PSI: Precise Security Instrumentation for Enterprise Networks

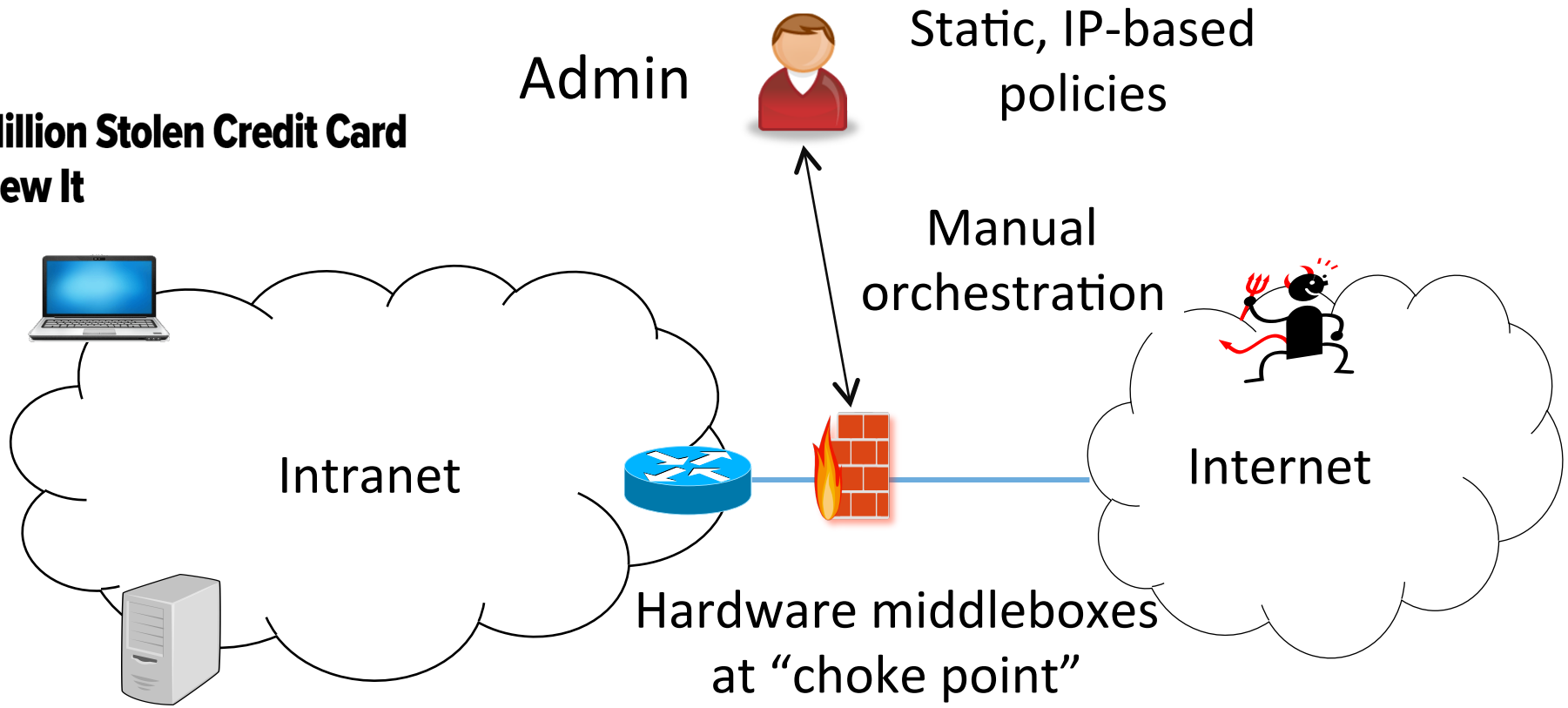
Tianlong Yu[1], Seyed K. Fayaz[1], Michael Collins[2],
Vyas Sekar[1] and Srini Seshan[1]

[1]CMU [2]Redjack

Operational network security still abysmal!

False +/-

Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It



Defense not agile

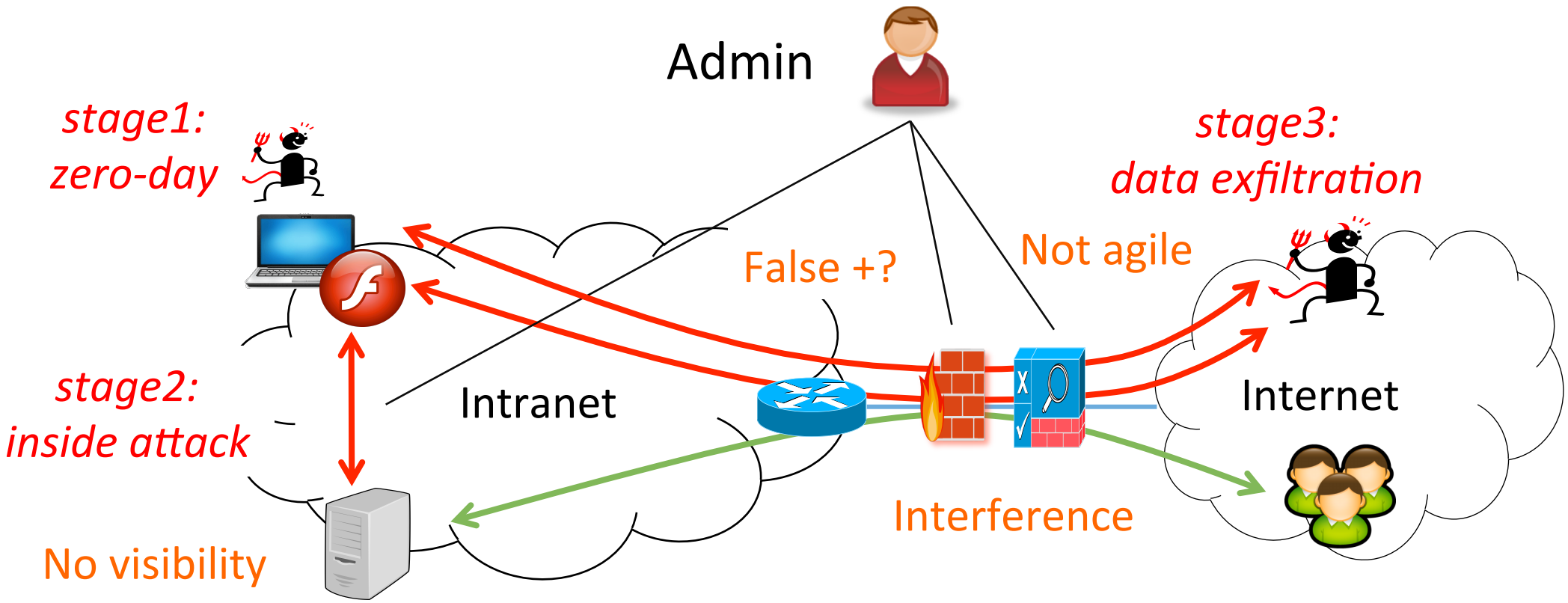
Multistage Exploit Kits Boost Effective Malware Delivery

Performance interference

IT Admins Often Turn off DPI and Other Firewall Features

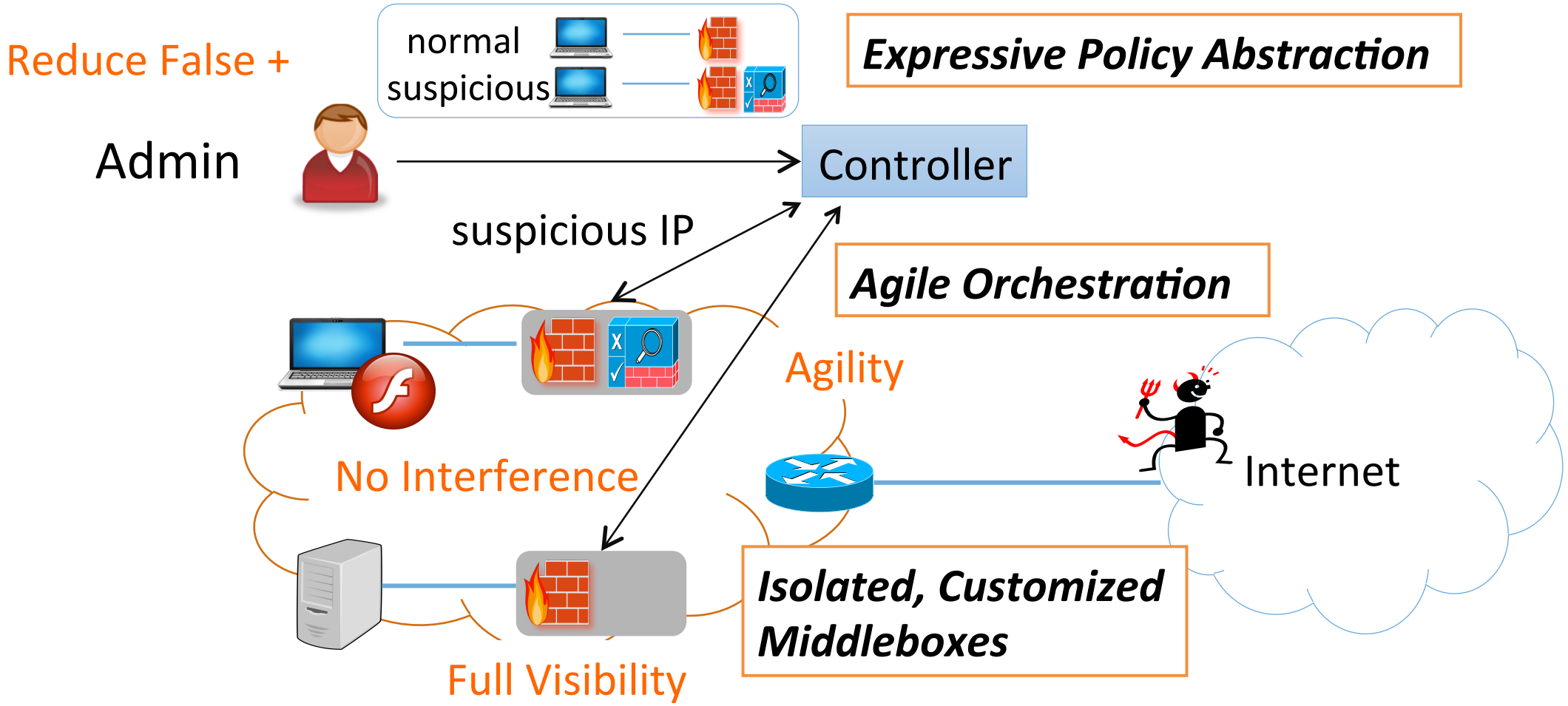
Motivating example: current defense has key limitations

Lack Isolation | ***Lack Context*** | ***Lack Agility***

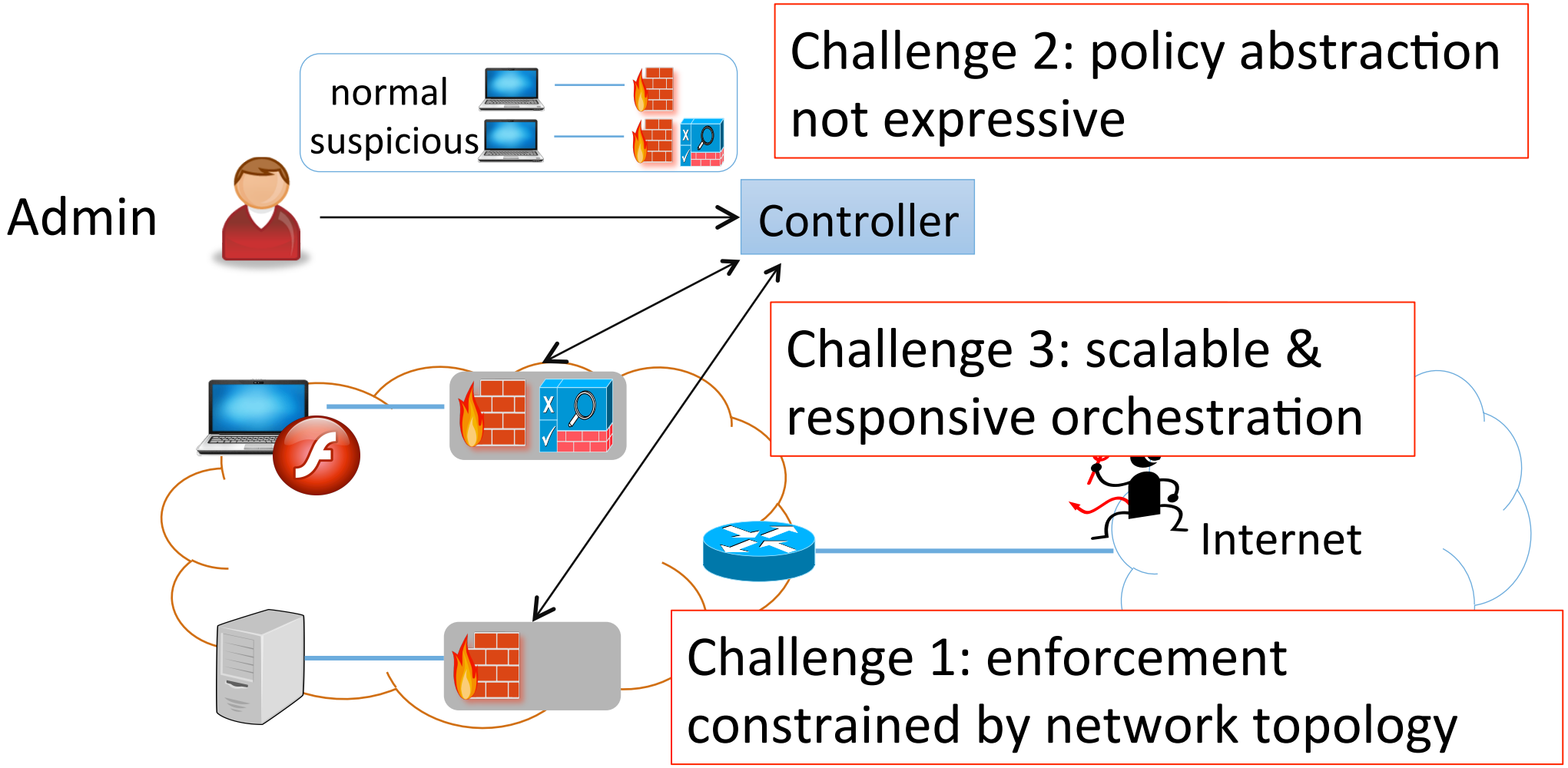


Ideal solution

Isolation | ***Context*** | ***Agility***



Challenges to realize ideal solution



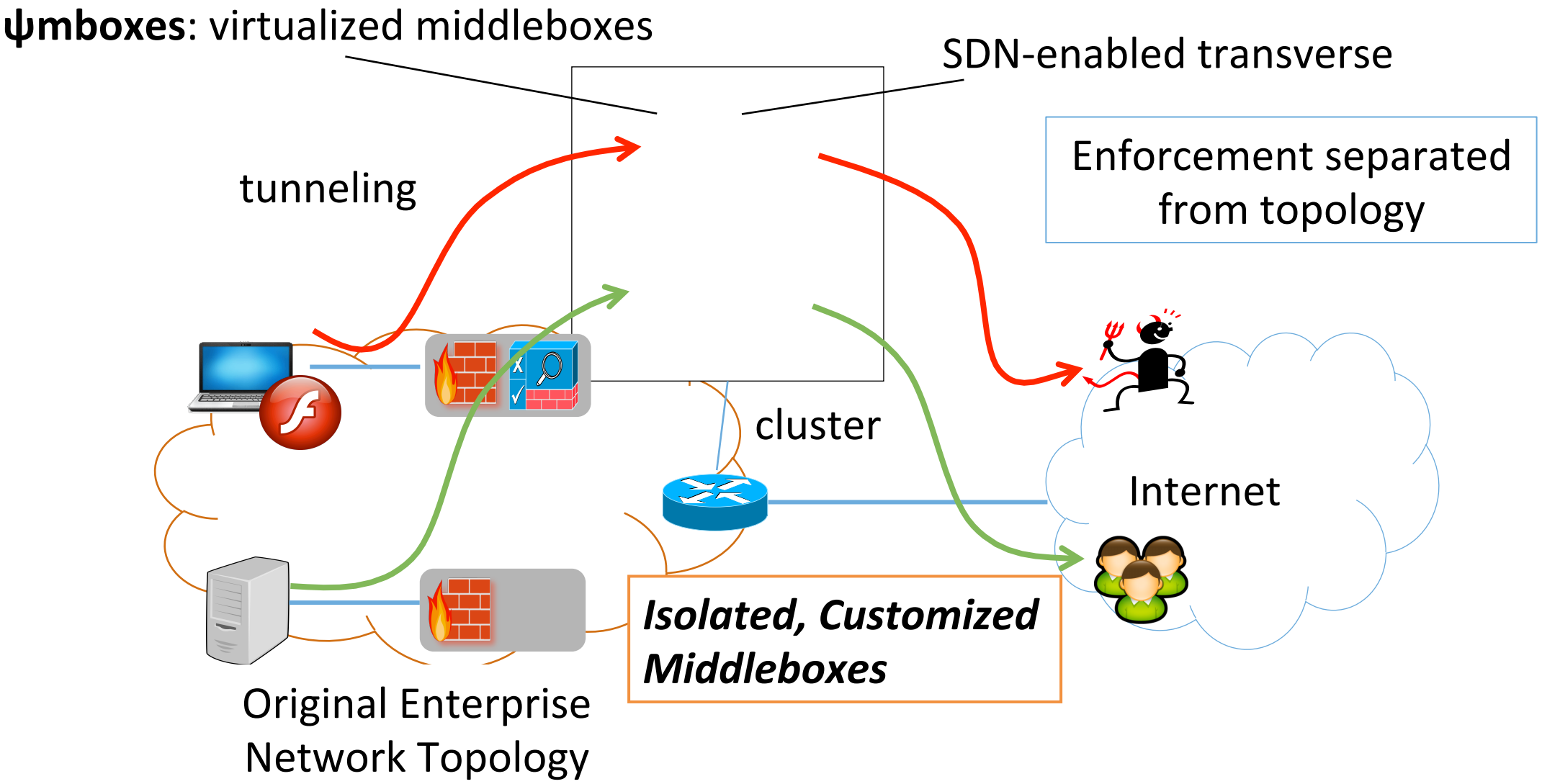
How PSI addresses the challenges

Challenge 1: enforcement constrained by network topology

Challenge 2: Realize expressive policy abstraction

Challenge 3: Realize scalable & responsive orchestration

PSI enforcement



How PSI addresses the challenges

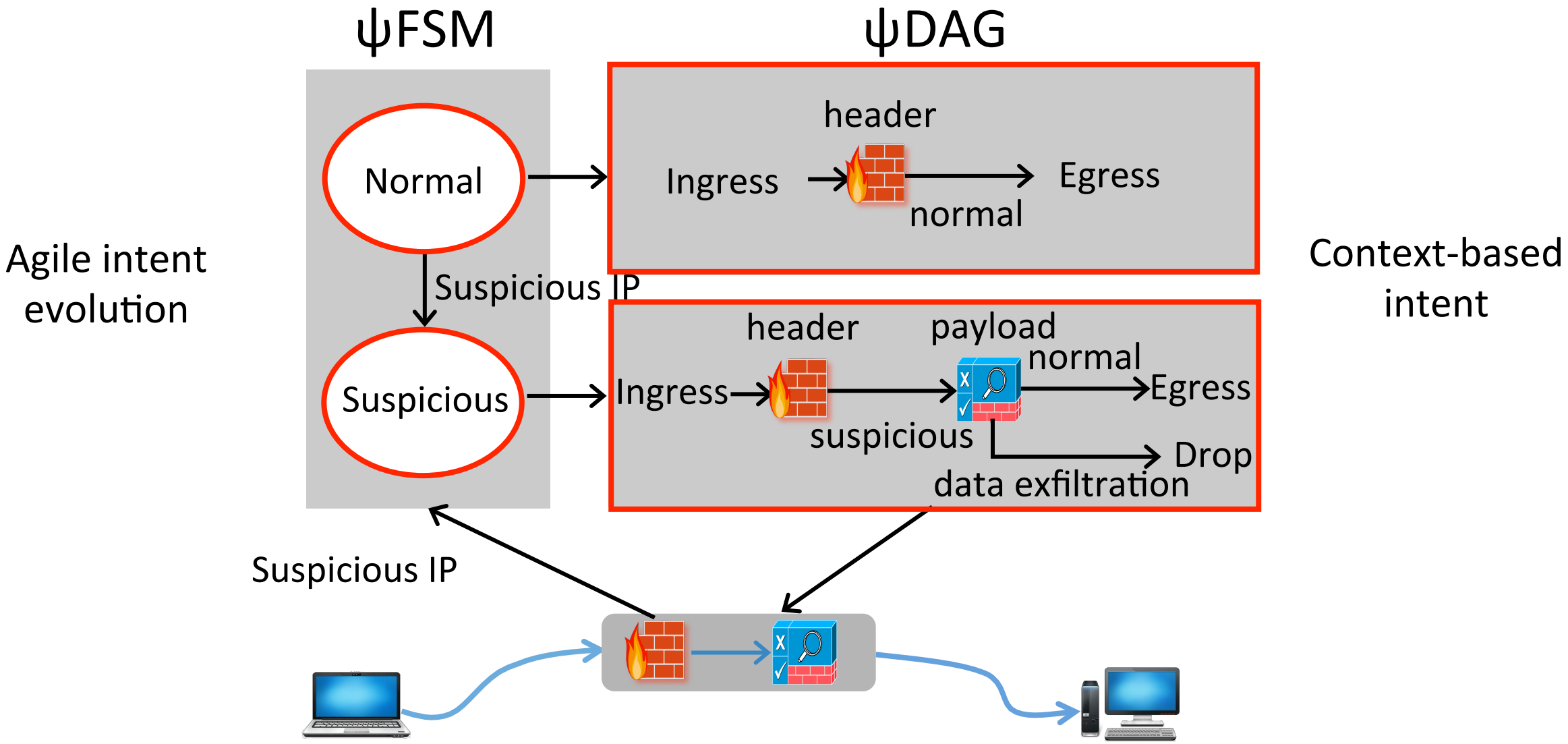
Challenge 1: enforcement constrained by network topology

Leverage NFV & SDN to decouple enforcement from network topology

Challenge 2: realize expressive policy abstraction

Challenge 3: Realize scalable & responsive orchestration

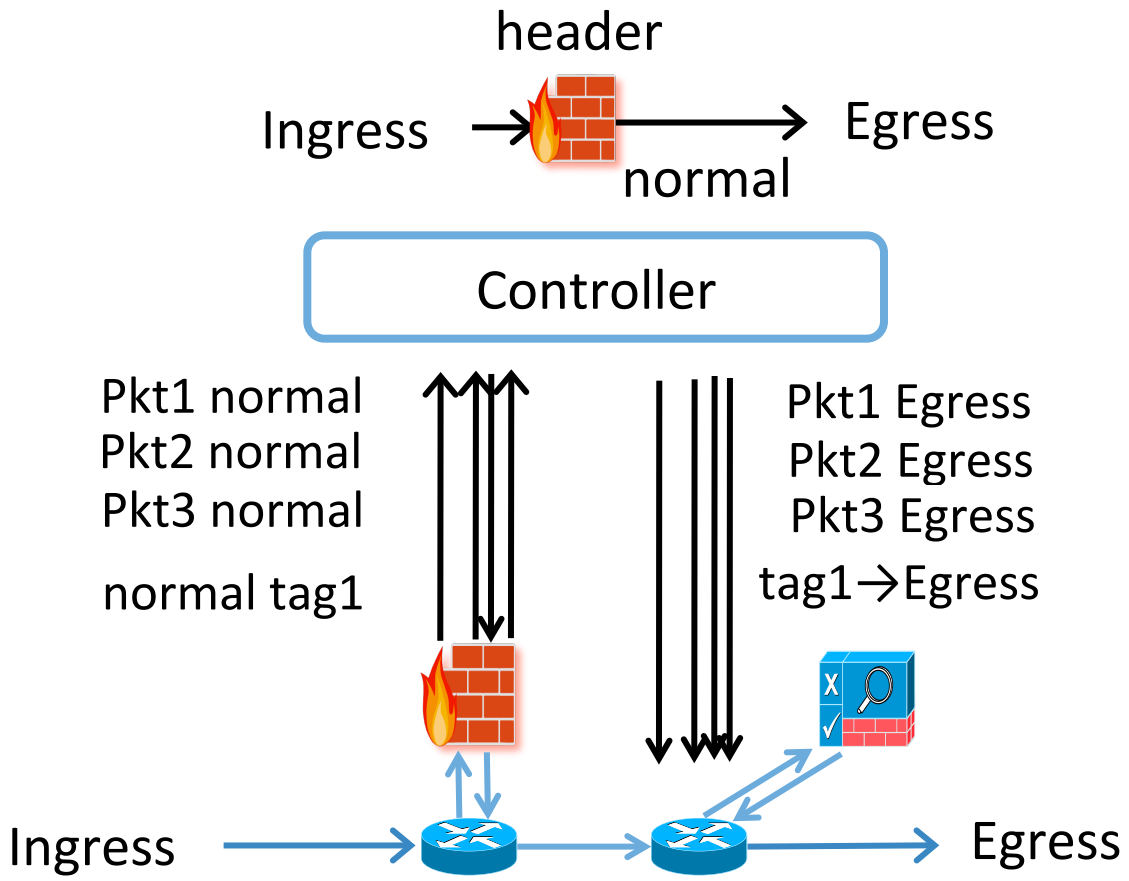
PSI policy abstraction



How PSI addresses the challenges

Challenge 1: enforcement constrained by network topology	Leverage NFV & SDN to decouple enforcement from network topology
Challenge 2: realize expressive policy abstraction	Provide context-based & agile policy abstraction
Challenge 3: realize scalable & responsiveness orchestration	

PSI orchestration



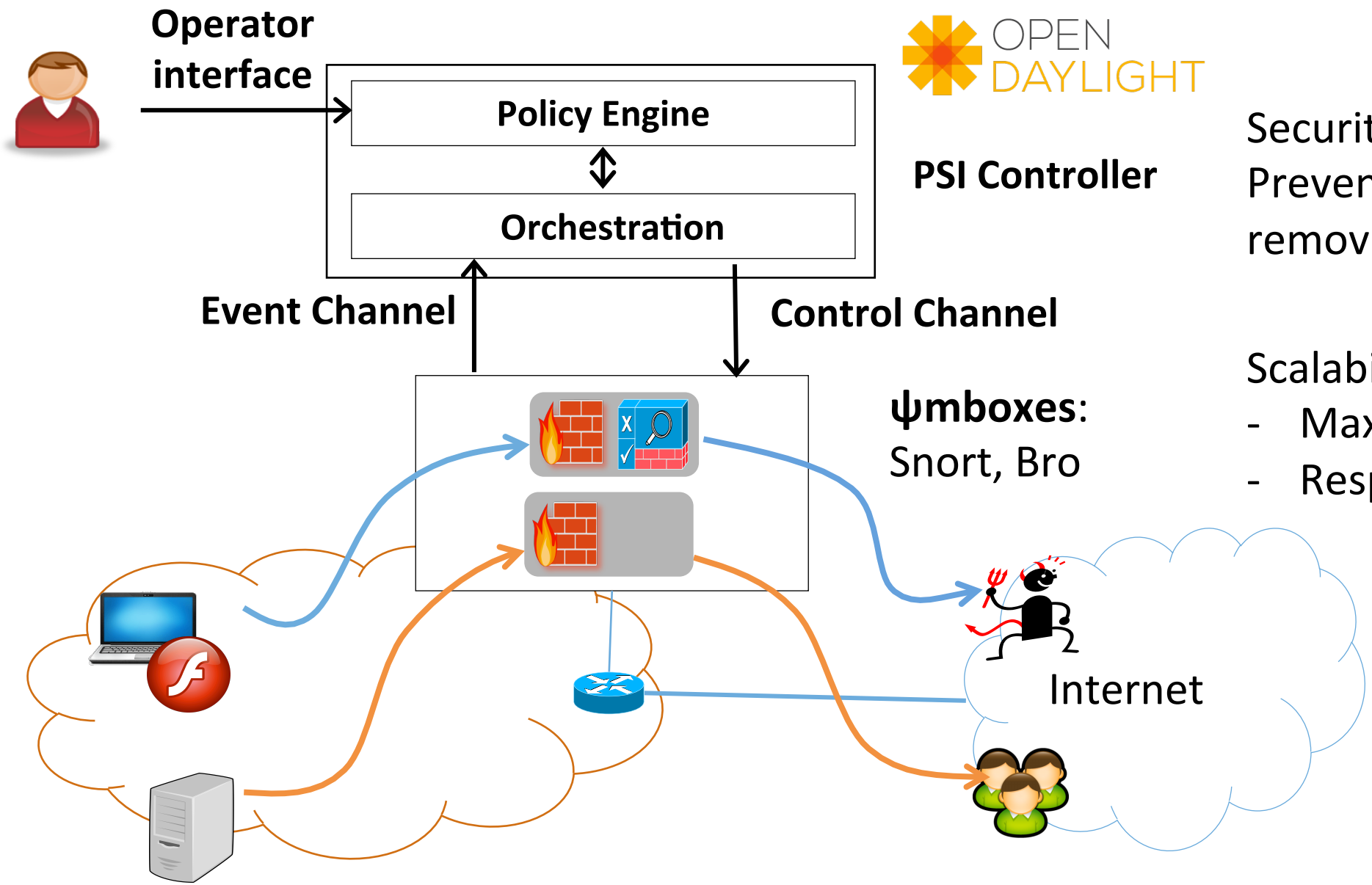
Scalability: controller has to process the control messages for every packet.

Proactive tag-based forwarding:
- Middleboxes tags the packets
- Switches forwards the packets based on tags

How PSI addresses the challenges

Challenge 1: enforcement constrained by network topology	Leverage NFV & SDN to decouple enforcement from network topology
Challenge 2: realize expressive policy abstraction	Provide context-based & agile policy abstraction
Challenge 3: realize scalable & responsiveness orchestration	Extend SDN controller to build scalable and responsive orchestration

PSI implementation



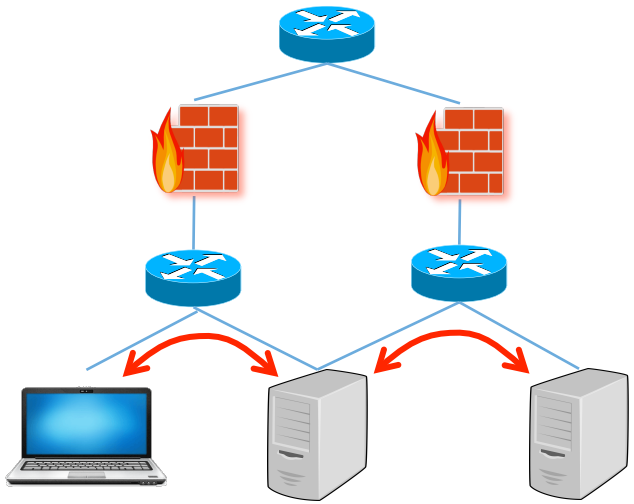
Security Benefit:
Prevent more attacks by removing topology constraints.

Scalability of PSI controller:
- Maximum throughput
- Response time

Security benefit: prevent more attacks by removing topology constraints

Attack Trace1:
Advanced Persistent Threats (Angler EK/Magnitude EK)

Attack Trace2:
Insider attack (FTP/DNS-based data-exfiltration)



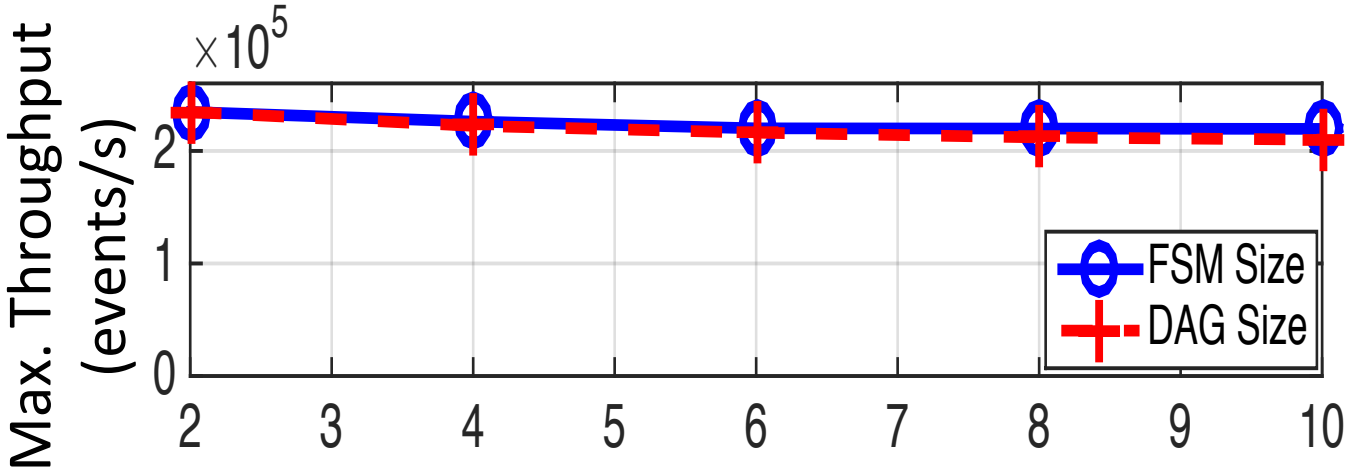
Topology	Distributed Firewall/IPS	PSI
Apt-mcafee	59%	91%
Pix-cisco	56%	89%
Mini-stanford	52%	92%
All	56%	91%

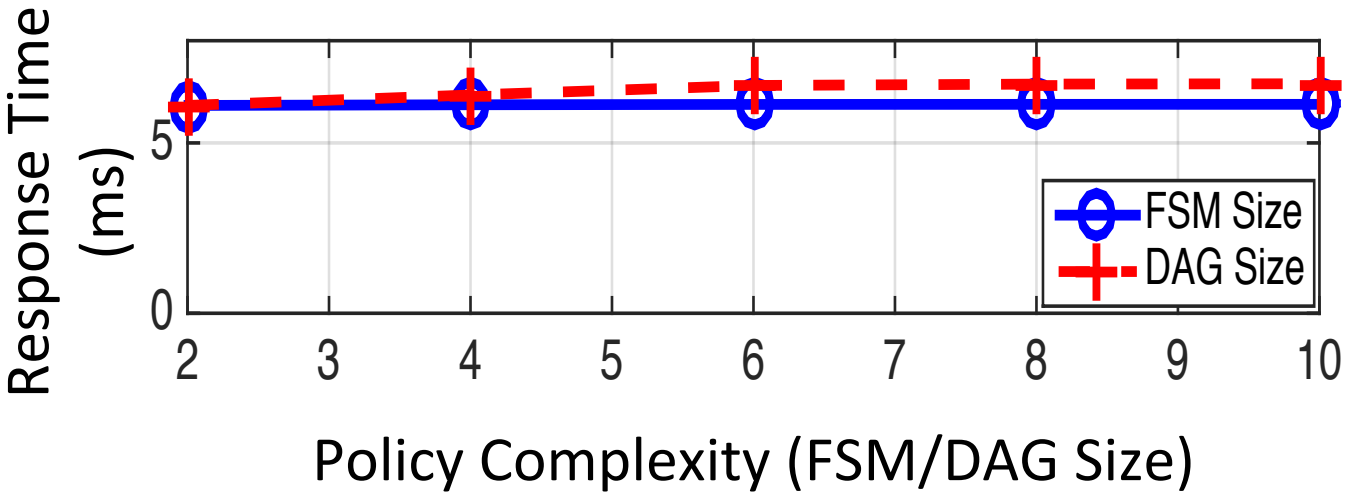
The fraction of attacks prevented

Topological constraints causes “blind spots” in Distributed Firewall/IPS defense:

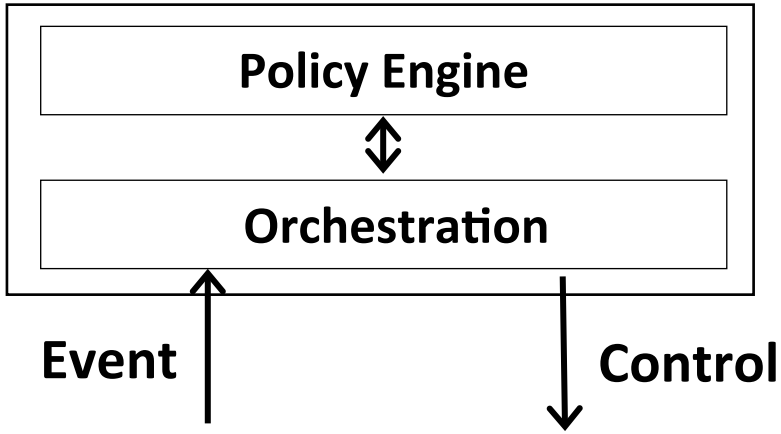
- unmanageable switches
- devices connected to multiple switches
- NAT/DHCP that hides device identity

Scalability of PSI controller





ψFSM ⟶ ψDAG



PSI Controller

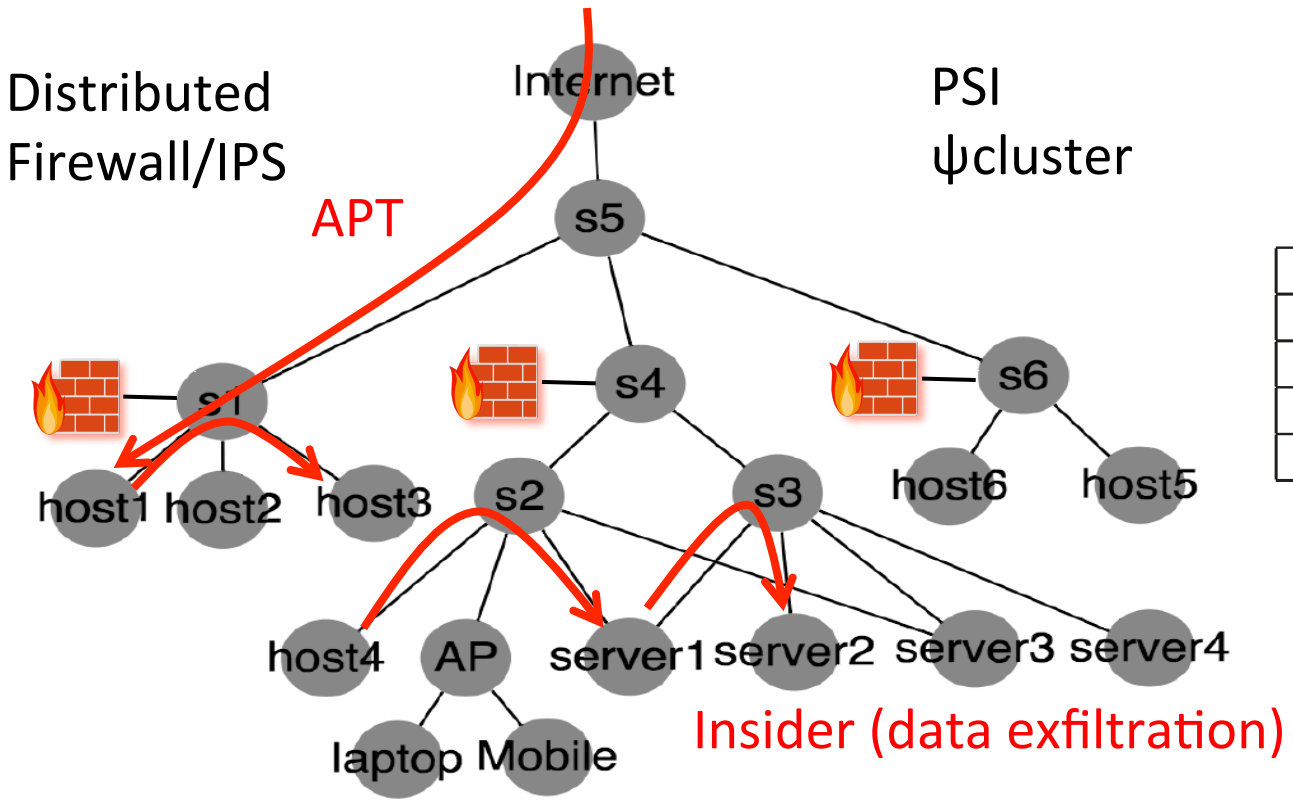
- Max. Throughput: 20K events/s, support **100K device** if every device generates an event every 5s.
- Response Time: **< 10 ms**

Conclusion

- Traditional enterprise security solutions have key limitations:
  - Context, agility, and isolation
- PSI: Leverage SDN/NFV to have a cleaner architecture
- PSI contributions:
  - *Isolated and customized middleboxes*
  - *Expressive policy abstraction*
  - *Scalable & responsive orchestration*
- Security benefits
  - PSI prevents 35% more attacks (APT, insider attacks) than distributed Firewall/IPS.
  - PSI reduces performance interference by 85% (See paper)
  - Enabler for new capabilities (See paper)
- Scalability
  - A single PSI controller can support a network with 100k devices

Backups

Security benefit: increase coverage over attacks



An enterprise network from MacAfee's report

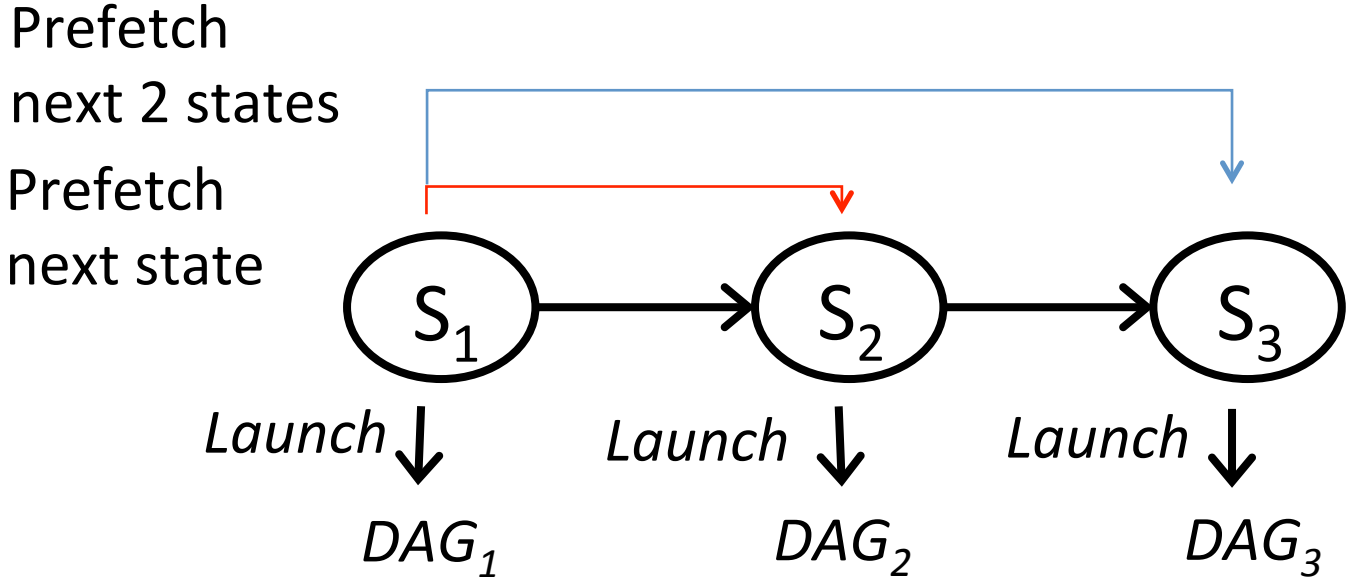
$$coverage = \frac{num.\ of\ prevented\ attacks}{num.\ of\ all\ possible\ attacks}$$

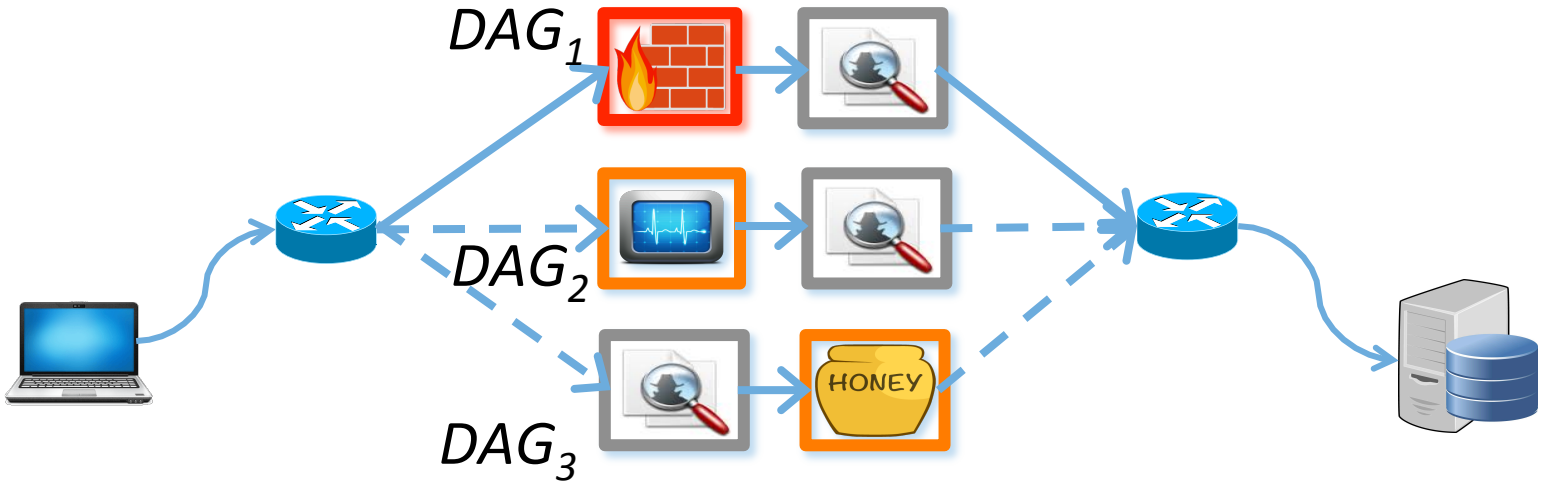
Topology	distributed Firewall/IPS Coverage	PSI Coverage
mini-stanford [42]	52%	92%
apt-mcafee [10]	59%	91%
pix-cisco [22]	56%	89%
all	56%	91%

PSI decouples enforcement from fundamental topology constrains:

- unmanageable switches
- devices connected to multiple switches
- NAT/DHCP

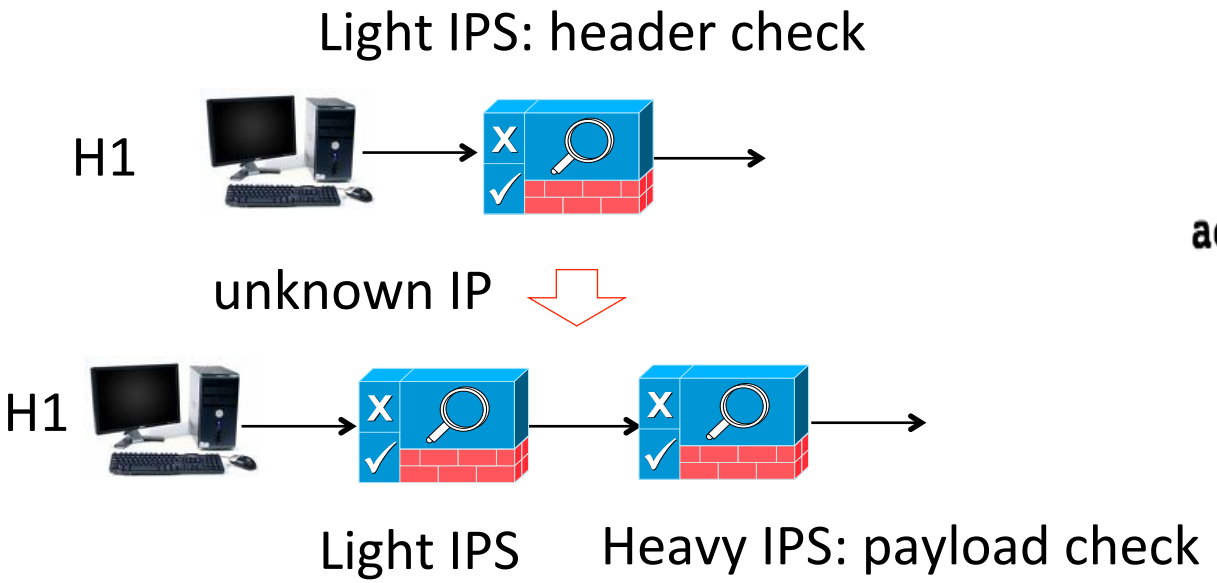
ψDAG prefetching





Challenges for expressive policy abstraction

Desired policy



Check the packet header of H1's outbound traffic. And if H1 is accessing an unknown IP. Then enforce a payload check.

Current ACL policy

IP with no context

```
access-list OUT extended permit ip host 209.168.200.3 any
```

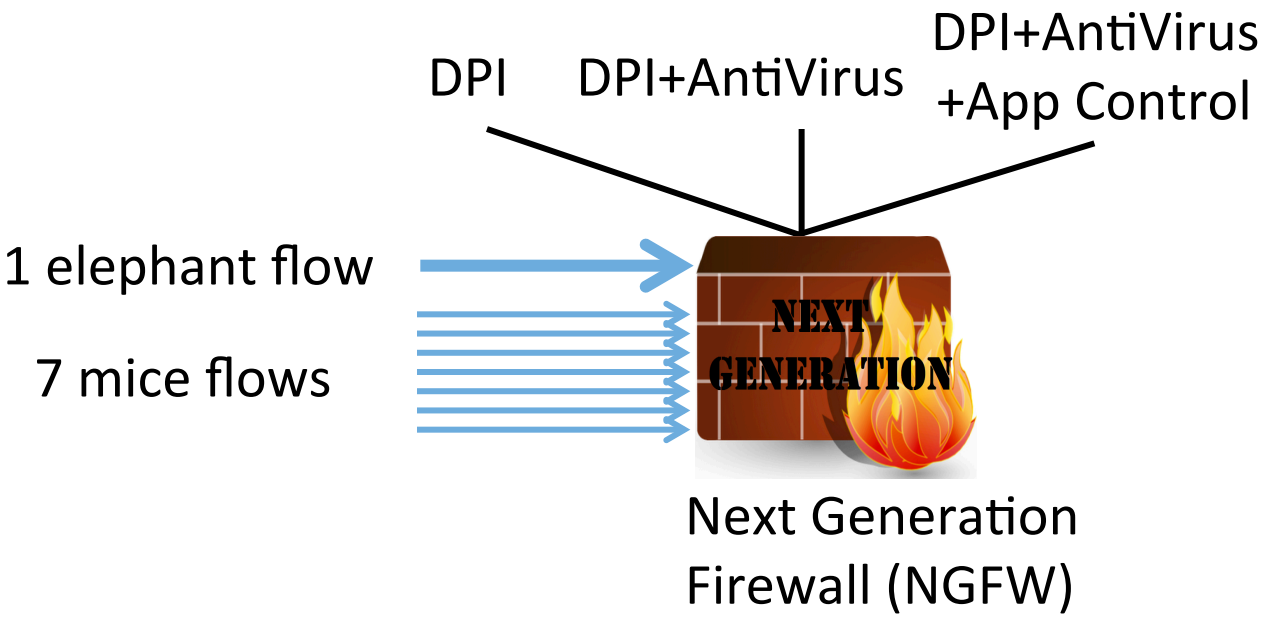
ACL rule for Cisco PIX firewall

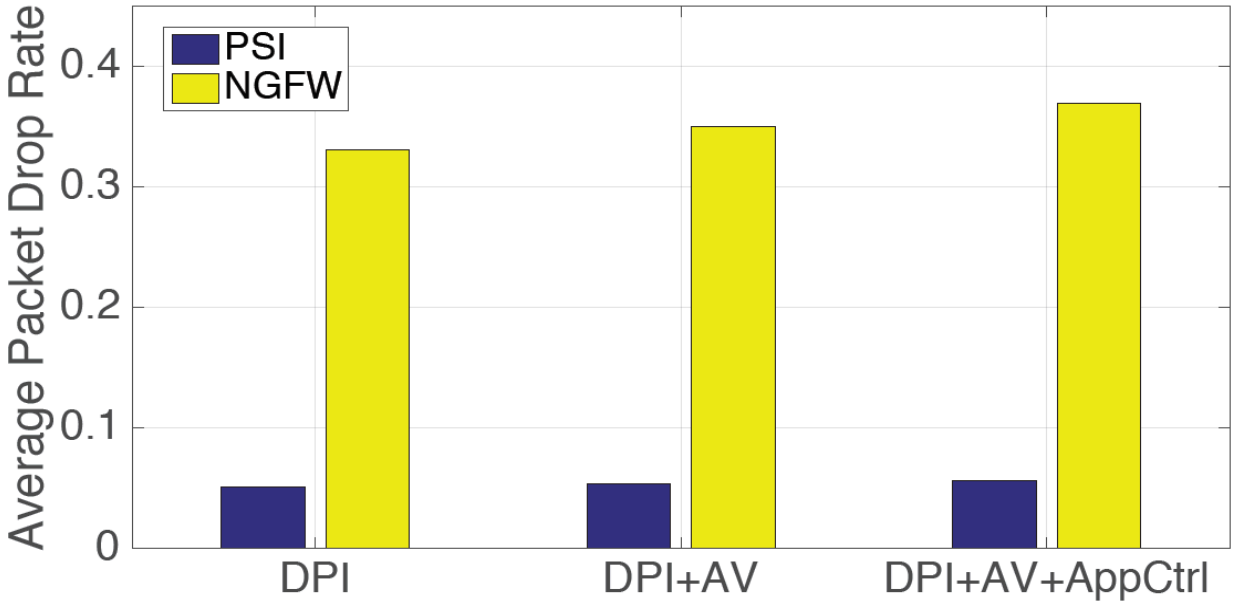
Static intent

Cannot express:

- Context-based forwarding & processing
- Agile intent evolution

Security benefit: reducing collateral damage





Collateral damage measured by average packet drop rate for each flow

PSI reduces performance interference by 85%

Benefits of PSI optimizations

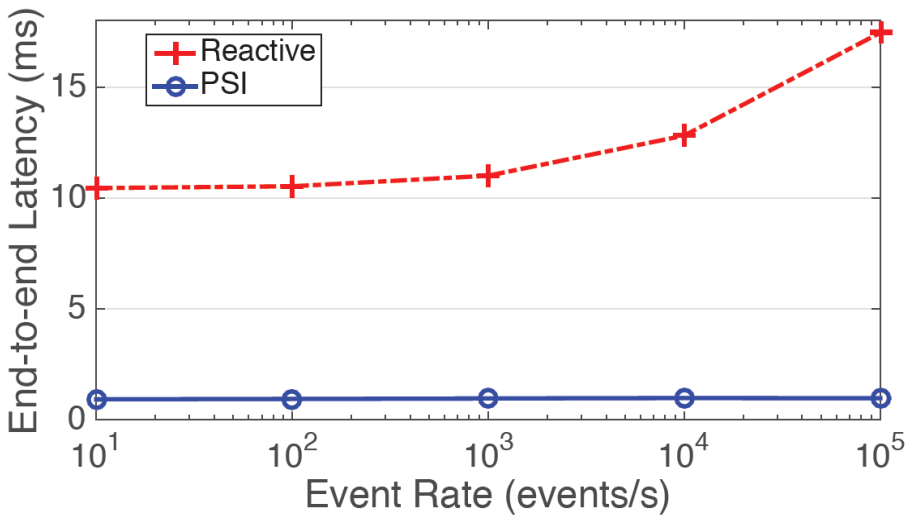


Fig. 15: Proactive context-based forwarding.

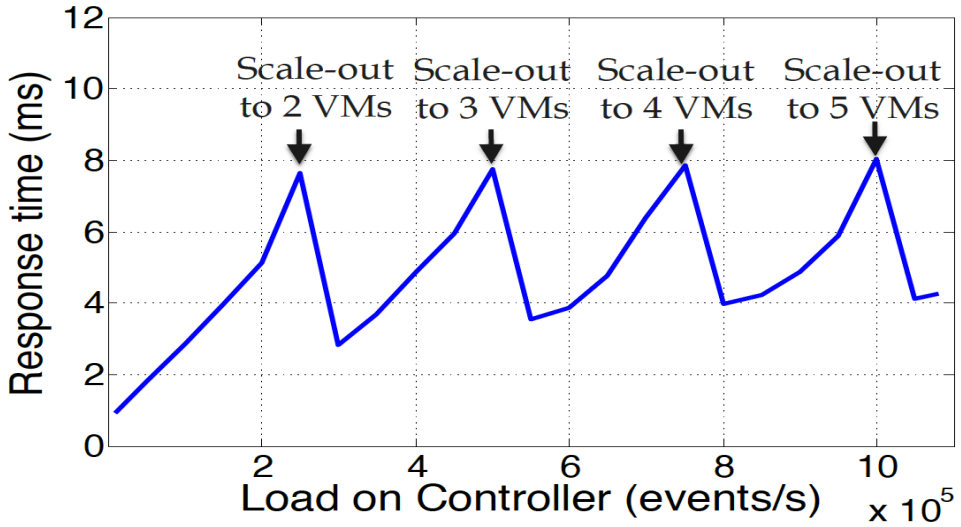


Fig. 17: PSI controller scale-out.

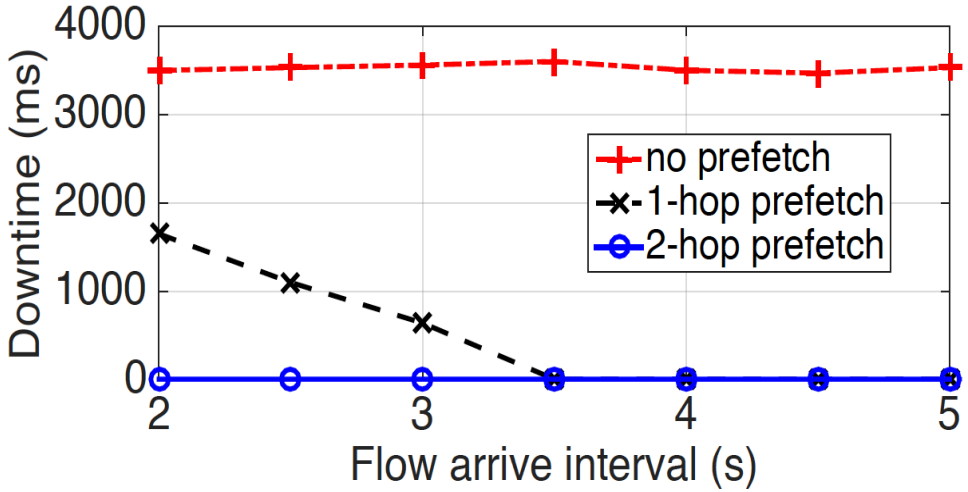


Fig. 16: Effect of ψDAG prefetching.

- Proactive context-based forwarding reduces latency by 10X.
- DAG prefetching mechanism reduces security downtime to zero.
- Scale-out scheme cuts the response time down to 10ms.
- With the optimizations, a single PSI controller can support a network with 100K devices.