Hauptstudie

Anomalie Detection in Netzwerken

Ives Schneider

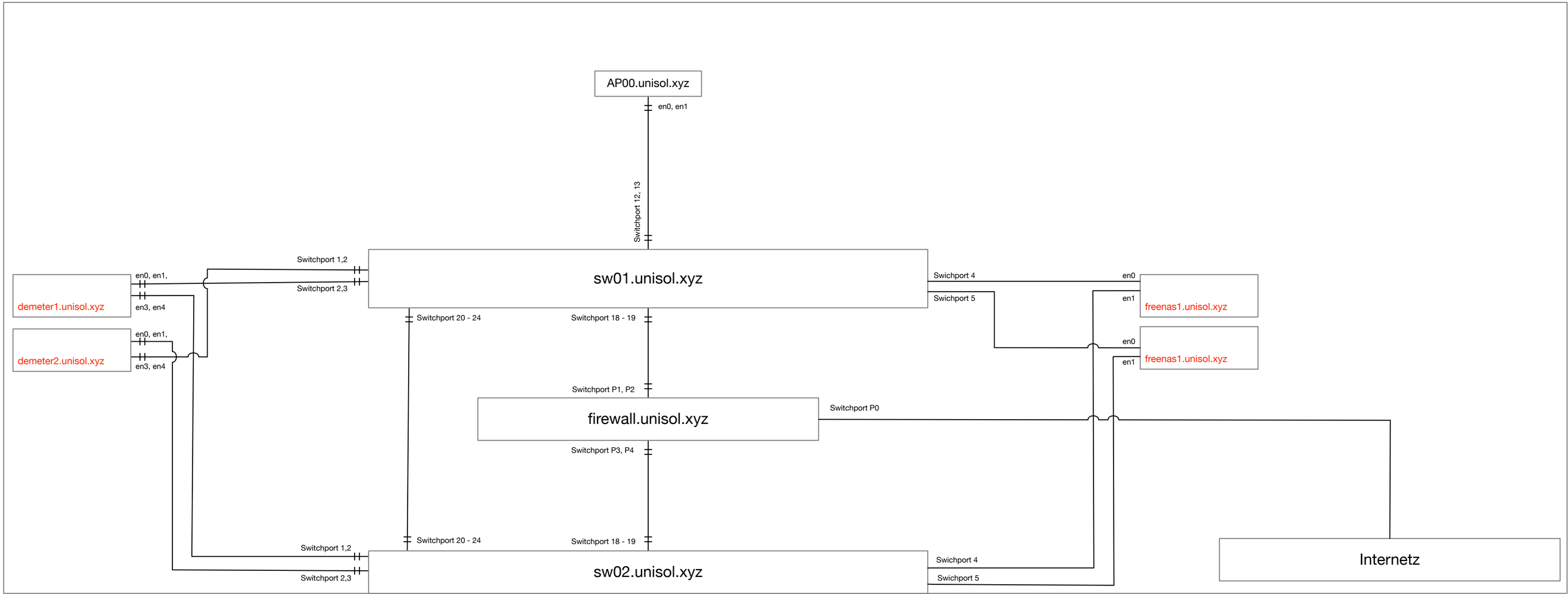
Index

1. Management Summary

2. Erhebung

2.1. Netzwerk

UNISOL NW physischer Netzwerkplan



3. Anomalie

3.1. Definition

> Anomalien sind unerwartete Abweichungen von Regeln, im Kontext der Produktion also Abweichungen von "normalen Betriebszuständen". Diese treten meist in einem Fehlerfall auf. Sie können allerdings auch ein Hinweis auf einen Angriff bzw. eine Manipulation innerhalb eines Produktionsnetzwerkes sein. Das gilt insbesondere dann, wenn Ereignisse erstmalig auftreten, Prozesse sich anders verhalten oder Geräte miteinander kommunizieren, die es bisher nicht getan haben.
>
> — BSI, Monitoring und Anomalieerkennung in Produktionsnetzwerken

3.2. Erkennung

Die Erkennung soll anhand eines Algorithmus erfolgen. Dabei soll der Algorithmus mehrere Merkmale analysieren. TODO

3.3. Einstufung

Die Einstufung erfolgt anhand mehrerer Sicherheitsstufen mit zusätzlichen Unterstufen.

Stufen

Event

- Unknown
- Common
- Important

Alert

- Unkown
- Common
- Important

Incident

- Unknown
- Common
- Important

3.3.1. Event

Events sind normale Meldungen welche nicht auf schwerwiegende Anomalien hindeuten.
z.Bsp. Hoher Netzwerkspike ohne zusätzliche Anomalien. Beispiel:

NOTE	High Bandwith: {IP}

3.3.2. Alert

Meldungen welche auf Downtime oder neue Geräte hinweisen. Allerdings ohne zusätzliche Informationen
Beispiel:

CAUTION	New device found: {IP} {MAC}

3.3.3. Incident

Anomalien welche auf lateral movement hinweisen könnten. Beispiel:

WARNING	New Port: {PORT} on {IP}

4. Baseline

Die Baseline wird mithilfe von PRTG erstellt.
TODO

4.1. Netzwerk

TODO

4.2. Load

TODO

5. Applikation

Die Applikation welche unter dem Namen "Nidhogg" entwickelt wird, soll als Anlaufstelle für Anomalieerkennungen dienen.
Anhand diversen Merkmalen, soll erkannt werden, ob eine gemeldete Abweichung sich um eine Anomalie handelt welche genauer untersucht werden soll, oder aber um eine Abweichung, welche nicht weiterverfolgt werden muss.

Zugegriffen wird dabei auf folgende Möglichkeiten mit den Umsystemen zu kommunizieren.

Protokolle

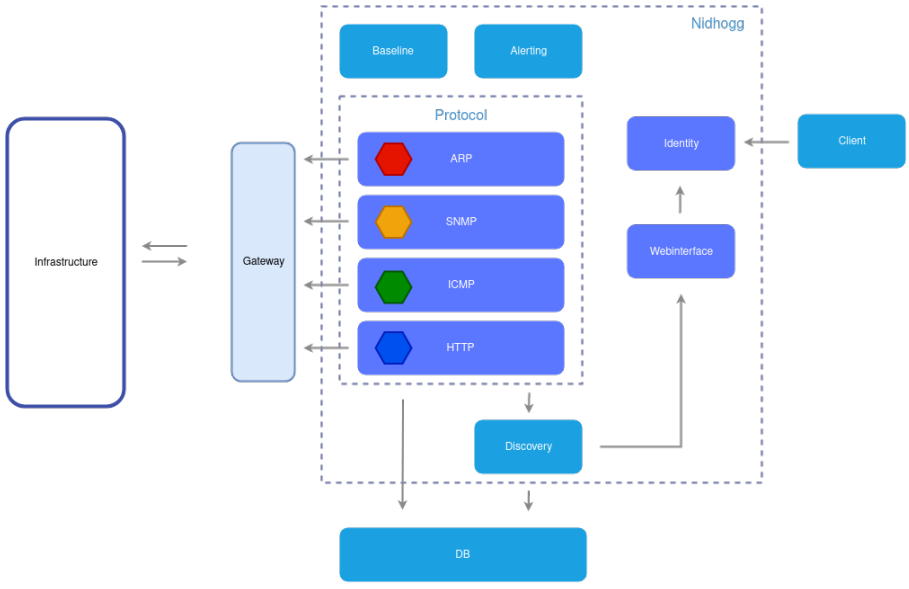
- ICMP
- SNMP
- HTTP
- ARP

Es wird versucht den Code möglichst low-level zu halten um die Performance der Umsysteme möglichs wenig zu beeinträchtigen.

5.1. Technology

Die Applikation wird in Rust geschrieben. Dies ermöglicht es, sicheren Quellcode zu schreiben ohne dabei Geschwindigkeit zu verlieren.
Von grossem belangen wird hierbei der Borrowchecker, lifetimes sowie das Secure Memory Management um die Applikation möglichst erweiterbar und ressourcenschonend zu schreiben.

5.2. Architektur



5.3. Diagramme

TODO

5.4. Implementation

TODO

6. Weiteres vorgehen

TODO

6.1. Installation

TODO

6.2. Konfiguration

TODO

7. Controlling

TODO

7.1. Testing

TODO

8. Kosten

TODO

9. Reflextion

TODO

10. Freigabe

TODO

11. Anhang

TODO

11.1. Installationsdokumentation

TODO

11.2. Wartungsdokumentation

TODO