Intrusion Detection System

Changwei Cao (45983485), Yuanchen Wang (45326493)


Imaging…

Introduction

IDS vs. IPS

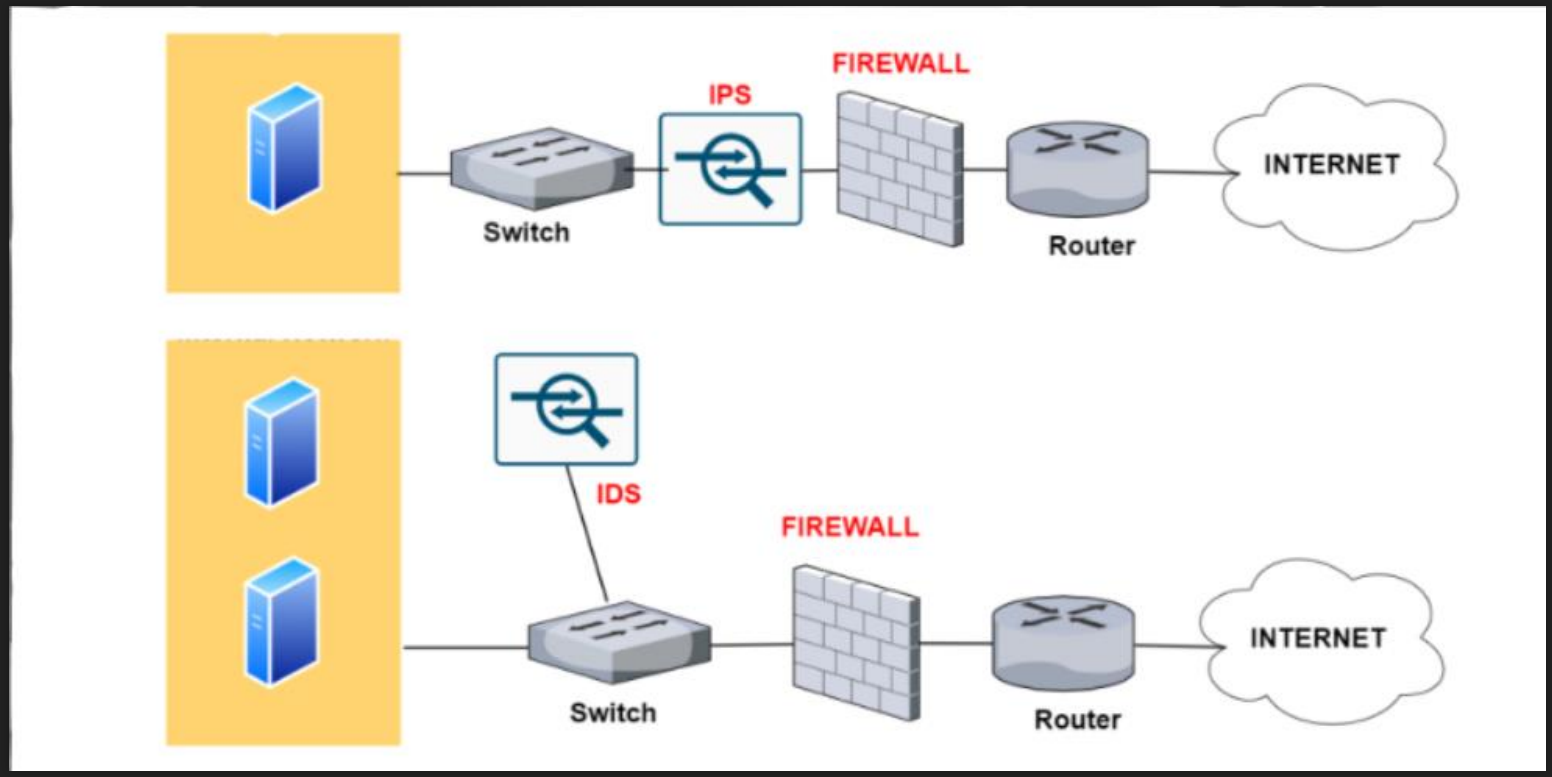
IDS

- Copy data from switches
- Not inline with traffic --- but in parallel

IPS

- Inline with traffic (stop attacks when see attacks)
- Placed within the firewall
- All traffic must go through IPS

What is IDS ?


FIREWALL
IPS
Switch
Router
INTERNET
IDS
FIREWALL
Switch
Router
INTERNET

Performance

The Performance for IDS

$$TPR = \frac{TP}{TP + FN}$$

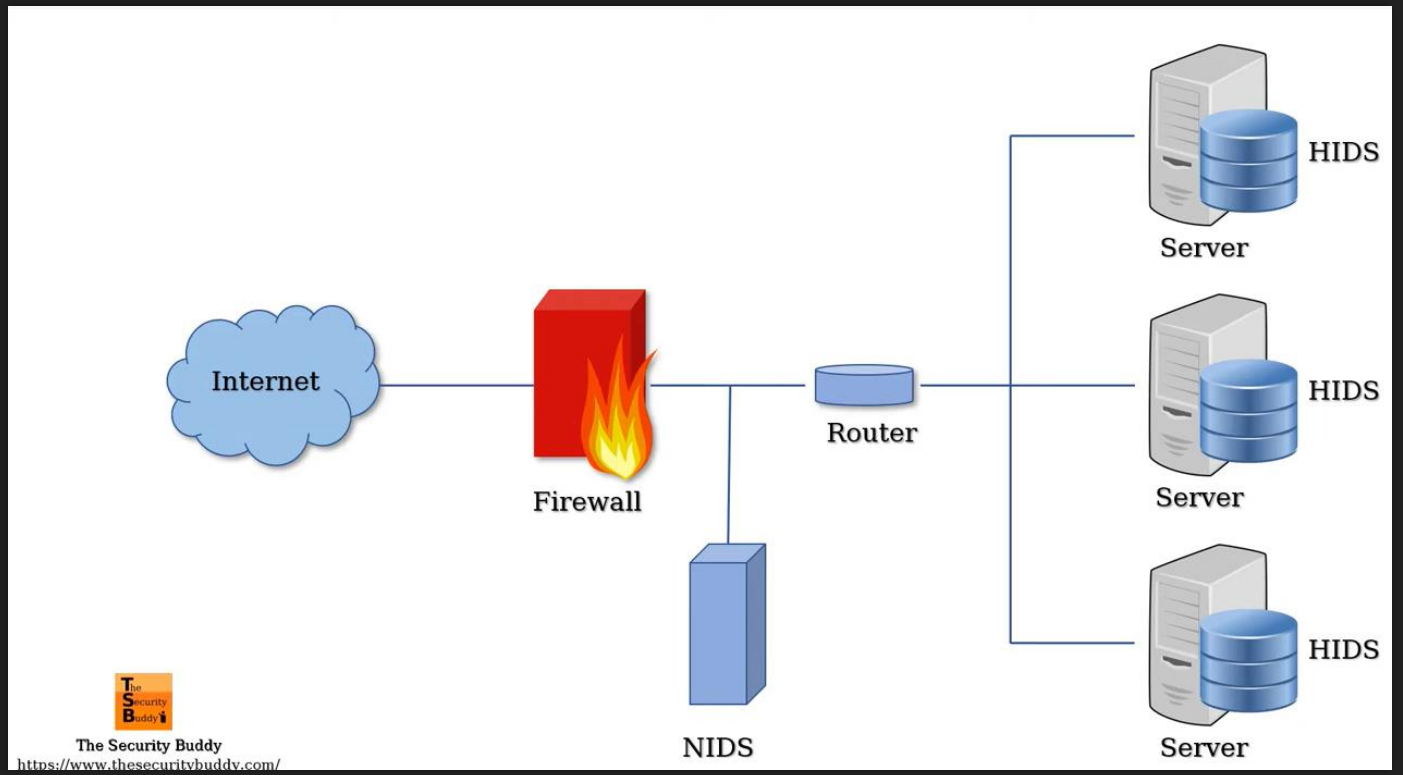
$$FNR = \frac{FN}{FN + TP}$$

$$FPR = \frac{FP}{FP + TN}$$

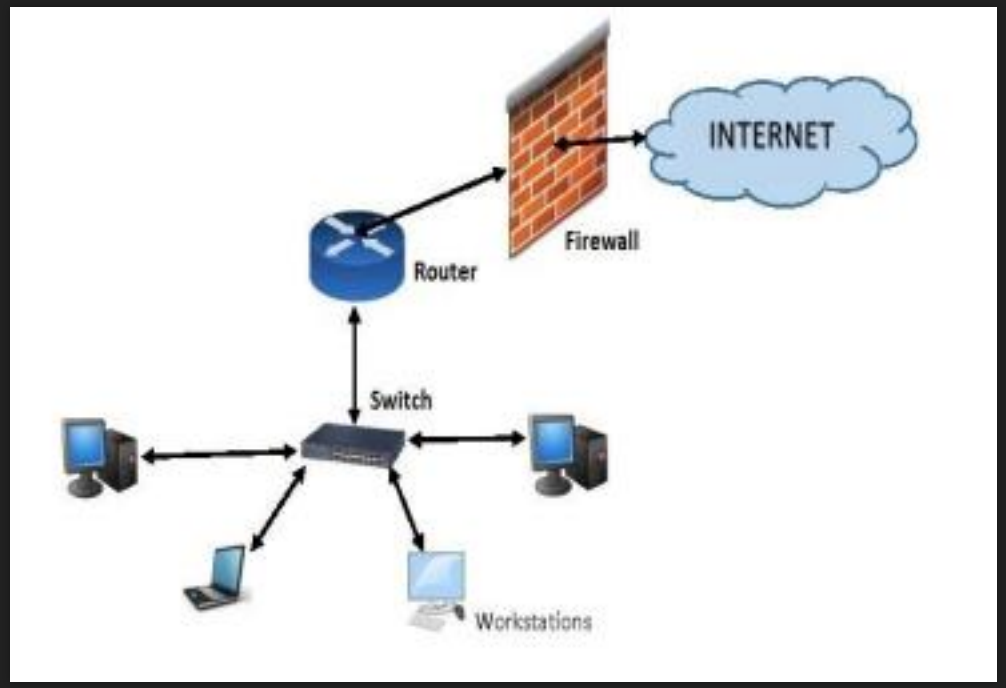
$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

Deployment

Deployment for IDS (HIDS, NIDS)

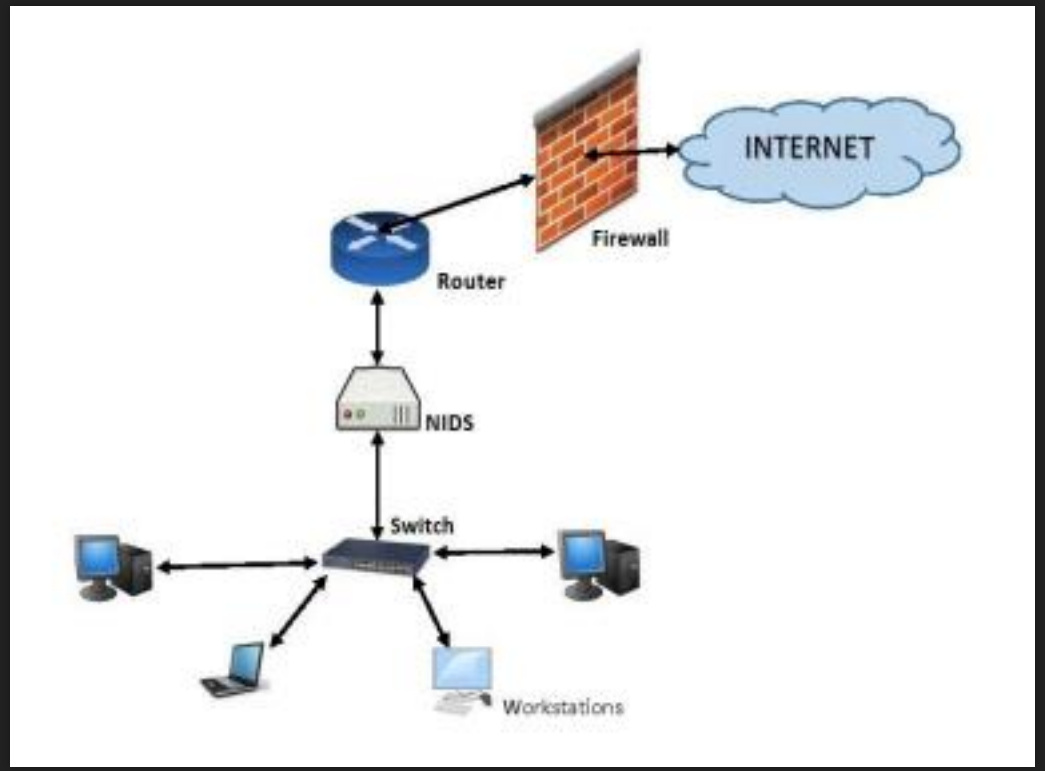


Host Based IDS (HIDS)



- Run on the server, router, switch or network machines
- Check communication traffic and system files
- No good at real time response

Network Based IDS (NIDS)



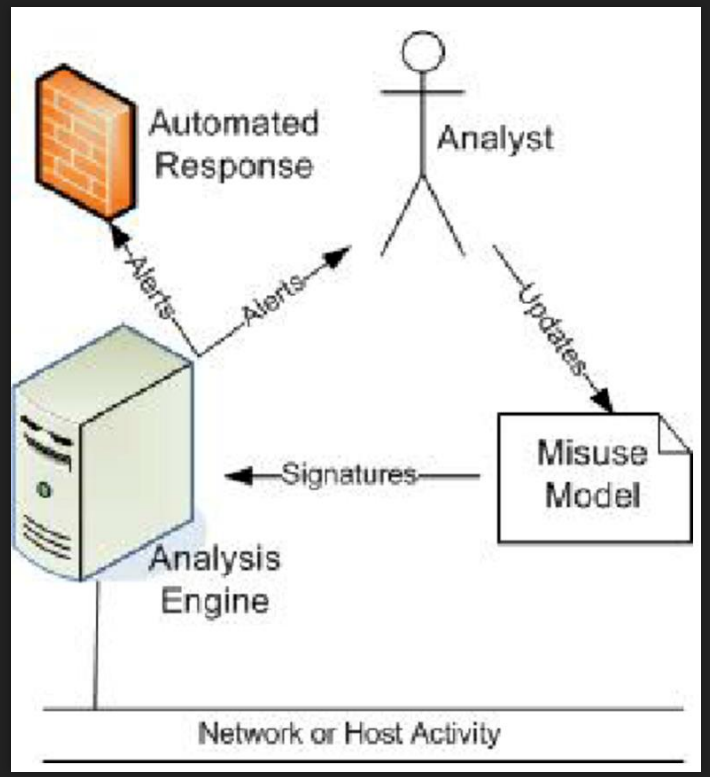
- Capture and Analyze the network traffic packets
- Minute effect on the performance of network

HIDS vs. NIDS

HIDS	NIDS
Insider detection is strong while outsider detection is weak.	Outsider detection is strong while insider detection is weak
Weak real time response but good for long term attacks.	Strong response against outside attacks.
Damage assessment capability is excellent.	Damage assessment capability is very weak.
It analyzes logs and consists of information related to the status of the system.	It analyzes network traffic directly and checks every network event.
It offers protection even if the LAN is off.	It offers protection only on LAN.
It is more versatile.	It is less versatile.
It can detect suspicious behavior patterns properly.	It can't detect suspicious patterns.
These systems are more expensive to implement.	These systems are less expensive to implement.
Its scope is narrow	Its scope is broad.
It is complex to setup and configure.	Is easier to setup and configure.
In these systems, detection is based on records in any single machine.	In these systems, detection is based on records in entire network.
It is operating system specific.	It is operating system independent.

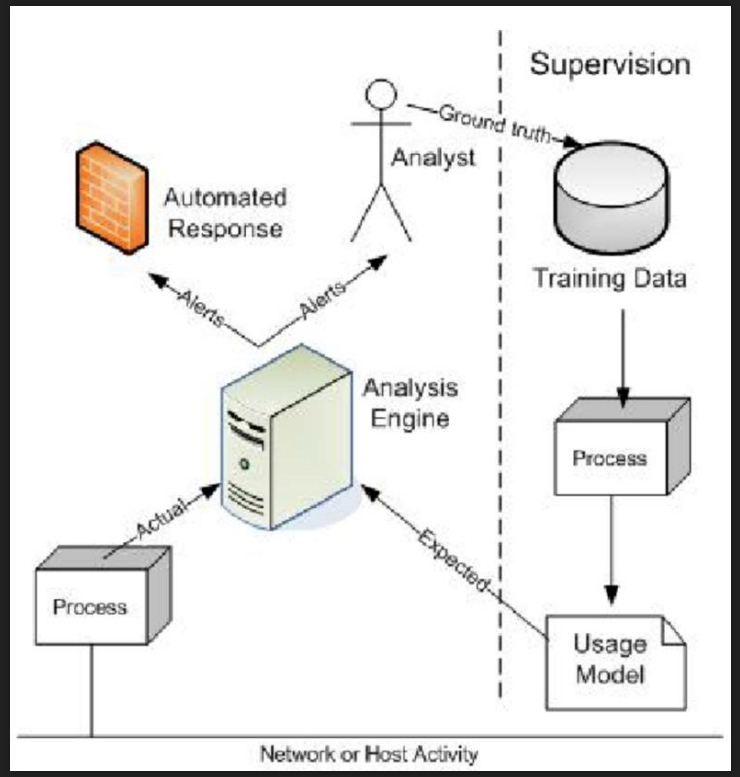
Types for IDS

Signature Based IDS



- Known patterns of unauthorized behavior (Signatures)
- Easy to create
- Only detect predefined pattern

Anomaly Based IDS



- Identify abnormal patterns of behavior
- Have capability to detect new errors
- Various measures used in detection
- Generate false alarms
- Need huge amount of normal information

Signature Based vs. Anomaly Based

Signature Based IDS	Anomaly Based IDS
It can't detect novel attacks.	It has the ability to detect novel attacks.
The attack knowledge is operating environment dependent.	It is less dependent on operating environment.
It's database increases as the number of new attacks increases.	It needs a large set of training data with network environment system logs.
They seemed to have difficulty in handling internal attacks. Abuse of legitimate user privileges is not sensed as a malicious activity	It has the ability to detect abuse of user privileges
A signature characterizes the direct manifestation of intrusion activities in terms of packet headers and payload content.	Anomalies are identified without getting inside their causes and characteristics.
It has very low false alarm rate	It has a substantial false alarm rate
It has simple algorithms.	Its algorithms are complex.
Signatures are easy to develop and understand if you know what network behavior you're trying to identify.	Rules are difficult to define.

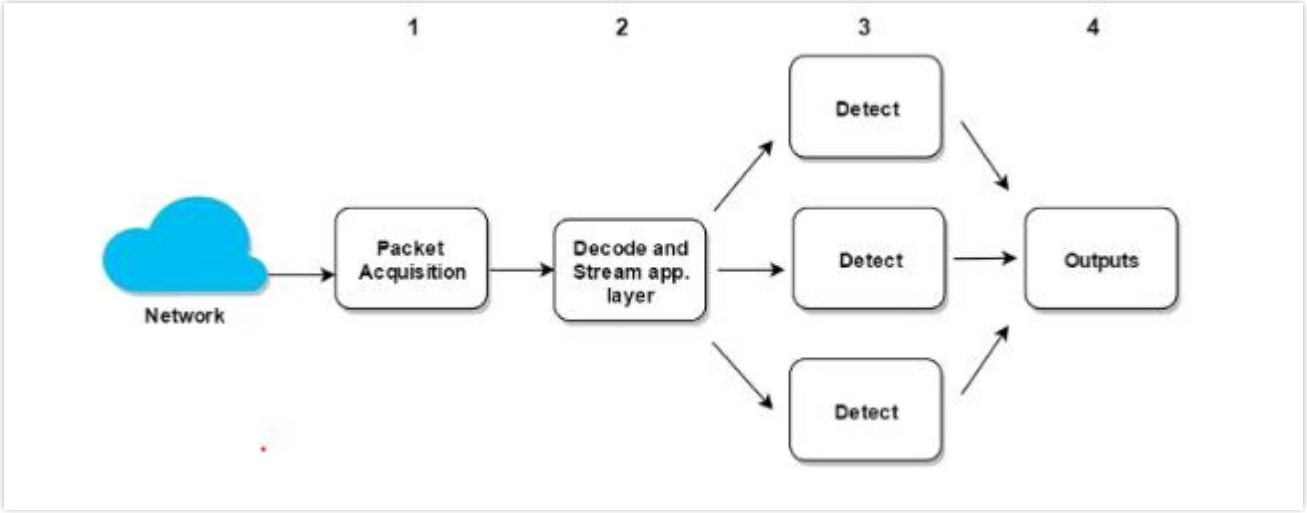
Signature Based IDS	Anomaly Based IDS
Implementation is easy.	Implementation is not easy.
It has minimal system resource usage.	It requires more resources to create protocols and to test their accuracy.
Difficulties in updating information on every new types of attacks.	No need to update database for every new type of attack. It requires a constant update of the normal behavior profile database.
It can't scale quickly and easily because a new signature has to be created for every attack.	The engine can scale more quickly and easily.

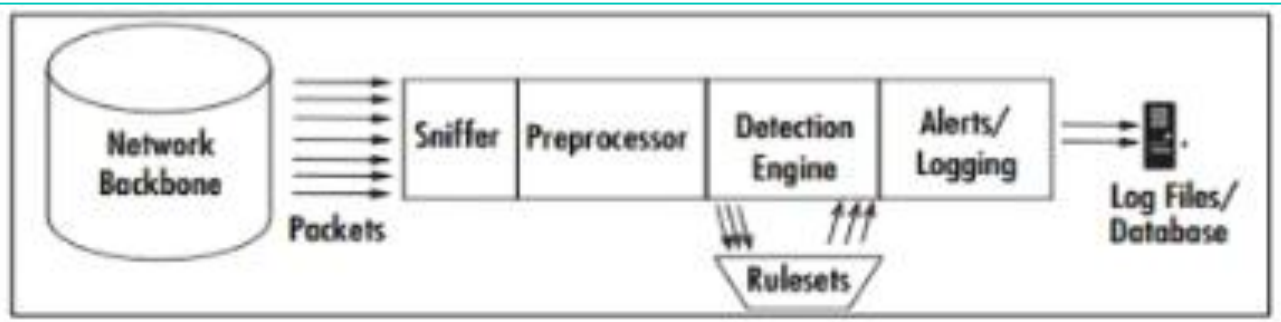
Hybrid Detection

Signature Based IDS  Anomaly Based IDS

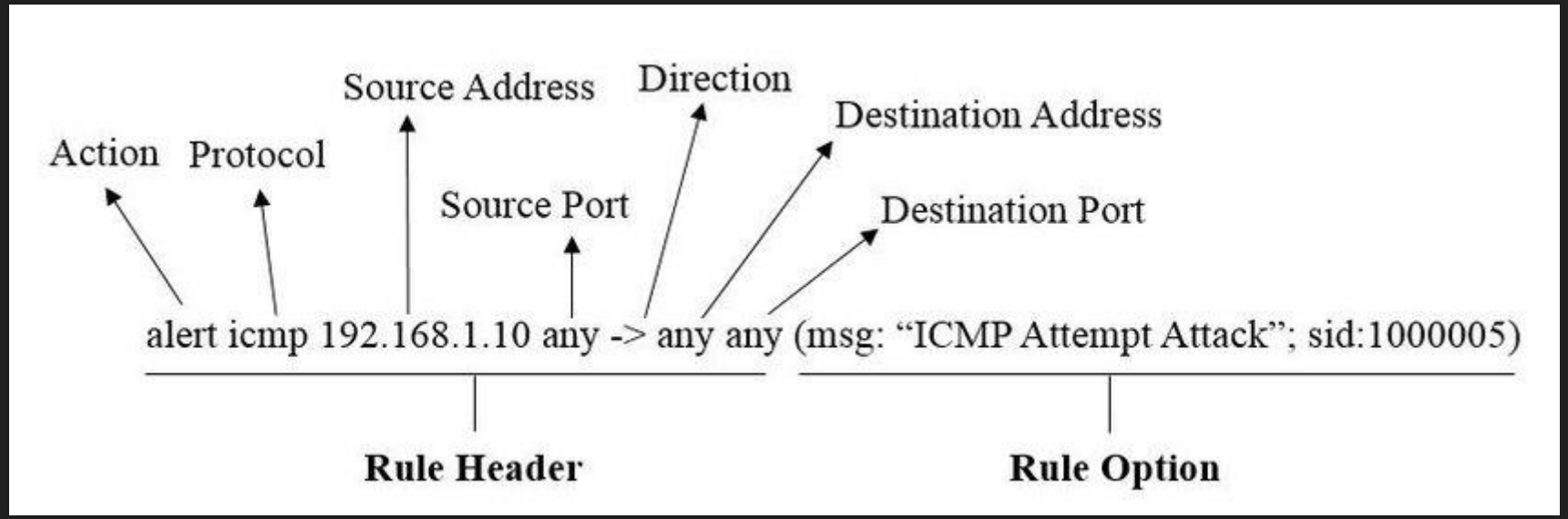
Examples of traditional IDS

Rule based IDS SNORT /SURICATA

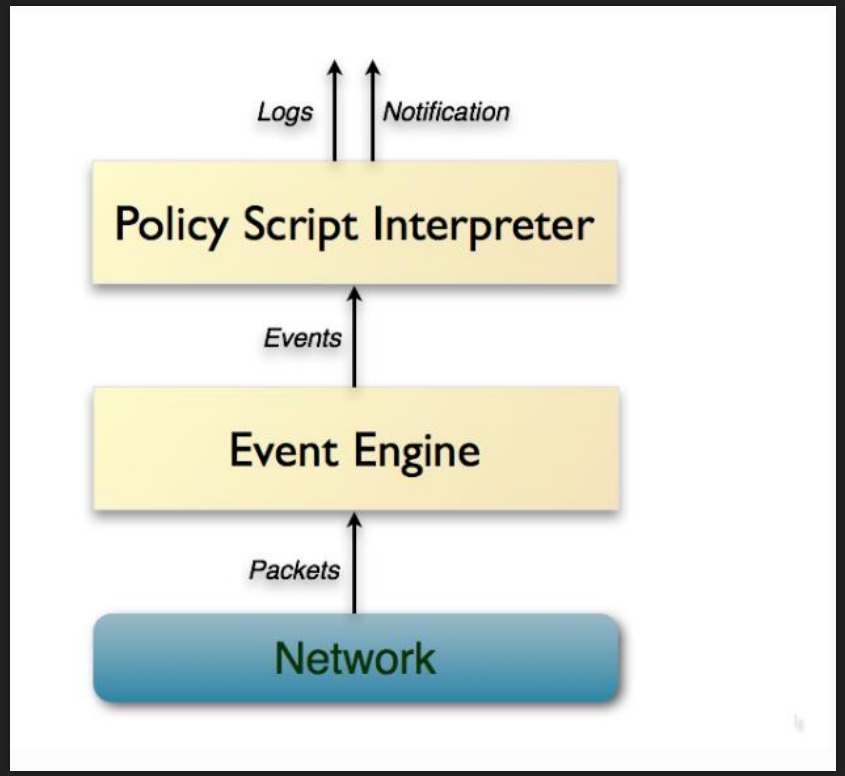




Snort Rules

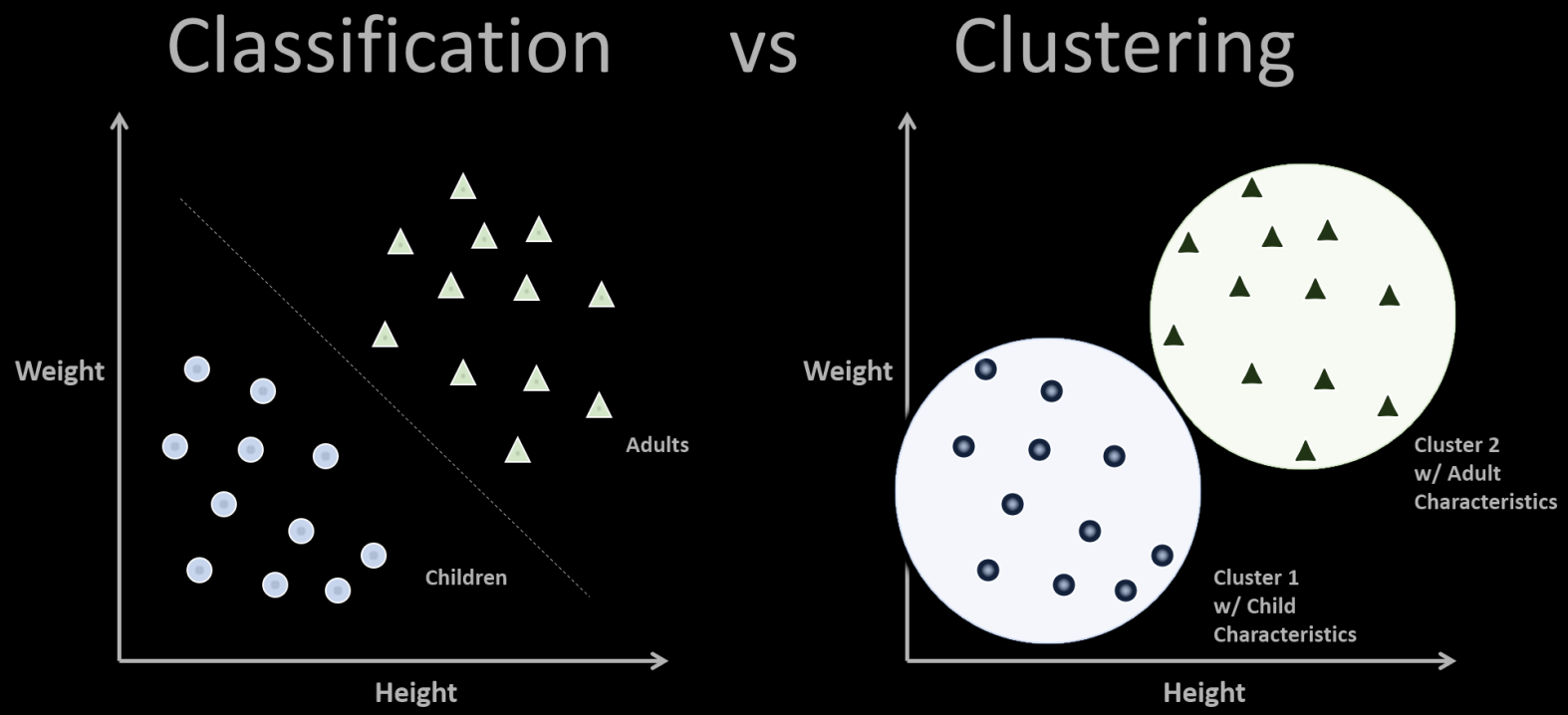

Source Address
Direction
Destination Address
Action
Protocol
Source Port
Destination Port
alert icmp 192.168.1.10 any -> any any (msg: “ICMP Attempt Attack”; sid:1000005)
Rule Header
Rule Option

BRO/ZEEK IDS

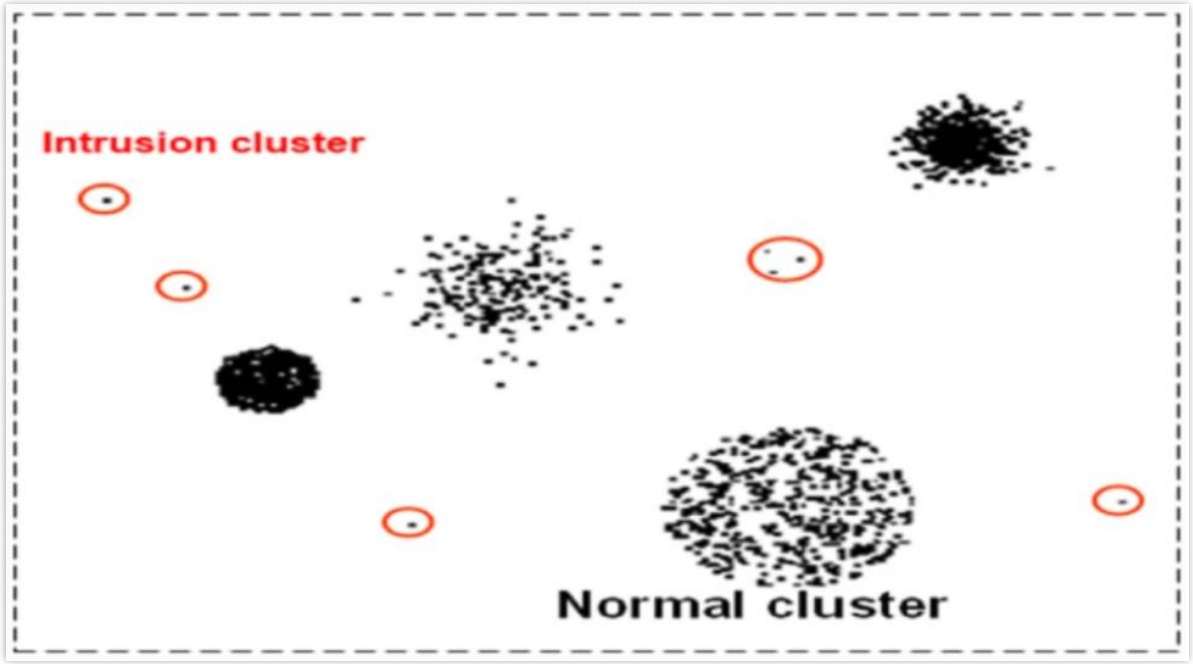

Logs
Notification
Policy Script Interpreter
Events
Event Engine
Packets
Network

Anomaly based intrusion detection

- Supervised based IDS
- Unsupervised

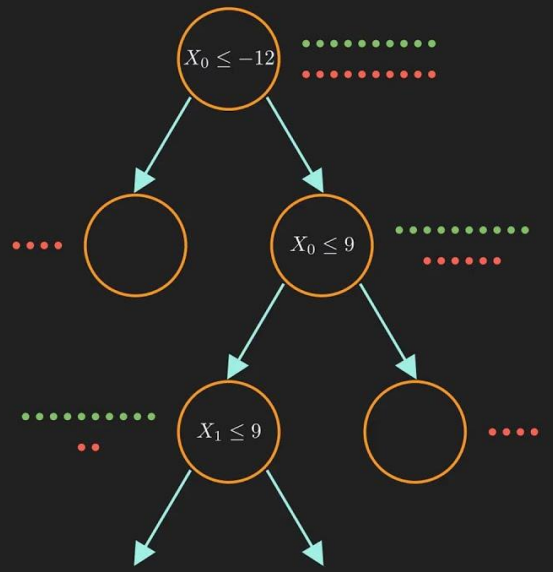


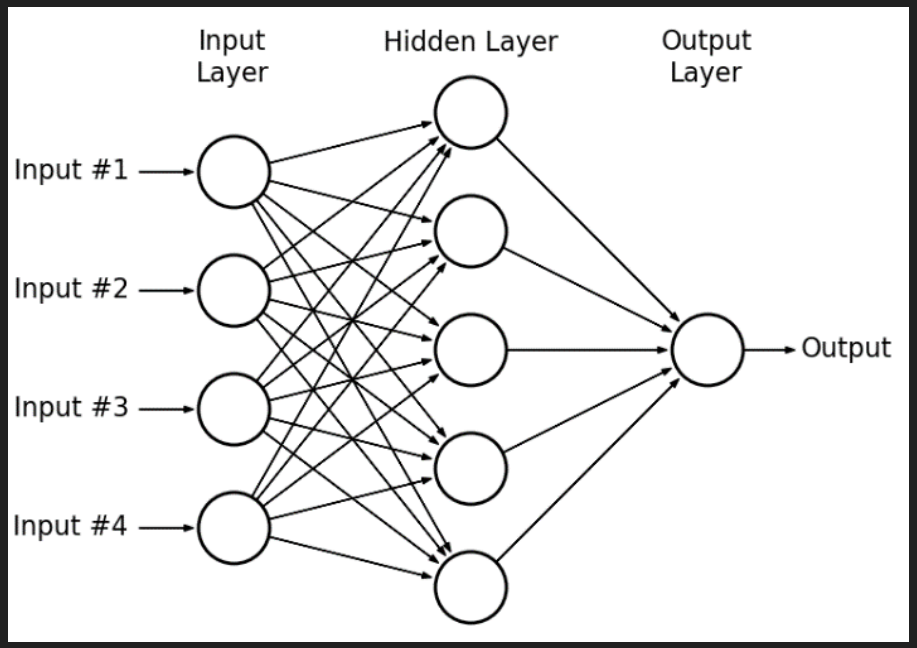
K-means (ML) IDS



Tree, MLP and SVM

Decision Tree Classifier





Future

The Future for IDS

- Rise of machine learning classifiers
- Even traditional ids could combine with machine learning
- Combine unsupervised with supervised machine learning

Reference

1. Saylor Academy, Intrusion Detection Systems, viewed 30 May, https://learn.saylor.org/mod/book/view.php?id=29755&chapterid=5439
2. Security Boulevard, Intrusion Detection Systems: A Deep Dive Into NIDS & HIDS, viewed 30 May, https://securityboulevard.com/2020/03/intrusion-detection-systems-a-deep-dive-into-nids-hids/
3. M. R. Ayyagari, N. Kesswani, M. Kumar, and K. Kumar, "Intrusion detection techniques in network environment: a systematic review," Wireless networks, vol. 27, no. 2, pp. 1269–1285, 2021, doi: 10.1007/s11276-020-02529-3.
4. A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," Journal of network and computer applications, vol. 36, no. 1, pp. 25–41, 2013, doi: 10.1016/j.jnca.2012.08.007.
5. Bo Dong and Xue Wang, "Comparison deep learning method to traditional methods using for network intrusion detection," in 2016 8th IEEE International Conference on Communication Software and Networks (ICCSN), 2016, pp. 581–585. doi: 10.1109/ICCSN.2016.7586590.
6. Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: A systematic study of machine learning and deep learning approaches," Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, p. e4150, 2021.
7. P. Laskov, P. Düssel, C. Schäfer, and K. Rieck, "Learning Intrusion Detection: Supervised or Unsupervised?," in *Image Analysis and Processing – ICIAP 2005*, 2005, pp. 50–57. doi: 10.1007/11553595_
8. S. Anwar *et al.*, "From intrusion detection to an intrusion response system: Fundamentals, requirements, and future directions," *Algorithms*, vol. 10, no. 2, p. 39, 2017, doi: 10.3390/a1002003
9. W. Park and S. Ahn, "Performance Comparison and Detection Analysis in Snort and Suricata Environment," *Wireless personal communications*, vol. 94, no. 2, pp. 241–252, 2016, doi: 10.1007/s11277-016-3209-
10. Bricata | Network Detection & Response | Visibility & Analytics | Threat Hunting. 2022. Bro IDS. [online] Available at: <https://bricata.com/blog/what-is-bro-ids/> [Accessed 16 May 2022].

Thanks for listening