MSNETVIEWS: GEOGRAPHICALLY DISTRIBUTED MANAGEMENT OF ENTERPRISE NETWORK SECURITY POLICY

Iffat Anjum, Jessica Sokal, Hafiza Ramzah Rehman, **Ben Weintraub**, Ethan Leba, William Enck, Cristina Nita-Rotaru, Bradley Reaves

NC STATE UNIVERSITY

NORTHEASTERN UNIVERSITY 18 98 LVX VERITAS VIRTVS

SACMAT 2023

Talk outline

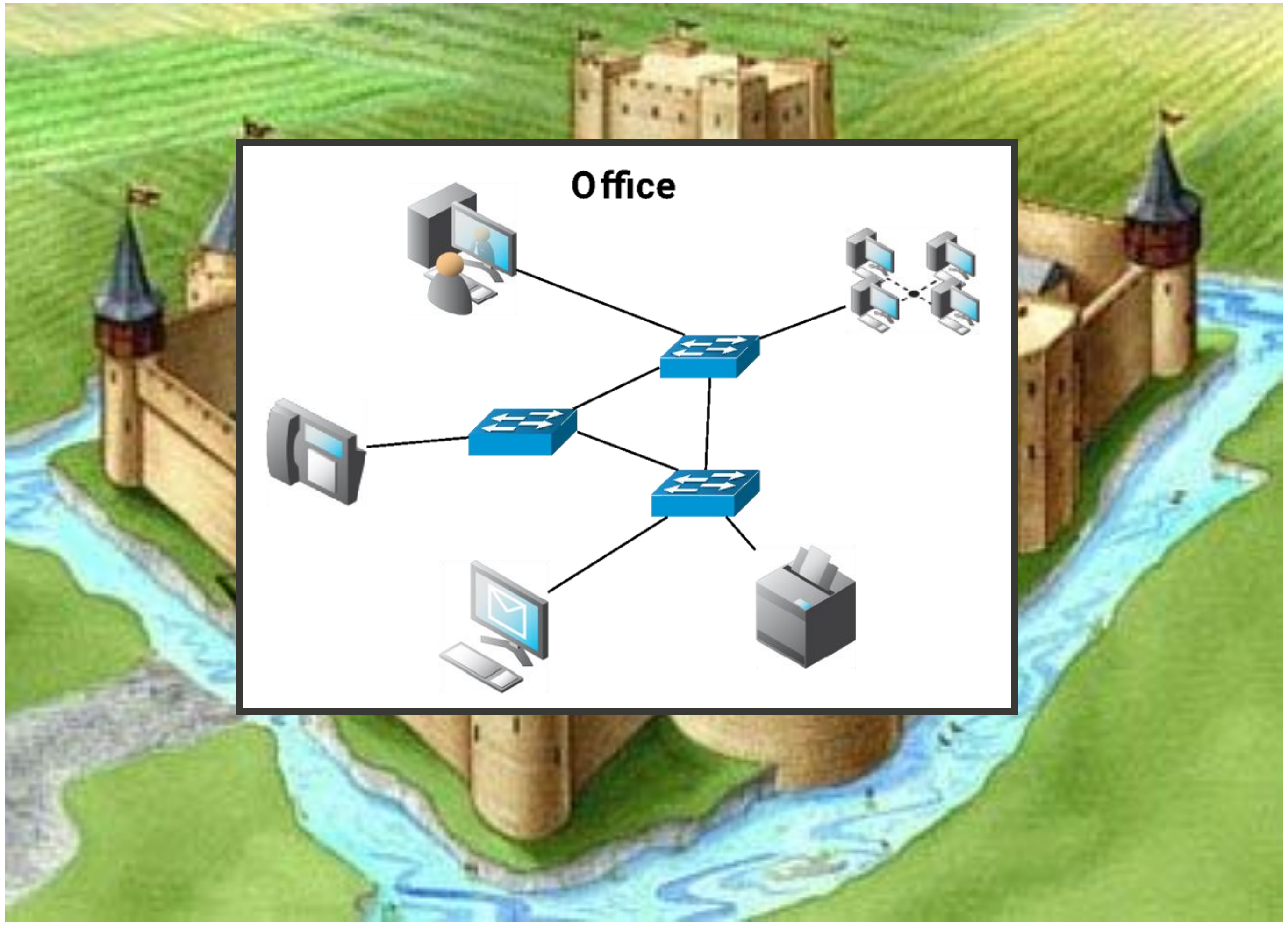
- Motivation
- Zero Trust and Prior Work
- MSNetViews
- Evaluation

Talk outline

- Motivation
- Zero Trust and Prior Work
- MSNetViews
- Evaluation

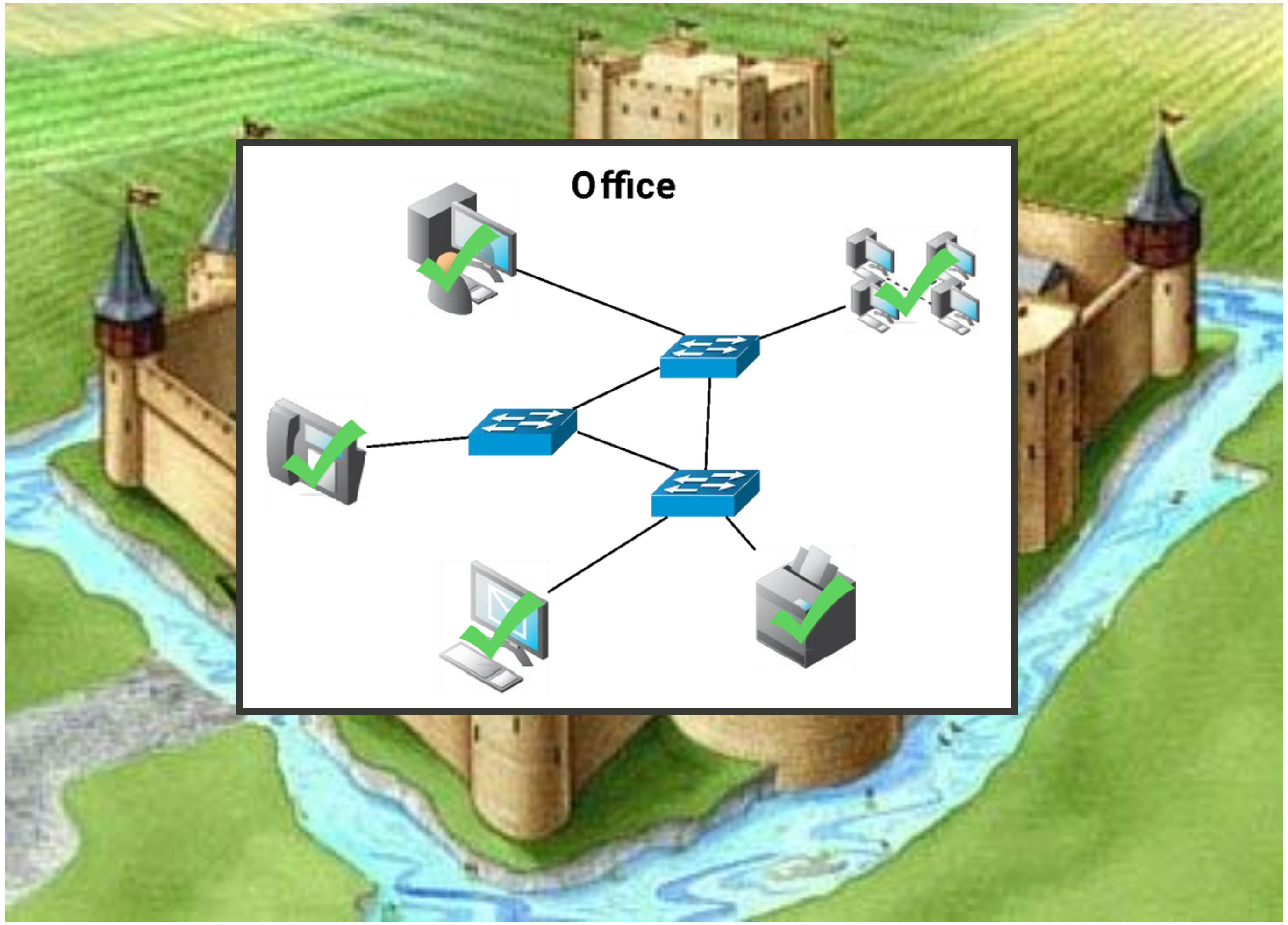
Once upon a time…

- Networks were protected by secure perimeters
  - "Castle-and-moat defense"



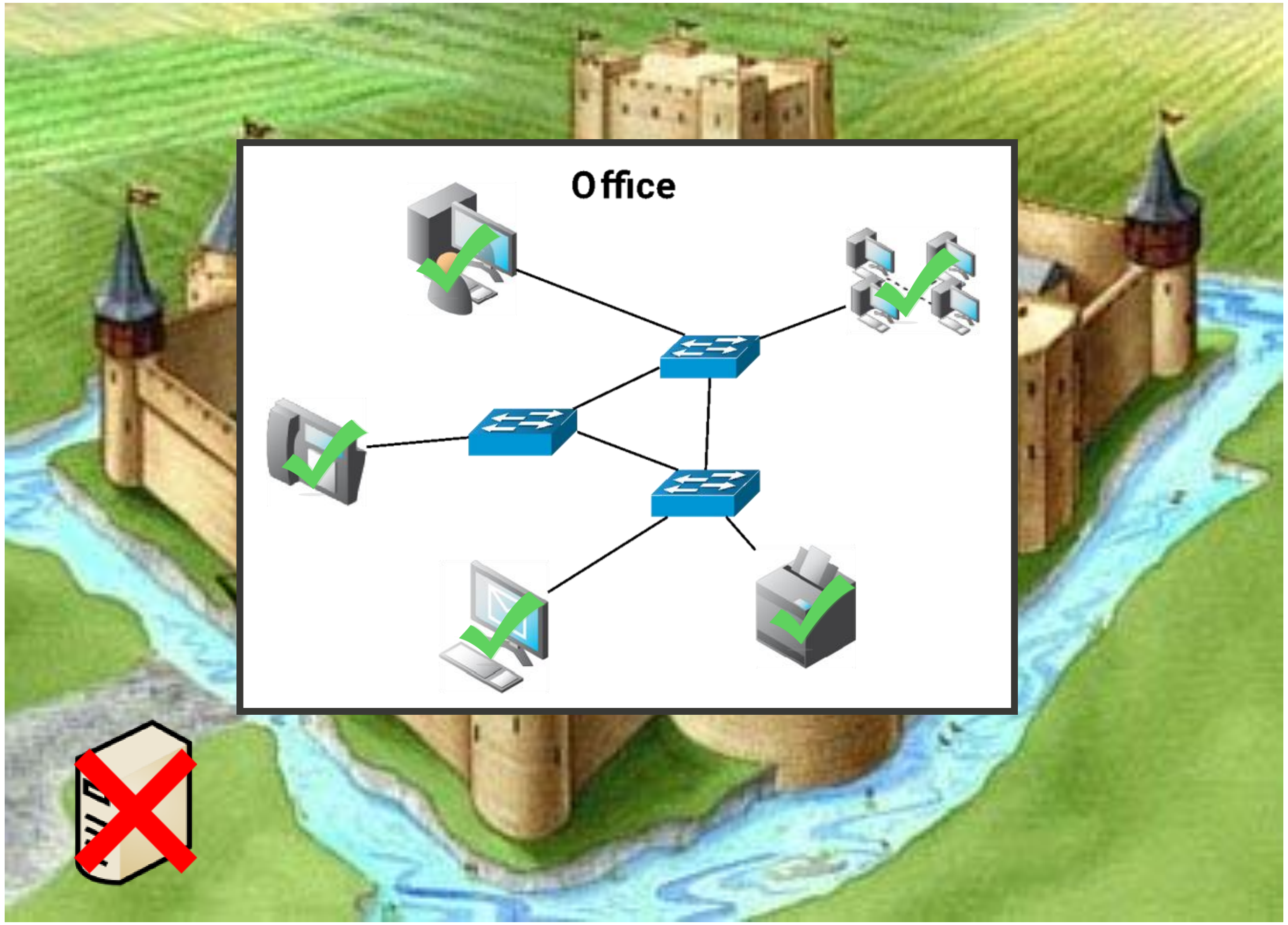
Once upon a time…

- Networks were protected by secure perimeters
  - "Castle-and-moat defense"
- Users on the inside were trusted



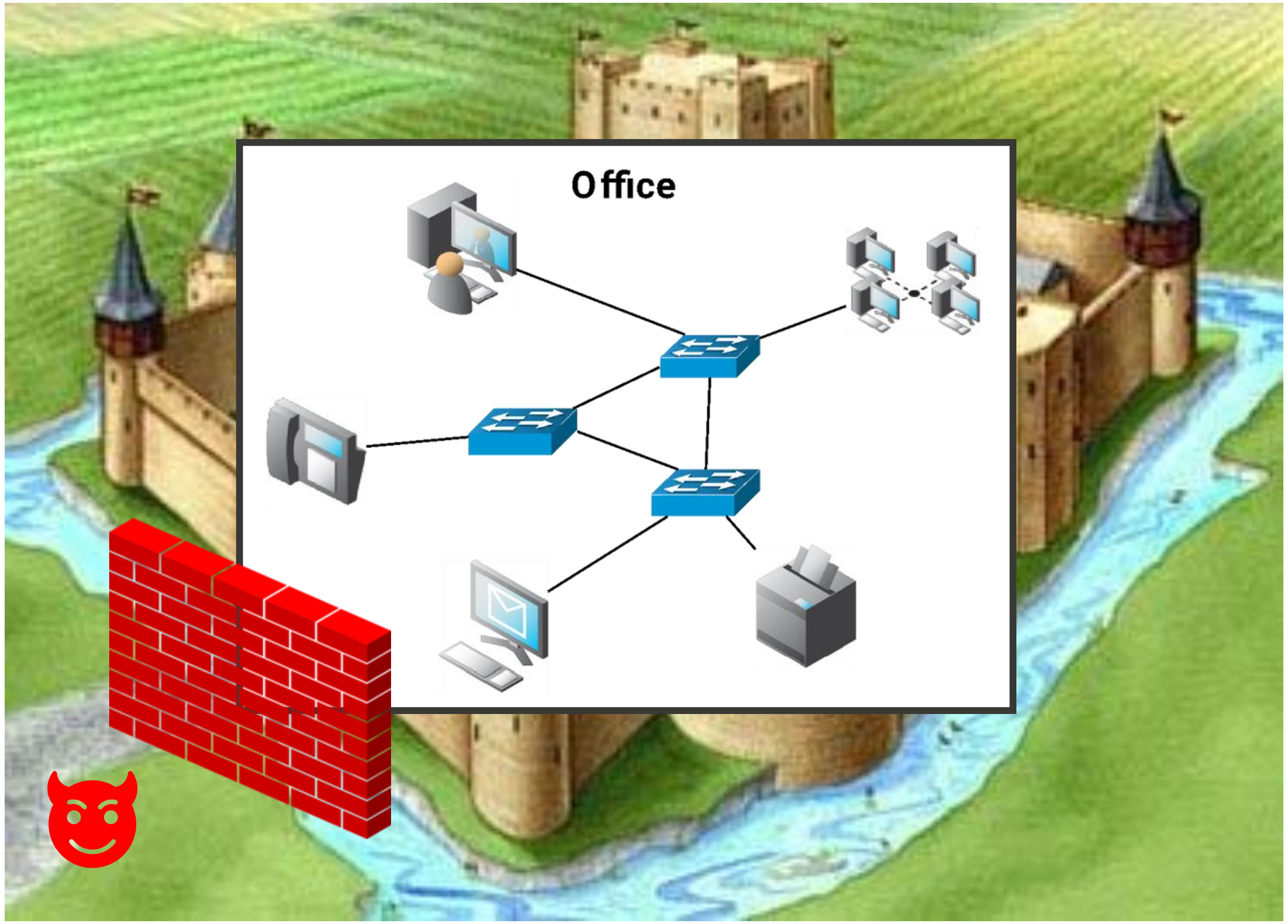
Once upon a time...

- Networks were protected by secure perimeters
  - "Castle-and-moat defense"
- Users on the inside were trusted
- Users on the outside were not



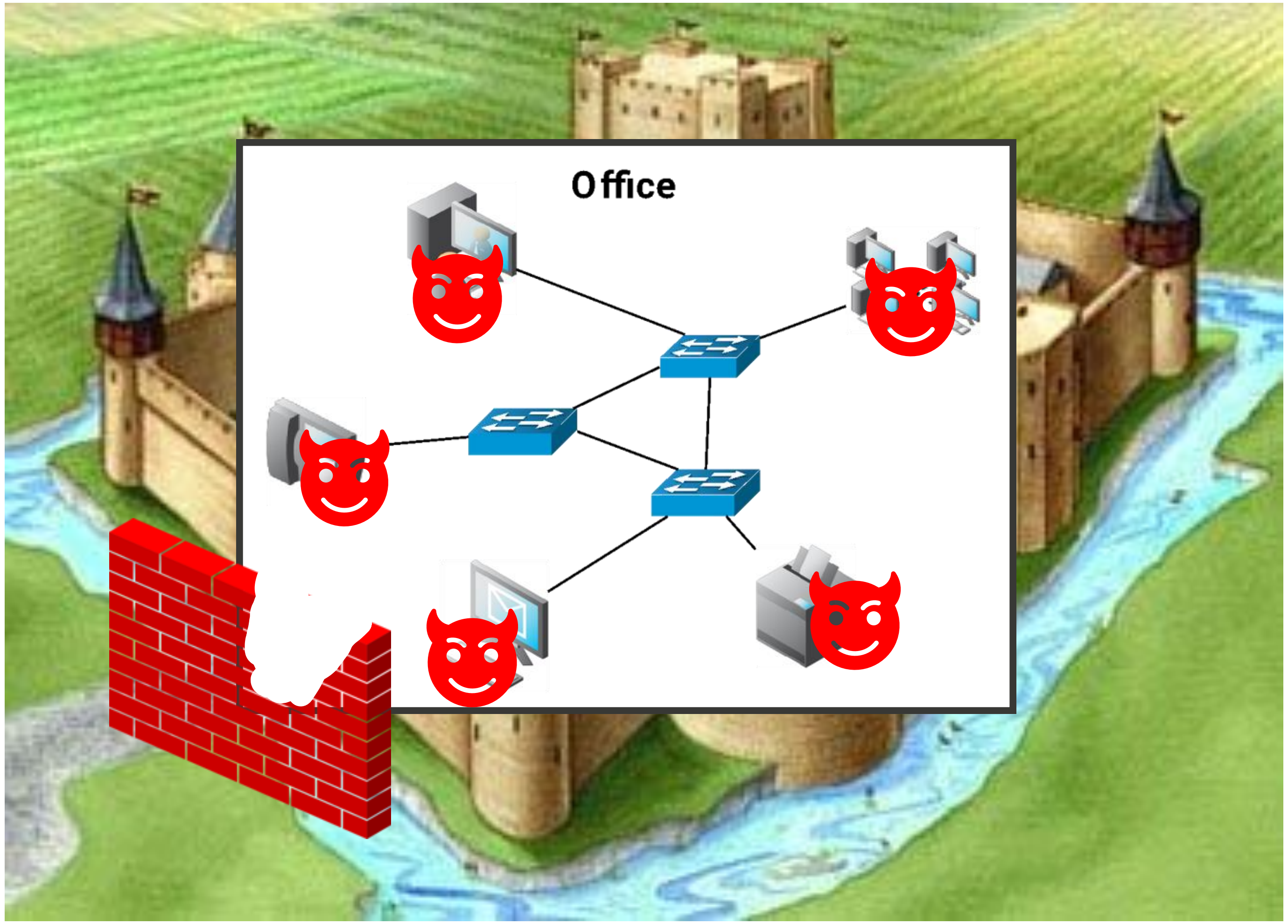
Problem #1: Lateral movement

- Attackers had a hard time getting in



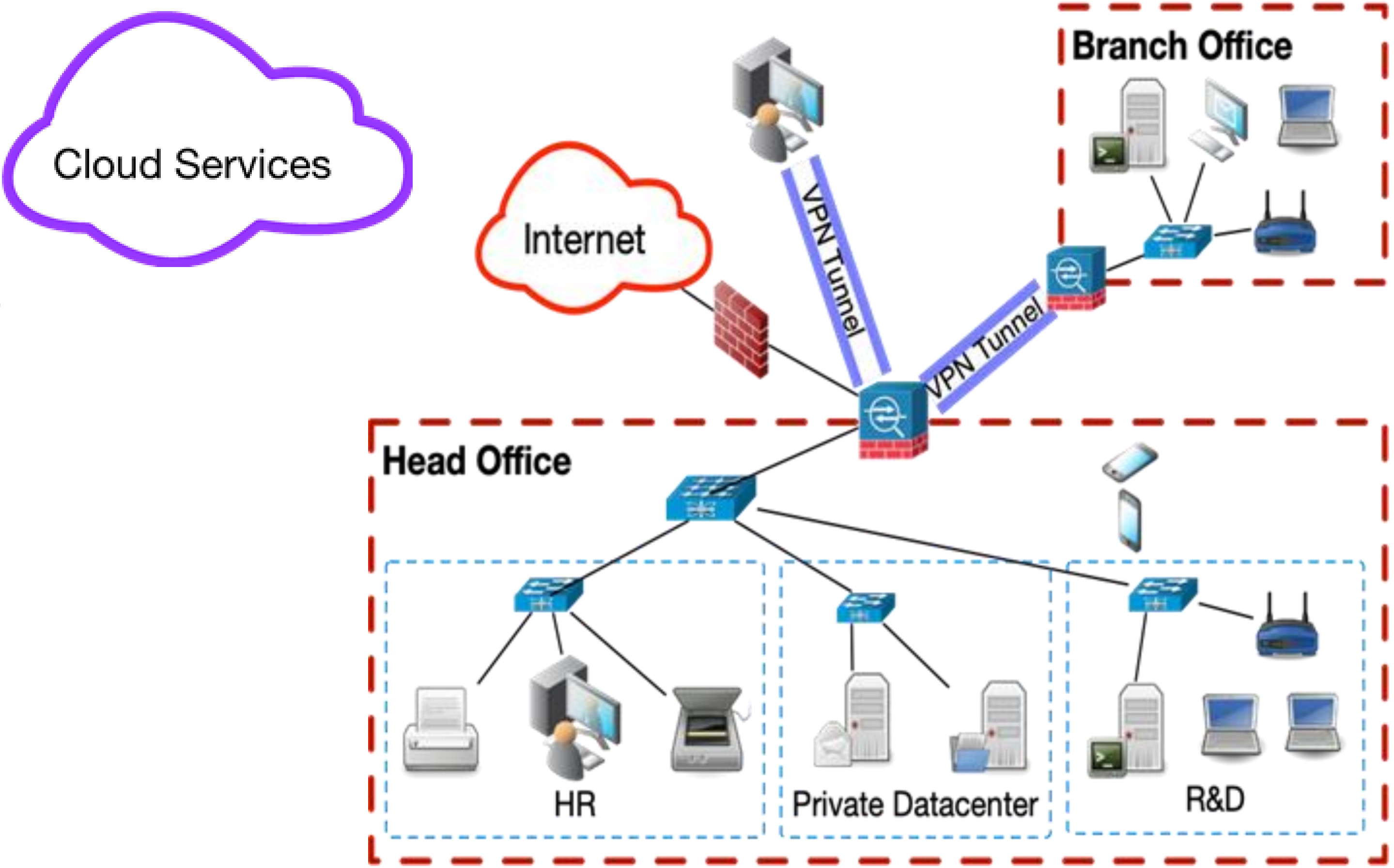
Problem #1: Lateral movement

- Attackers had a hard time getting in
- But once inside,
  became hard to contain



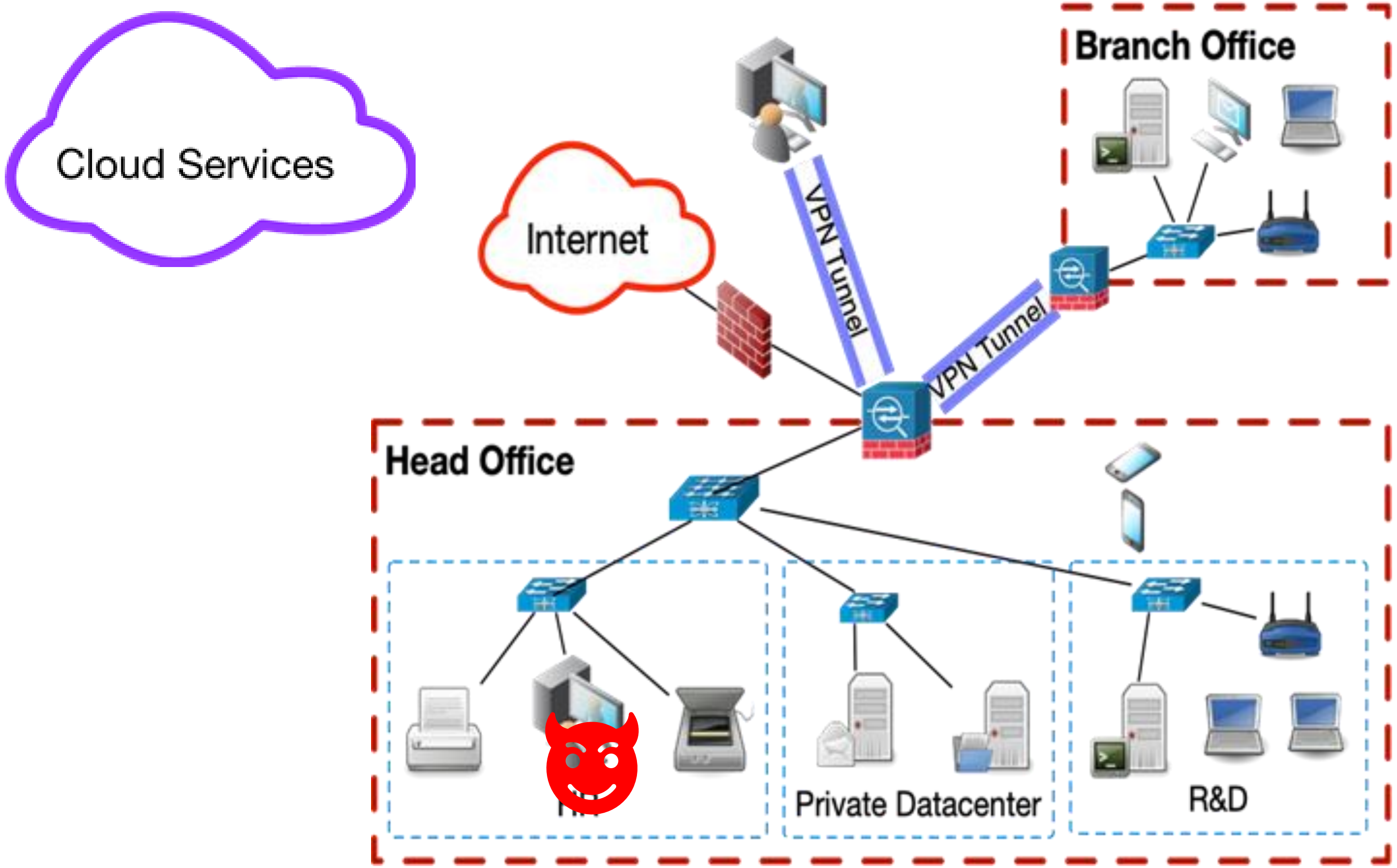
Problem #2: Distributed offices

- Enterprises no longer have their data or users in just one place
- Where should the perimeter be?



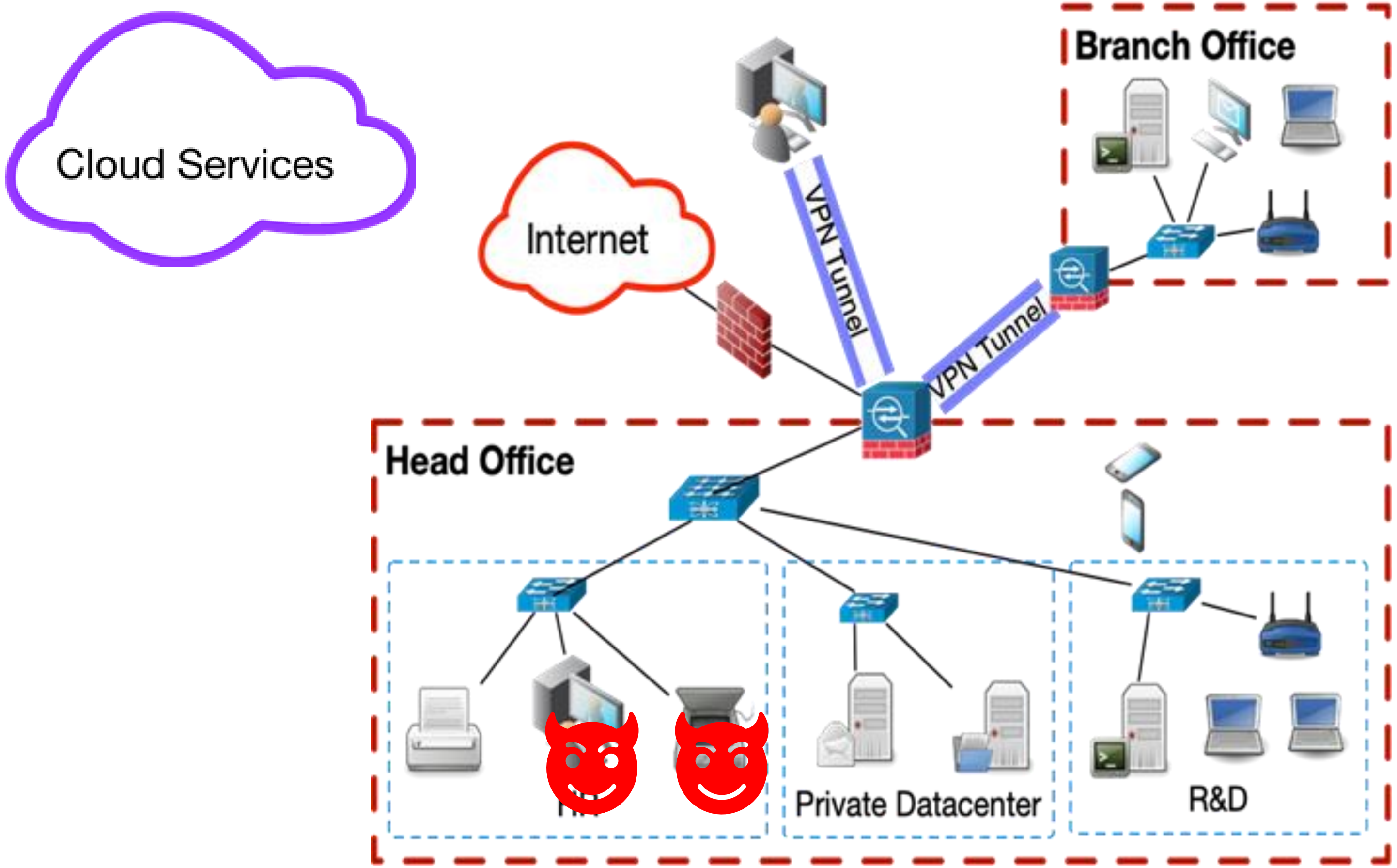
Problem #3: Advanced persistent threats

- An attacker may infiltrate a system on day one



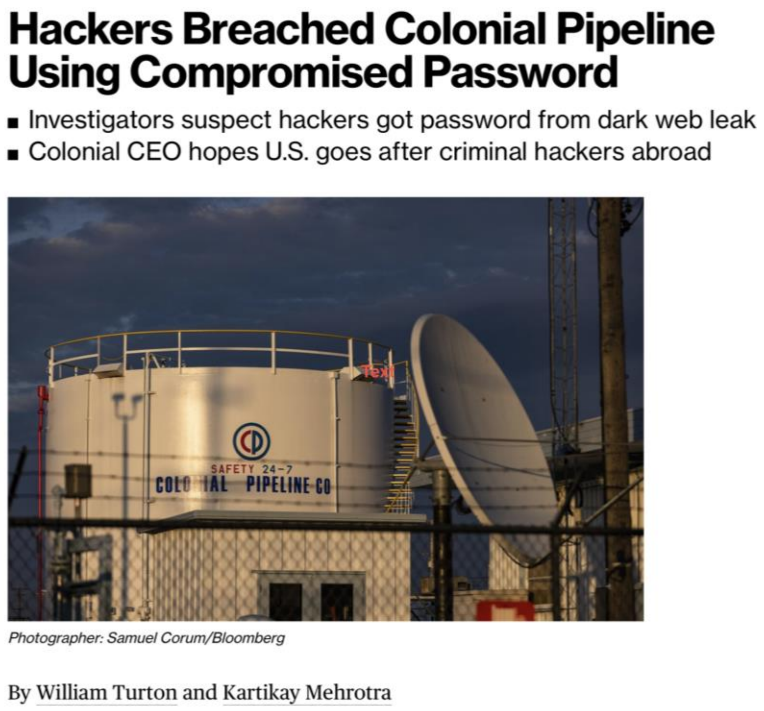
Problem #3: Advanced persistent threats

- An attacker may infiltrate a system on day one
- But not move laterally until many days later
  - Makes detection difficult



These problems are real

- Colonial Pipeline temporarily halted all **5,500 miles** of pipeline operations
- **45% of pipeline operators** were affected
- **17 states** declared a state of emergency
- Paid a ransom of **4.4M USD**



Hackers Breached Colonial Pipeline Using Compromised Password

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

Photographer: Samuel Corum/Bloomberg

By William Turton and Kartikay Mehrotra

Talk outline

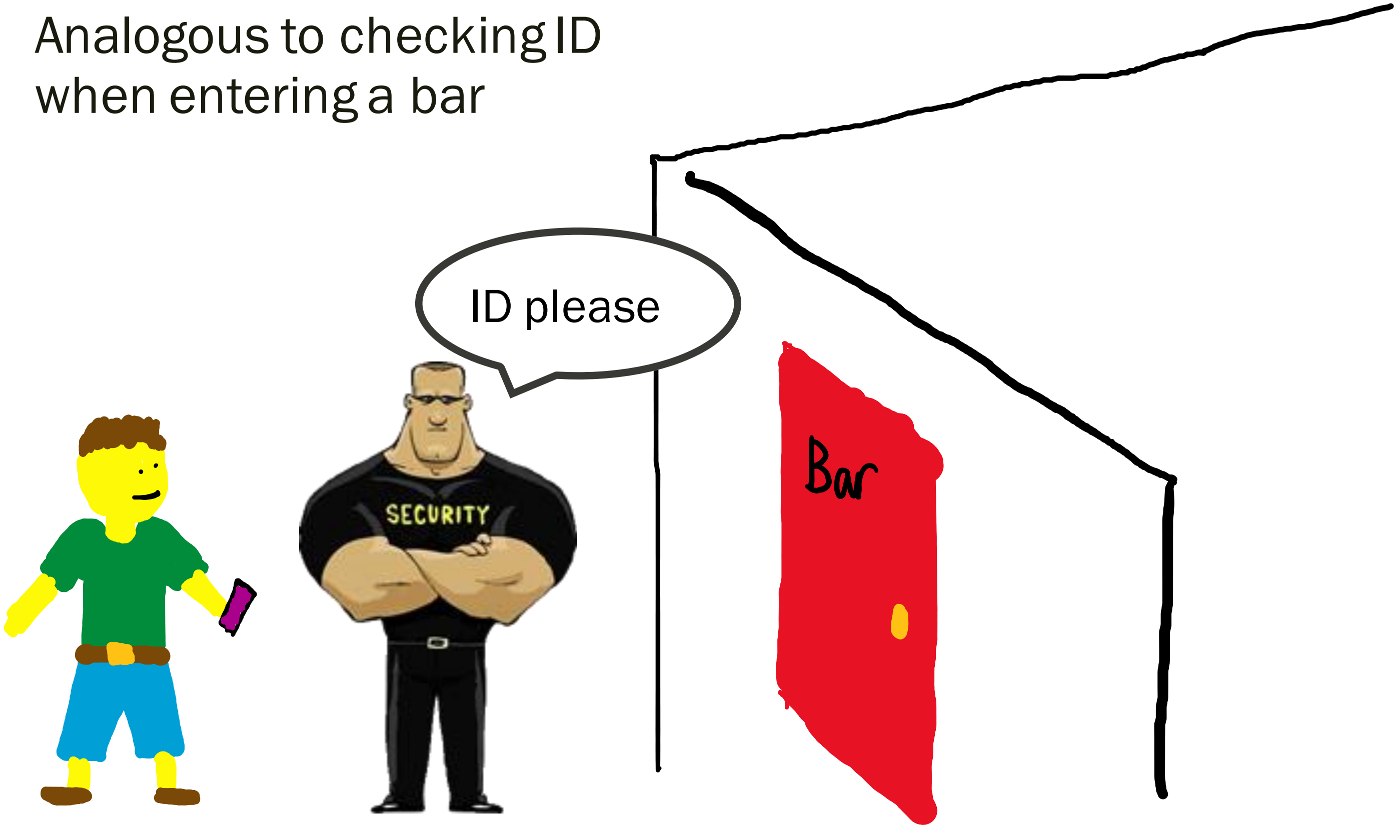
- Motivation
- Zero Trust and Prior Work
- MSNetViews
- Evaluation

Zero trust

- Old paradigm
  - "Trust but verify"

Zero trust

- Old paradigm
  - "Trust but verify"
  - Analogous to checking ID when entering a bar

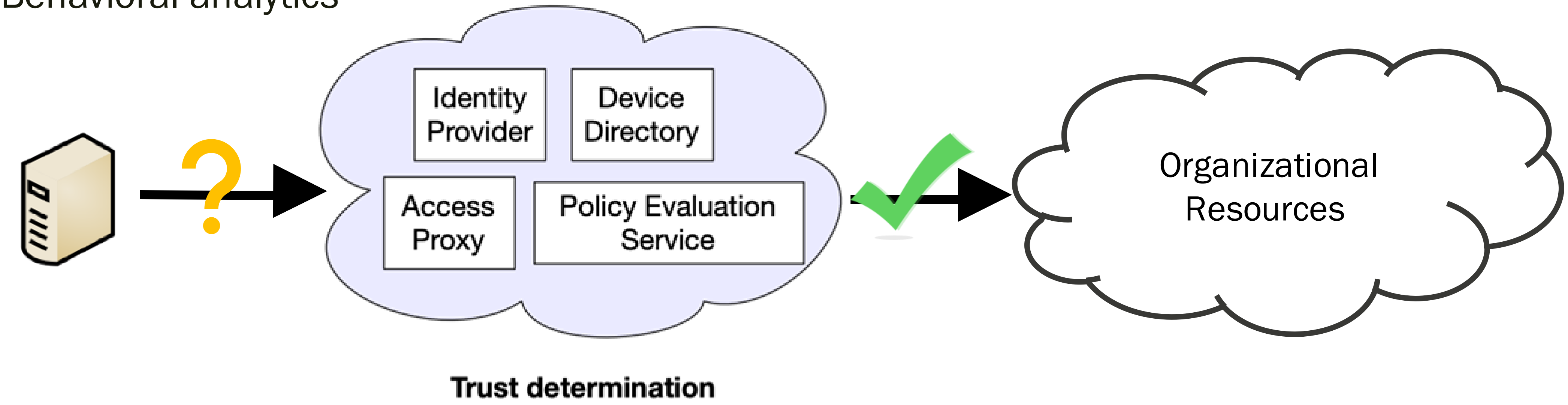


Zero trust

- Old paradigm
  - "Trust but verify"
  - Analogous to checking ID when entering a bar
- Zero trust paradigm
  - "Never trust, always verify"
  - Like checking ID when ordering each drink

Zero trust in practice

- Popularized by Google's BeyondCorp
- Critical services operate in cloud
- Multi-factor authentication
- Device attestation
- Behavioral analytics



ZT is nice in theory, but …

- It's not possible to move everything to Cloud
  - Workstations
  - development/file servers,
  - device management interfaces
  - Etc.
- What about the on-premises network?

ZT is nice in theory, but …

- It's not possible to move everything to Cloud
  - Workstations
  - development/file servers,
  - device management interfaces
  - Etc.
- What about the on-premises network?

In-network defenses are still needed

Prior work: **NetViews**

(SACMAT '22)

- Addresses access control for non-cloud infrastructure
- Uses NGAC policy language
- Relies on SDN infrastructure

  Flow rules enforce access control
- Does not address distributed enterprises

Prior work: **NetViews**

(SACMAT '22)

Addresses access control for non-cloud infrastructure

✓ Uses NGAC policy language

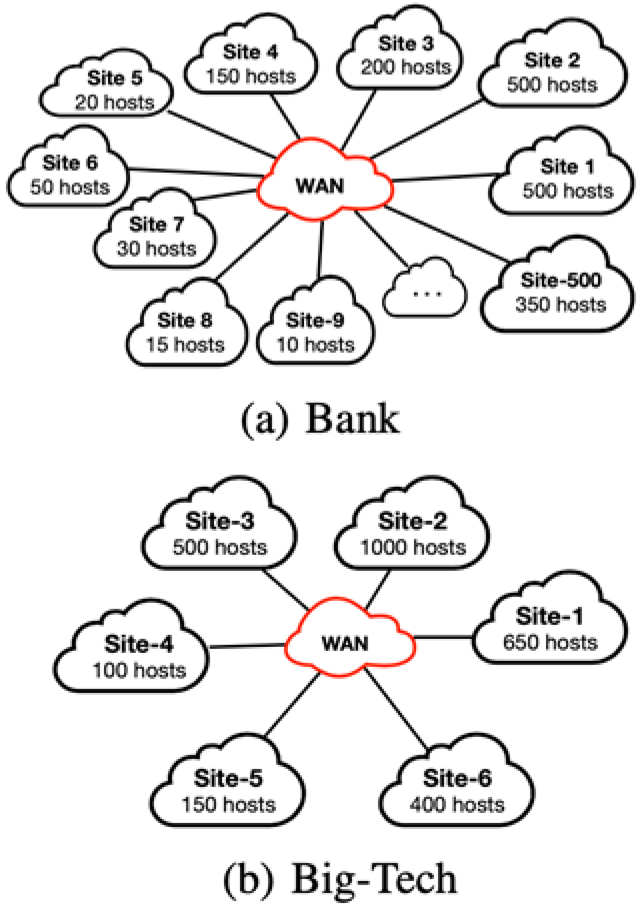
Relies on SDN infrastructure

Flow rules enforce access control

Does not address distributed enterprises

Enterprises with geographically distributed sites introduce new challenges…

- Users commonly move between sites
  - require differentiated **access based on location**

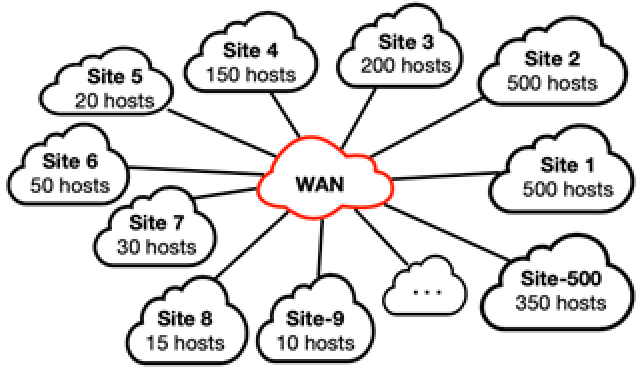


(a) Bank

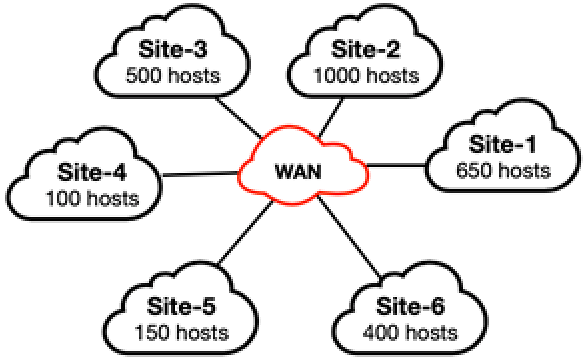
(b) Big-Tech

Enterprises with geographically distributed sites introduce new challenges…

- Users commonly move between sites
  - require differentiated **access based on location**
- Compromise of a single site should **not leak the global policy**



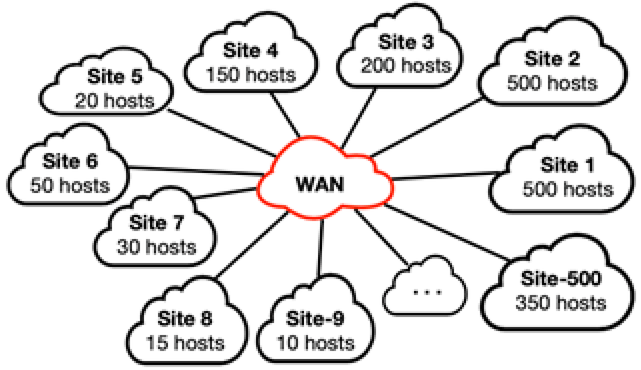
(a) Bank



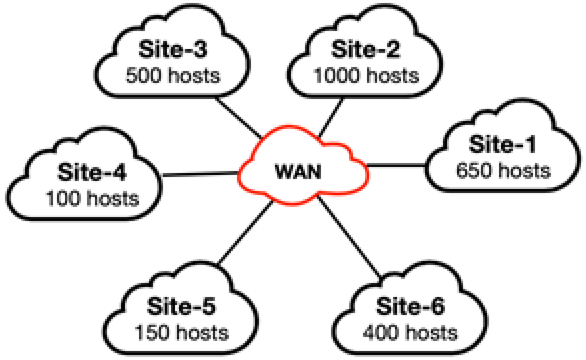
(b) Big-Tech

Enterprises with geographically distributed sites introduce new challenges…

- Users commonly move between sites
  - require differentiated **access based on location**
- Compromise of a single site should **not leak the global policy**
- Only **site administrators should modify policies** for their local resources



(a) Bank



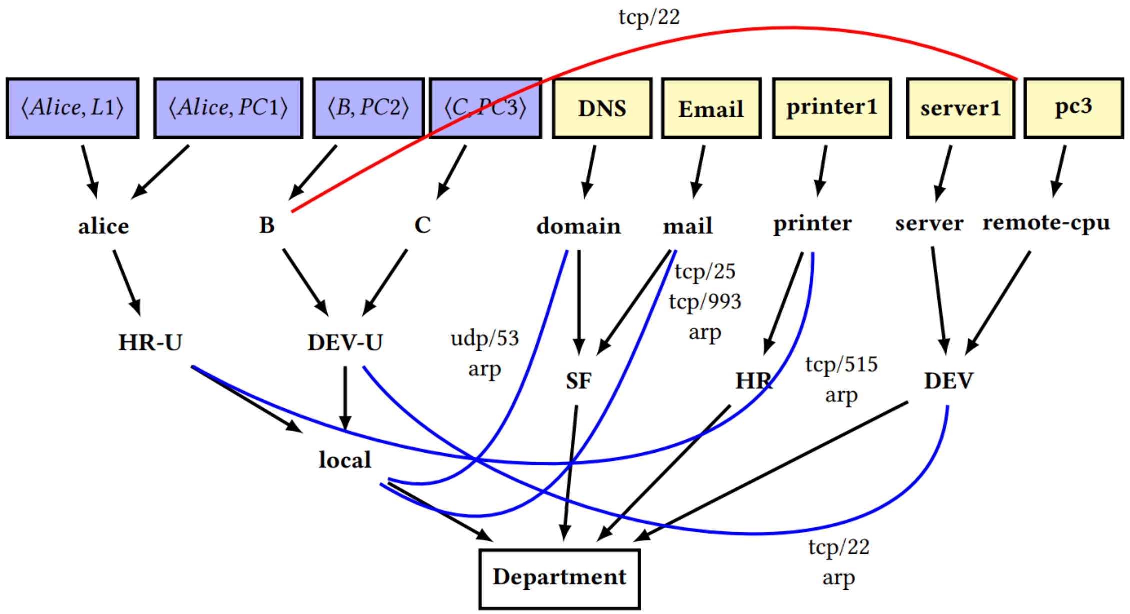
(b) Big-Tech

Talk outline

- Motivation
- Zero Trust and Prior Work
- MSNetViews
- Evaluation

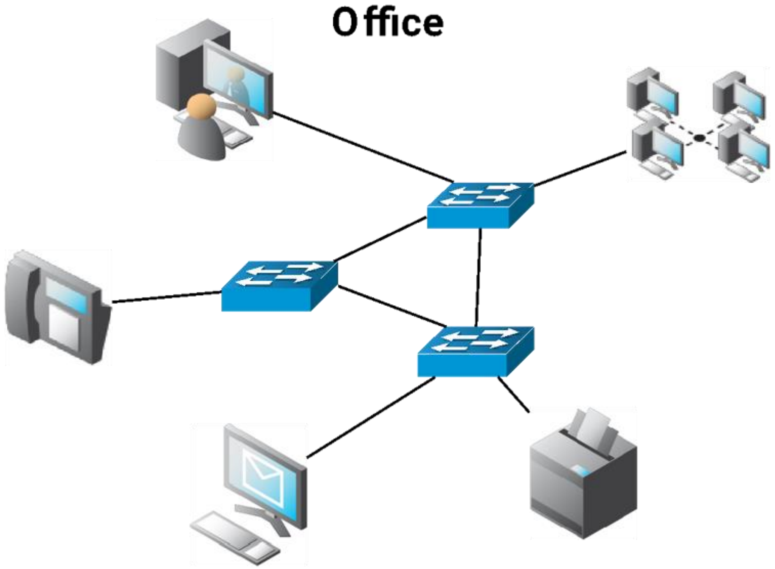
NGAC policies

- NGAC is a policy definition language
  - Defined by NIST in 2015
- Can model both ABAC and RBAC policies
- **Assignments** define hierarchy
- **Associations** define granted permissions
- **Prohibitions** define denied permissions



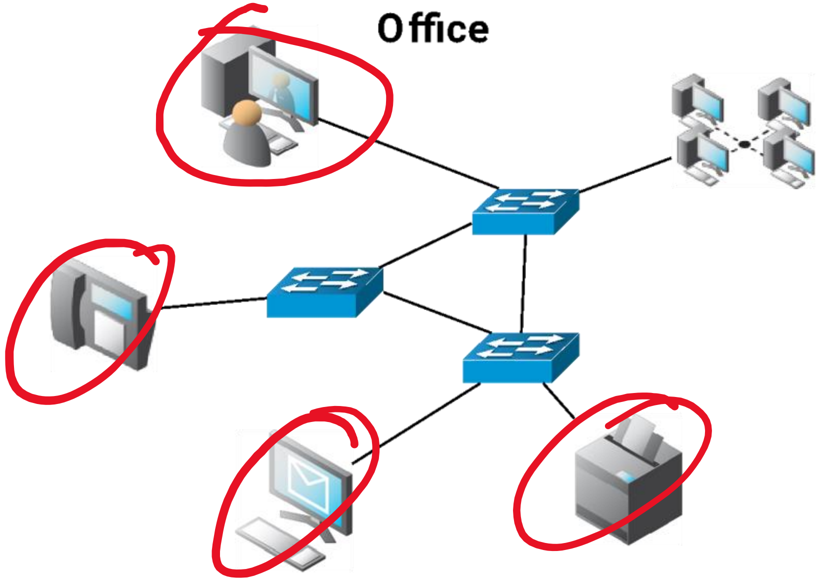
(Anjum et al., 2022)

Software-defined Networking (SDN)



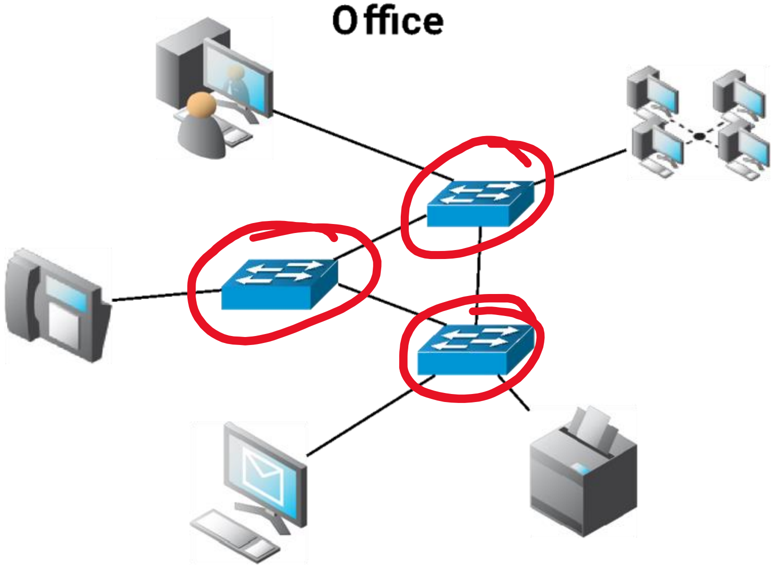
Software-defined Networking (SDN)

- Network consists of
  - Devices



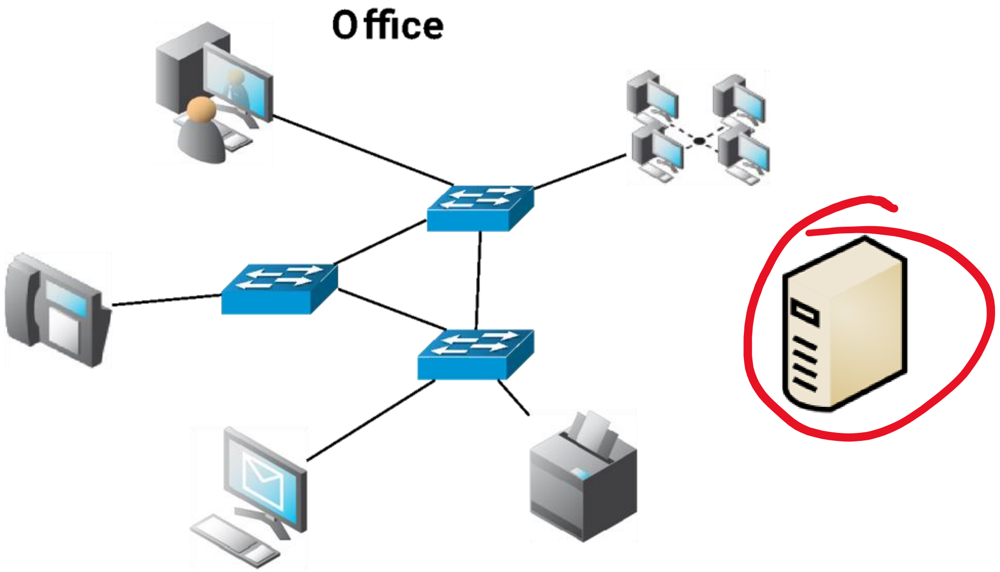
Software-defined Networking (SDN)

- Network consists of
  - Devices
  - Switches



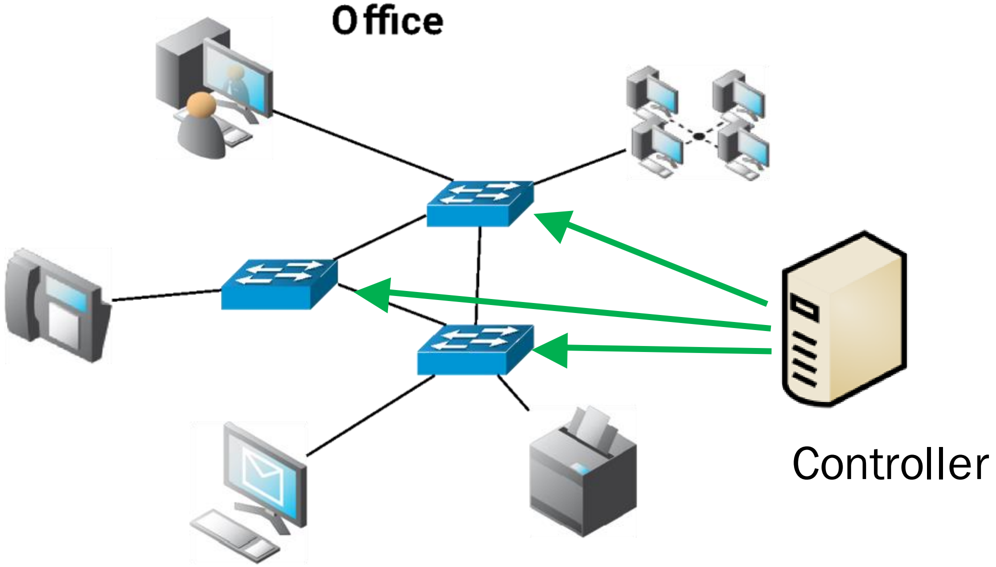
Software-defined Networking (SDN)

- Network consists of
  - Devices
  - Switches
  - Controllers



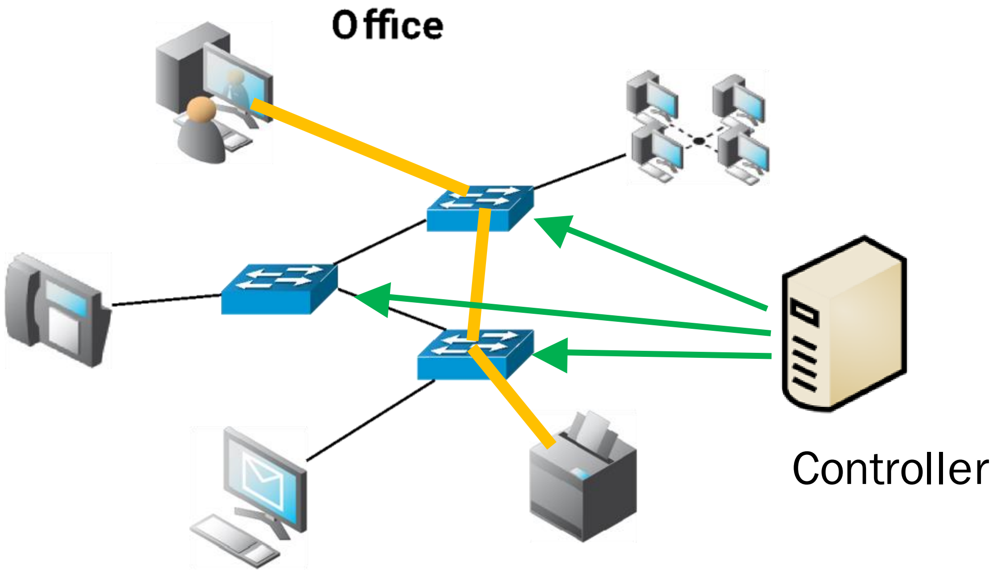
Software-defined Networking (SDN)

- Network consists of
  - Devices
  - Switches
  - Controllers
- Controllers install flow rules on network switches

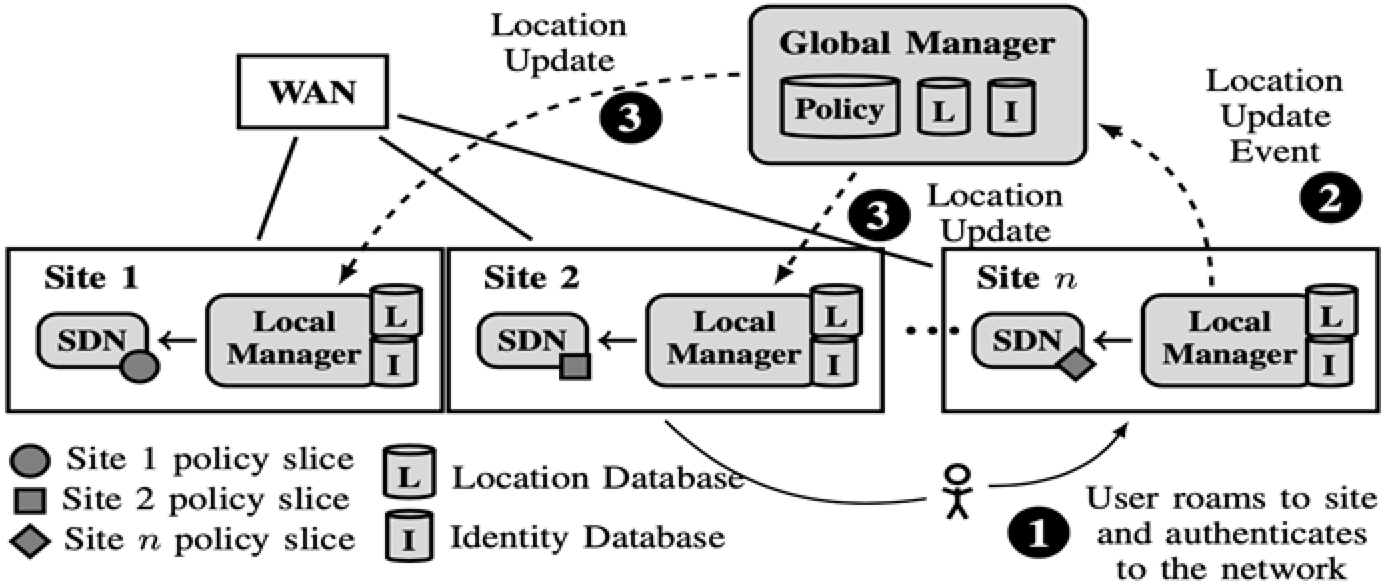


Software-defined Networking (SDN)

- Network consists of
  - Devices
  - Switches
  - Controllers
- Controllers install flow rules on network switches
- Switches use flow rules to route packets between devices and other switches

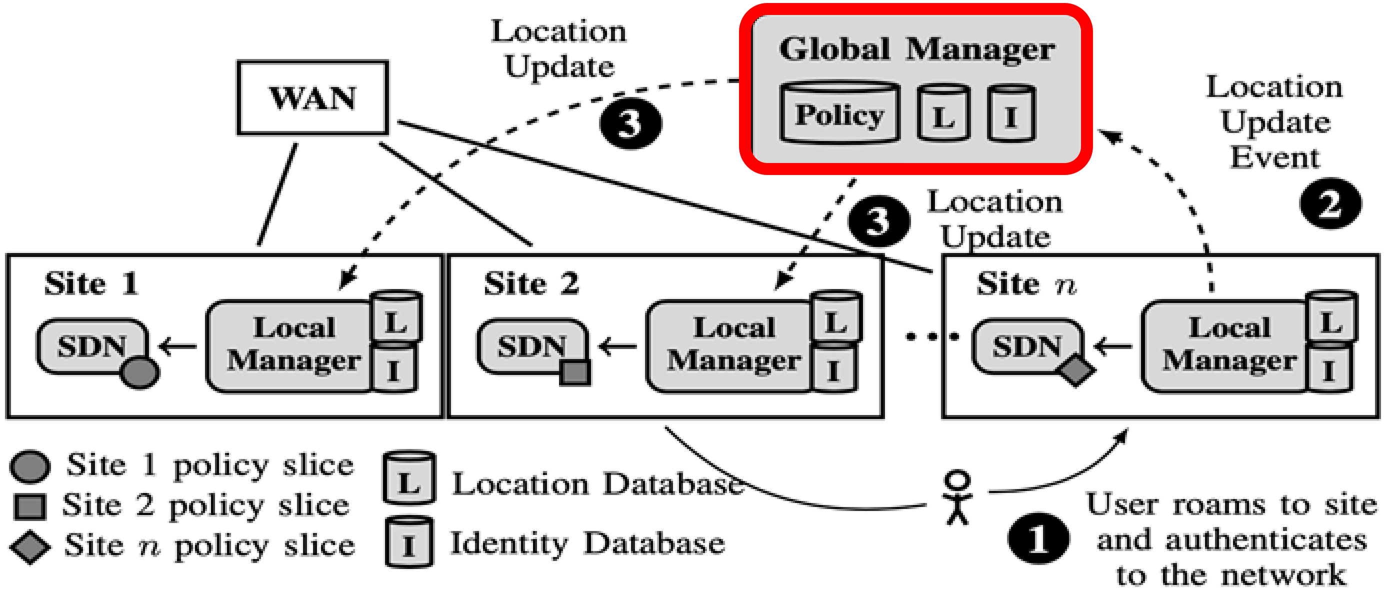


Overview of Multi-Site NetViews



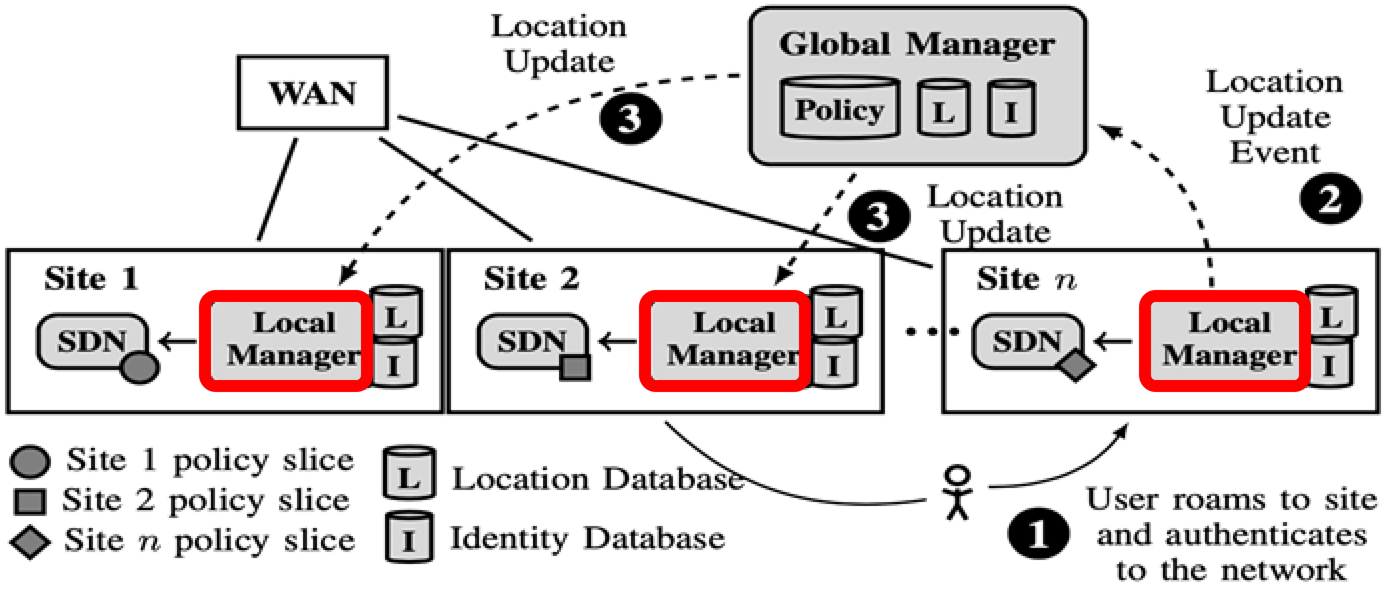
Overview of Multi-Site NetViews

- Global policy management



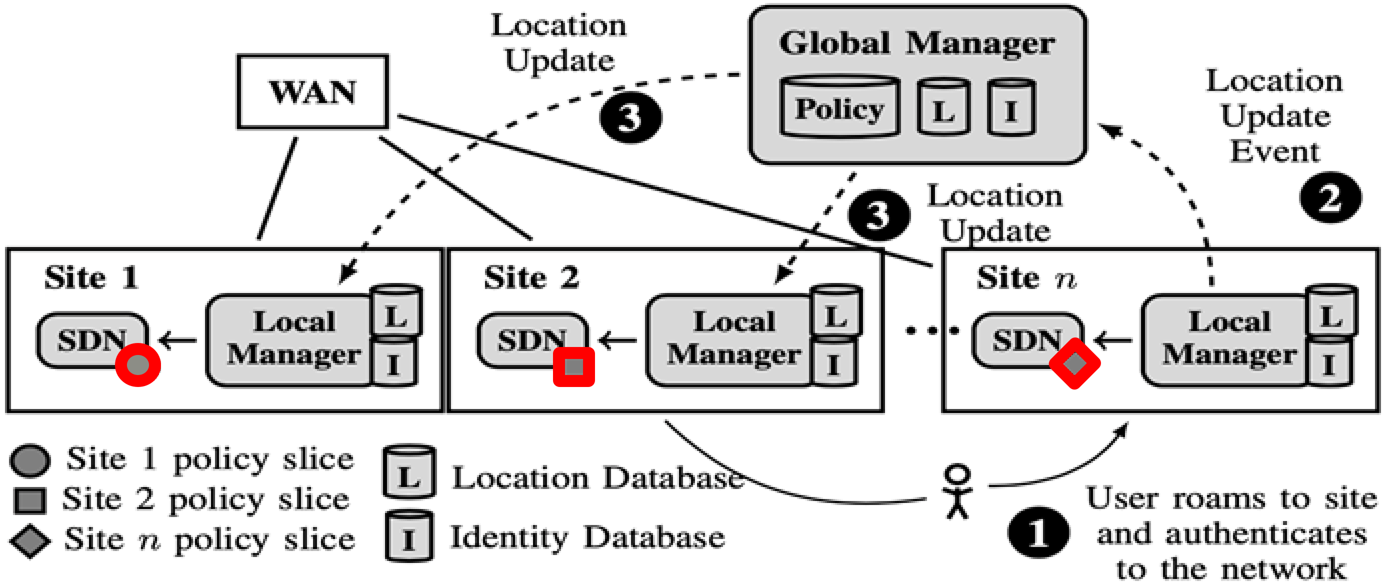
Overview of Multi-Site NetViews

- Global policy management
- Site-local policy management



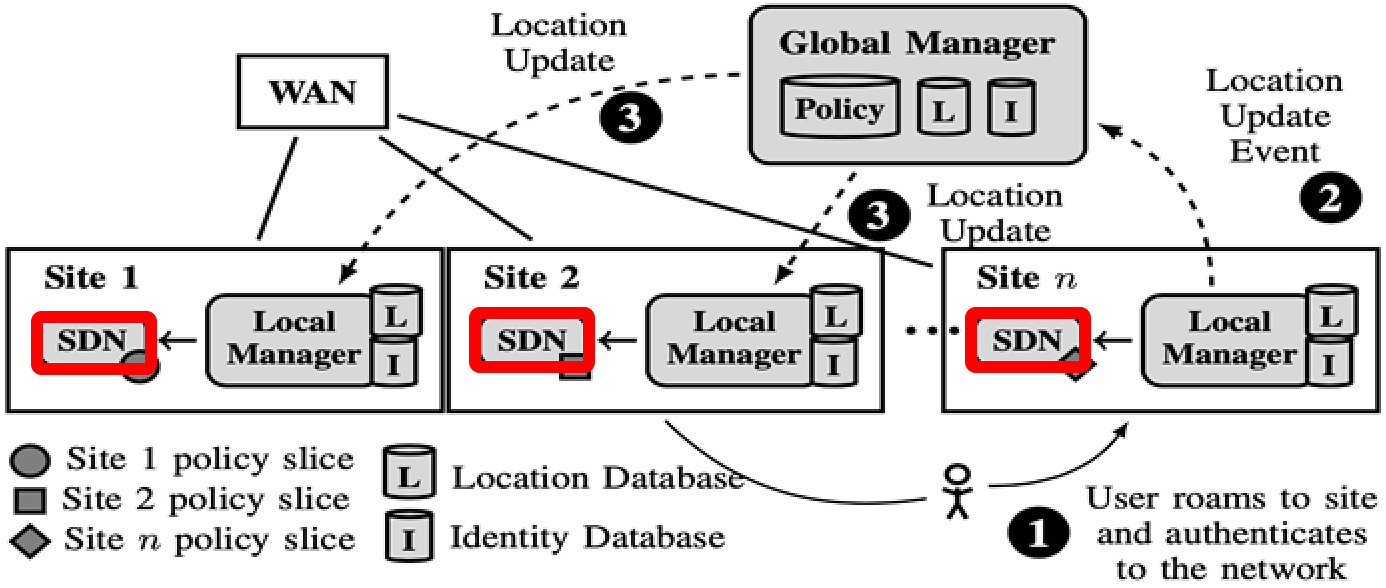
Overview of Multi-Site NetViews

- Global policy management
- Site-local policy management
- Polices defined with NGAC language



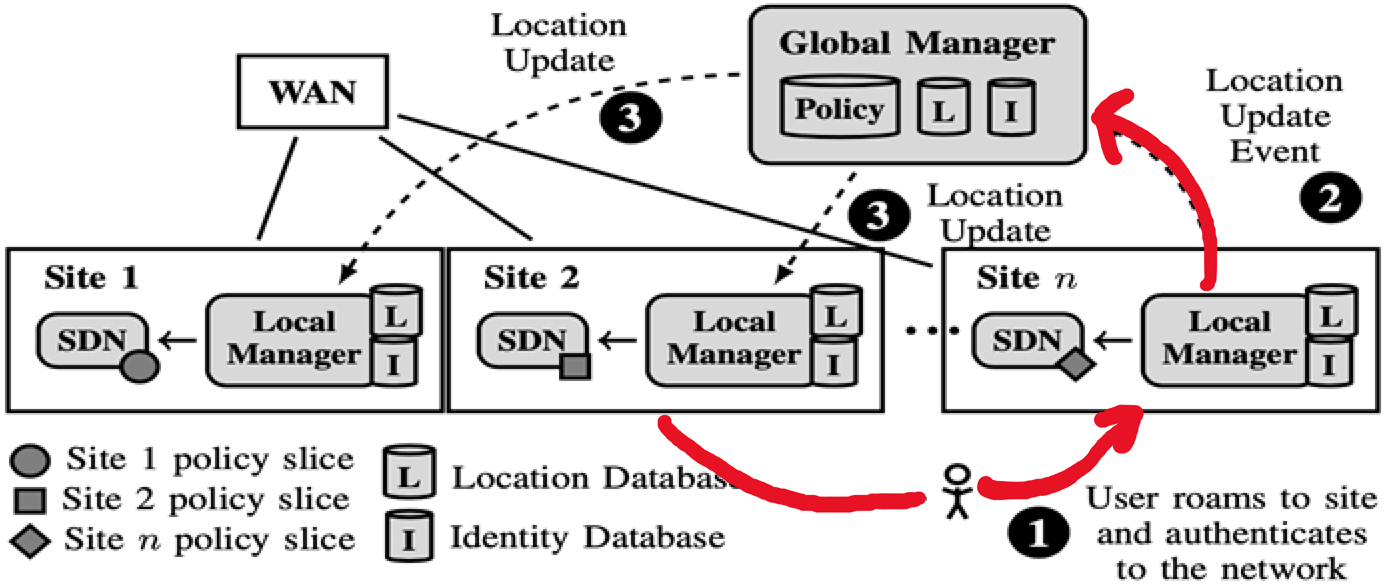
Overview of Multi-Site NetViews

- Global policy management
- Site-local policy management
- Polices defined with NGAC language
- Enforced by SDN flow rules



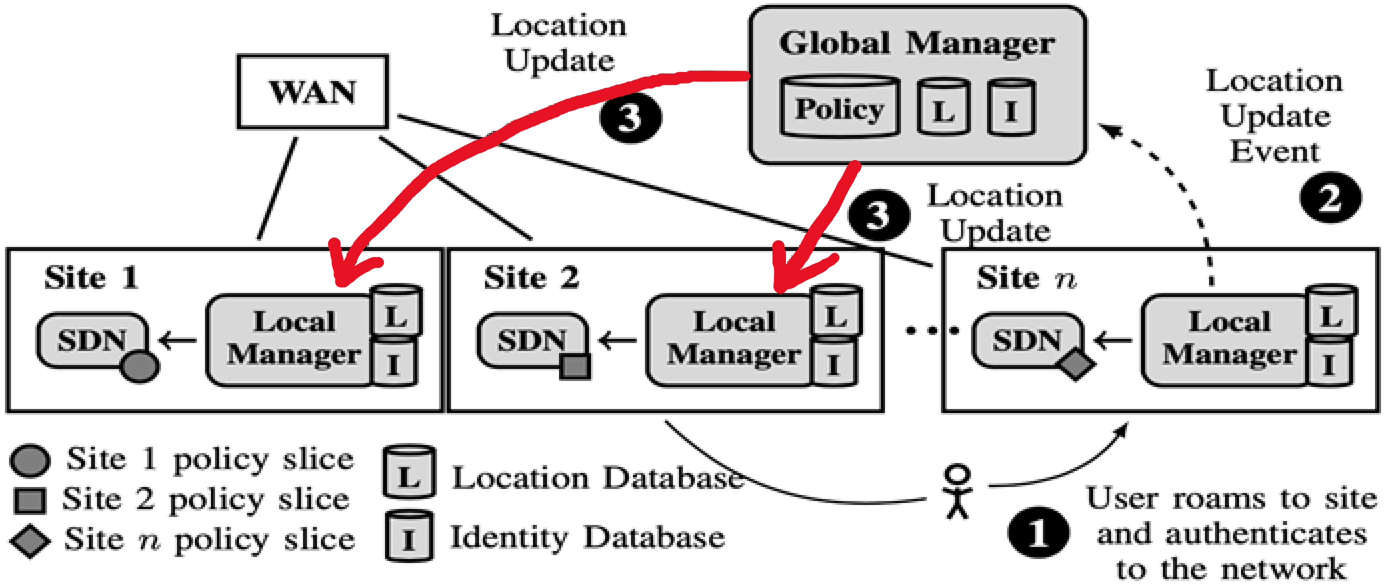
Overview of Multi-Site NetViews

- Global policy management
- Site-local policy management
- Polices defined with NGAC language
- Enforced by SDN flow rules
- Policy reacts to users roaming between sites



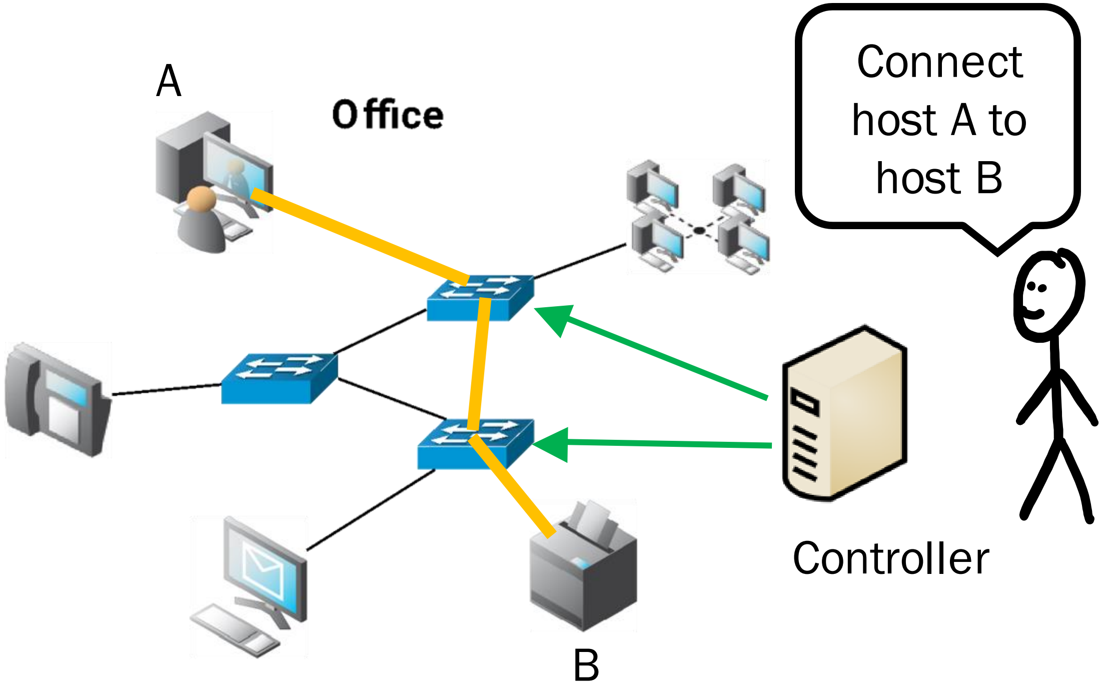
Overview of Multi-Site NetViews

- Global policy management
- Site-local policy management
- Polices defined with NGAC language
- Enforced by SDN flow rules
- Policies react to users roaming between sites
- Policy state is coordinated with a global manager



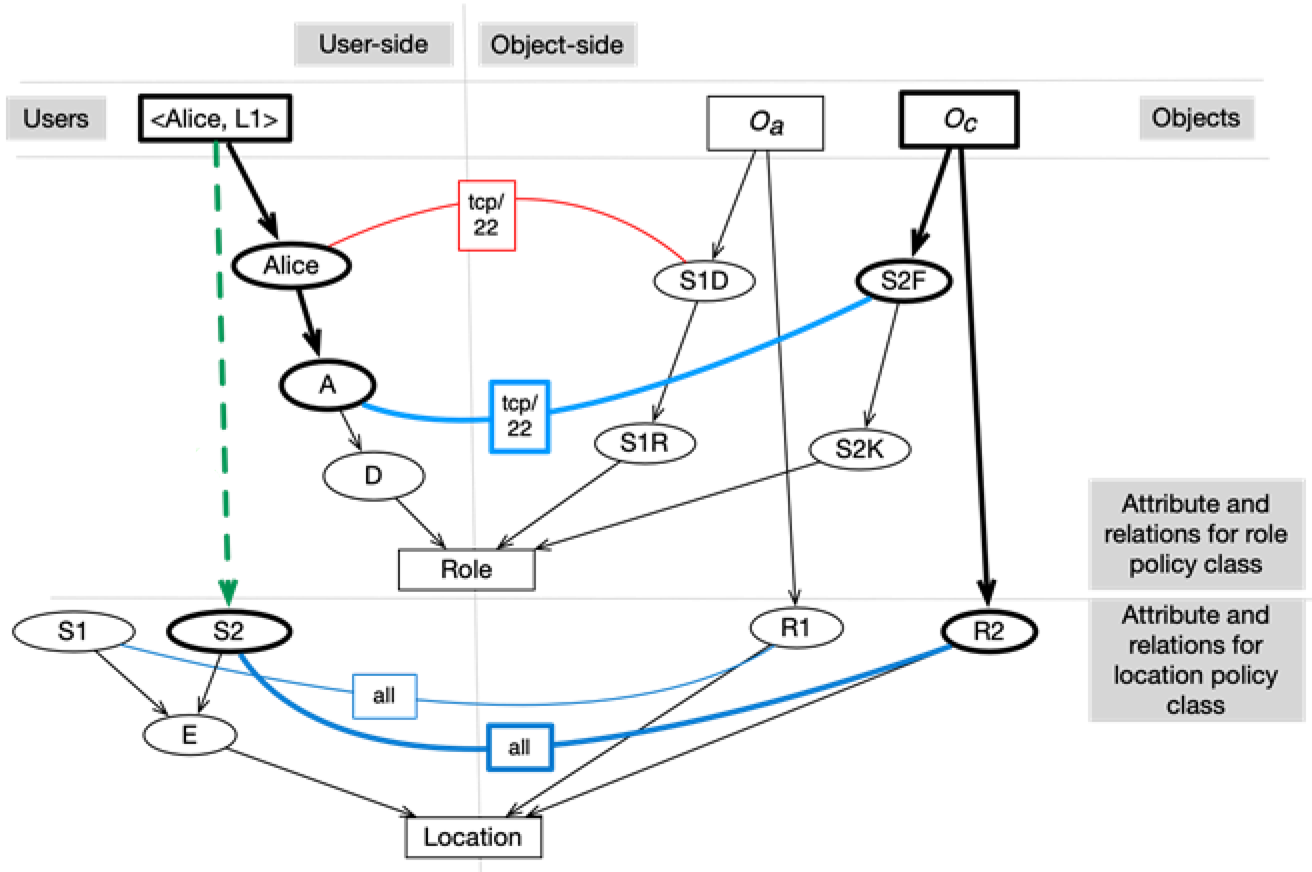
Policy Enforcement: Intent-based Networking

- Abstract "intent" from multiple flow rules
- Intents are compiled from NGAC policy



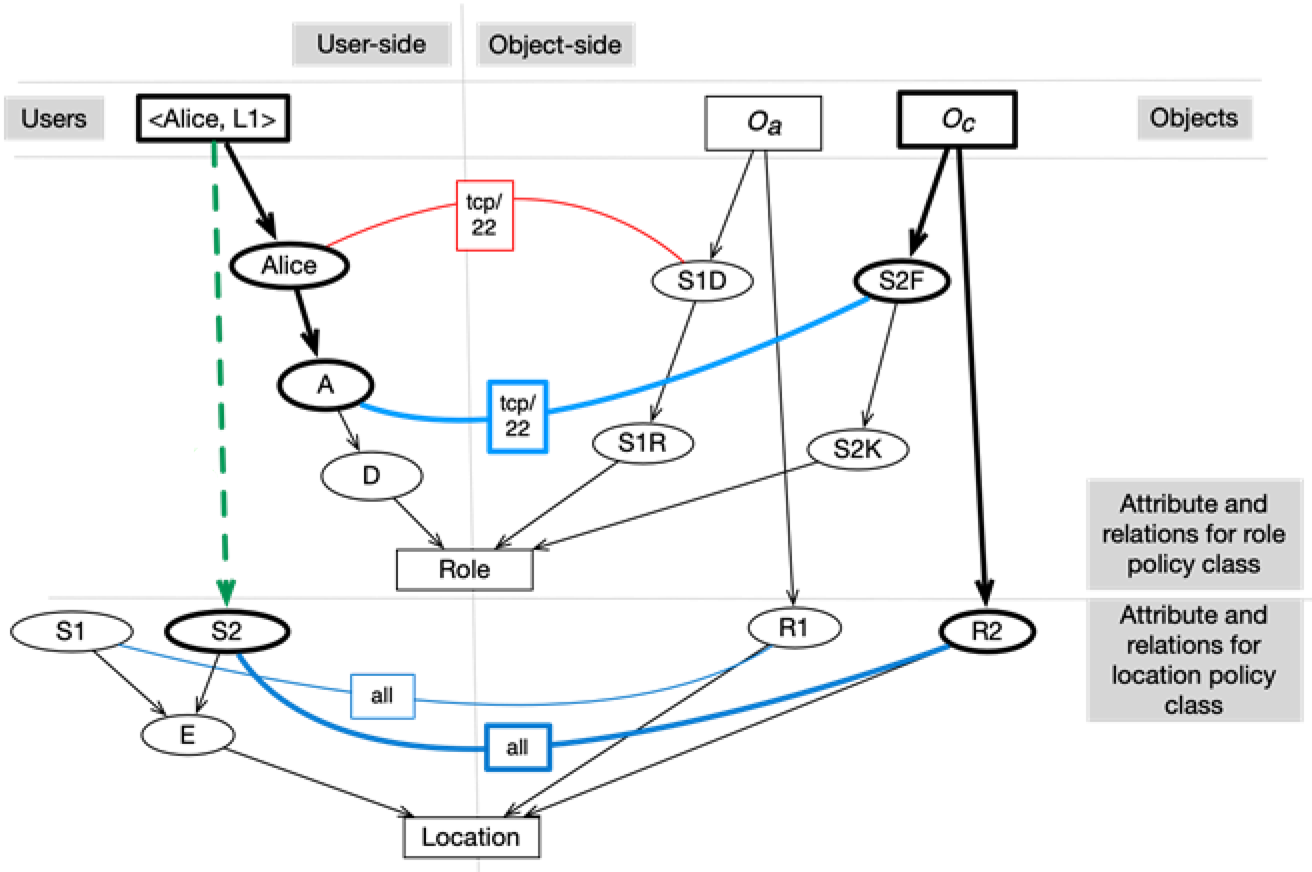
Roaming

- Users may move between sites
- User's access should be informed by location



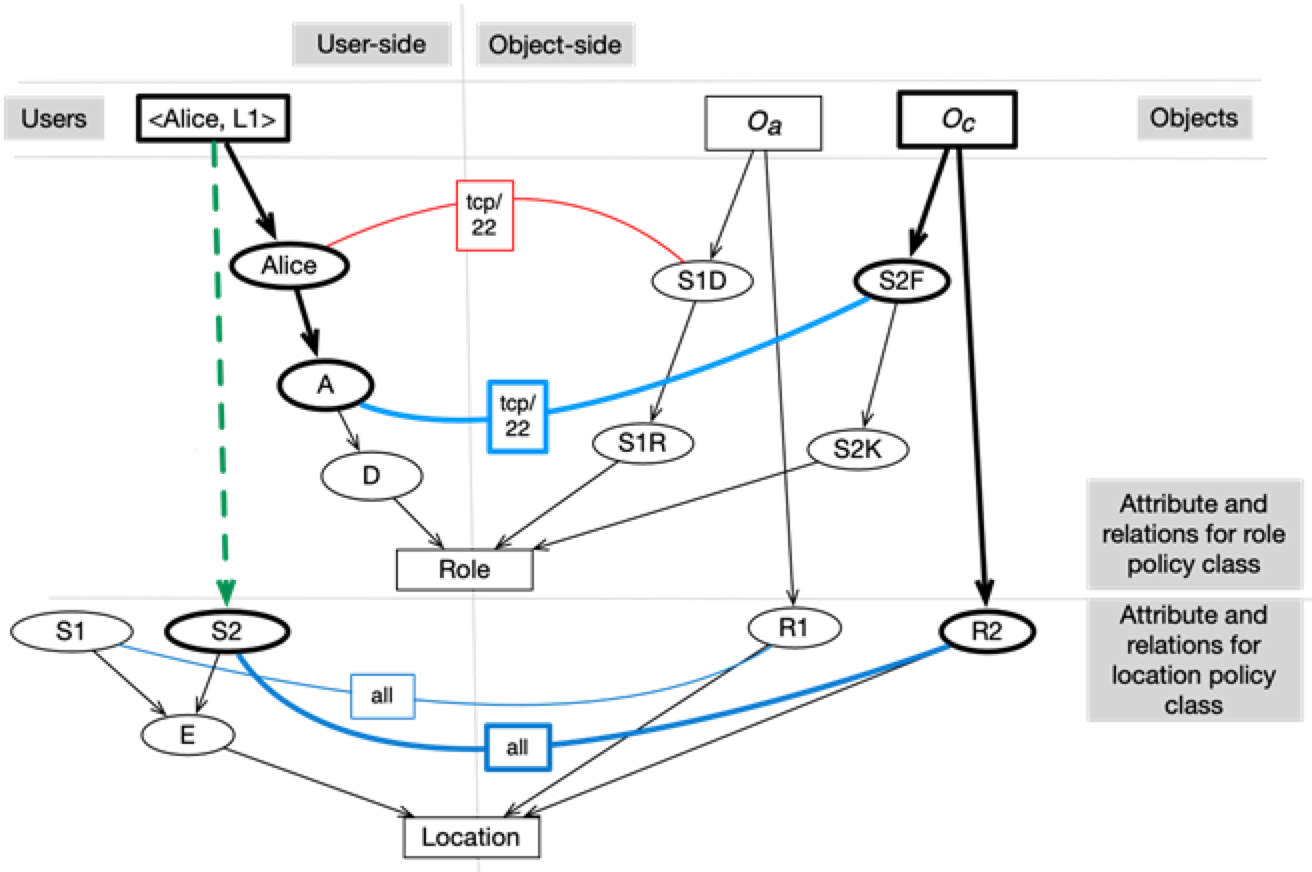
Roaming

- Users may move between sites
- User's access should be informed by location
- Uses NGAC obligations
  - Dynamic, event-based policy elements



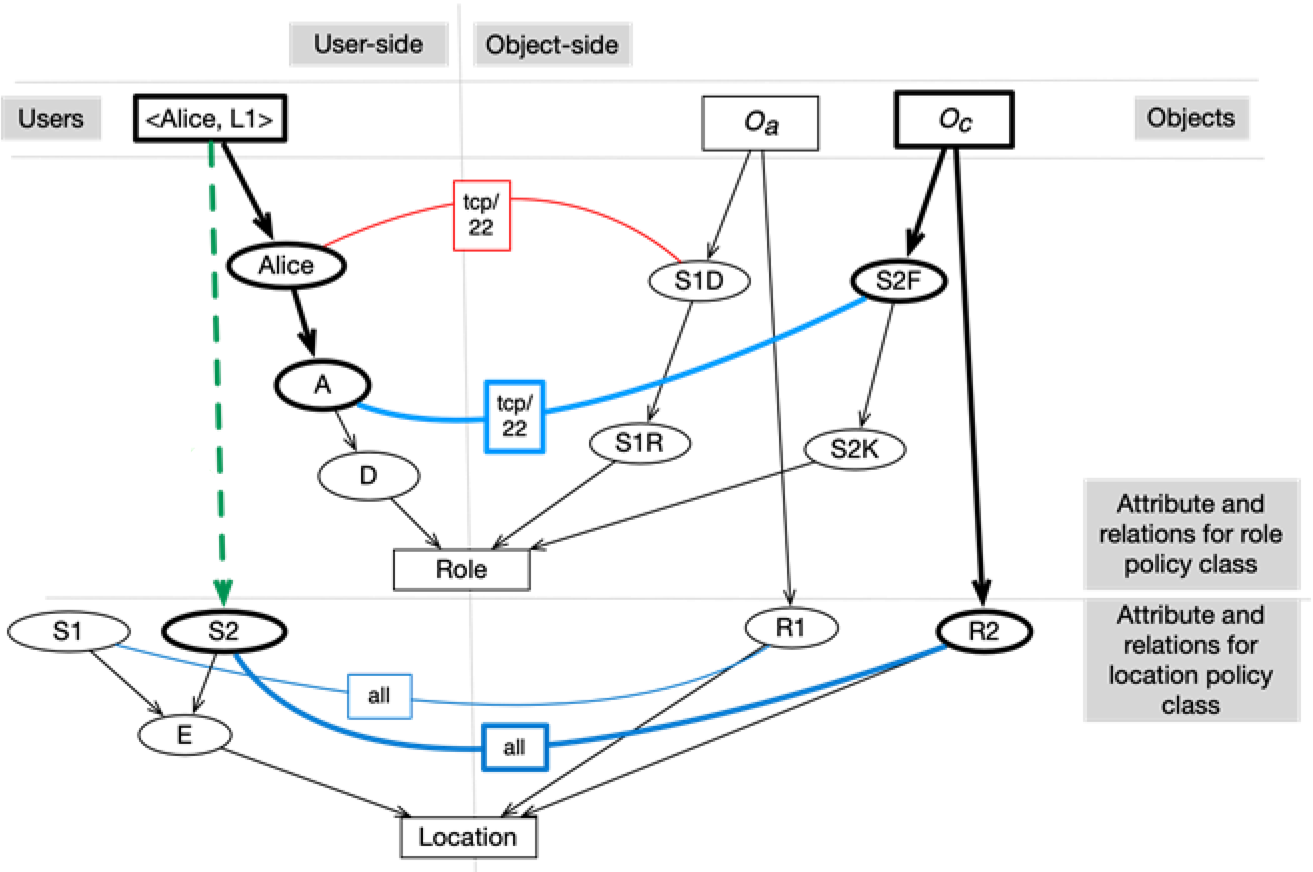
Roaming

- Users may move between sites
- User's access should be informed by location
- Uses NGAC obligations
  - Dynamic, event-based policy elements
- Creates assignments from **users to location** attributes



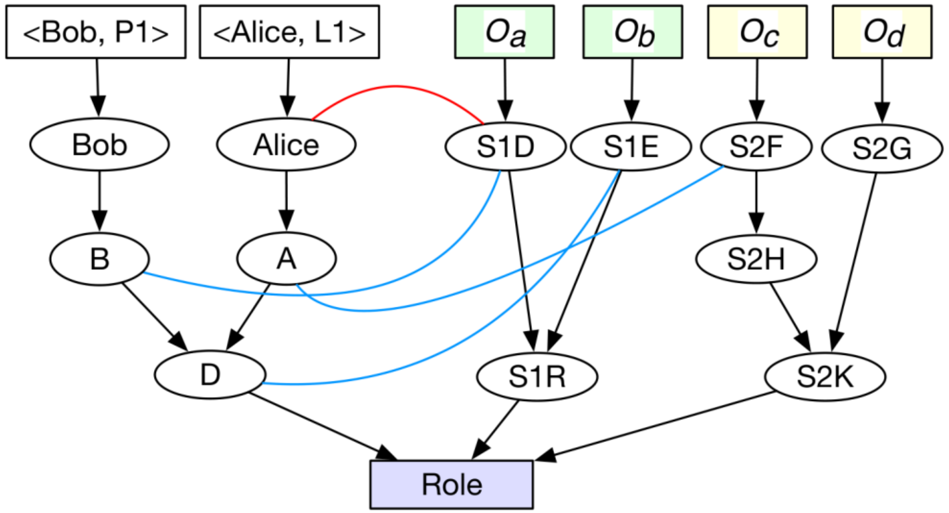
Roaming

- Users may move between sites
- User's access should be informed by location
- Uses NGAC obligations
  - Dynamic, event-based policy elements
- Creates assignments from **users to location** attributes
- Detected locally at new site
  - Local manager informs global manager
  - Global manager informs the other sites



Policy slicing

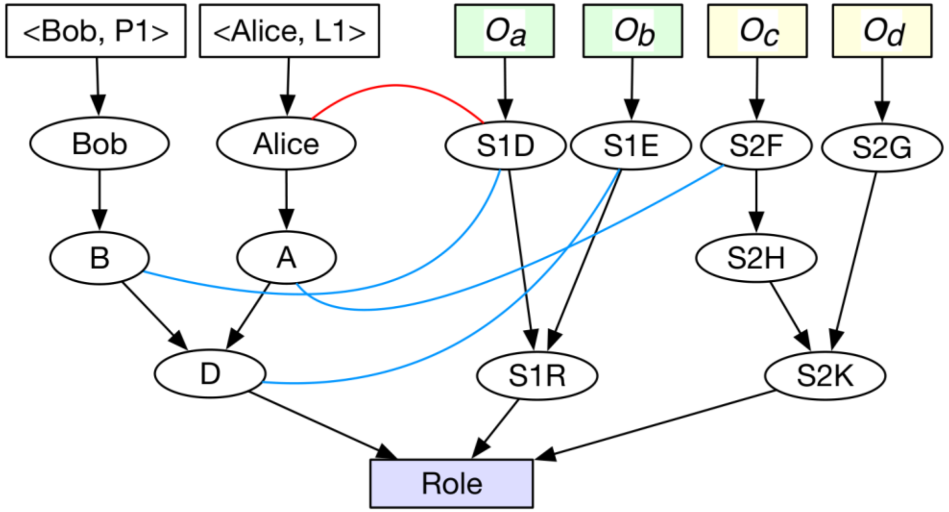
- Global policy can leak confidential information about the organization



Global policy

Policy slicing

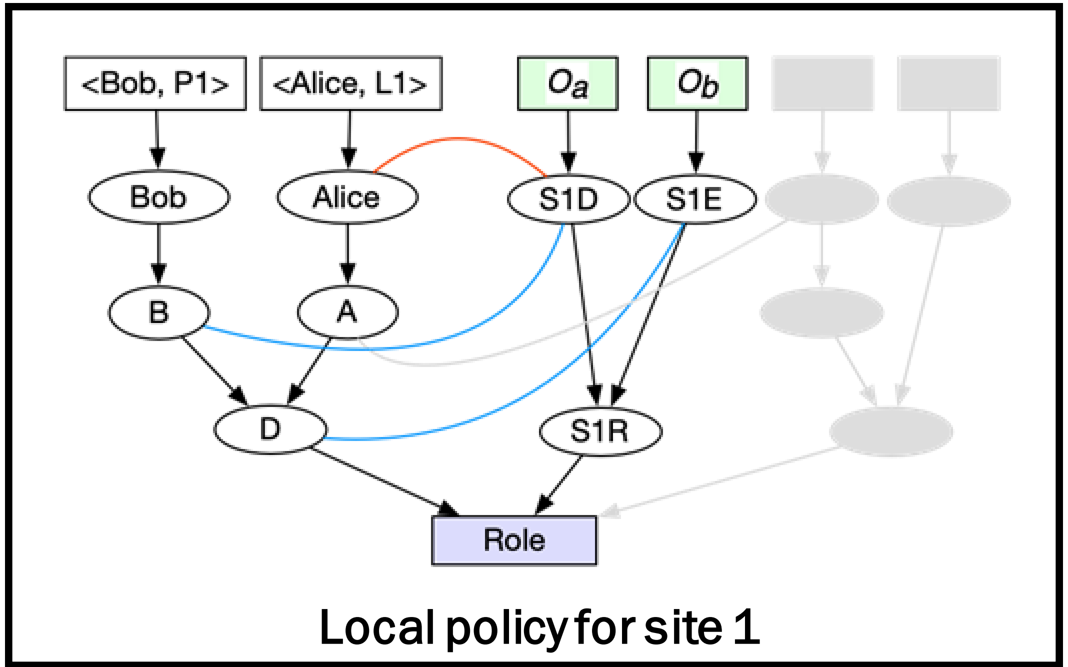
- Global policy can leak confidential information about the organization
- Sites need not be aware of the local policies at other sites



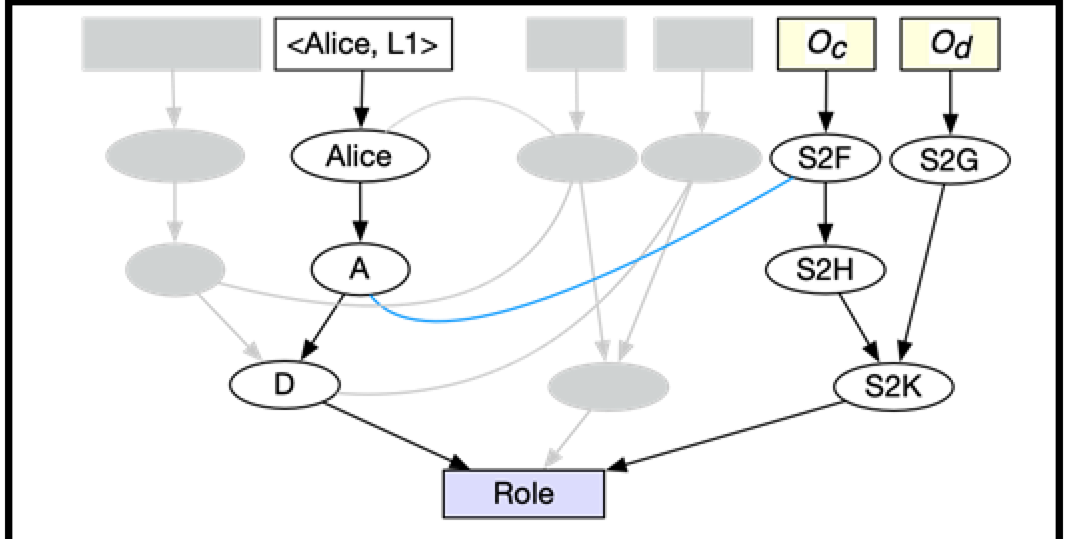
Global policy

Policy slicing

- Global policy can leak confidential information about the organization
- Sites need not be aware of the local policies at other sites
- Policies can be sliced on a "need-to-know" basis
- Slicing algorithm uses depth-first traversal to find relevant policy elements



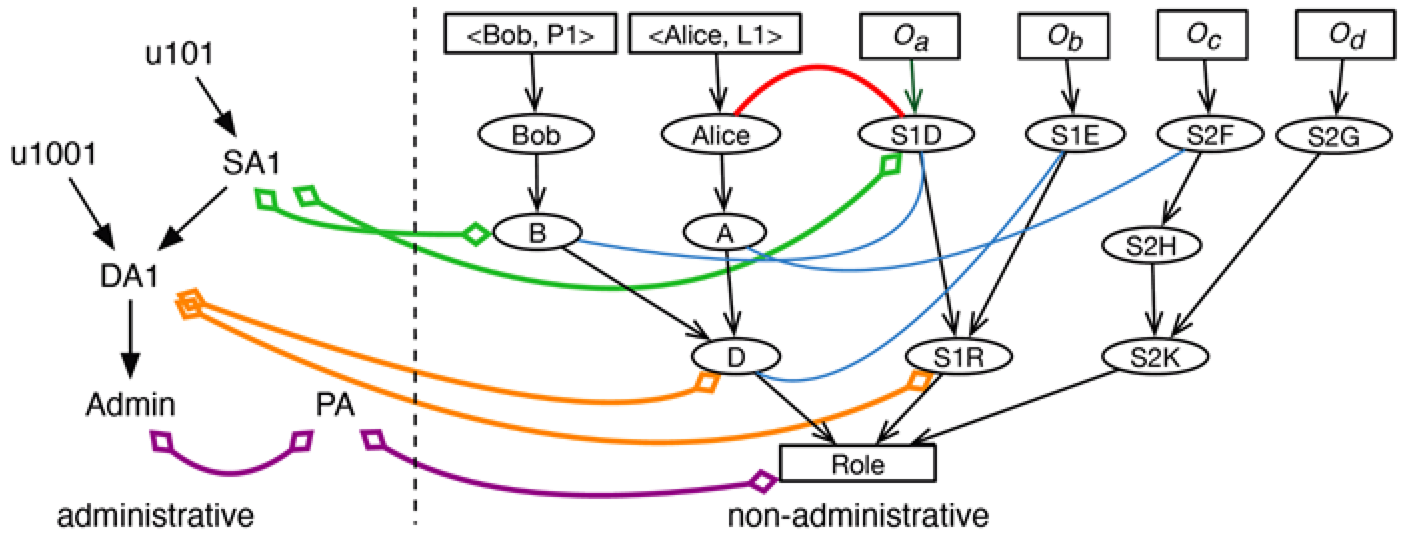
Local policy for site 1



Local policy for site 2

Administrative Policies

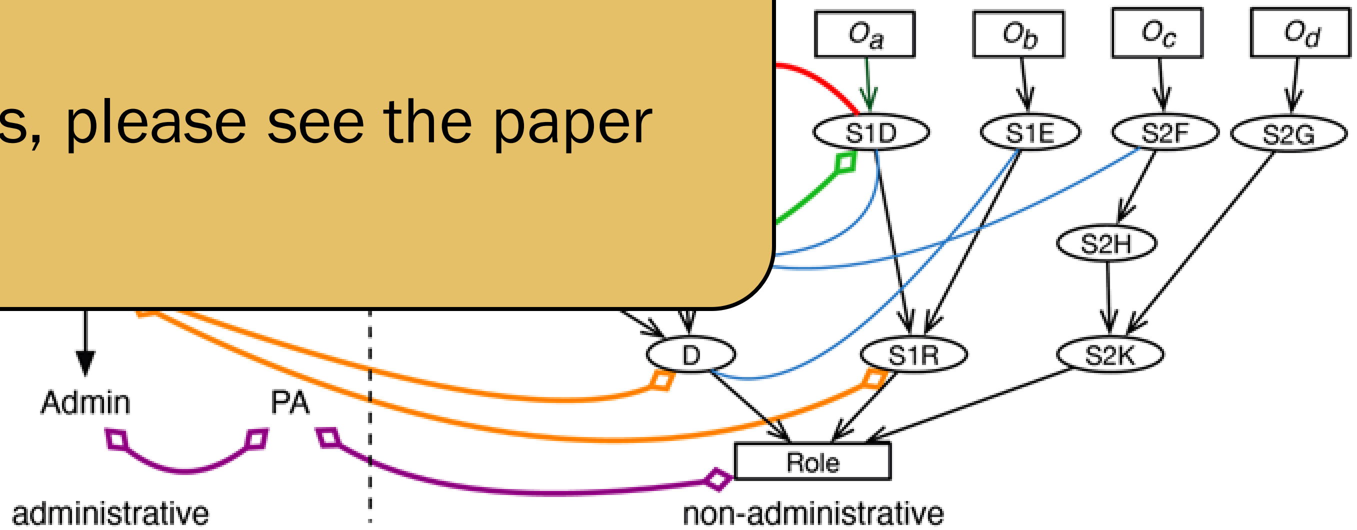
- Defines what individual administrators can update in a policy
- Policy invariant rules to maintain policy semantics
- Leverages NGAC administrative policy semantics



Administrative Policies

- Defines what individual administr policy
- Policy inva maintain
- Leverages policy semantics

For more details, please see the paper



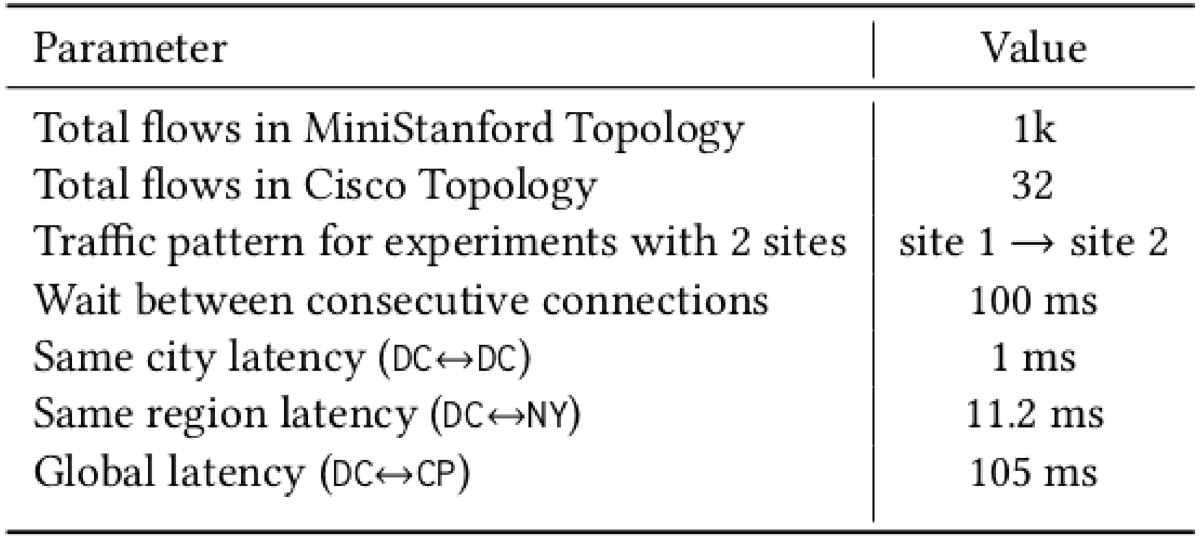
Talk outline

- Motivation
- Zero Trust and Prior Work
- MSNetViews
- Evaluation

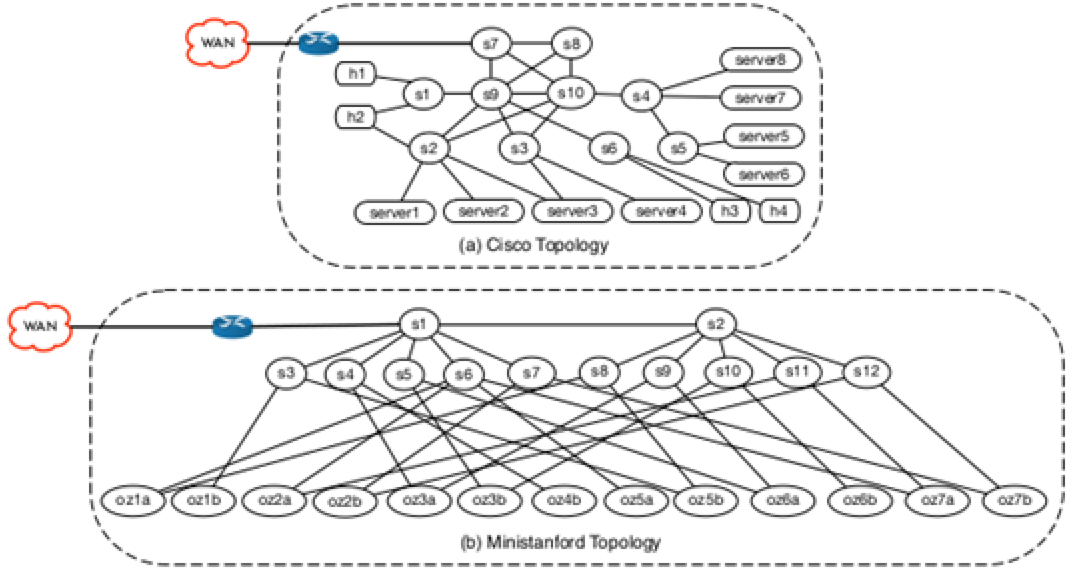
Experimental Setup

Compare

- Baseline (ONOS ifwd)
- NetViews
- MSNetViews

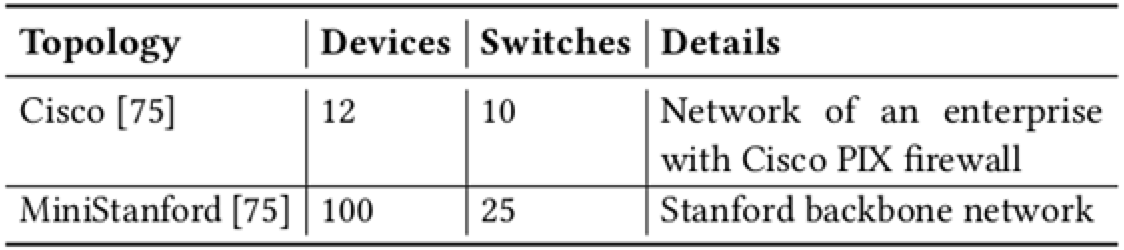


Parameter	Value
Total flows in MiniStanford Topology	1k
Total flows in Cisco Topology	32
Traffic pattern for experiments with 2 sites	site 1 ⟶ site 2
Wait between consecutive connections	100 ms
Same city latency (DC↔DC)	1 ms
Same region latency (DC↔NY)	11.2 ms
Global latency (DC↔CP)	105 ms



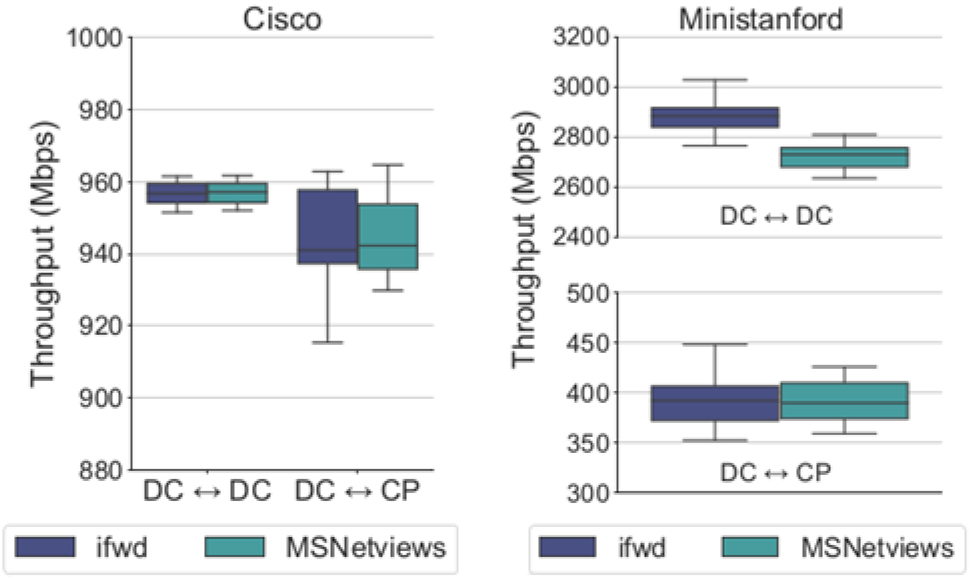
(a) Cisco Topology

(b) Ministanford Topology



Topology	Devices	Switches	Details
Cisco [75]	12	10	Network of an enterprise with Cisco PIX firewall
MiniStanford [75]	100	25	Stanford backbone network

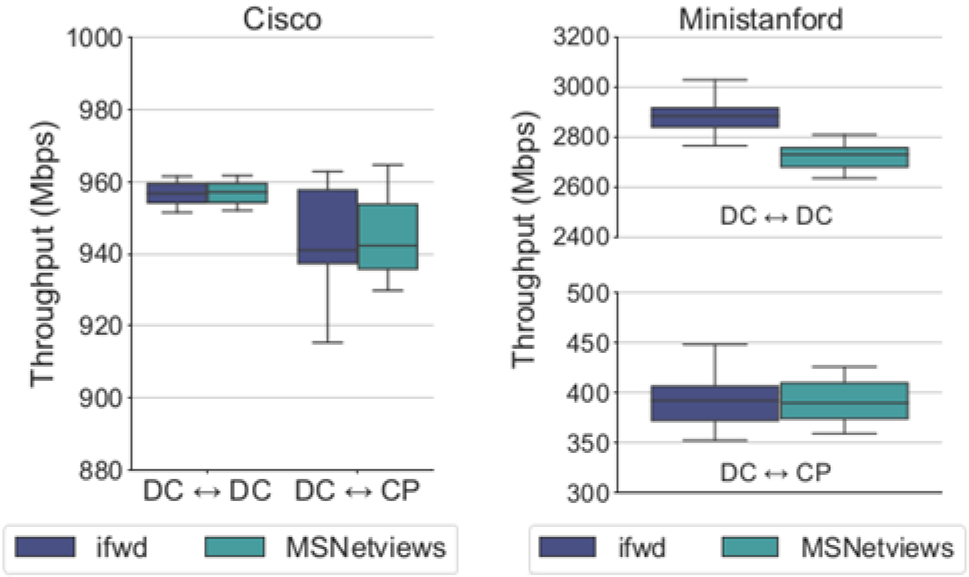
Throughput and Latency Results



(a) Cisco **(b) Ministanford**

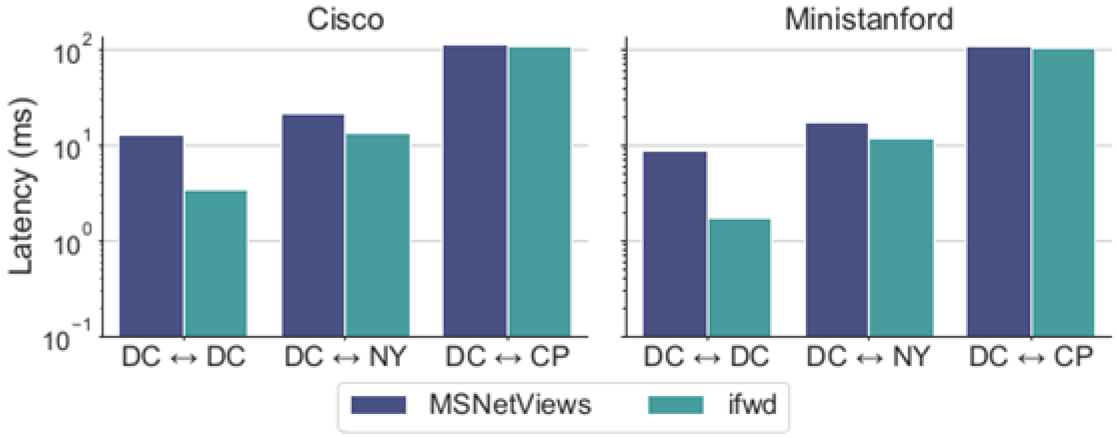
(scales differ for readability)

Throughput and Latency Results

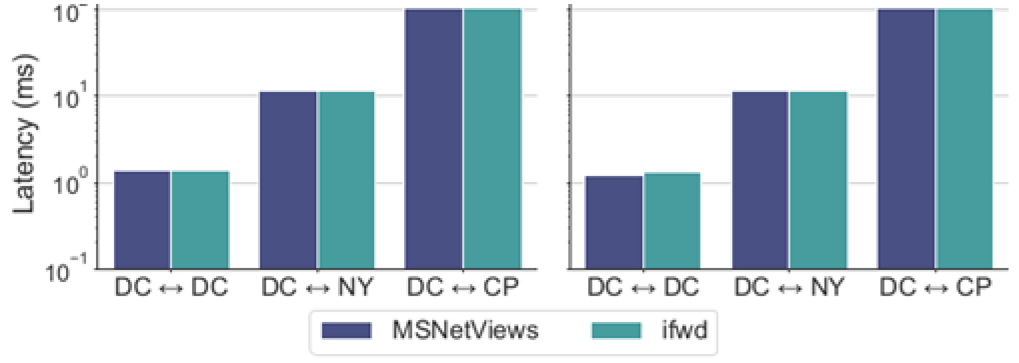


(a) Cisco **(b) Ministanford**

(scales differ for readability)



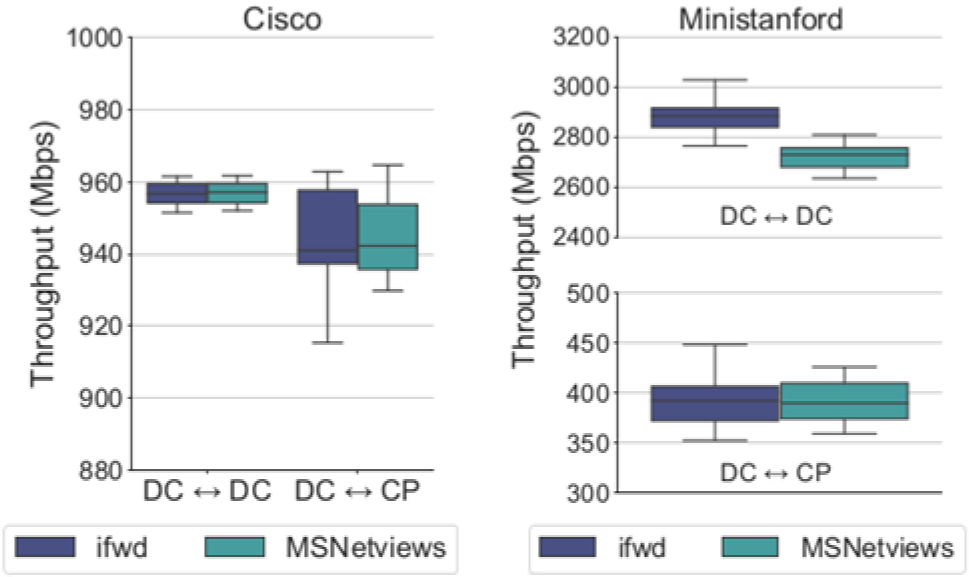
(a) Average Initial Packet Latency



(b) Average n^{th} Packet Latency

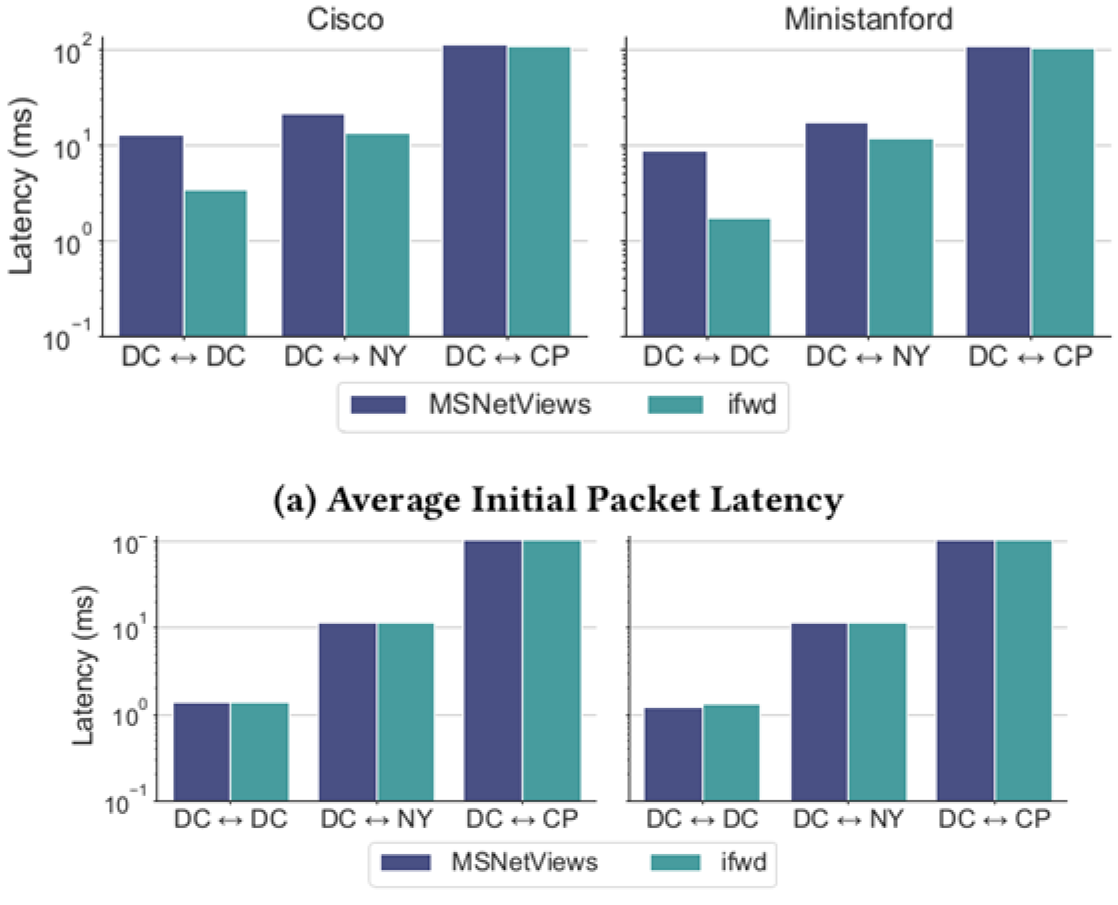
Throughput and Latency Results

MSNetViews overhead is negligible, particularly when sites are far apart.



(a) Cisco **(b) Ministanford**

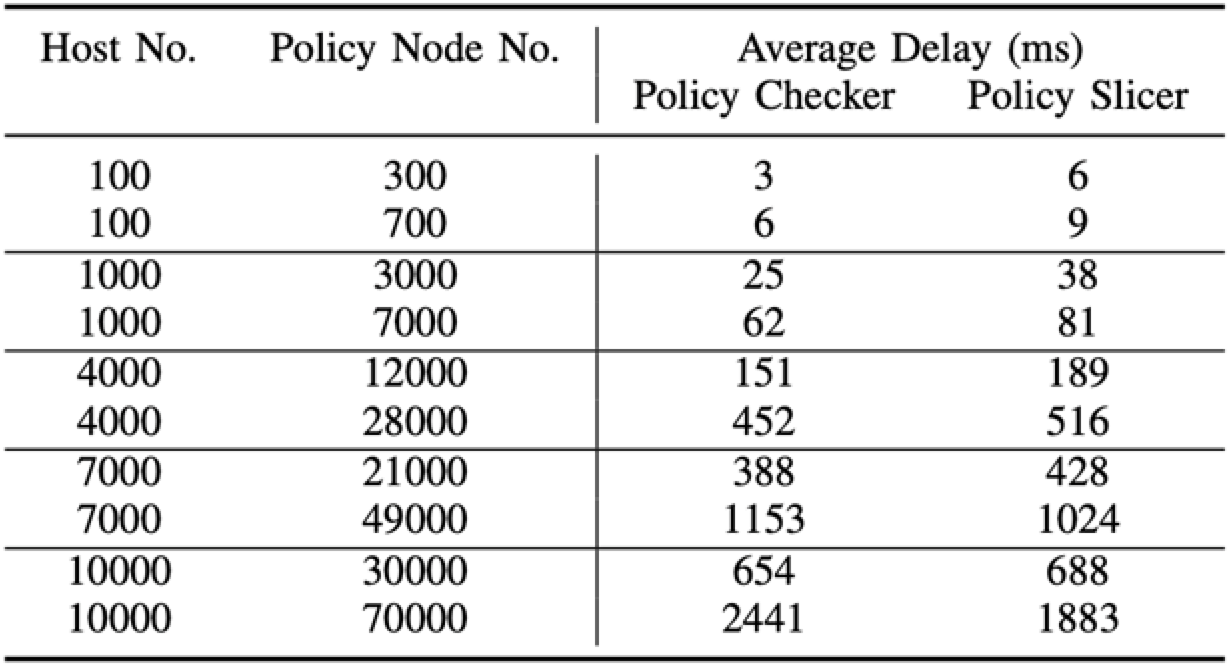
(scales differ for readability)



(a) Average Initial Packet Latency

(b) Average n^{th} Packet Latency

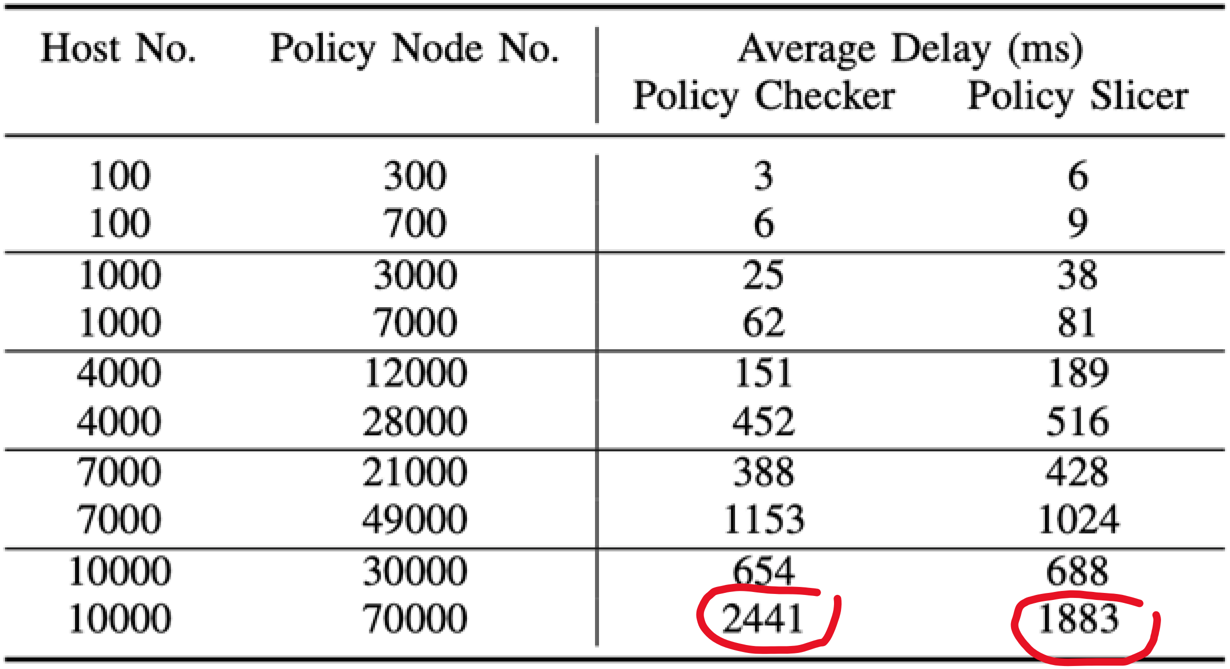
Policy Update Performance



Host No.	Policy Node No.	Average Delay (ms)	
		Policy Checker	Policy Slicer
100	300	3	6
100	700	6	9
1000	3000	25	38
1000	7000	62	81
4000	12000	151	189
4000	28000	452	516
7000	21000	388	428
7000	49000	1153	1024
10000	30000	654	688
10000	70000	2441	1883

Table: Effect of Policy Graph Complexity on Average Policy Checking and Slicing Delay

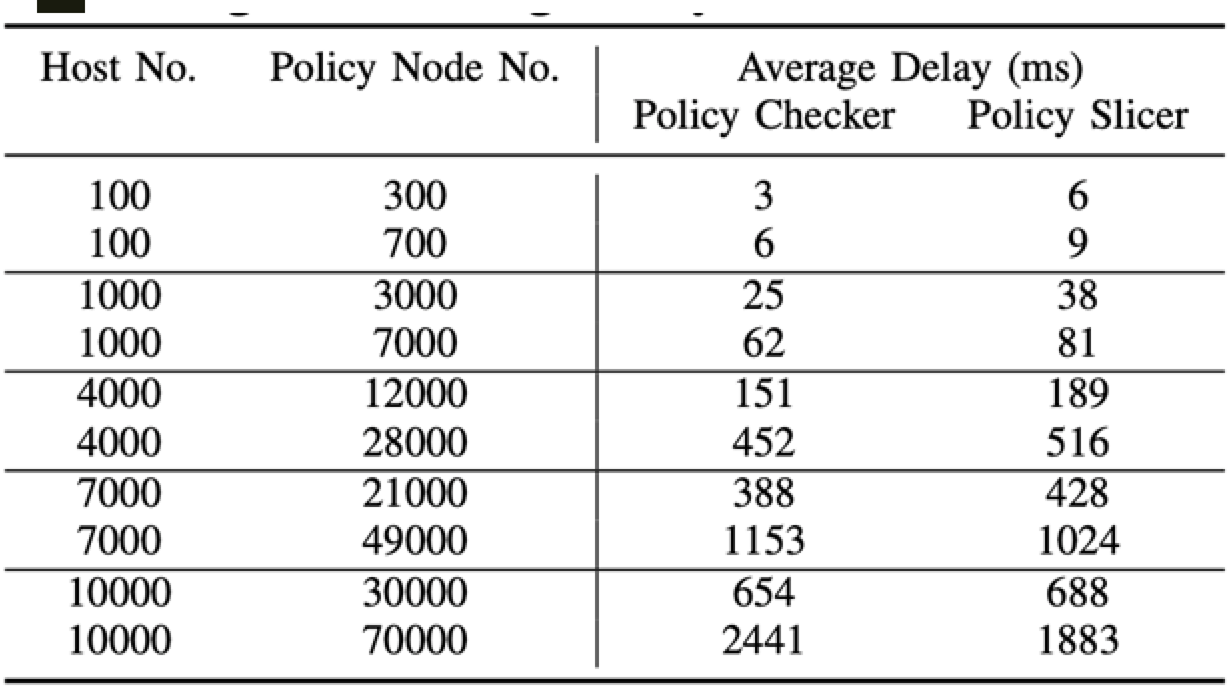
Policy Update Performance



Host No.	Policy Node No.	Average Delay (ms)	
		Policy Checker	Policy Slicer
100	300	3	6
100	700	6	9
1000	3000	25	38
1000	7000	62	81
4000	12000	151	189
4000	28000	452	516
7000	21000	388	428
7000	49000	1153	1024
10000	30000	654	688
10000	70000	2441	1883

Table: Effect of Policy Graph Complexity on Average Policy Checking and Slicing Delay

Policy Update Performance



Host No.	Policy Node No.	Average Delay (ms) Policy Checker	 Policy Slicer
100	300	3	6
100	700	6	9
1000	3000	25	38
1000	7000	62	81
4000	12000	151	189
4000	28000	452	516
7000	21000	388	428
7000	49000	1153	1024
10000	30000	654	688
10000	70000	2441	1883

Table: Effect of Policy Graph Complexity on Average Policy Checking and Slicing Delay

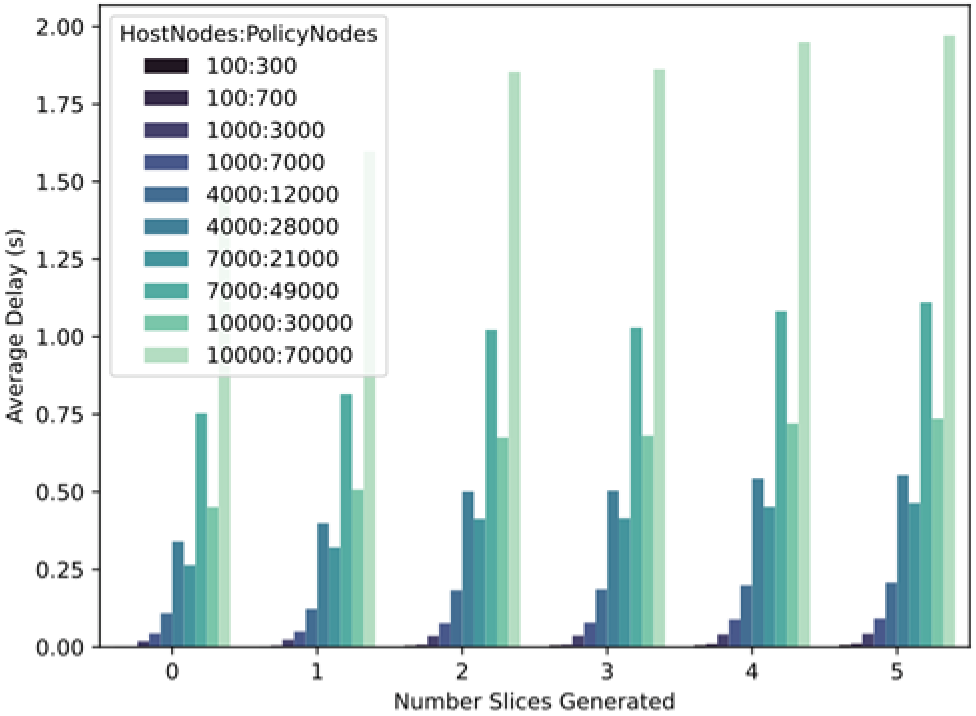


Figure: Effect of Number of Slices Needed to be Generated for Policy Updates.

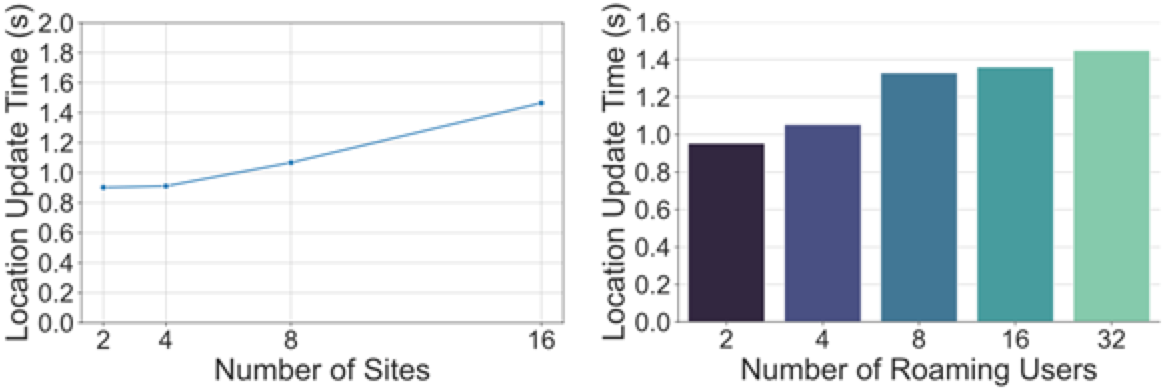
Summary

- Zero trust is needed in today's enterprise network landscape
- MSNetViews solves problems of previous solutions
  - On-premises networks
  - Distributed sites
- MSNetViews addresses
  - Roaming
  - Policy slicing
  - Distributed administrative policies
- Performance comparable to single site setting

- Source code available: https://github.com/netviews/ms-netviews
- Paper available here:

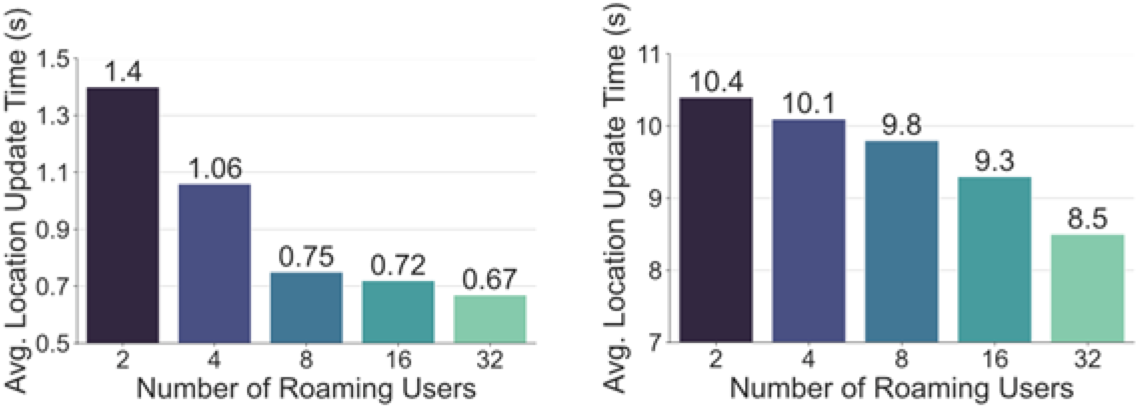
MSNetViews: Backup Slides

Post-Roaming Stabilization



(a) Location update time of one roaming user as a function of number of *relevant* sites

(b) Avg. location update time per user as a function of number of users roaming between two sites



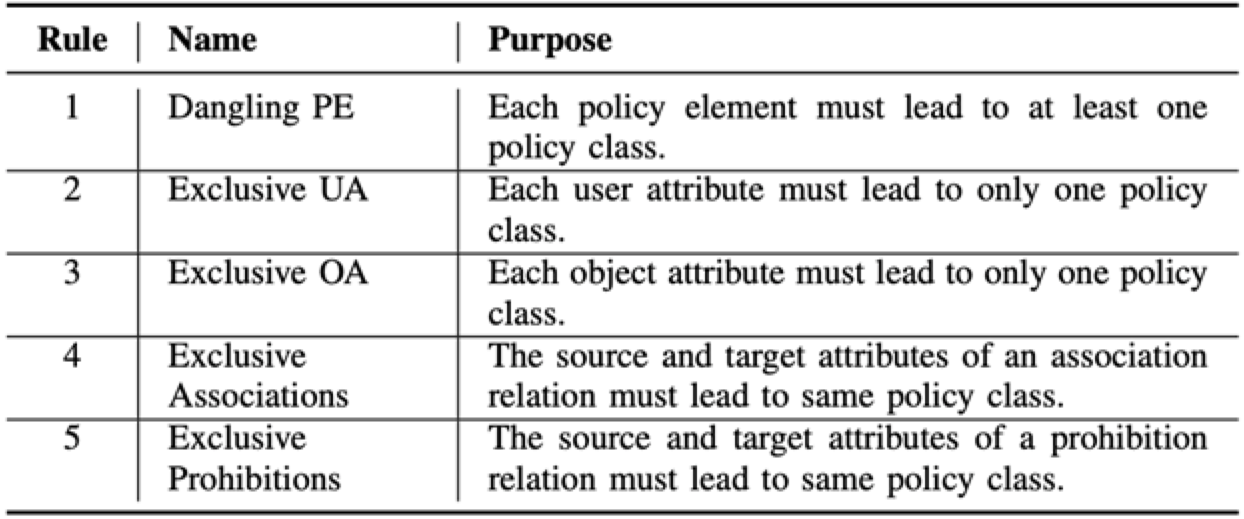
(a) Batch Interval of 1 sec

(b) Batch Interval of 10 sec

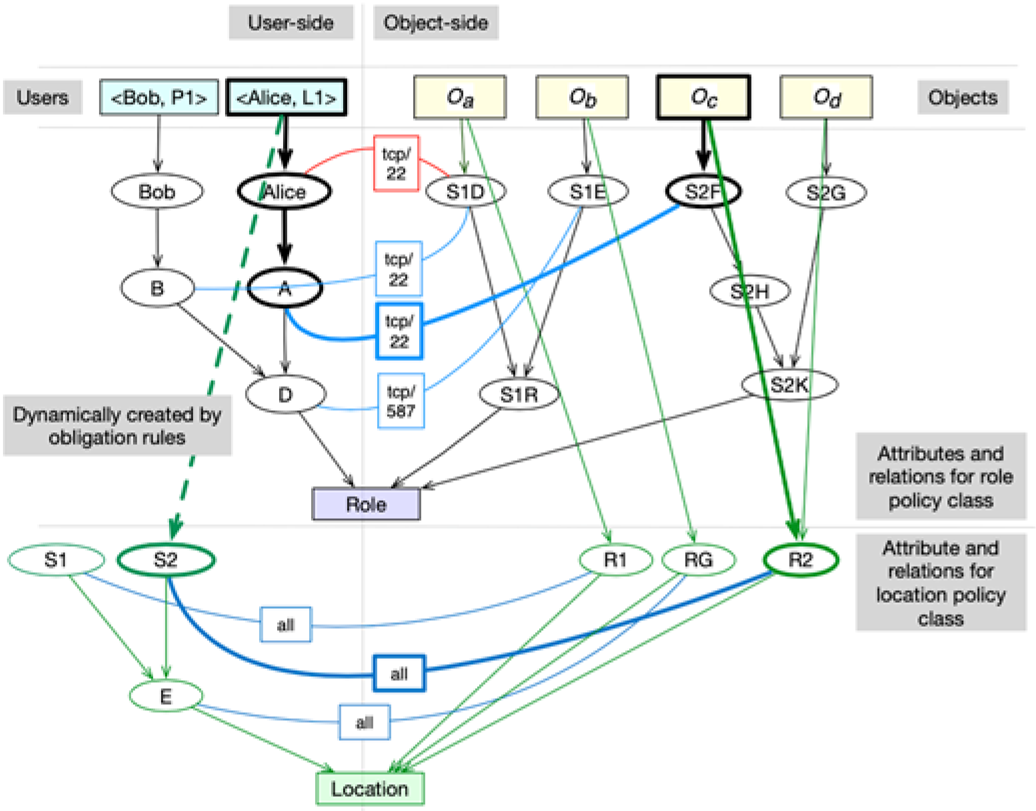
Figure: Effect of number of roaming users and number of *relevant* sites on average location update time per user for users roaming globally (between WashingtonDC↔Copenha- gen(CP)). Location update events are not batched.

Figure: Average location update time per user with batch processing at two different batch intervals as a function of number of users roaming globally (between WashingtonDC ↔Copenhagen(CP))

TABLE I: MSNetViews Policy Invariant Rules



Rule	Name	Purpose
1	Dangling PE	Each policy element must lead to at least one policy class.
2	Exclusive UA	Each user attribute must lead to only one policy class.
3	Exclusive OA	Each object attribute must lead to only one policy class.
4	Exclusive Associations	The source and target attributes of an association relation must lead to same policy class.
5	Exclusive Prohibitions	The source and target attributes of a prohibition relation must lead to same policy class.



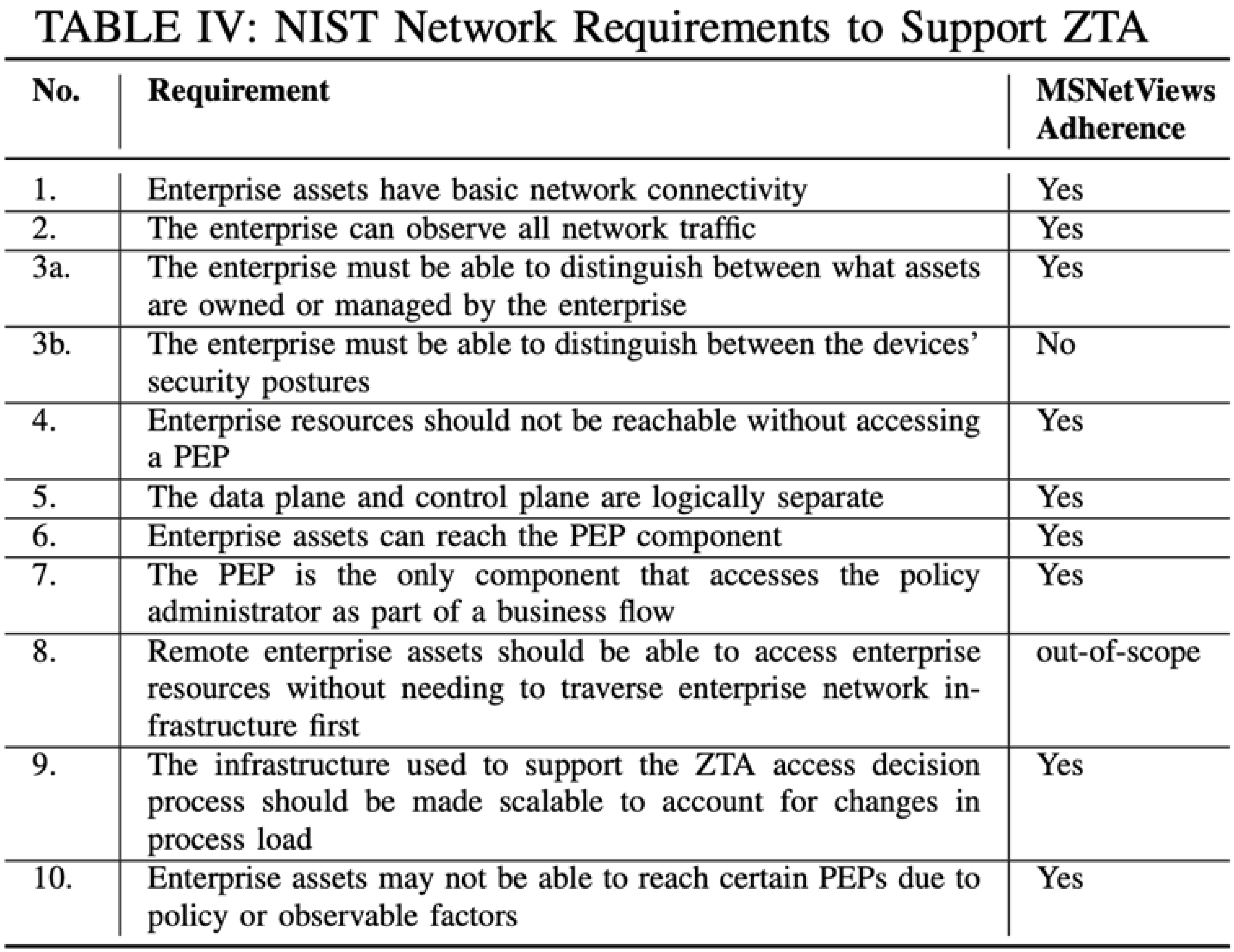


TABLE IV: NIST Network Requirements to Support ZTA

No.	Requirement	MSNetViews Adherence
1.	Enterprise assets have basic network connectivity	Yes
2.	The enterprise can observe all network traffic	Yes
3a.	The enterprise must be able to distinguish between what assets are owned or managed by the enterprise	Yes
3b.	The enterprise must be able to distinguish between the devices' security postures	No
4.	Enterprise resources should not be reachable without accessing a PEP	Yes
5.	The data plane and control plane are logically separate	Yes
6.	Enterprise assets can reach the PEP component	Yes
7.	The PEP is the only component that accesses the policy administrator as part of a business flow	Yes
8.	Remote enterprise assets should be able to access enterprise resources without needing to traverse enterprise network infrastructure first	out-of-scope
9.	The infrastructure used to support the ZTA access decision process should be made scalable to account for changes in process load	Yes
10.	Enterprise assets may not be able to reach certain PEPs due to policy or observable factors	Yes