IEC 62443: Using ntopng for creating a Software Defined Factory

Giacomo Tontini
(VEM Sistemi S.p.a.)

Agenda

- IEC 62443
- Sd-factorii
  - Basic concepts
  - Architecture
  - Ntopng integration
  - What’s next

IEC 62443

- A set of international standards for the security of *industrial automation and control systems* (IACS)

- Risk-based framework that helps organizations identify, assess, and mitigate cyber security risks

- Widely recognized as the leading standard for IACS security

- Flexible and scalable

- Involves a contiuous process of review and update of security controls

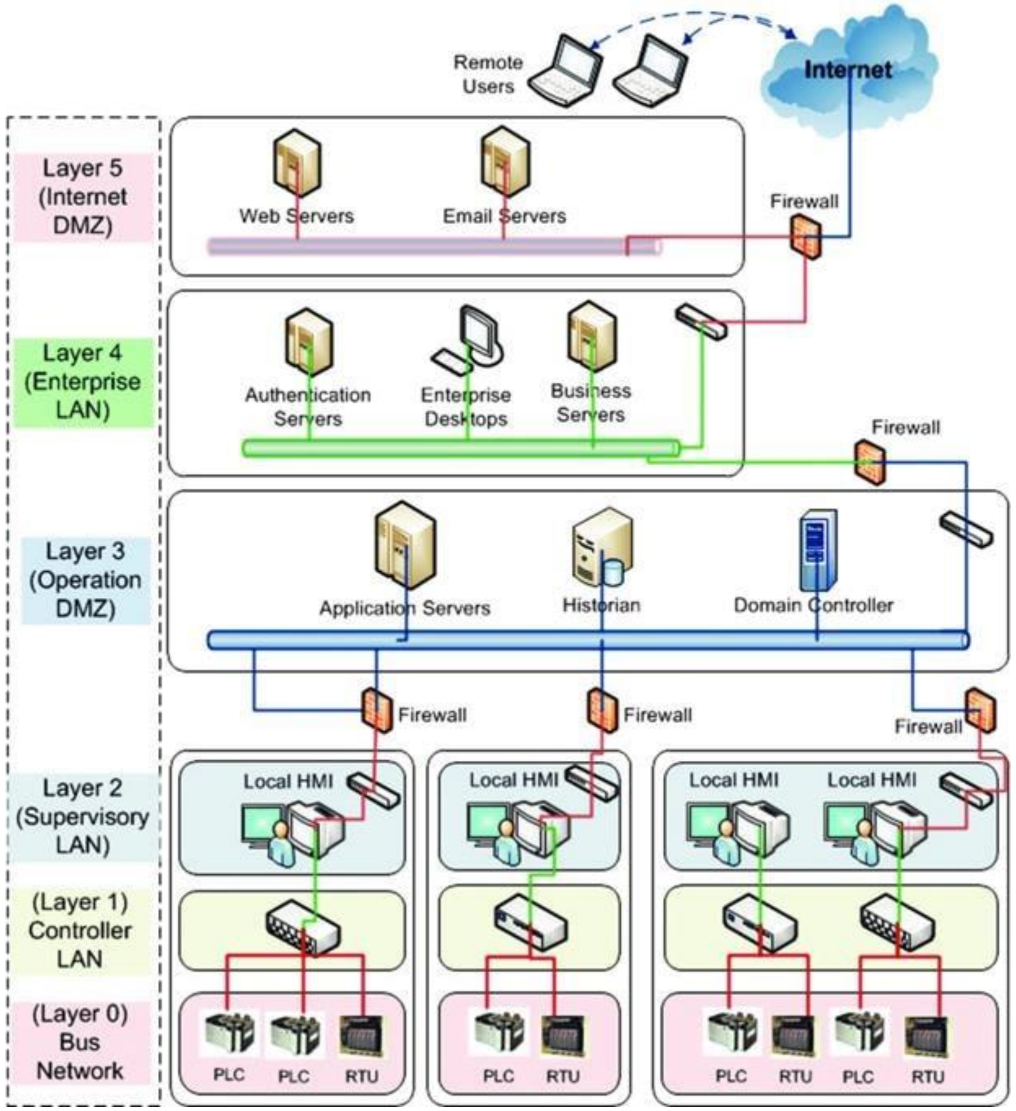
IEC 62443

Made of four parts:

- General: This part provides an overview of the standard and defines common terms and concepts.
- Security for systems and networks: This part focuses on the technical aspects of IACS security, such as network security, device security, and security management.
- Security for components and systems engineering: This part focuses on the development and implementation of secure IACS components and systems.
- Security assessment and certification: This part provides guidance on how to assess and certify the security of IACS.

IEC 62443 – Cybersecurity within OT environment

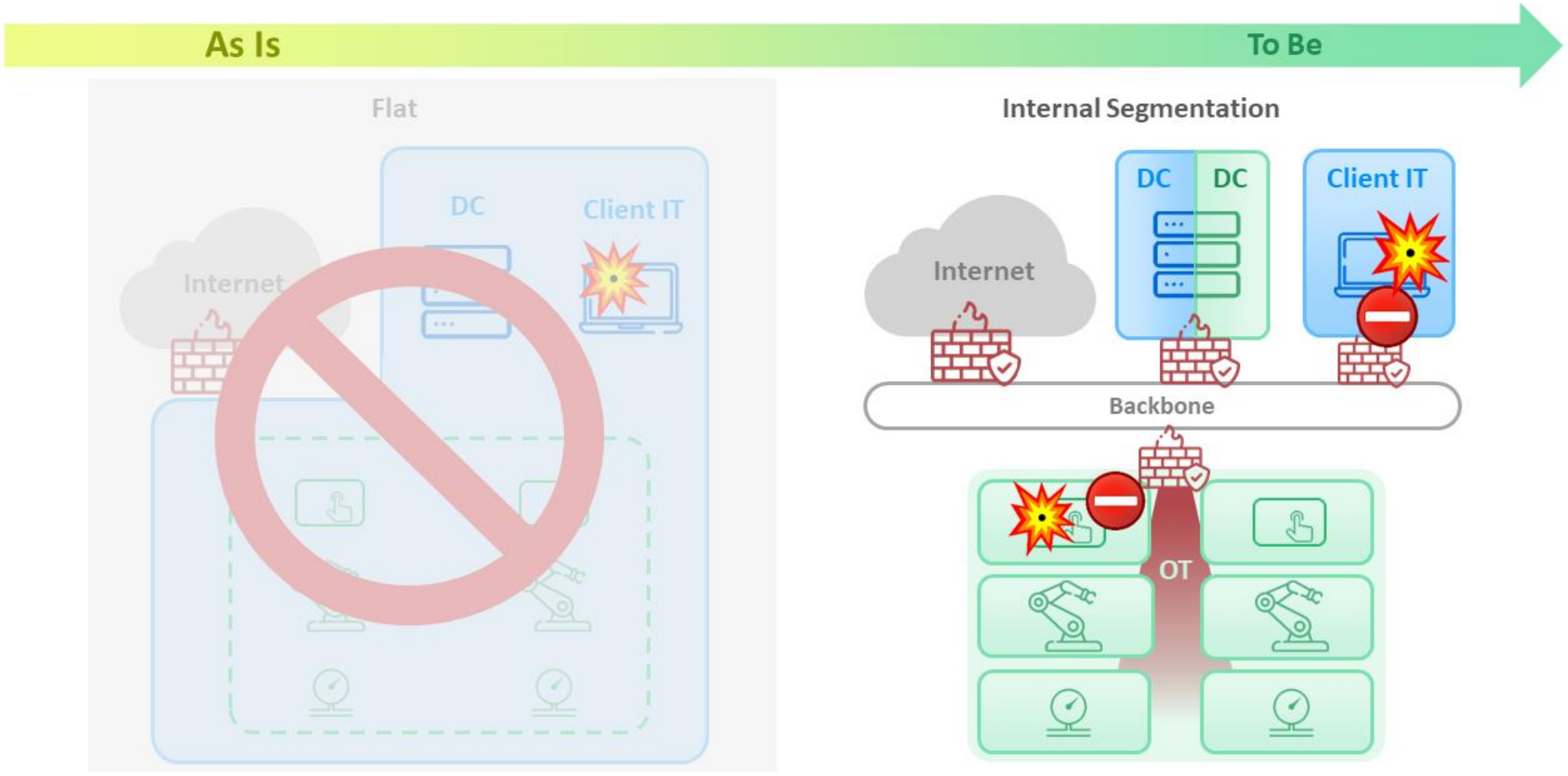
- Identification of different security levels
- Subdivision of the various production lines into multiple isolated environments
- Segregation between environments enabled by firewall rules



OT hostilities

- OT devices are typically network endpoints whose traffic is "unknown“
- OT environments are typically offered off the shelf with the production pipeline and are not structurally governed
- IT skills necessary to manage production plants are mostly absent within organization
- Infrastructures elements are non-homogeneous and lack minimum network level requirements
- OT environments mostly lack security governance and are therefore highly vulnerable spaces

Sd-factorii fundamental

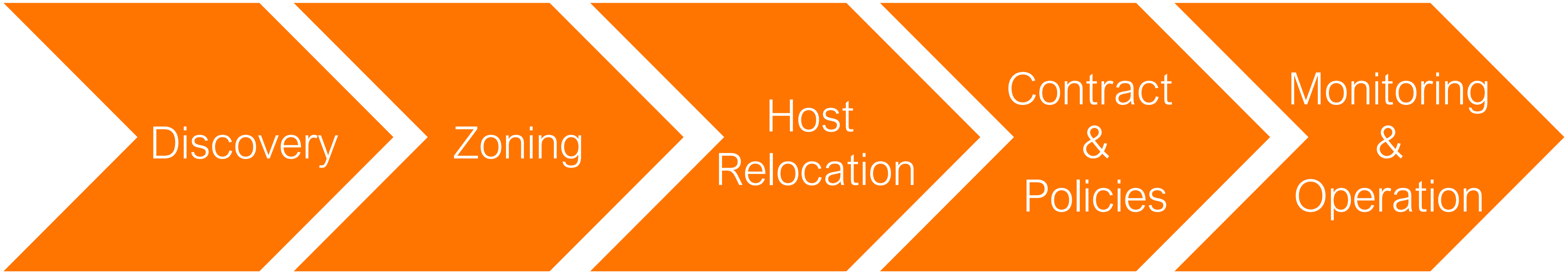


SD-Factorii

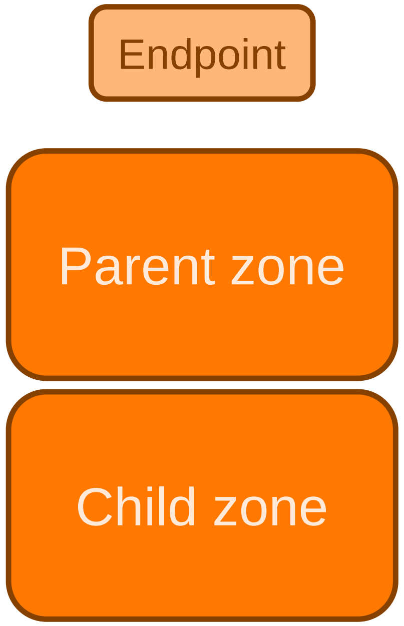
Software-Defined Factory intelligent infrastructure

- Zero trust approach
- OT traffic learning and visibility
- Infrastructure discovery and inventory
- No IP address change upon OT devices relocation and network segmentation
- Mostly based on open-source solutions
- Microservices architecture
Cloud native by design

Operative flow



Conceptual model: zones



Endpoint

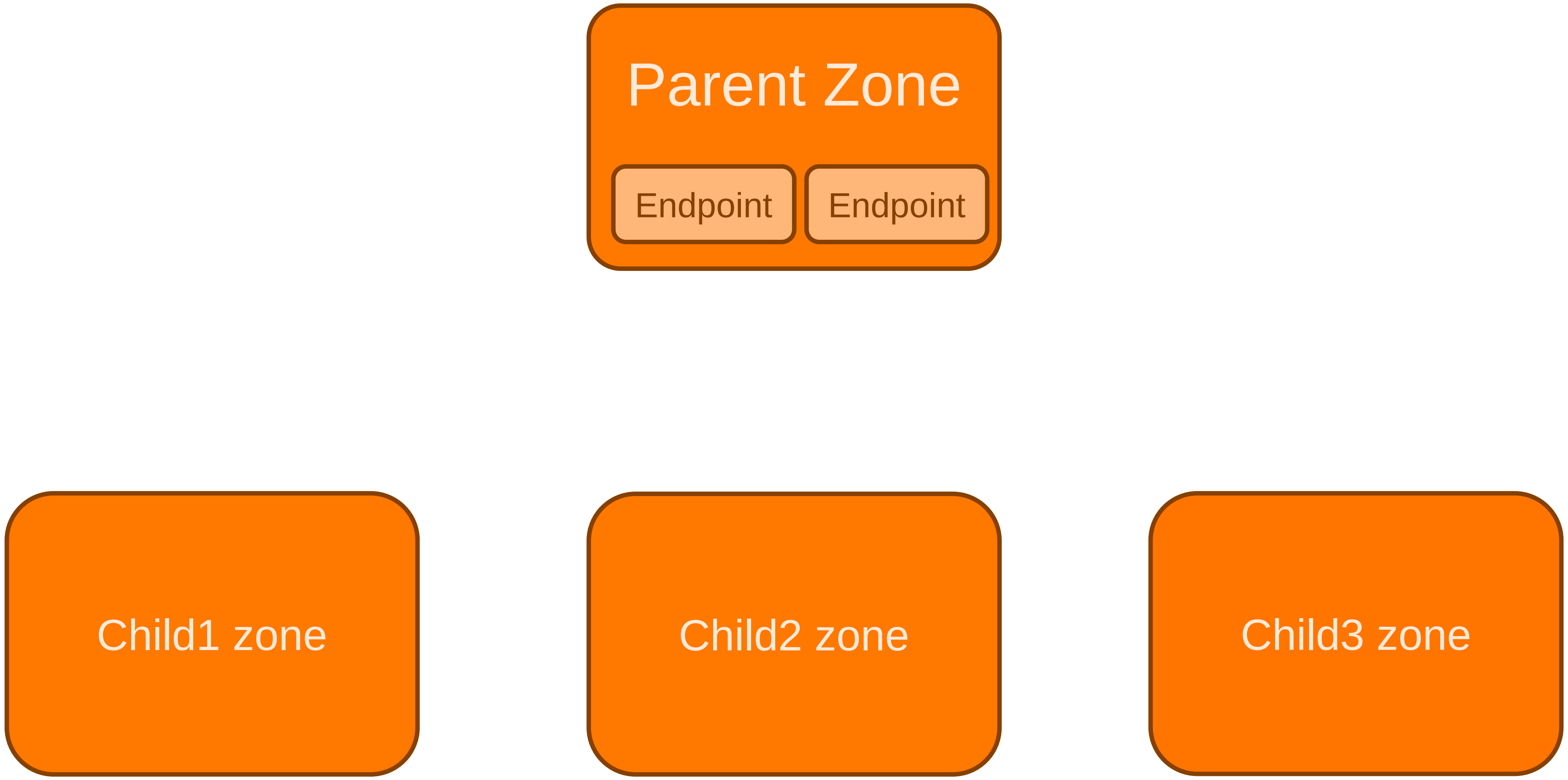
Parent zone

Child zone

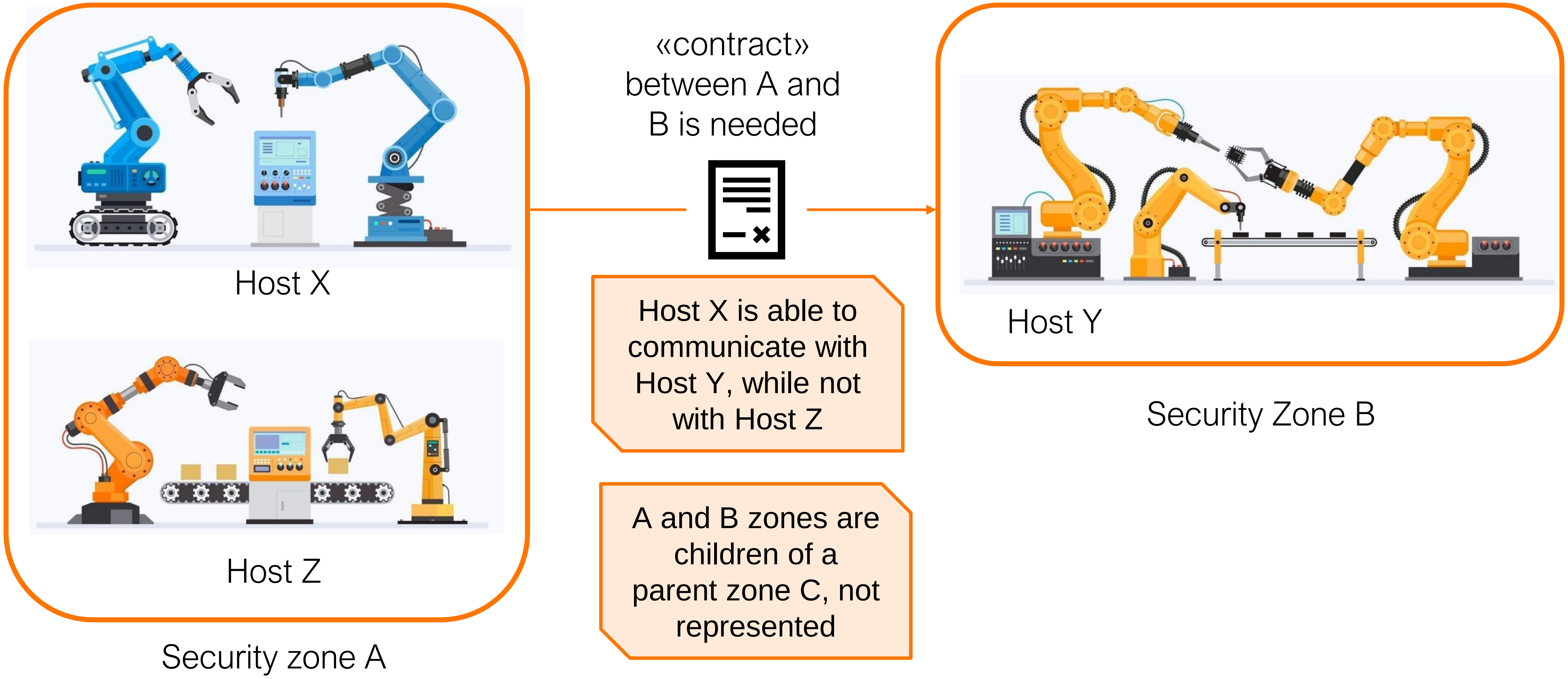
- Any device connected to IT or OT network that must be collocated into a «zone»
- **Parent Zones**: represent a specific broadcast domain where originally endpoint belong.
- **Child Zone**: a new broadcast domain, separate from the other zone’s BD, where endpoints could be placed

- Parent Zone can have multiple Child Zones
- An endpoint can move from a Parent zone to one Child Zone and vice-versa.
- An endpoint can move freely from each child zone of the same Parent Zone

Endpoint and zones



Conceptual model: contract



Host X

Host Z

Security zone A

«contract» between A and B is needed

Host X is able to communicate with Host Y, while not with Host Z

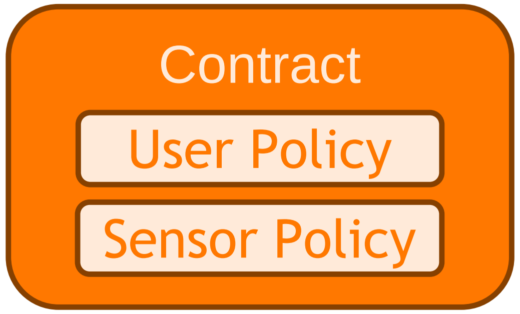
A and B zones are children of a parent zone C, not represented

Host Y

Security Zone B

Contracts and policies

- Represents a communication relationship between zones
- Unique for each pair of zones and communication direction
- Contracts cannot exist between parent zones

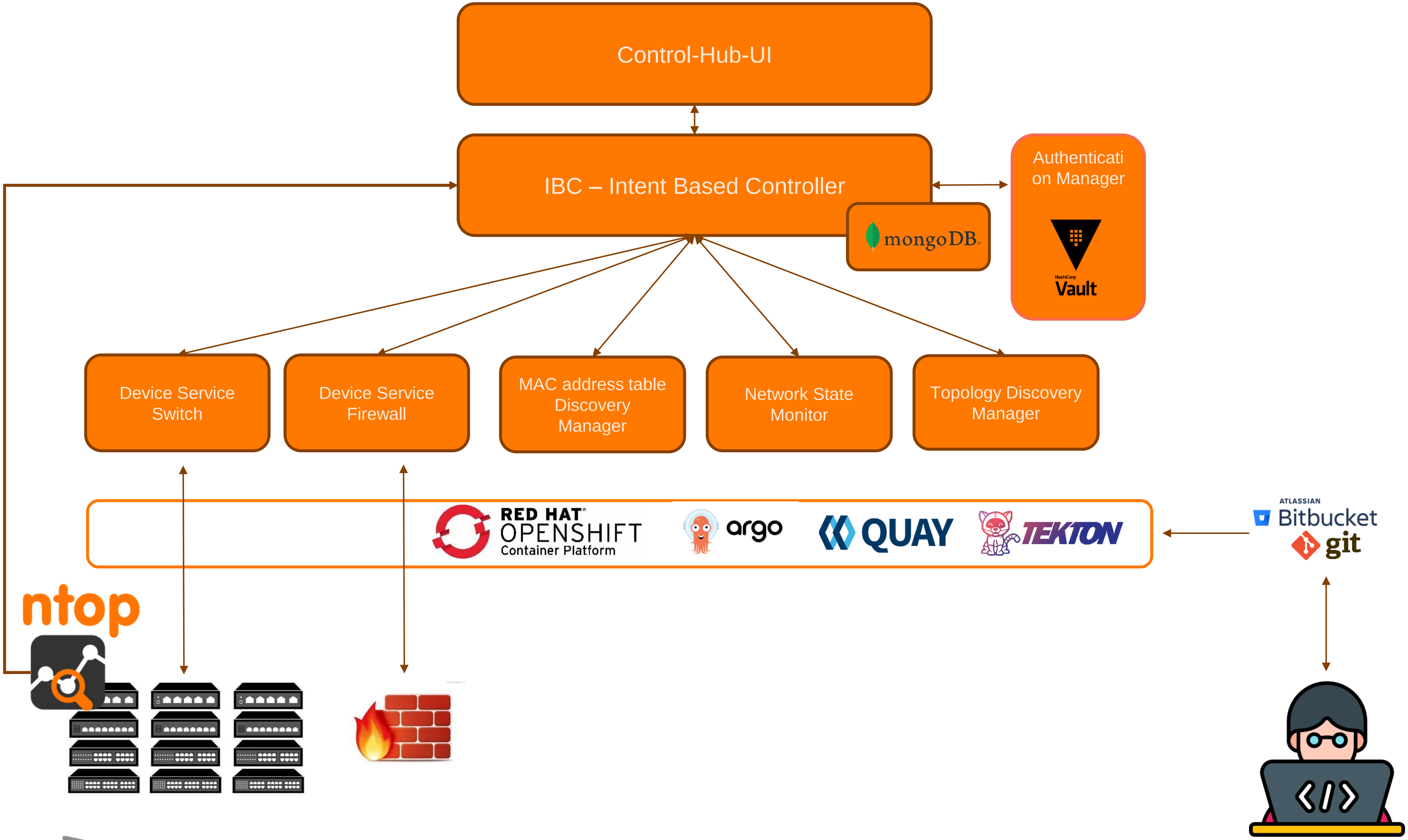

Contract

User Policy

Sensor Policy

- Each contract is made up of its atomic components called Policies
- Two types of policies: those provided by the user and those proposed by a sensor/probe
- A policy defines which traffic originating from a source zone can cross the boundaries towards a destination zone (parent zones or sister zones). Source ip / Dest IP/ Ports / Protocols

Sd-factorii architecture



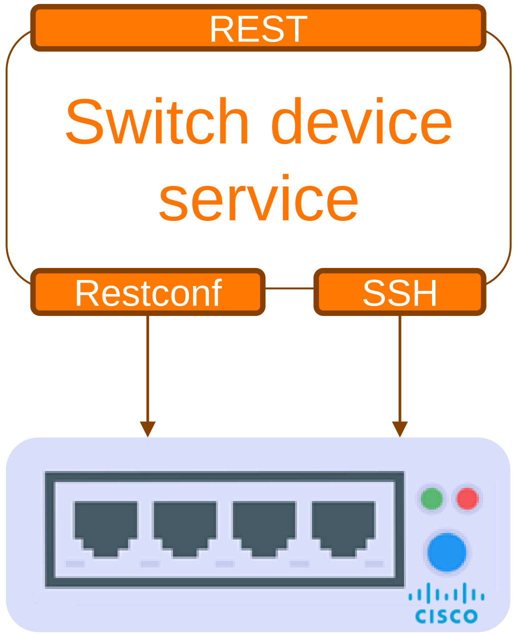
Device service

Switch device service

- Provides an abstraction layer for different switch vendor interfaces (Cisco, HP)
- Restconf and SSH as South Bound API (will support Netconf and gNMI)

Firewall device service

- Provides an abstraction layer for different firewall vendor interfaces (Fortinet, Checkpoint and Pfsense)
- REST as South Bound API and North Bound API

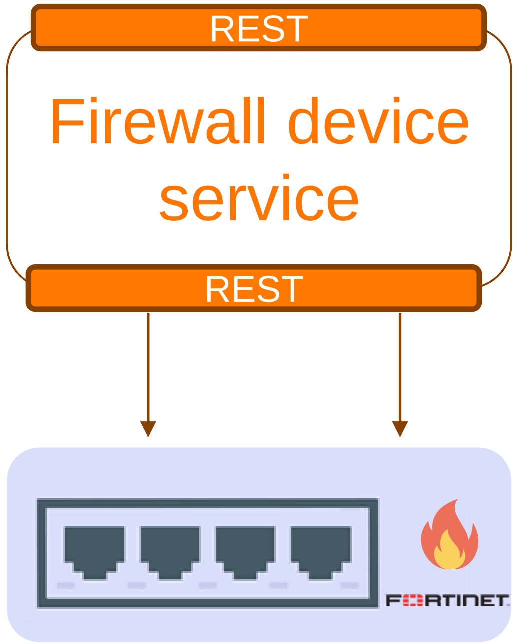


REST

Switch device service

Restconf

SSH

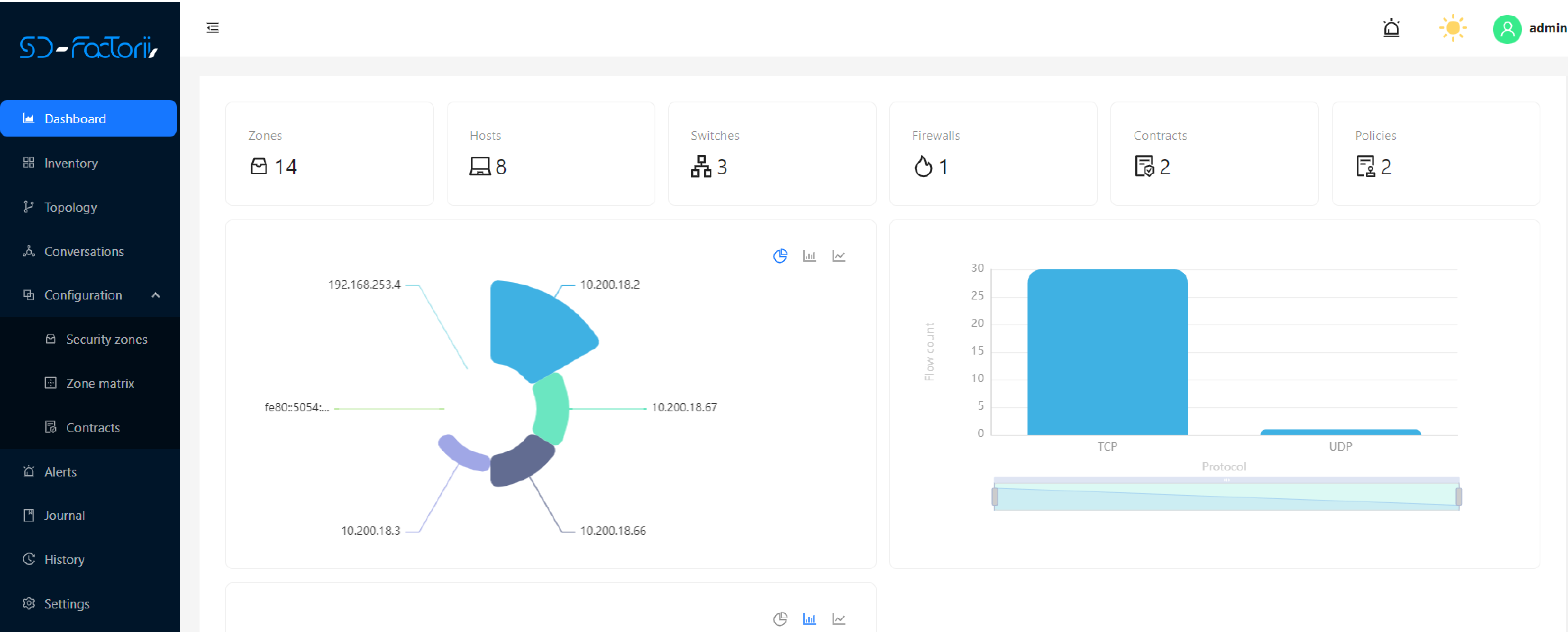


REST

Firewall device service

REST

Dashboard



Zones 14

Hosts 8

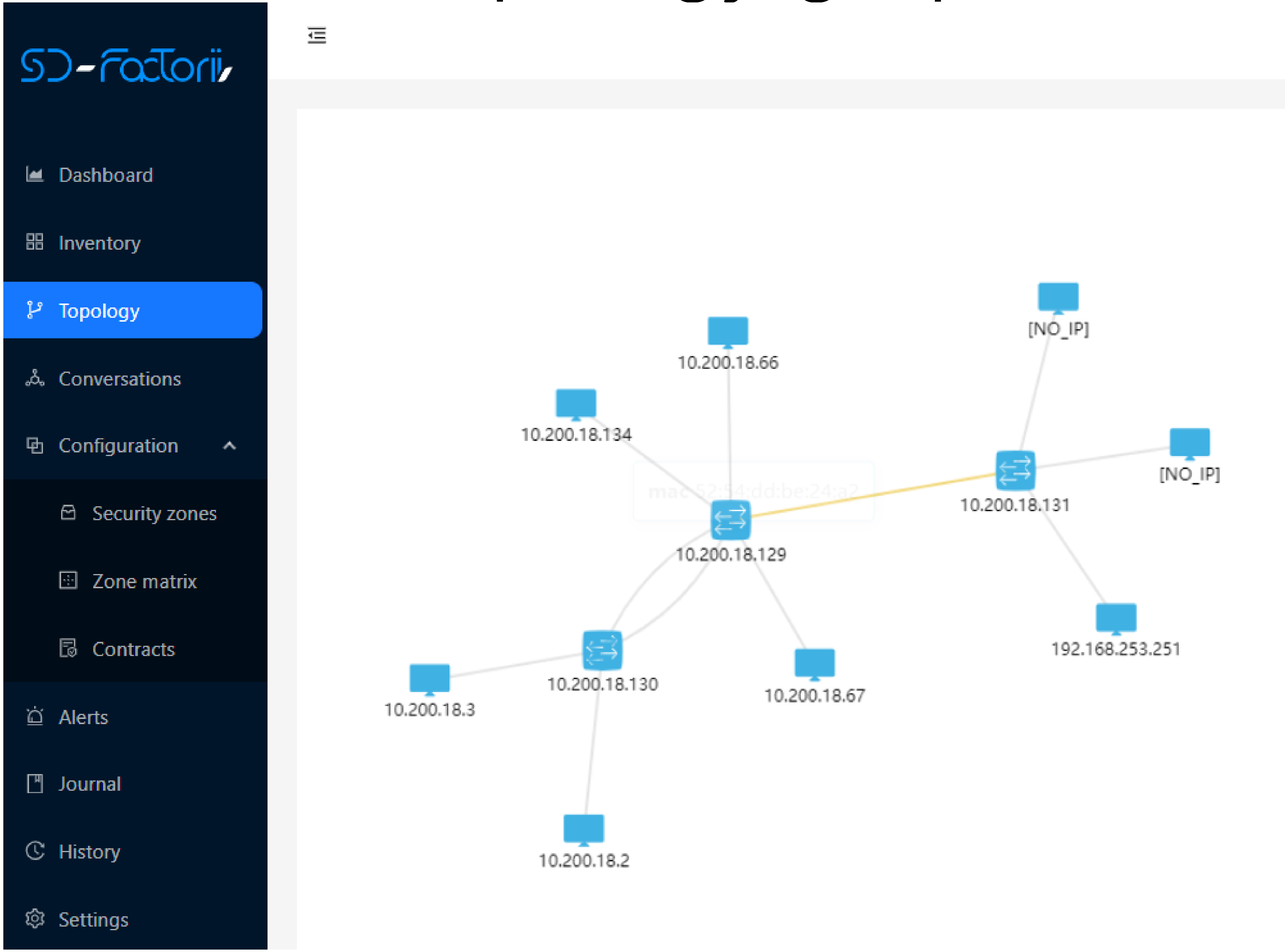
Switches 3

Firewalls 1

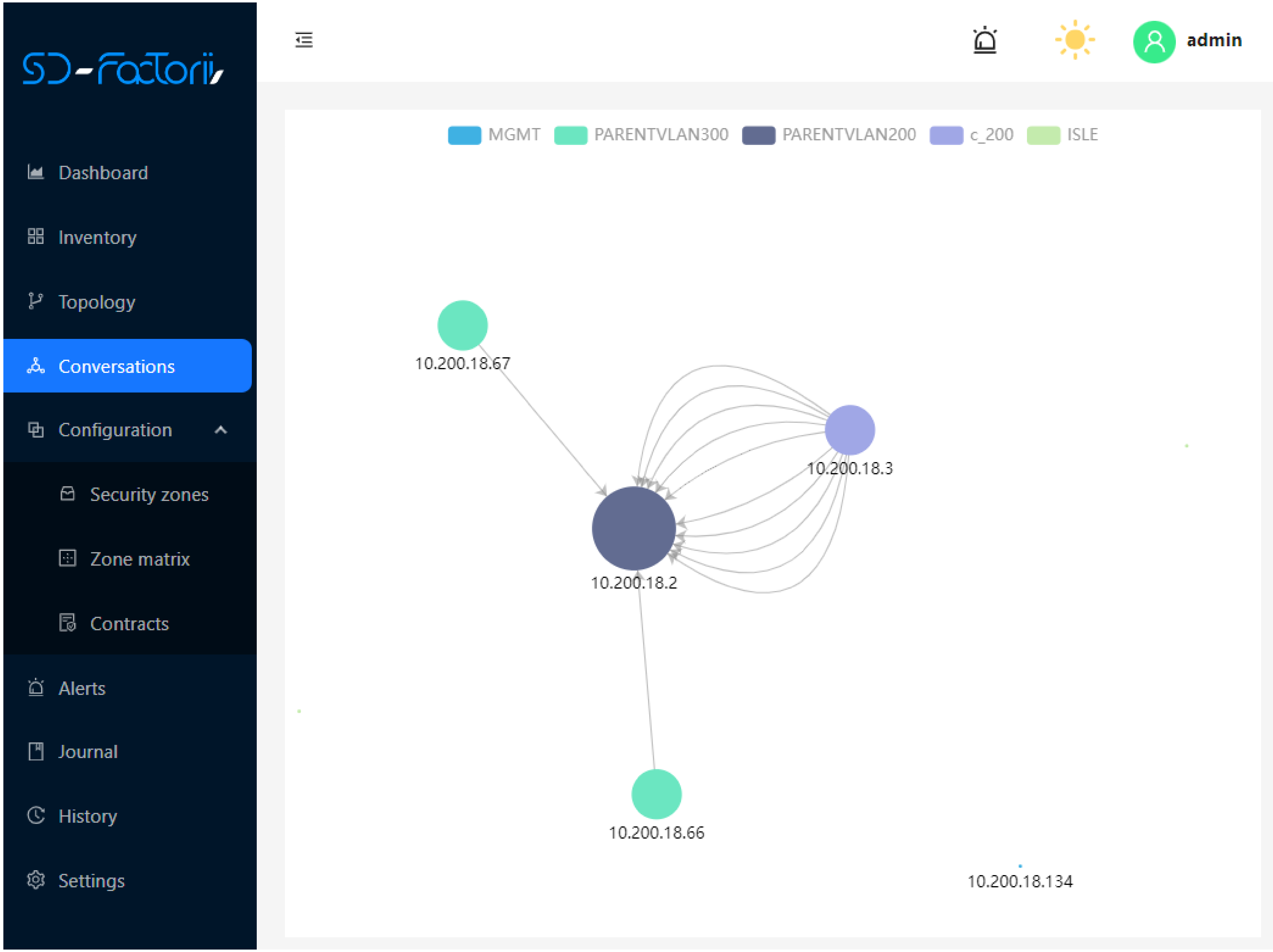
Contracts 2

Policies 2

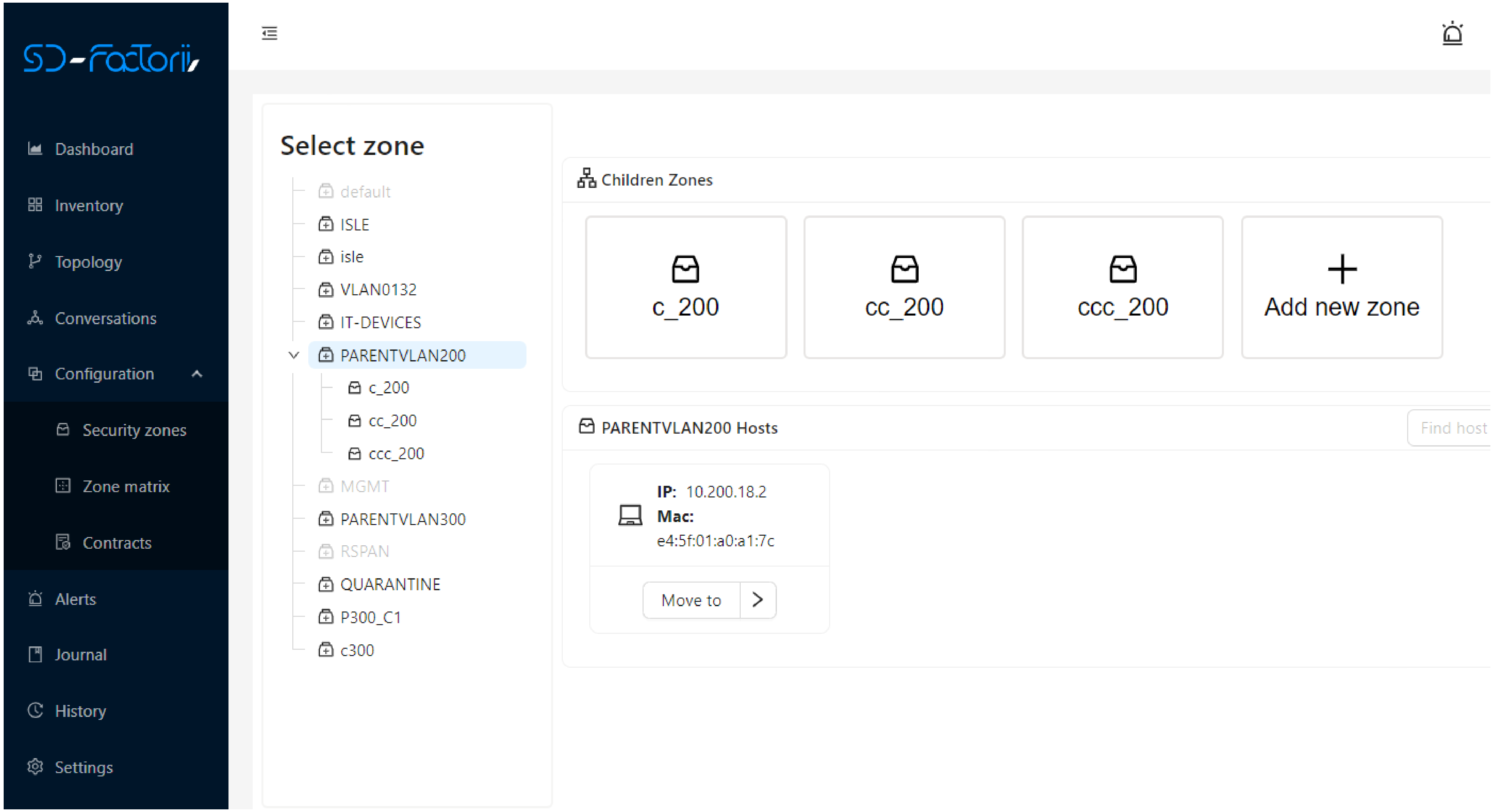
Topology graph



Conversation graph



Parent Zone



SD-Factori

Dashboard
Inventory
Topology
Conversations
Configuration
Security zones
Zone matrix
Contracts
Alerts
Journal
History
Settings

Select zone

- default
- ISLE
- isle
- VLAN0132
- IT-DEVICES
- PARENTVLAN200
  - c_200
  - cc_200
  - ccc_200
- MGMT
- PARENTVLAN300
- RSPAN
- QUARANTINE
- P300_C1
- c300

Children Zones

c_200 | cc_200 | ccc_200 | + Add new zone

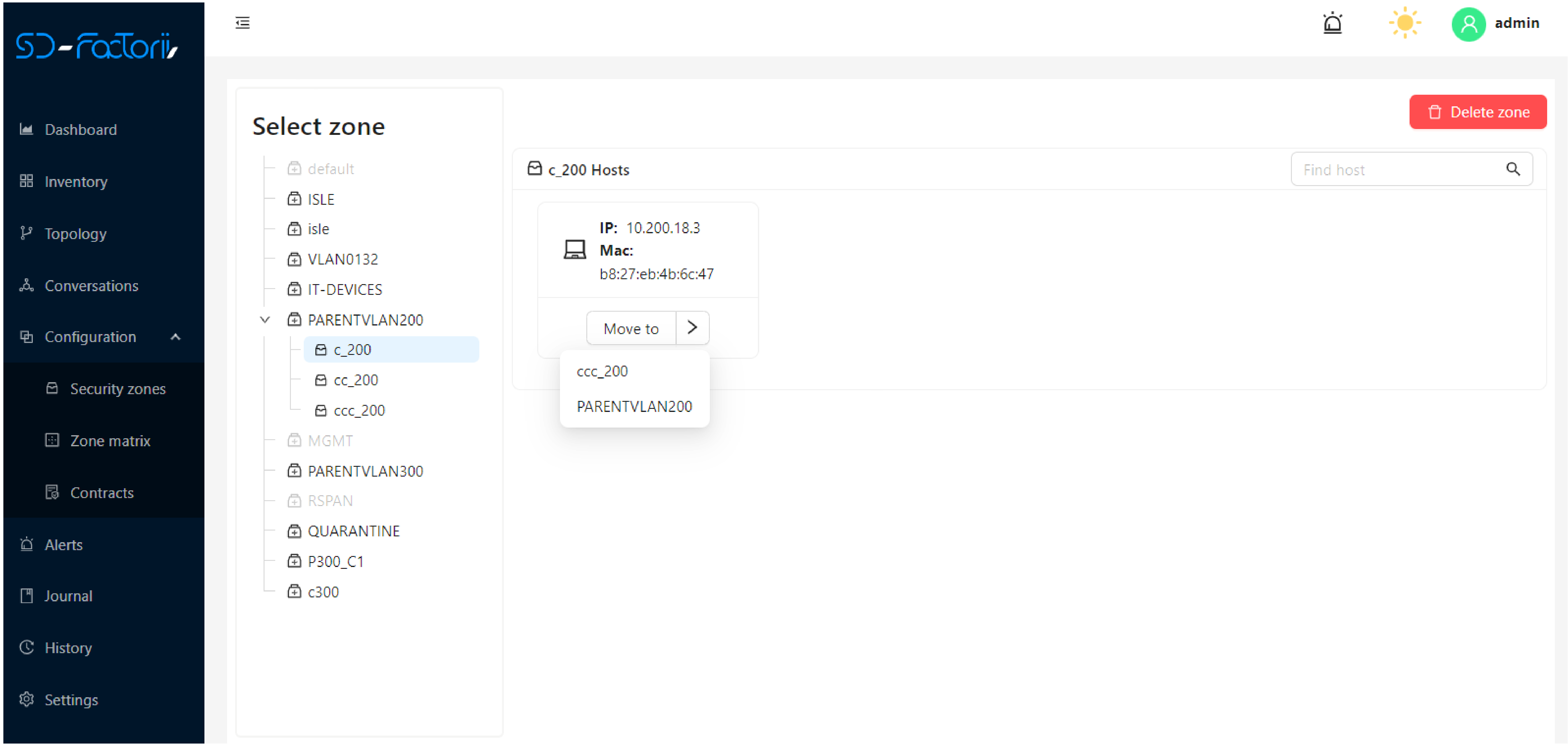
PARENTVLAN200 Hosts

Find host

IP: 10.200.18.2
Mac: e4:5f:01:a0:a1:7c

Move to >

Children Zone



Select zone

- default
- ISLE
- isle
- VLAN0132
- IT-DEVICES
- PARENTVLAN200
  - c_200
  - cc_200
  - ccc_200
- MGMT
- PARENTVLAN300
- RSPAN
- QUARANTINE
- P300_C1
- c300

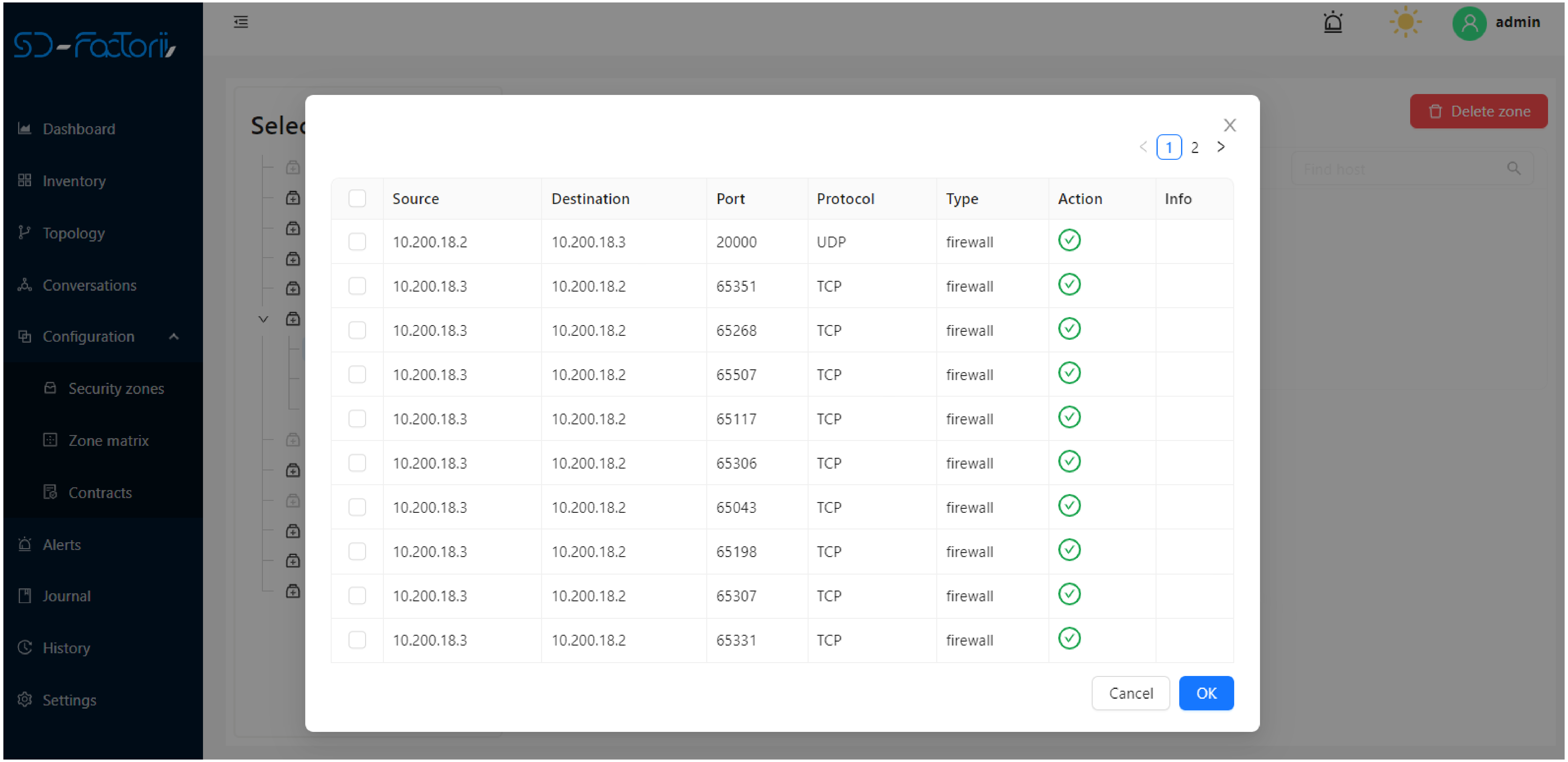
c_200 Hosts

IP: 10.200.18.3
Mac: b8:27:eb:4b:6c:47

Move to:
- ccc_200
- PARENTVLAN200

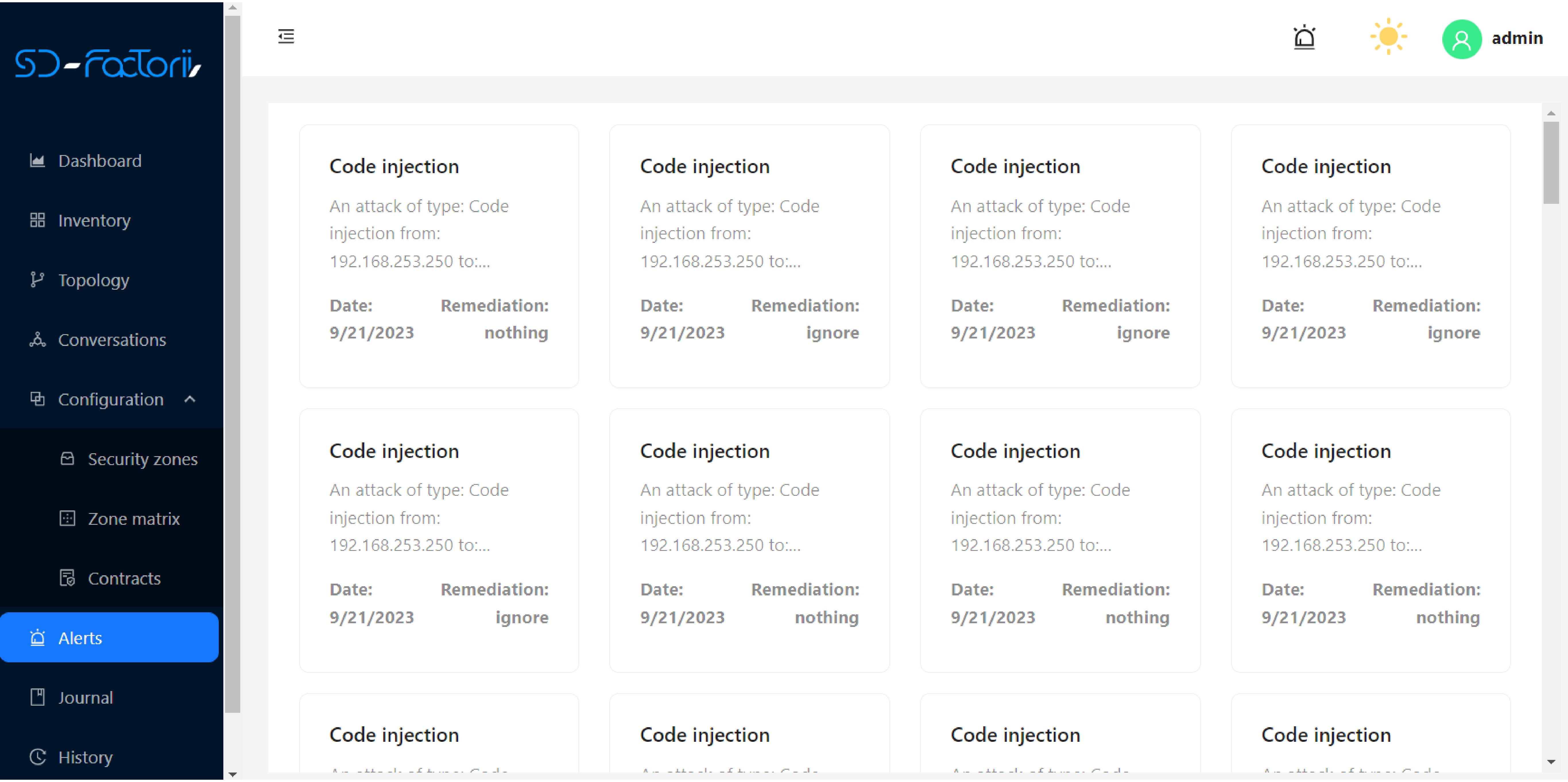
ntopConf'23

Policy adaptation (nTop)



□	Source	Destination	Port	Protocol	Type	Action	Info
□	10.200.18.2	10.200.18.3	20000	UDP	firewall	✓	
□	10.200.18.3	10.200.18.2	65351	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65268	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65507	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65117	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65306	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65043	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65198	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65307	TCP	firewall	✓	
□	10.200.18.3	10.200.18.2	65331	TCP	firewall	✓	

Alerts and remediation



Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: nothing

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: ignore

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: ignore

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: ignore

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: ignore

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: nothing

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: nothing

Code injection

An attack of type: Code injection from: 192.168.253.250 to:...

Date: 9/21/2023 Remediation: nothing

Code injection

An attack of type: Code

Code injection

An attack of type: Code

Code injection

An attack of type: Code

Code injection

An attack of type: Code

What’s next

- Multi-site/Multitenancy
- Multi-sensor distributed in crucial network nodes
- Pro-active network segmentation suggestions in compliance with IEC 62443 standard
- Pro-active remediation upon events coming from probe or third-party sources
- Visualization widget of current compliance level to IEC 62443 standard

Thank you for the attention.

giacomo.tontini@vem.com