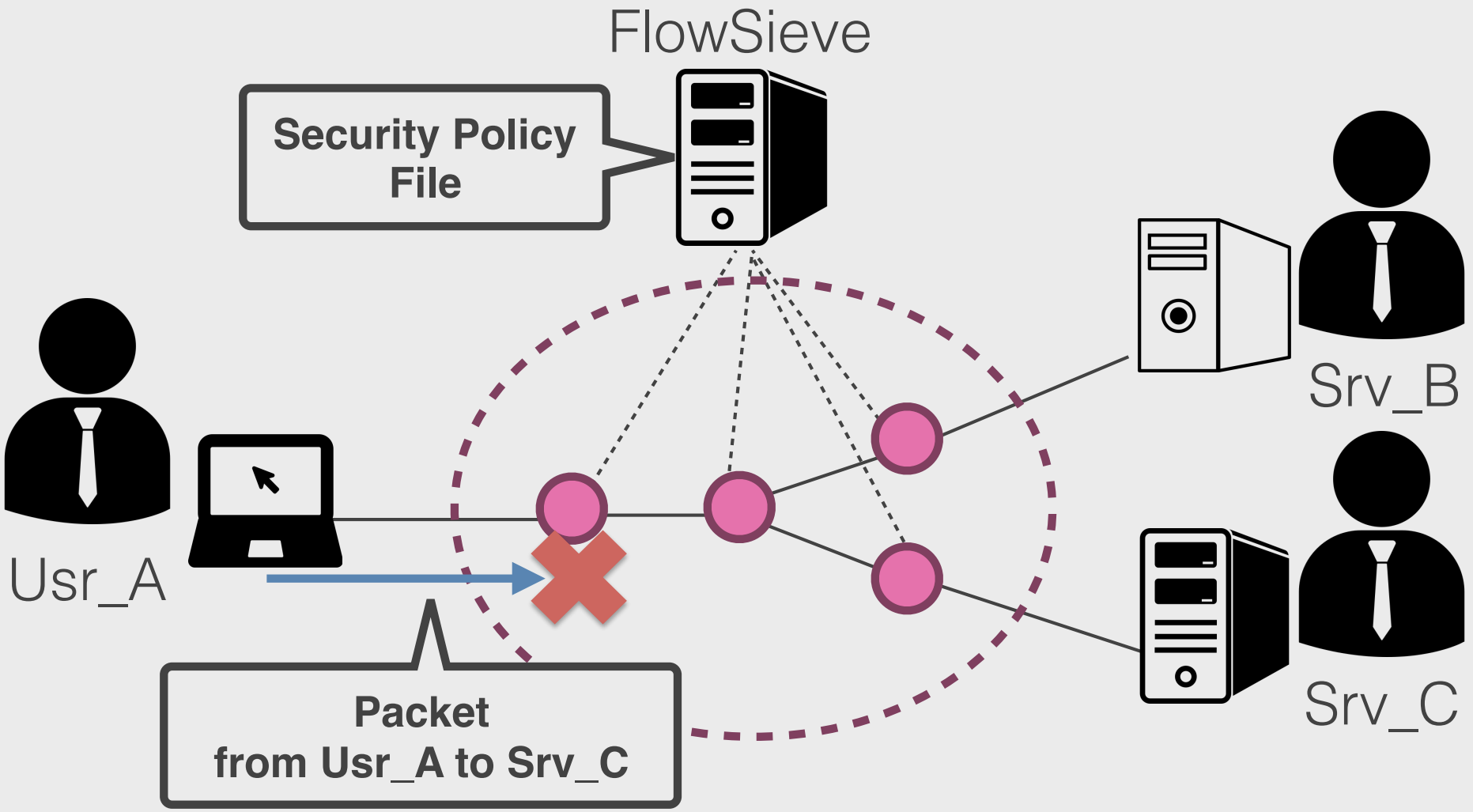
When a user sends a packet,
FlowSieve judge this access is allowed or not.

FlowSieve in Action



If FlowSieve denies that access,
the packet is dropped in an OpenFlow switch.

FlowSieve in Action

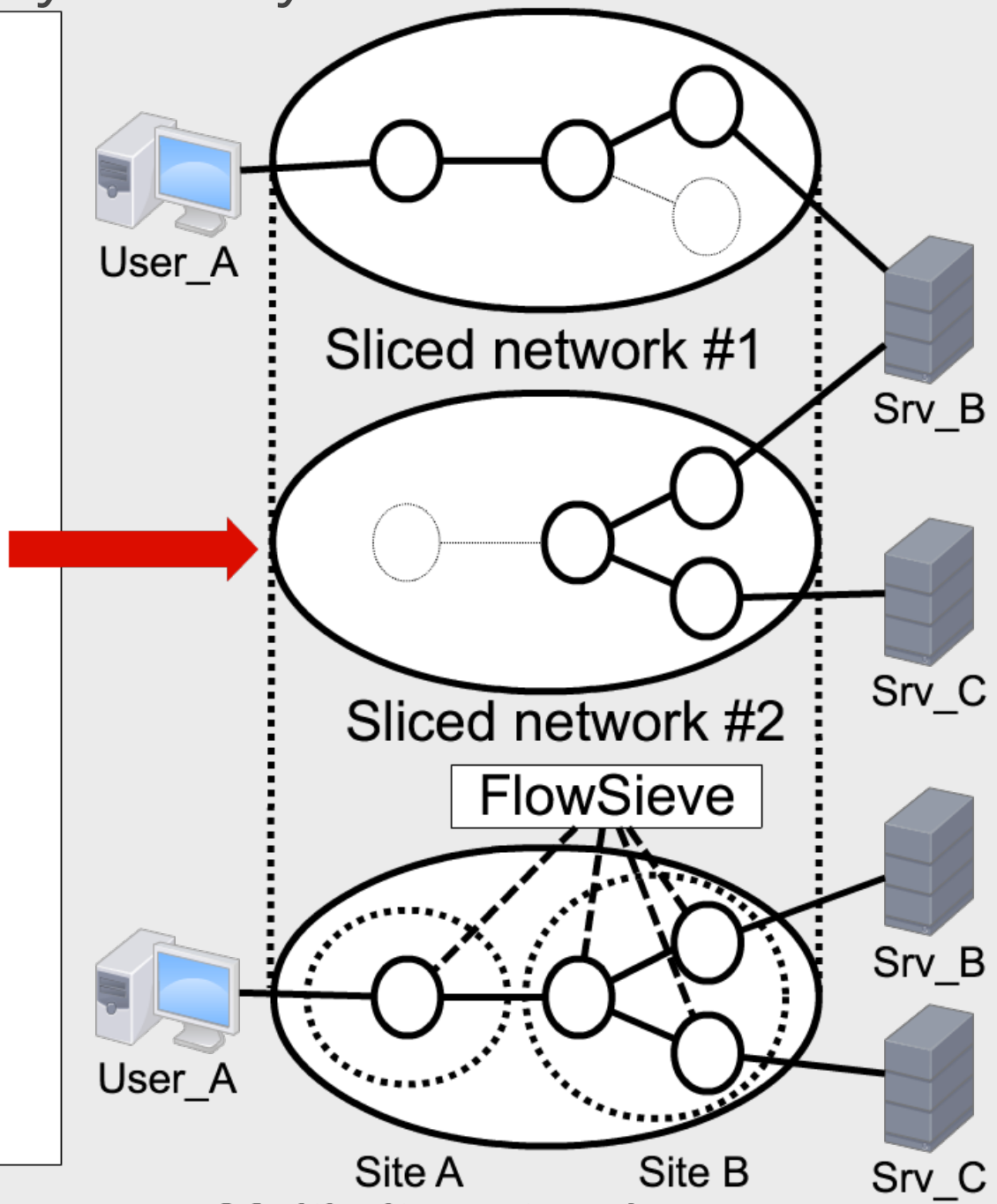


If FlowSieve denies that access,
the packet is dropped in an OpenFlow switch.

Sample of Security Policy & Sliced Network

```
roles:
      - name: A
        allowed_roles:
          - B
      - name: B
        allowed_roles:
          - A
          - C
      - name: C
        allowed_roles:
          - B
users:
      - name: User_A
        role: A
      - name: Srv_B
        role: B
      - name: Srv_C
        role: C
```

Security Policy File



Multi-site network resources