

SDAIA Project

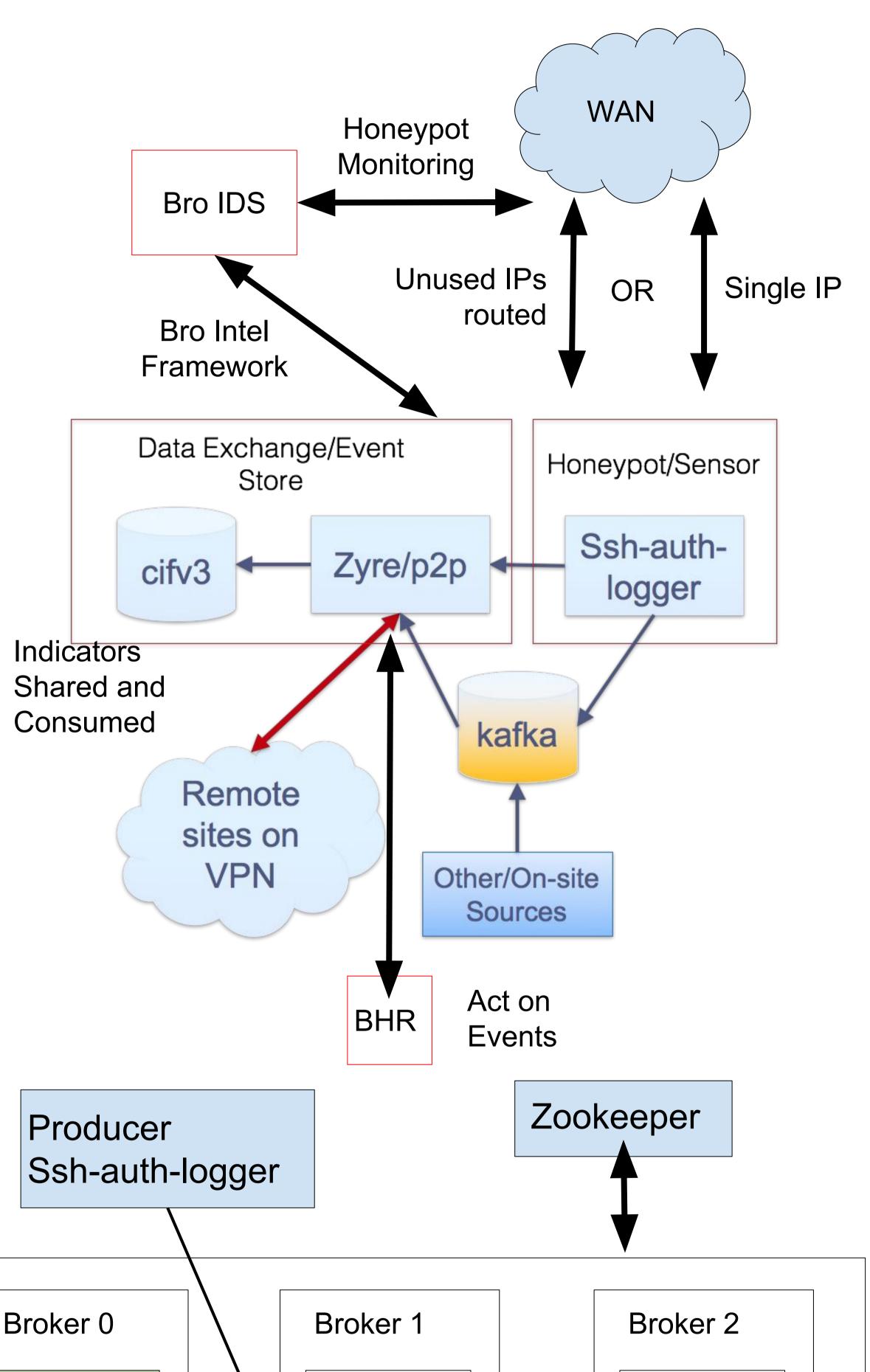
The Science DMZ Actionable Intelligence Appliance (SDAIA) project addresses a critical need for security solutions for open science networks, such as the Science DMZ model, and addresses the special architecture of these networks through a virtual security appliance that benefits from shared intelligence to protect the site, and further provide intelligence to the wider community.

- Decentralized model.
- Authentication logging honeypot software.
- Scalable, near realtime dissemination of threat intelligence data.

Components:

Building a Real-time Distributed Intelligence Feed Network

Alex Withers <<u>alexw1@illinois.edu</u>> Justin Azoff <<u>jazoff@illinois.edu</u>> Jim Marsteller <<u>jam@psc.edu</u>> Shane Filus <<u>filus@psc.edu</u>> Linh Cao <<u>linhcao2@illinois.edu</u>>



- Ssh-auth-logger
 - Low interaction SSH honeypot written in Go.
 - Collects: src ip, user, password, etc.
- Zyre (zeromq+p2p)
 - Very fast p2p 1:N message passing with elliptical curve encryption
- Simple Service Discovery for peer discovery and key management
- CIFv3
 - Major performance improvements, stores events.
- Apache Kafka
 - Message/event passing queue for extensibility.
- Bro IDS
 - Monitors network traffic going into honeypot.
 - Monitors and alerts on indicators seen at other sites.

Components deployed with Ansible playbooks.

Apache Kafka Architecture

- Producer (Ssh-auth-logger)
- Kafka Cluster
 - One Topic
 - Three brokers Ο
 - Each broker has one leader and two

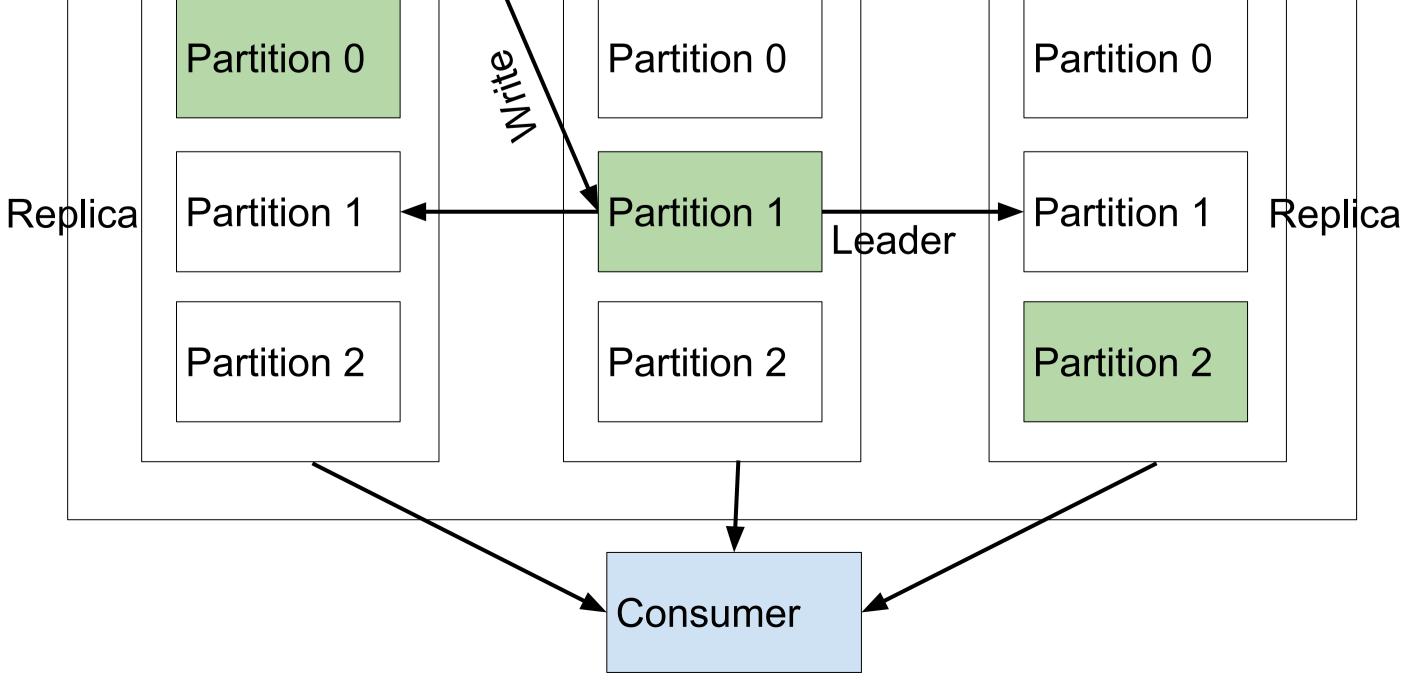
replicas

- Consumer
- Zookeeper controls different nodes, Kafka topics, messages, etc.

Future Work:

- Passing message to cifv3
- Test on real system





Special thanks to Wes Young and the Research and Education Networking Information Sharing and Analysis Center (REN-ISAC) This material is based upon work supported by the United States National Science Foundation under grant number 1547249.

Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the United States Government or any agency thereof.