\Orchestrating a brighter world NEC

SECURWARE 2023
30021
Lightweight Fine-grained Access Control Mechanism Based on Zero Trust in CPS

September 25, 2023

Nakul D Ghate, Shohei Mitani, Hirofumi Ueda
Secure Systems Platforms Research Laboratories
NEC Japan

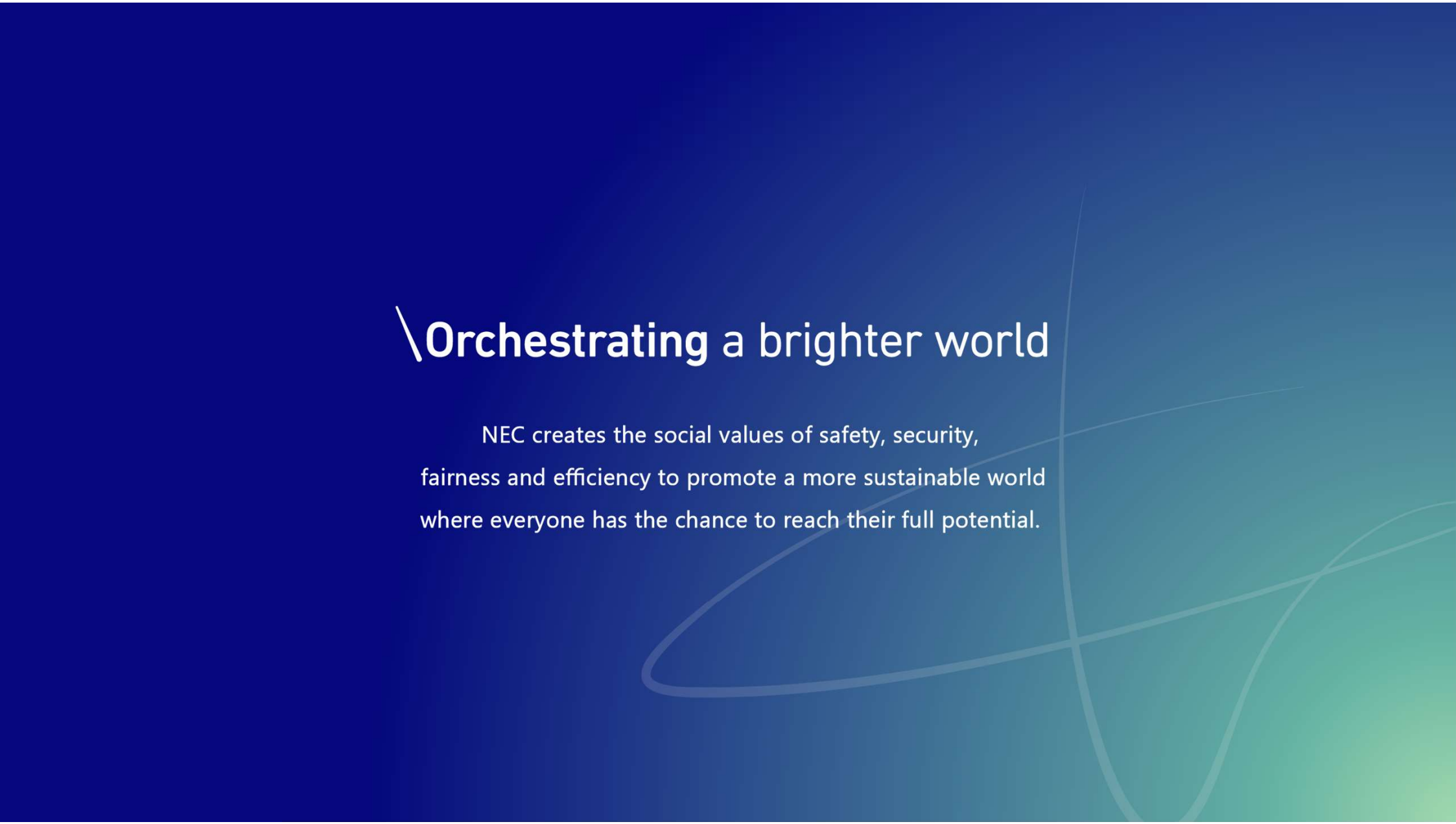
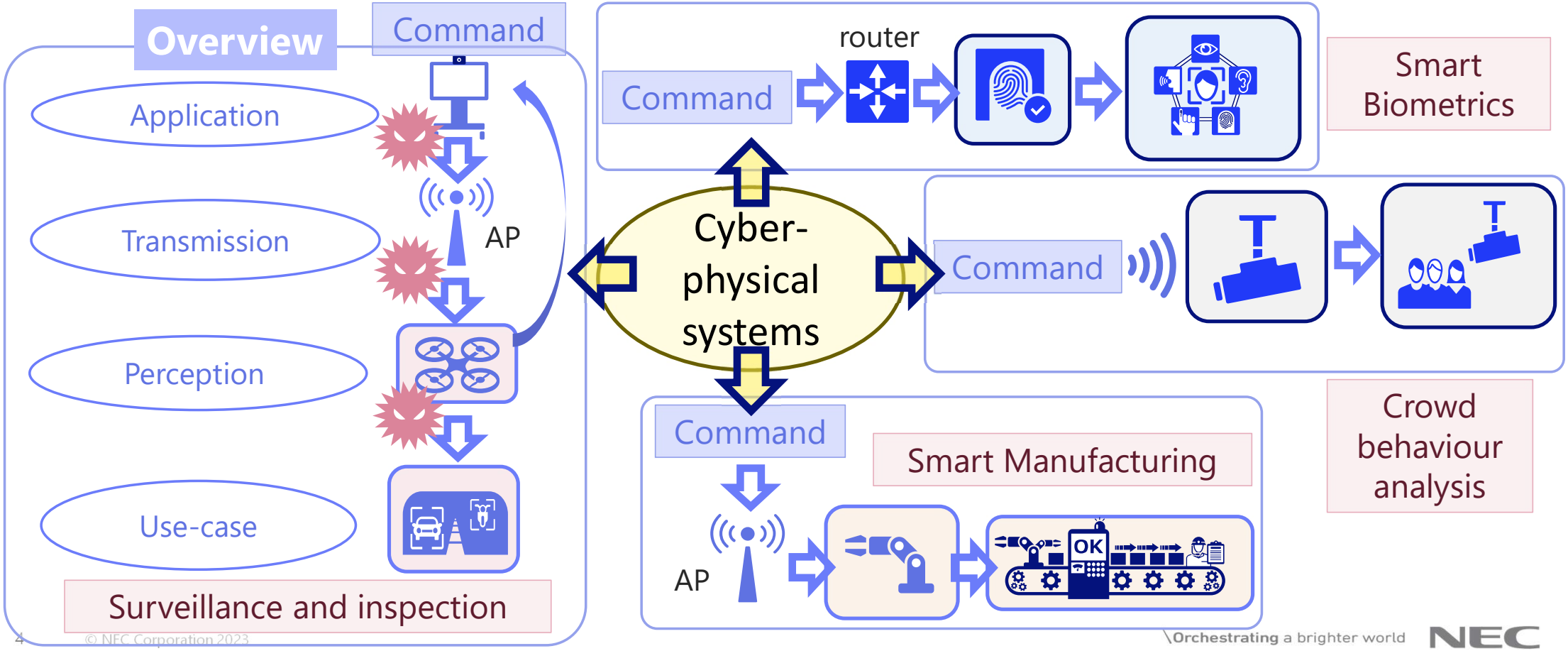

\Orchestrating a brighter world
NEC creates the social values of safety, security,
fairness and efficiency to promote a more sustainable world
where everyone has the chance to reach their full potential.

Table of Contents

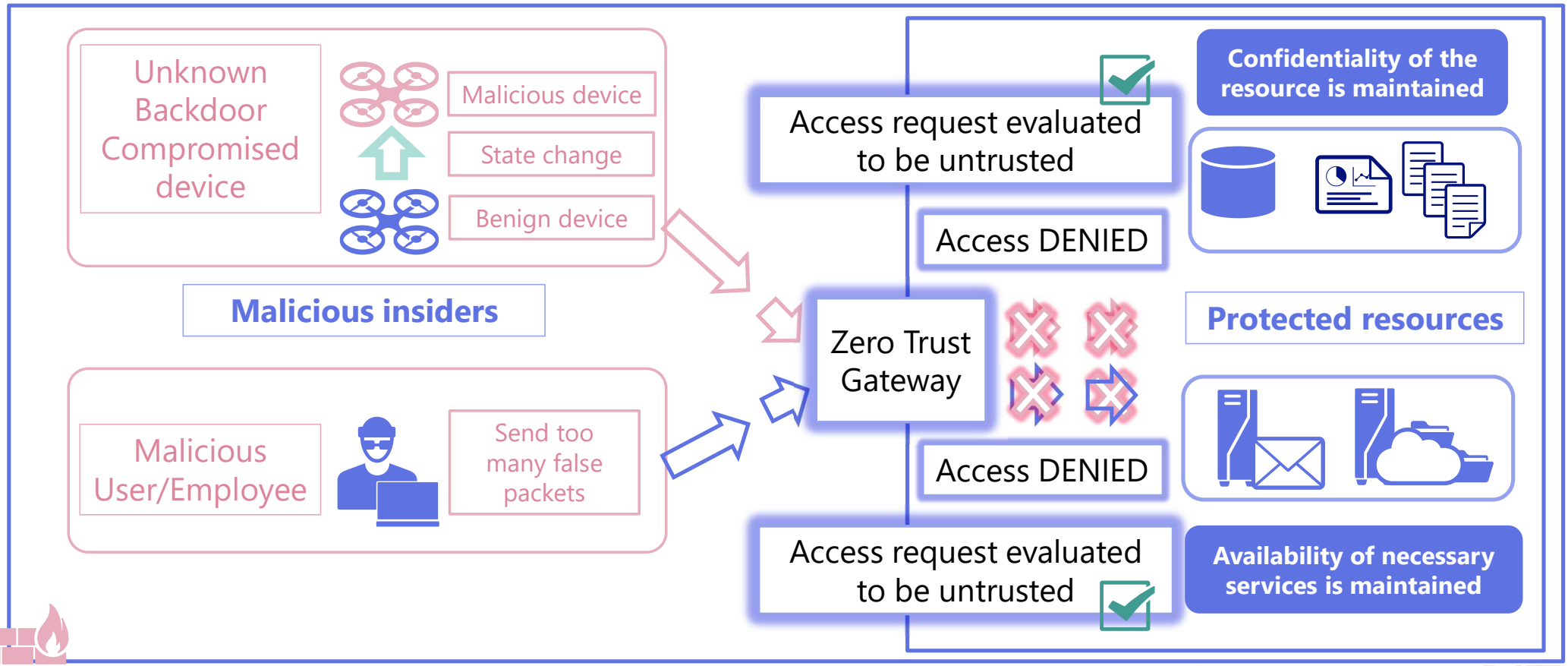
Background: Cyber-Physical Systems

CPS is a combination of closely integrated physical processes, networking and communication
- Difficult to deploy perfect security solutions owing to heterogeneity and resource limitations
  - => Attacks and threats exist on end devices, transmission, application and its actuation



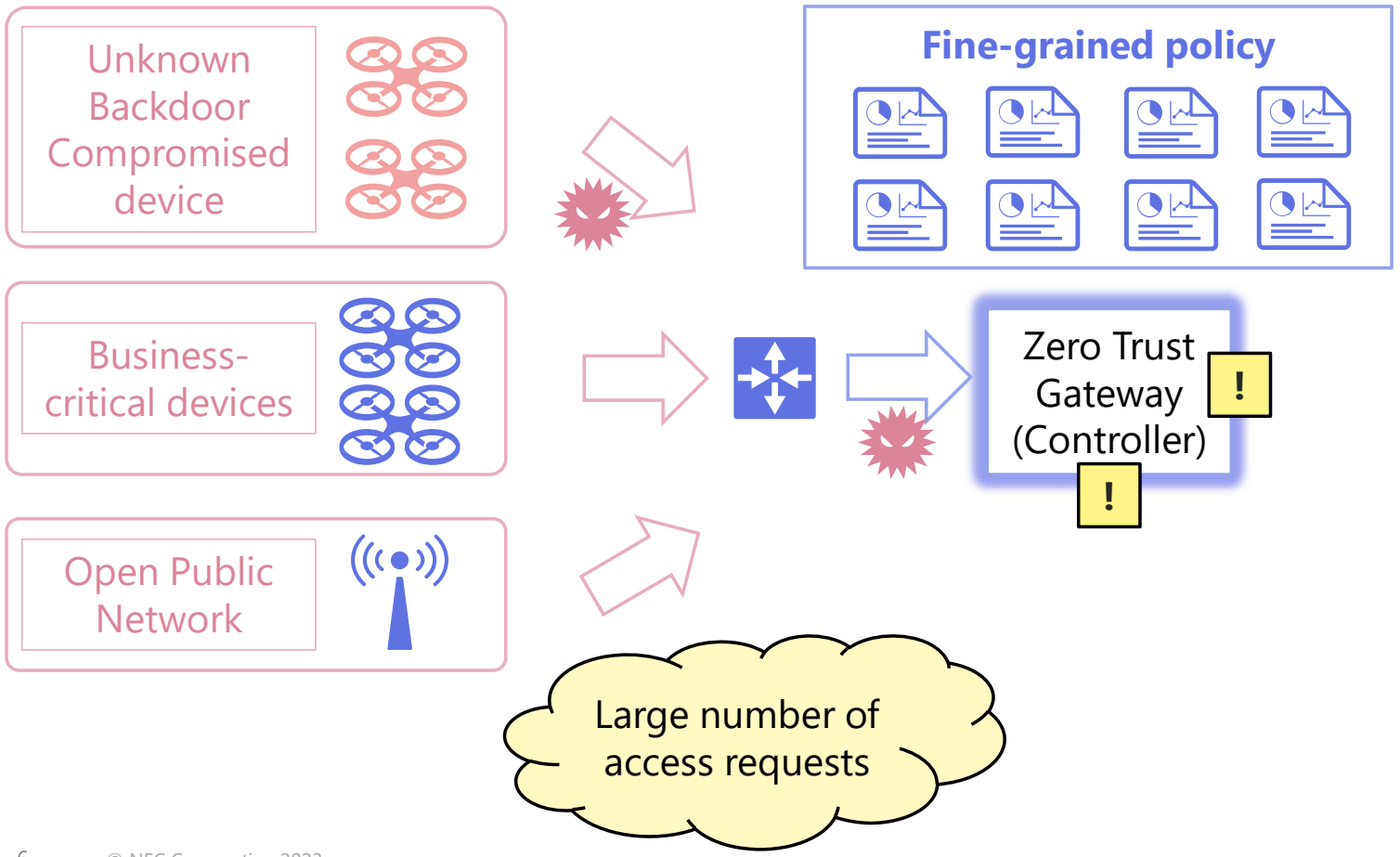
Existing Approach: Zero Trust Access Control Model

In Zero Trust, all assets are monitored, all communications are evaluated to be secured
Uses Fine-grained access policies for achieving high levels of security



Fine-grained policies increase the workload

Fine-grained policies increase the workload on the Zero Trust controller



Too many policies increase the processing load of the access controller

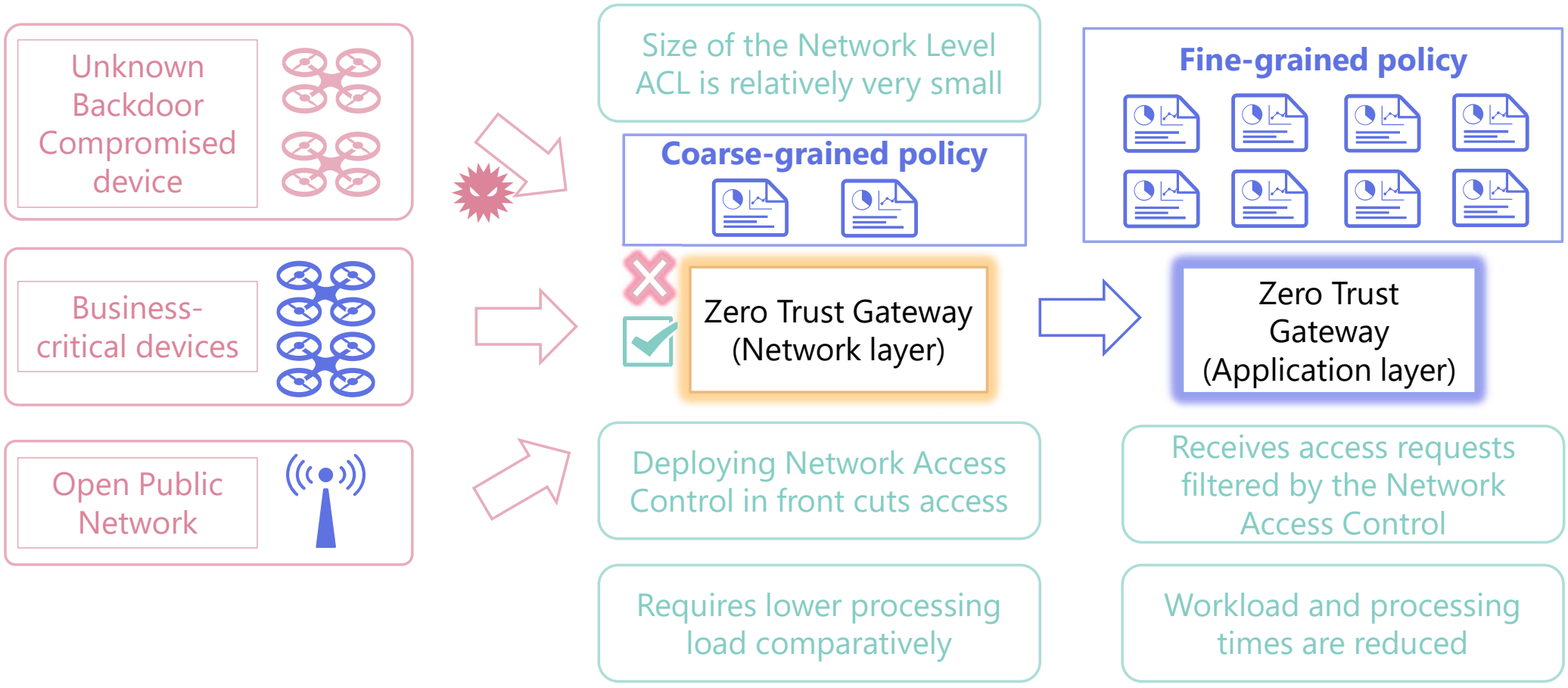
Too many policies increase the processing time and results in delays

Fine-grained access controller is vulnerable to DDOS attacks

Large cost of storage, computation (cryptography) and scalability issues

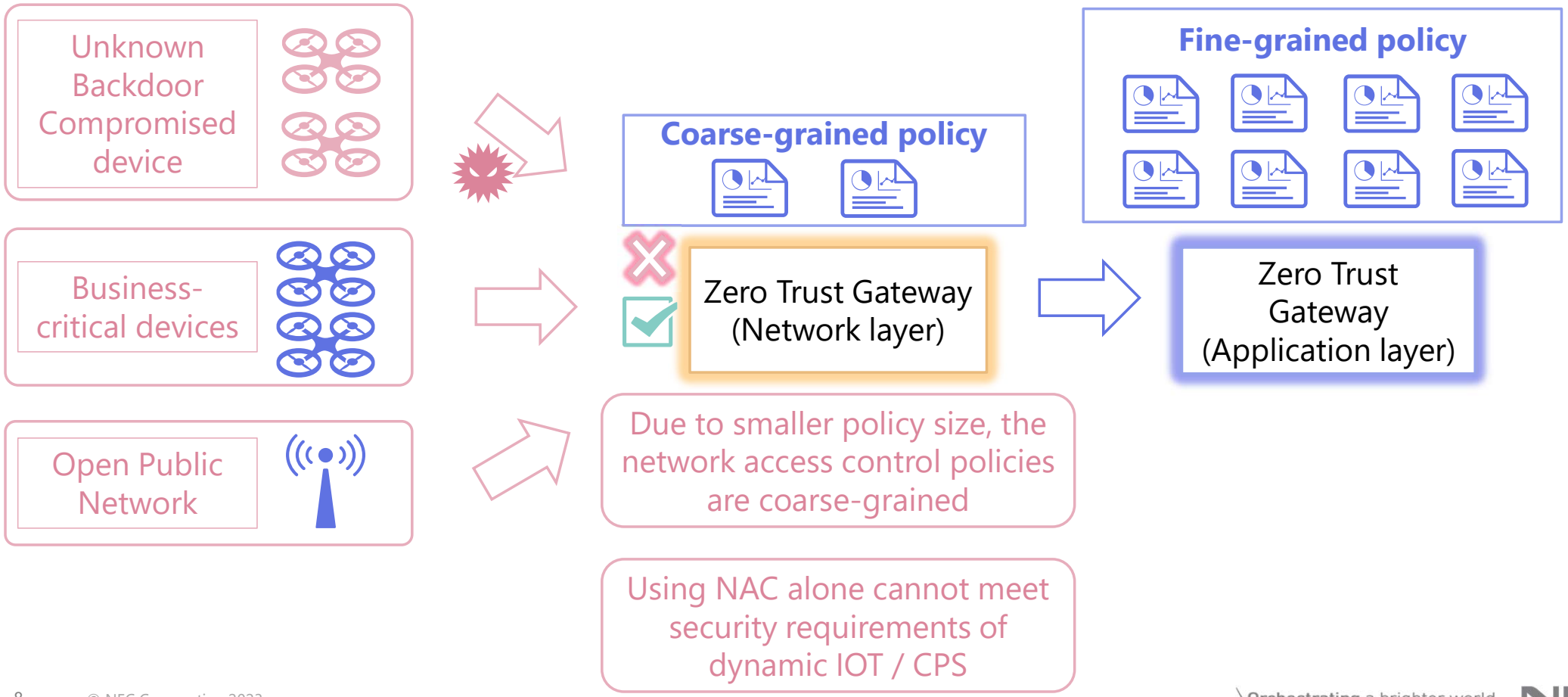
Network Access Control

Using Network Access control in front helps in reducing workload but with coarse-grained policies



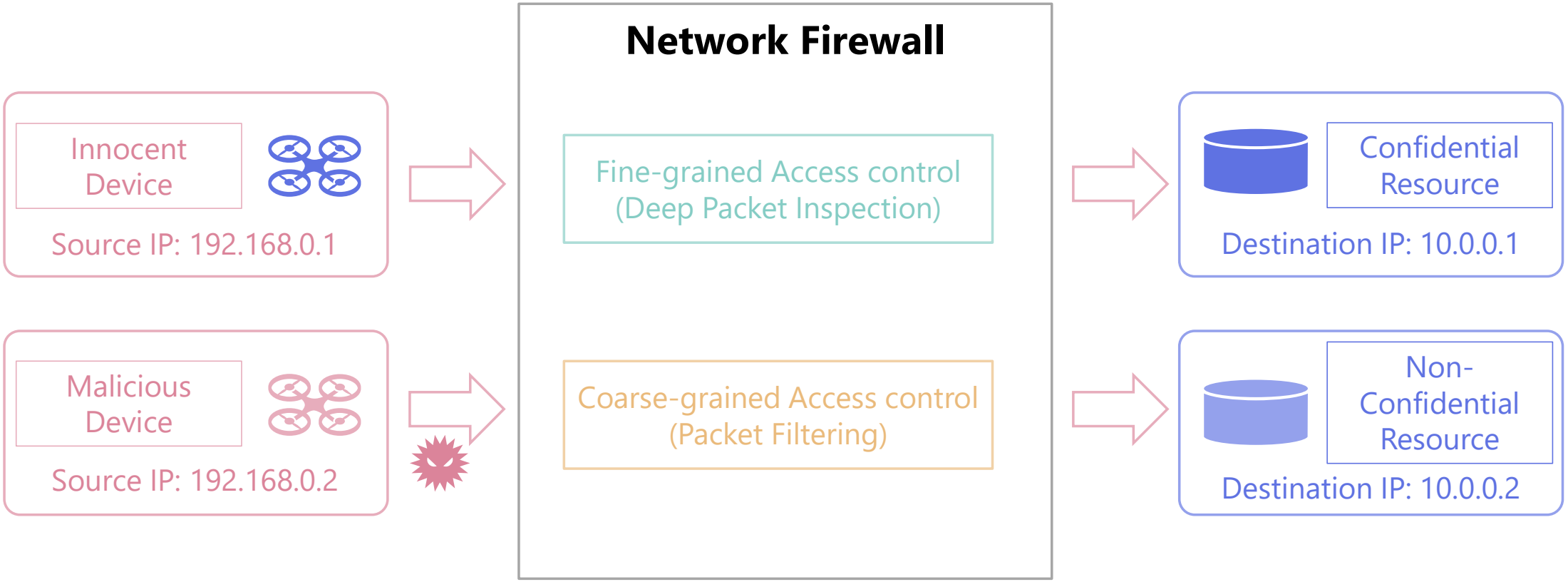
Network Access Control

Using Network Access control in front helps in reducing workload but with coarse-grained policies



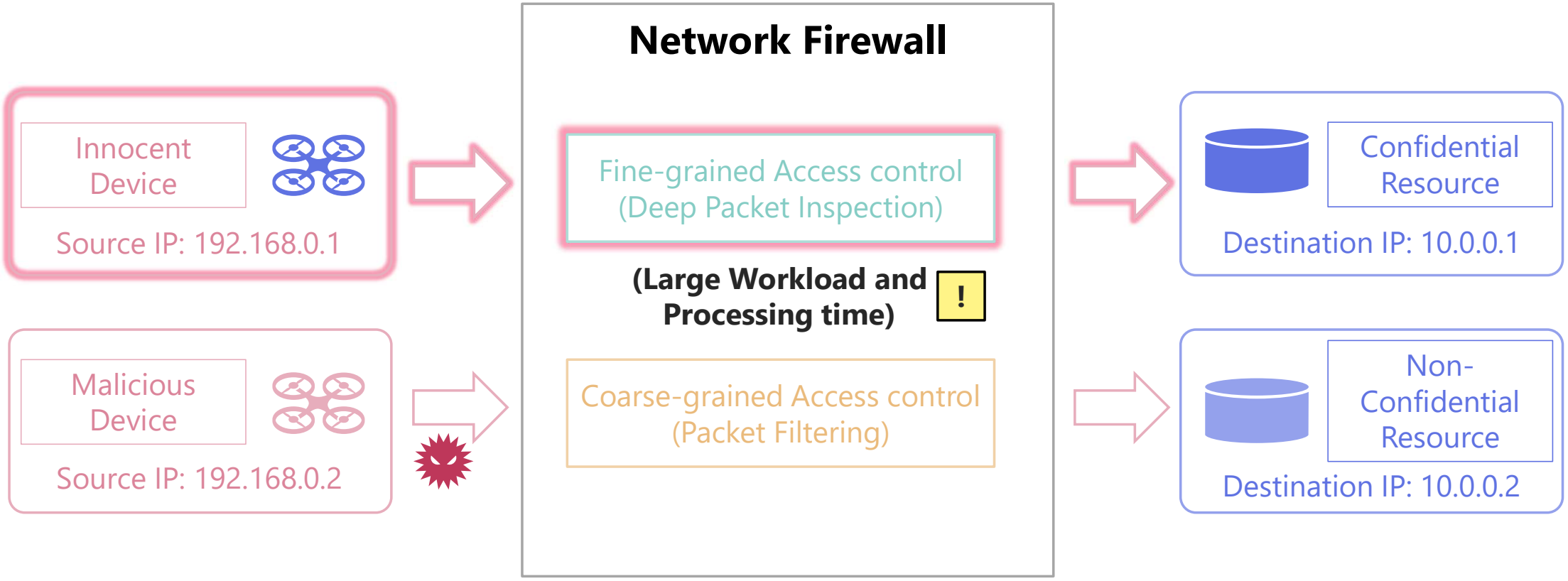
Past works – Liu et al [1]

The granularity of access control is switched based on application security requirements



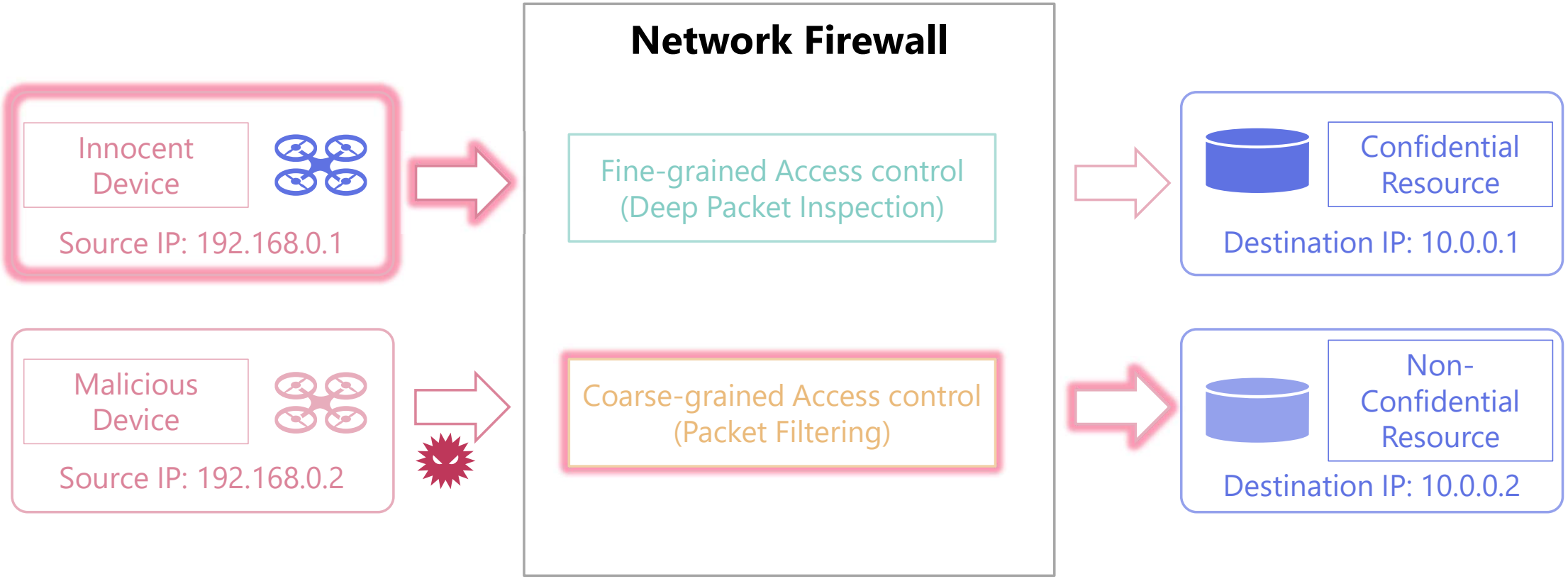
Past works – Liu et al [1]

Always use Fine-grained Deep inspection for Confidential Resources



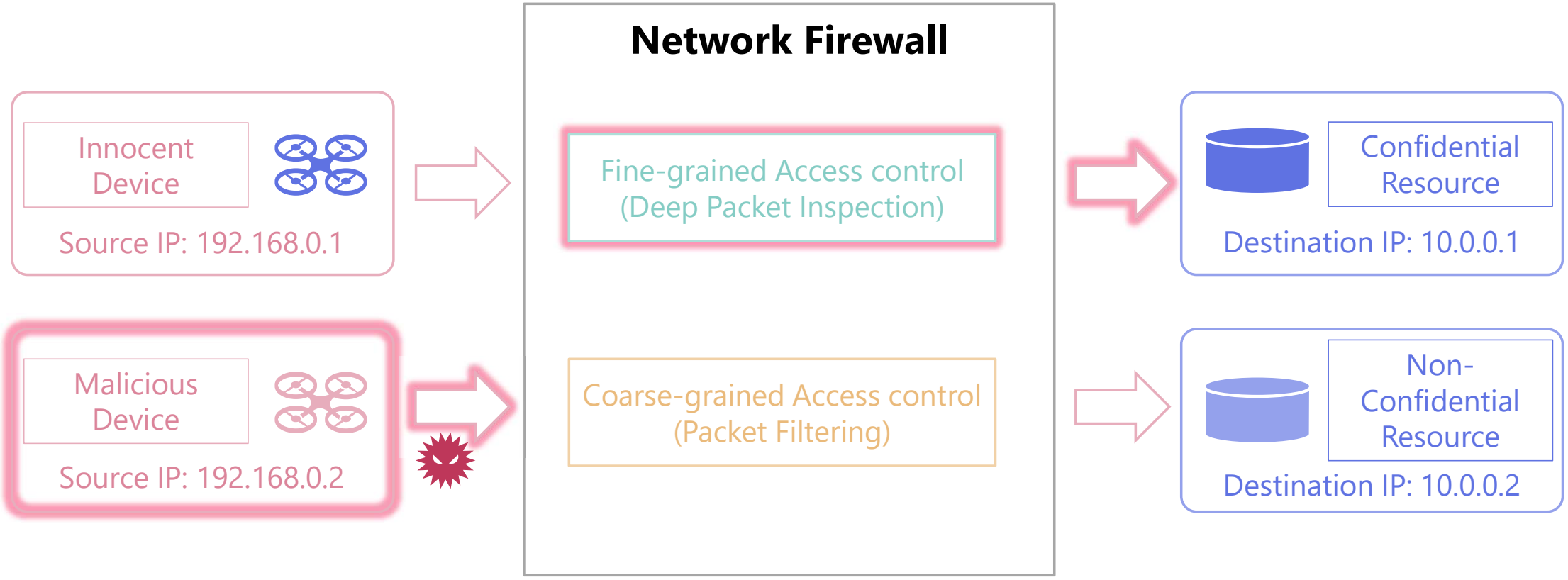
Past works – Liu et al [1]

Always use Coarse-grained Packet filtering for Non-Confidential Resource



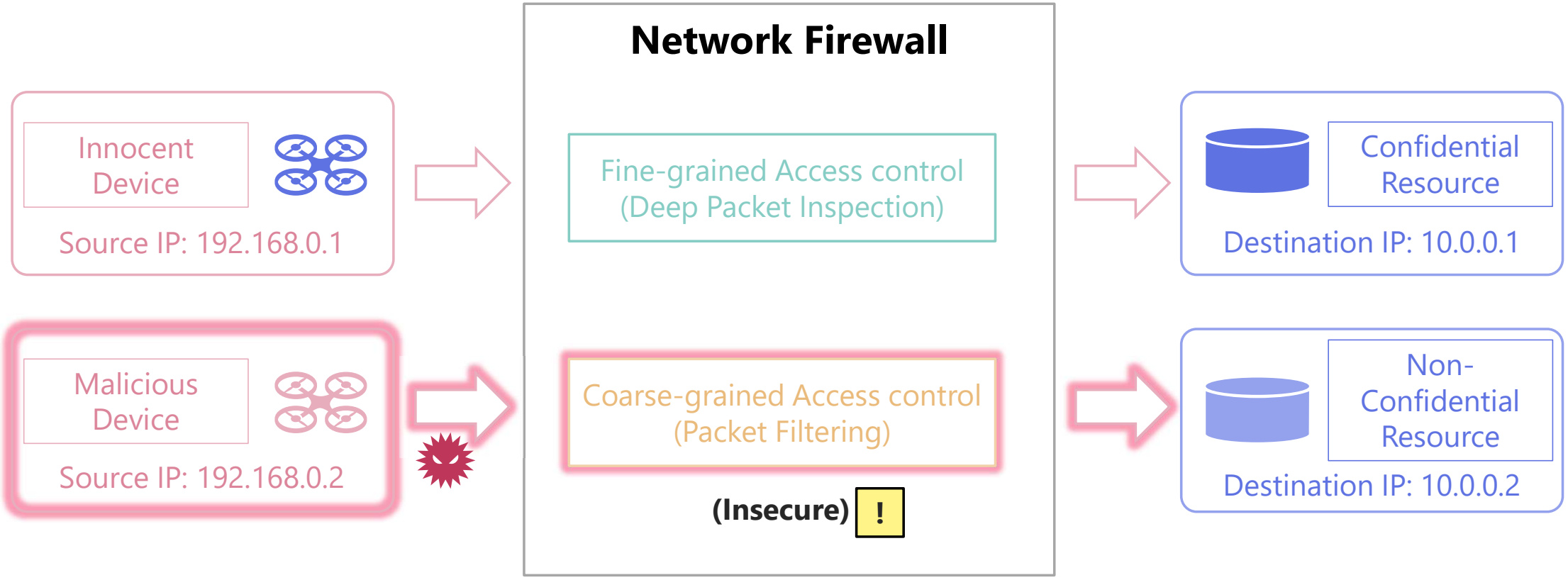
Past works – Liu et al [1]

Always use Fine-grained Deep inspection for Confidential Resources



Past works – Liu et al [1]

Always use Coarse-grained Packet filtering for Non-Confidential Resource



Can we do better ? (Recognizing the problems)

Decisions of granularity is based on comprehensive understanding of dynamic environment

Analyze the subjects

- Identify Subject
- Identify Risks
- Identify Behavior
- Identify Context

Analyze the Environment

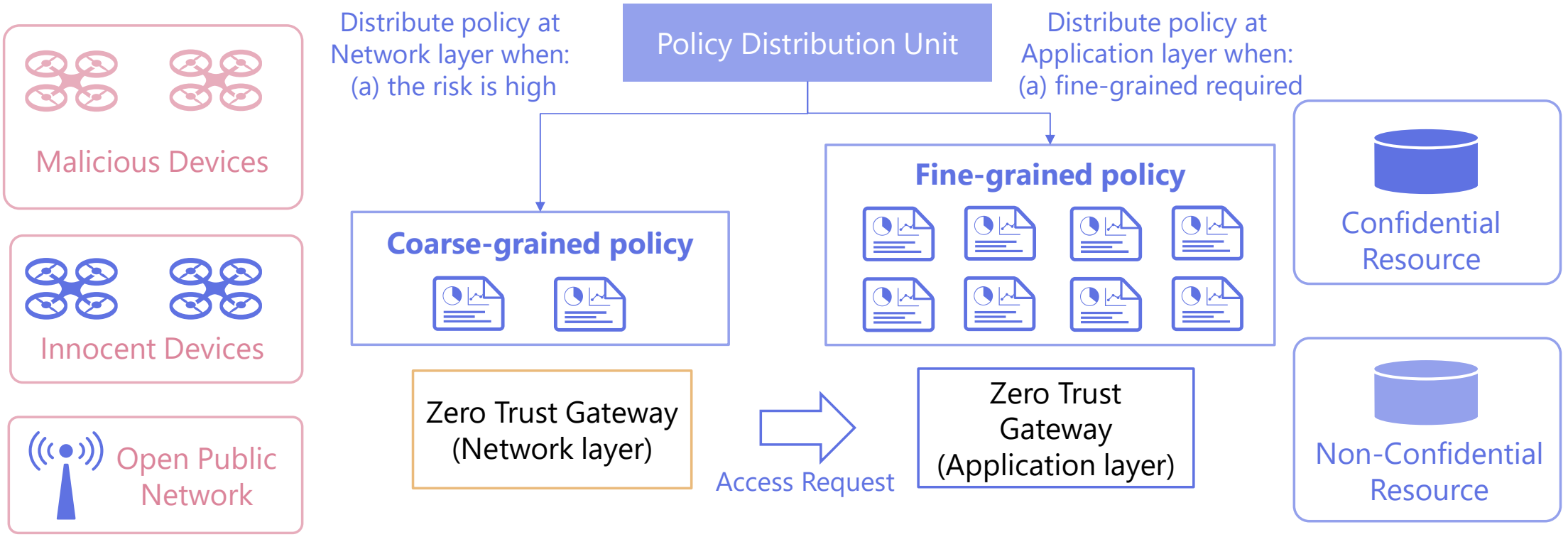
- Identify System State
- Identify Network Conditions
- Identify external threats
- Identify business impacts

Analyze the Resources

- Identify Type
- Identify Data Classification
- Identify Data Sensitivity
- Identify Access history

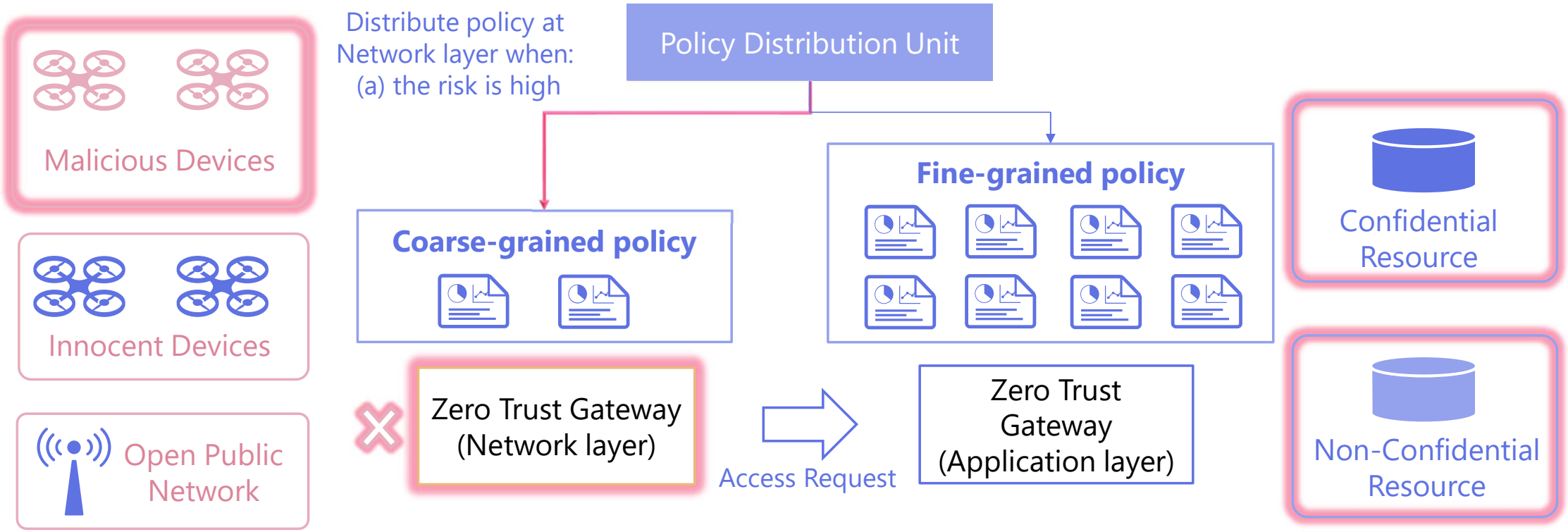
Our approach

The choice of policy enforcement location is dynamic based on the environment



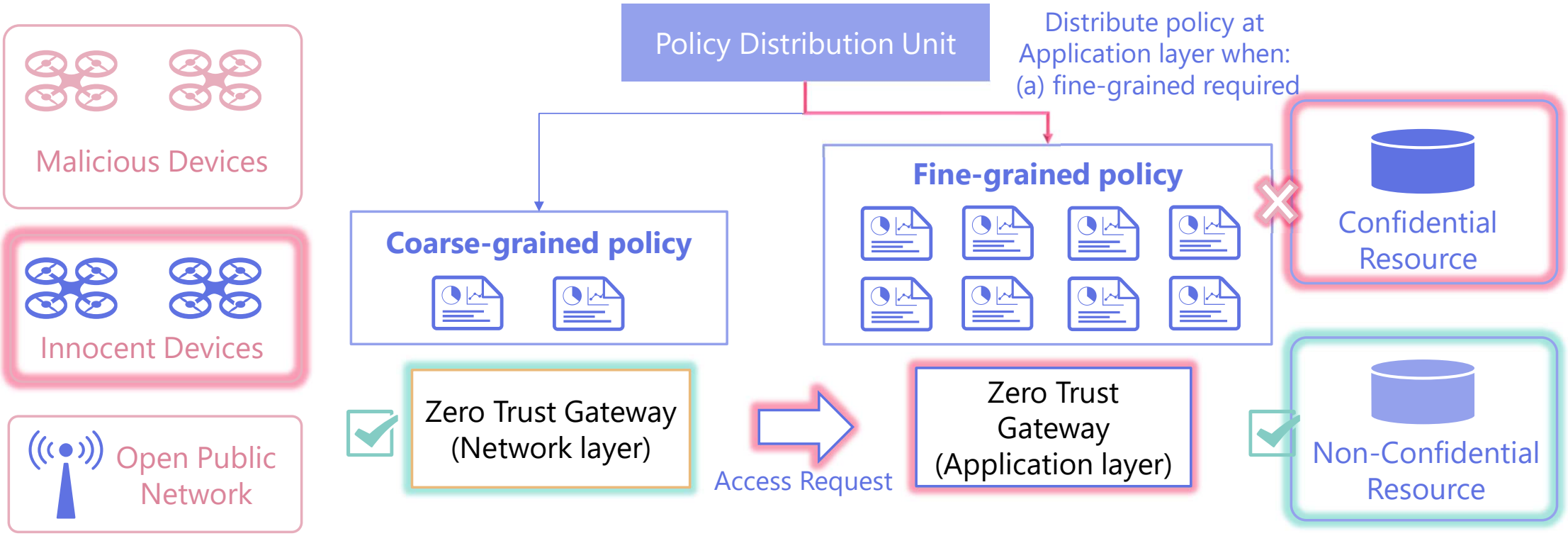
Our approach

The choice of policy enforcement location is dynamic based on the environment



Our approach

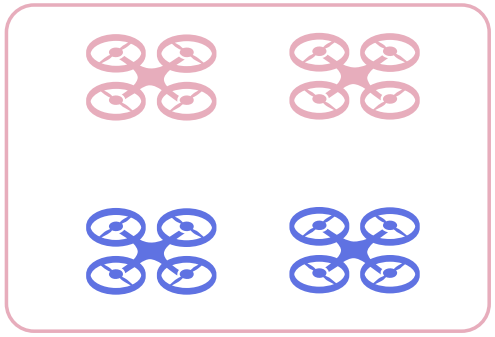
The choice of policy enforcement location is dynamic based on the environment



Assumptions and algorithm

Many IOT devices are identified by a common IP address under Network Address Translation (NAT)

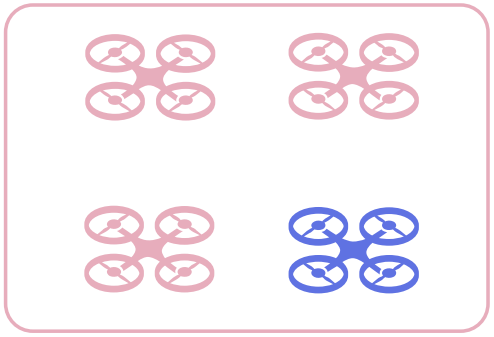
Source IP: 192.168.0.1



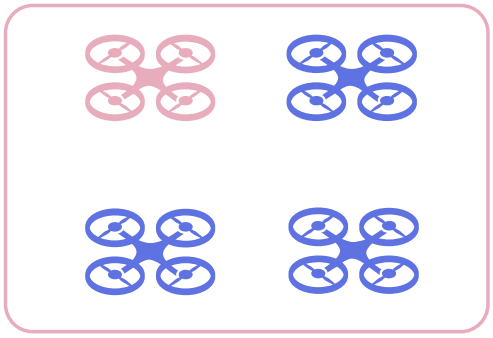
Network Layer will identify all devices only by their Source IP address

Network Layer cannot distinguish between different devices belonging to same Source IP

Source IP: 192.168.0.3

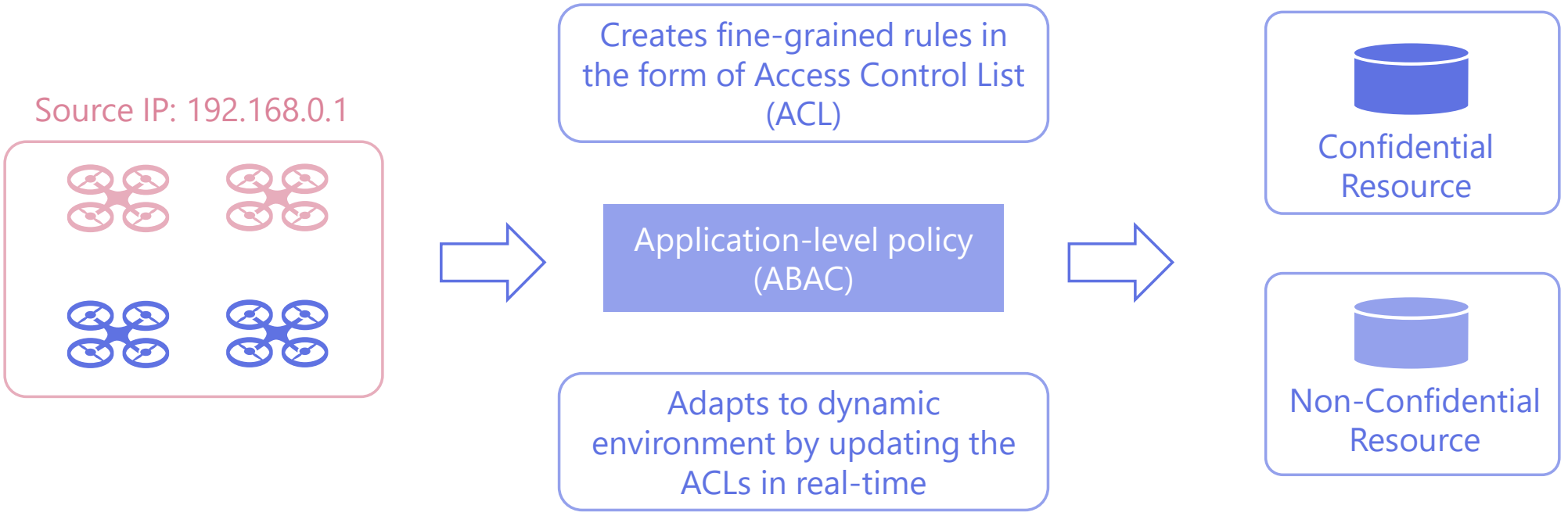


Source IP: 192.168.0.2



Assumptions and algorithm

Application-level policy creates fine-grained rules for each device and adapted to dynamic environment

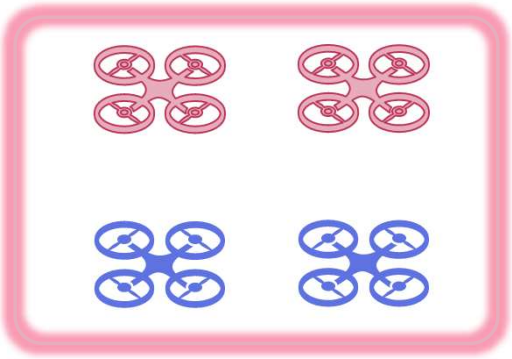


Assumptions and algorithm

Application-level policy creates fine-grained rules for each device and adapted to dynamic environment

Dev 1 and Dev 2 are identified to be malicious

Source IP: 192.168.0.1



Access to the resources is DENIED

Fine-grained ACL

(Dev 1, Rsc 1, *DENY*)
(Dev 1, Rsc 2, *DENY*)
(Dev 2, Rsc 1, *DENY*)
(Dev 2, Rsc 2, *DENY*)

Application-level policy (ABAC)

Creates fine-grained rules in the form of Access Control List (ACL)

Rsc 1

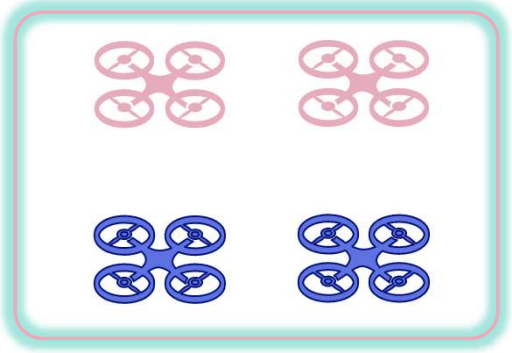
Rsc 2

Assumptions and algorithm

Application-level policy creates fine-grained rules for each device and adapted to dynamic environment

Dev 3 and Dev 4 are identified to be innocent

Source IP: 192.168.0.1



Access to the resources is ALLOWED

Fine-grained ACL

(Dev 3, Rsc 1, *ALLOW*)
(Dev 3, Rsc 2, *ALLOW*)
(Dev 4, Rsc 1, *ALLOW*)
(Dev 4, Rsc 2, *ALLOW*)

Application-level policy (ABAC)

Creates fine-grained rules in the form of Access Control List (ACL)

Rsc 1

Confidential Resource

Non-Confidential Resource

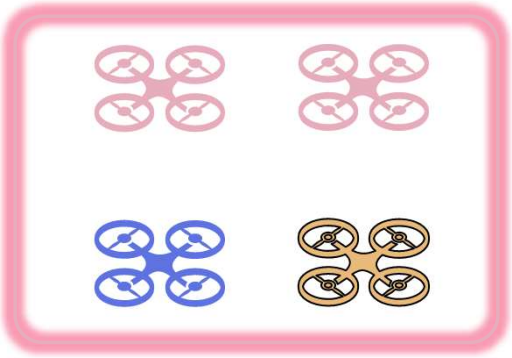
Rsc 2

Assumptions and algorithm

Application-level policy creates fine-grained rules for each device and adapted to dynamic environment

Dev 4 is suddenly identified to be suspicious

Source IP: 192.168.0.1



Access to the confidential resource is DENIED

Fine-grained ACL

(Dev 3, Rsc 1, *ALLOW*)
(Dev 3, Rsc 2, *ALLOW*)
(Dev 4, Rsc 1, *DENY*)
(Dev 4, Rsc 2, *ALLOW*)

Application-level policy (ABAC)

Adapts to dynamic environment by updating the ACLs in real-time

Rsc 1

Confidential Resource

Non-Confidential Resource

Rsc 2

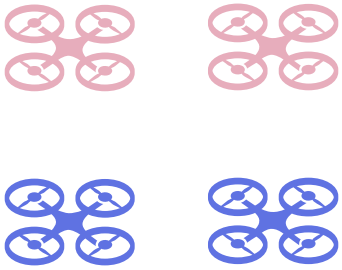
Assumptions and algorithm

Distribution of DENY rule on Network layer may lead to mis-control

Dev 1 and Dev 2: malicious

Dev 3 and Dev 4: innocent

Source IP: 192.168.0.1



Original ABAC policy (ACL)

Policy Distribution Unit

Coarse-grained policy

Fine-grained policy

Zero Trust Gateway (Network layer)

Access Request

Zero Trust Gateway (Application layer)

Confidential Resource

Non-Confidential Resource

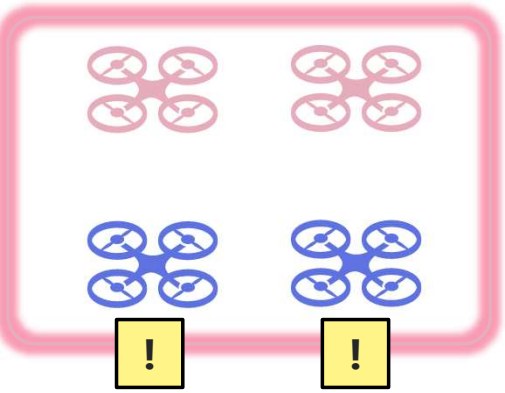
Assumptions and algorithm

Distribution of DENY rule on Network layer may lead to MIS-CONTROL

Dev 1 and Dev 2: malicious

Dev 3 and Dev 4: innocent

Source IP: 192.168.0.1



Mis-control of access from Dev 3 and Dev 4

Policy Distribution Unit

Coarse-grained policy

(192.168.0.1, 10.0.0.1, DENY)

Fine-grained policy

Zero Trust Gateway (Network layer)

Access Request

Zero Trust Gateway (Application layer)

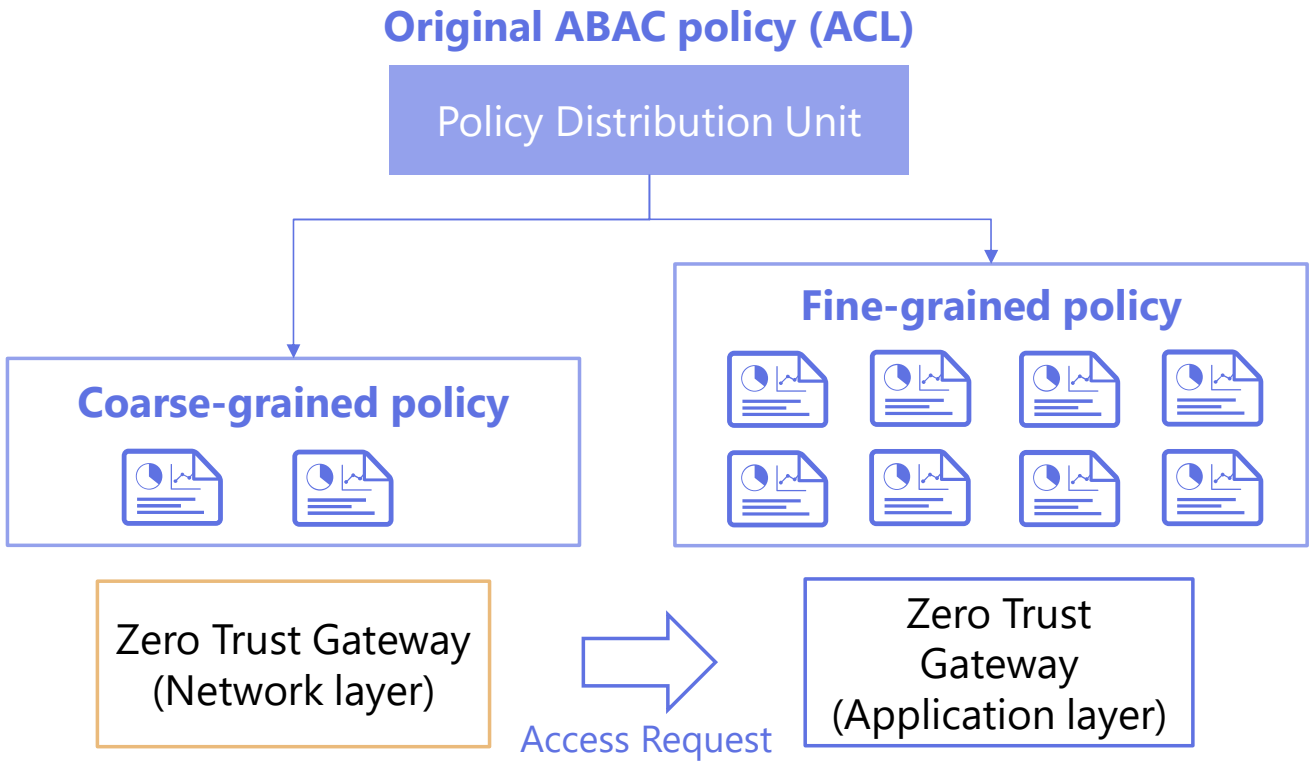
Destination IP: 10.0.0.1

Confidential Resource

Non-Confidential Resource

Assumptions and algorithm

Our Distribution Algorithm attempts to reduce such mis-control



Our algorithm calculates the mis-control of distributing the policy (ACL) to Network layer

If the mis-control is small, the algorithm distributes it to Network layer

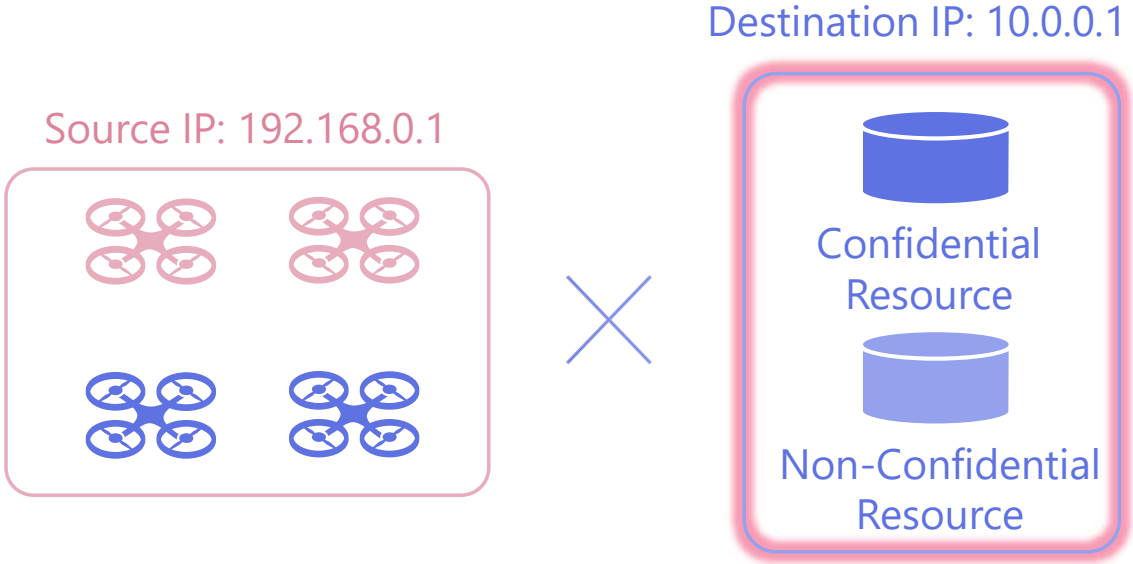
Algorithm optimally decides how many policies can be distributed at Network layer

Access control at Network layer helps in reducing the workload and prevents DDOS

The Algorithm

INPUT: Application level (ABAC) policy/ACL F

STEP 1: CREATE all (Source IP, Destination IP) pairs from (Device ID, Resource ID) pairs



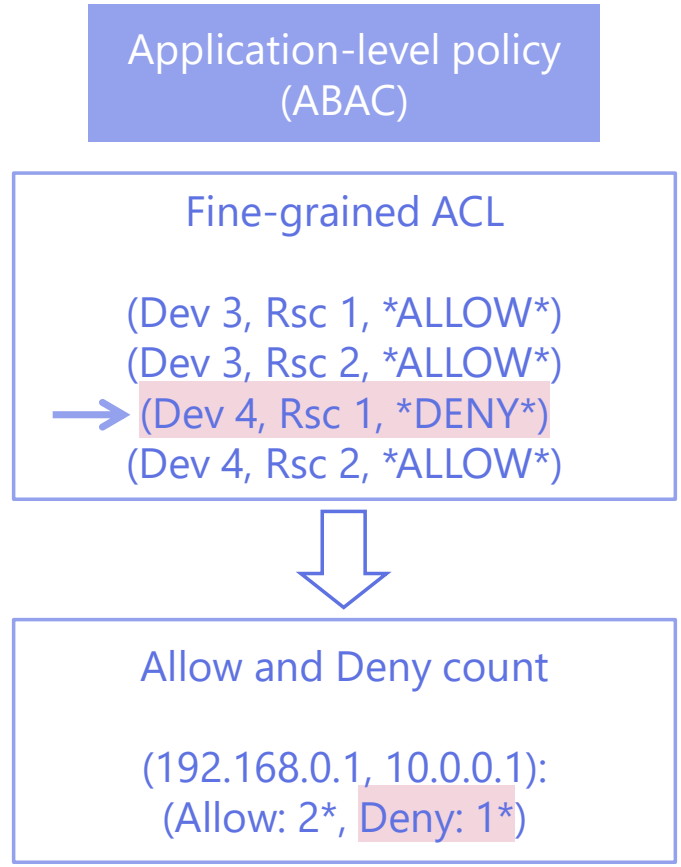
The Algorithm

INPUT: Application level (ABAC) policy/ACL F

STEP 1: CREATE all (Source IP, Destination IP) pairs from (Device ID, Resource ID) pairs

STEP 2: Iterate through F and check if the decision is ALLOWED or DENIED

STEP 3: If the decision is ALLOWED, increase the allow count corresponding to the (Source IP, Destination IP) pair else increase the deny count



(Note: "*" denotes that the process is in progress)

The Algorithm

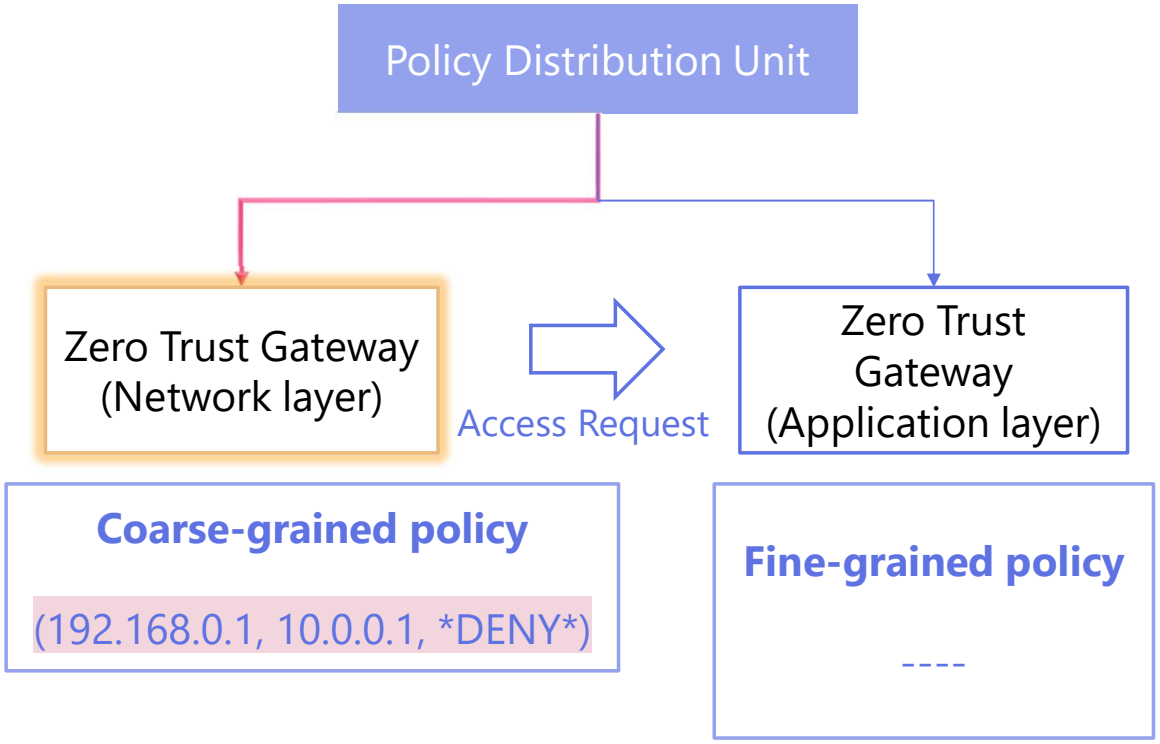
INPUT: Application level (ABAC) policy/ACL F

STEP 1: CREATE all (Source IP, Destination IP) pairs from (Device ID, Resource ID) pairs

STEP 2: Iterate through F and check if the decision is ALLOWED or DENIED

STEP 3: If the decision is ALLOWED, increase the allow count corresponding to the (Source IP, Destination IP) pair else increase the deny count

STEP 4: If the allow count < threshold, then append DENY decision to Network Layer else append ALLOW decision



The Algorithm

INPUT: Application level (ABAC) policy/ACL F

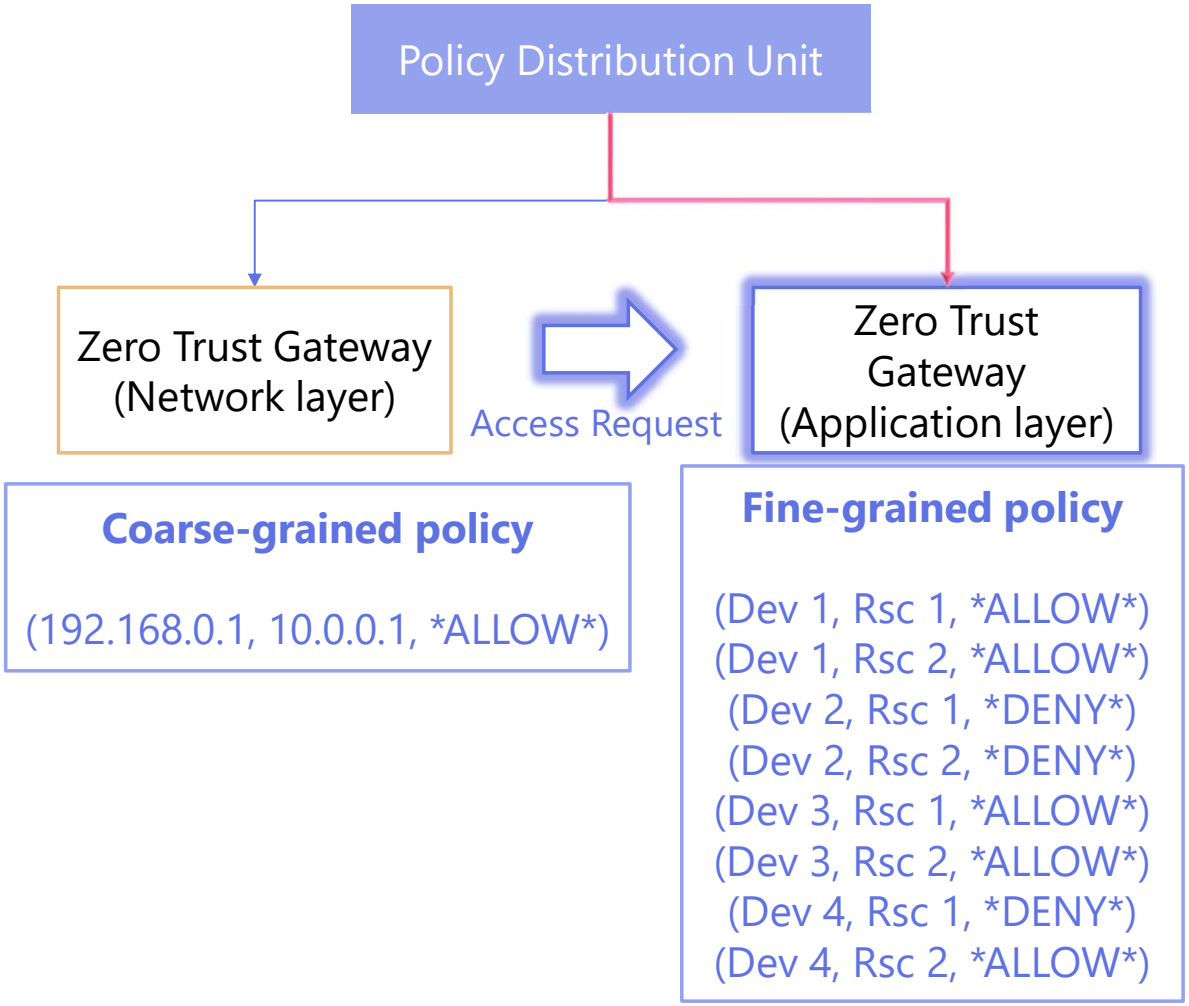
STEP 1: CREATE all (Source IP, Destination IP) pairs from (Device ID, Resource ID) pairs

STEP 2: Iterate through F and check if the decision is ALLOWED or DENIED

STEP 3: If the decision is ALLOWED, increase the allow count corresponding to the (Source IP, Destination IP) pair else increase the deny count

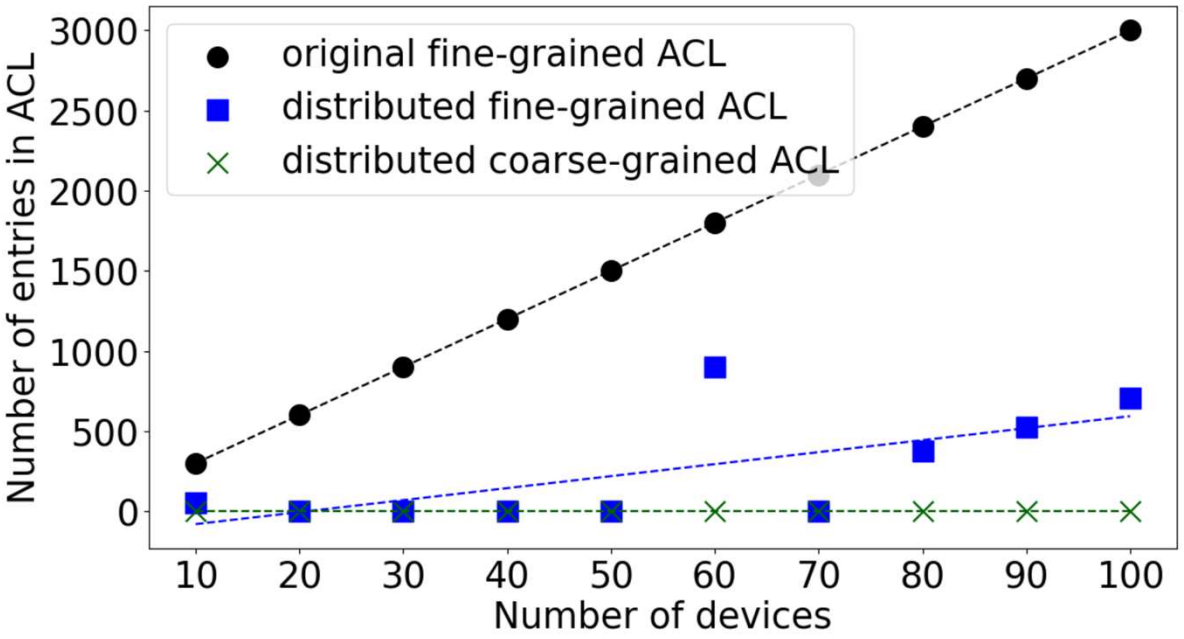
STEP 4: If the allow count < **threshold**, then append DENY decision to Network Layer else append ALLOW decision

STEP 5: If the ALLOW decision is distributed at Network Layer, then distribute the ACL at Application Layer for fine-grained control



Experiments and Results

Average ACL size reduces after applying the distribution algorithm



The size of the ACL varies linearly with the number of devices (given, the number of resources are constant)

We considered two destination IP address each containing 5 resources

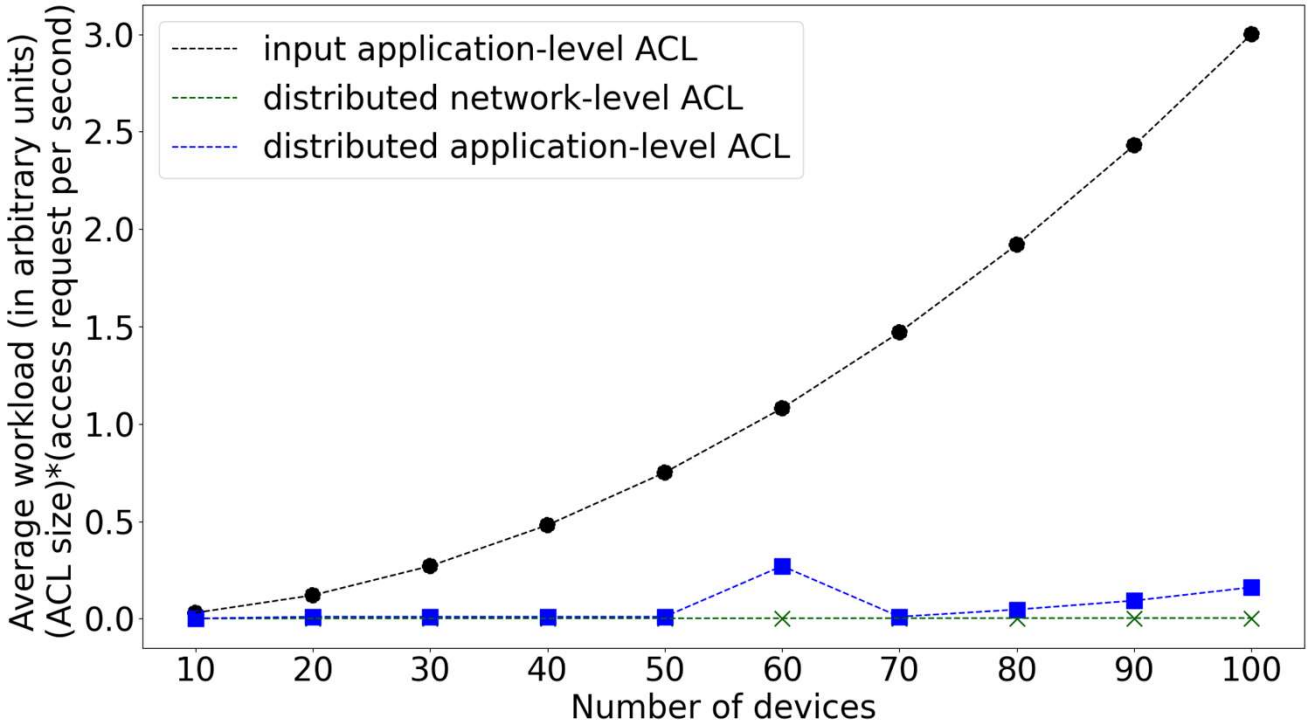
We considered two source IP addresses each containing equal number of devices

We increased the number of devices from 10 to 100

The resulting size of the ACL after distribution is much smaller

Experiments and Results

Average access workload is smaller after applying the distribution algorithm



The average access workload at each access control point varies quadratically with the number of devices

We defined access workload as the average time to process all the access requests at a time

For workload calculation, we artificially created 100 access requests per device

We quantified the average access workload as the product: ACL size × Access Requests

The resulting average access workload after distribution is much smaller

Experiments and Results

Our method performs better in reducing workload and preserving access granularity

Confusion Matrix	Denied (Before Distribution)	Allowed (Before Distribution)
Denied (After Distribution)	TP = 60%	FP = 15%
Allowed (After Distribution)	FN = 0%	TN = 25%

We quantify the security after distribution using Access Granularity metric

We calculate Granularity metric as a Confusion matrix

If all the decisions which are "denied" after distribution were also "denied" before are **True Positive (TP)**

If all the decisions which are "denied" after distribution were "allowed" before are **False Positive (FP)**

Overall Results

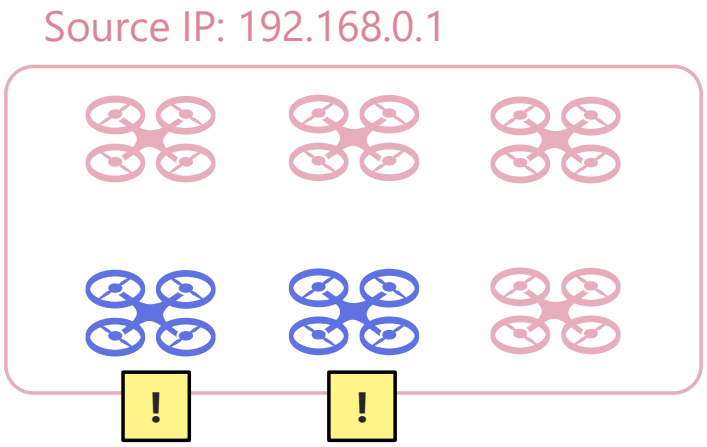
Metric	Original Application-level ACL	Network-level ACL	**Proposed method**
Access workload	(100%)	1%	**7%**
Access granularity	(100%)	38%	**85%**

Our proposed method performs better compared to just using Network Access Control or Application Layer Access control

Limitations and Improvements

The False Negatives may contain essential access requests whose mis-control can affect business

Confusion Matrix	Denied (Before Distribution)	Allowed (Before Distribution)
Denied (After Distribution)	TP = 60%	FP = 15%
Allowed (After Distribution)	FN = 0%	TN = 25%



Mis-control of these devices

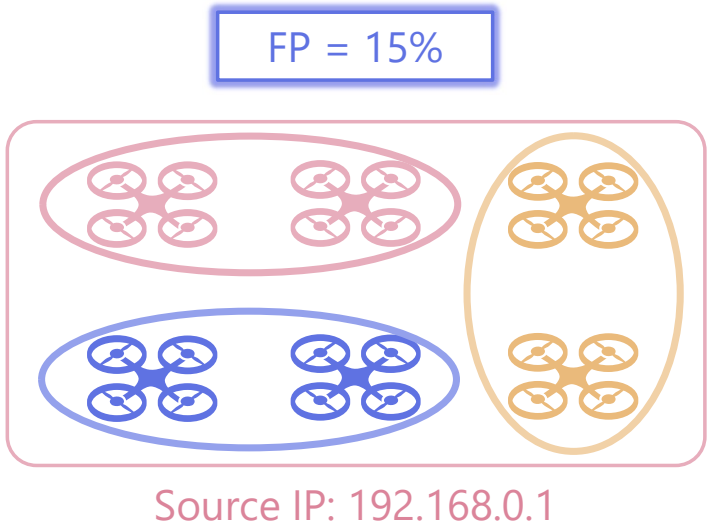
Mis-controlled cases may represent critical workflow such as emergency or mission

Denial of these requests may lead to negative business impacts

Availability for these devices is disrupted

Limitations and Improvements

A multi-threshold approach based on attributes of access can reduce the mis-control



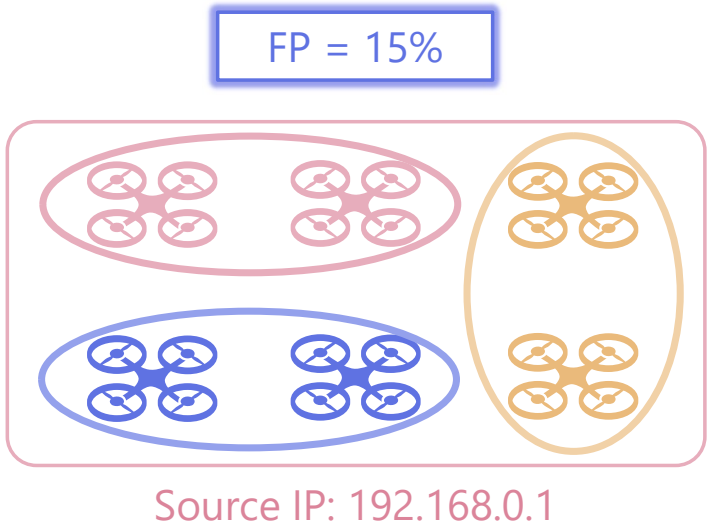
Devices (in Red) are detected to be malicious → **Set High Threshold**

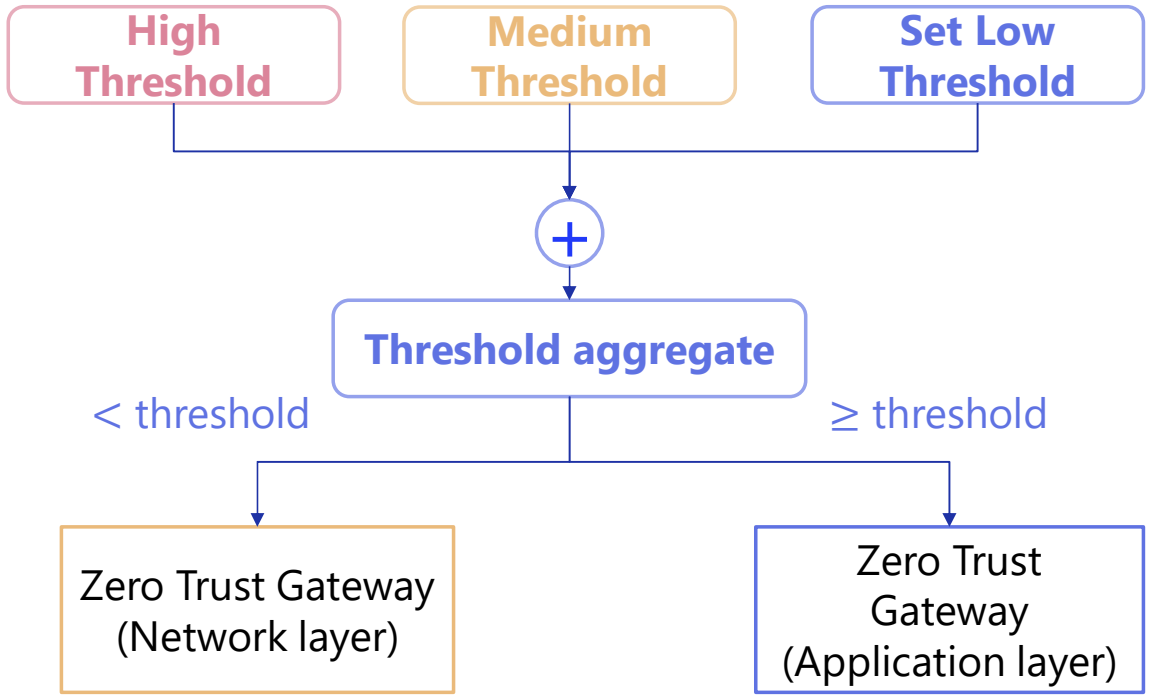
Devices (in Orange) are detected to be suspicious but require access → **Set Medium Threshold**

Devices (in Blue) are detected to be innocent and require necessary access → **Set Low Threshold**

Limitations and Improvements

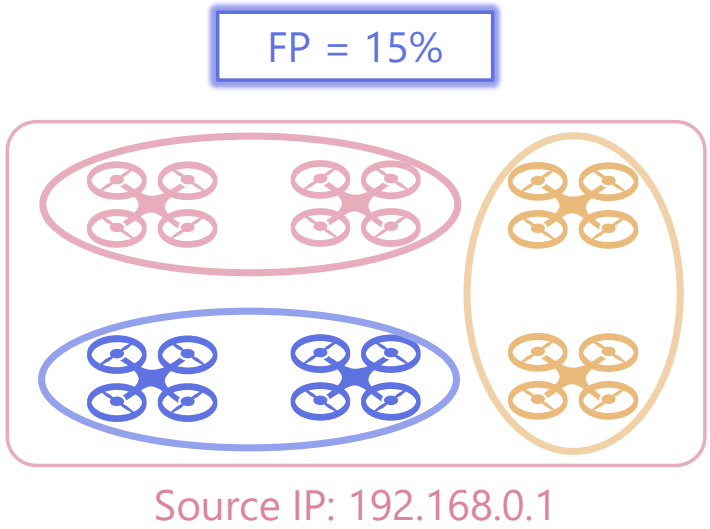
A multi-threshold approach based on attributes of access can reduce the mis-control

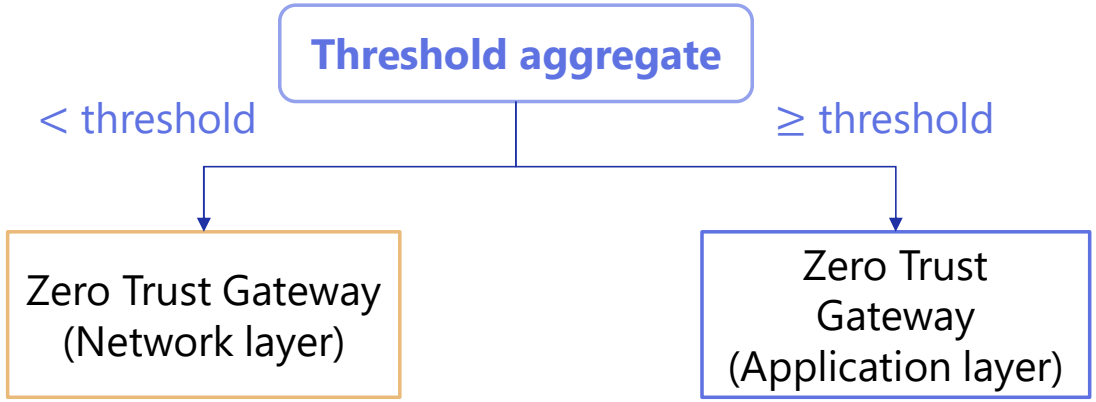




Limitations and Improvements

A multi-threshold approach based on attributes of access can reduce the mis-control





Metric	Method 1	**Method 2**
False Positive (FP)	15%	**3%**
Average Workload	7%	**12%**

Conclusion and Future Works

Summary of this proposal

Purpose: An optimal policy distribution mechanism based on Zero Trust principles to realize balance between workload and security trade-offs in CPS

Challenges: Decision of access control enforcement location in a highly dynamic environment is a non-trivial problem

Proposal: A distribution mechanism where granularity of access is adapted based on volatile environment conditions

Future Works: Analysis on real-environment

- Performance evaluation on a real-test bed system with focus on reproducibility, consistency, latency and scalability
- Performance evaluation on variable policy sets where decisions vary from "All DENY" to "All ALLOW"

References

[1] E. Liu, Huawei Technologies Co Ltd, “Firewall control system based on a next generation network service and method thereof”, U.S. Patent No. 7,987,503, Jul. 2011

[2] B. Alzahrani, , and N. Fotiou, “Enhancing internet of things security using software-defined networking”. Journal of Systems Architecture, 110, 101779, Nov 2020.

[3] C. Tang, X. Fu, and P. Tamg, “Policy-Based Network Access and Behavior Control Management”, IEEE 20th International Conference on Communication Technology (ICCT), vol. 20, pp. 1102-1106, Oct 2020.

[4] Z. Feng, P. Zhou, Q. Wang, and W. Qi, “A Dual-layer Zero Trust Architecture for 5G Industry MEC Applications Access Control”, IEEE International Conference on Electronic Information and Communication Technology (ICEICT), vol. 5, pp. 100-105, Aug 2022.

Q&A

Thank you everyone for your time.


Orchestrating a brighter world
NEC