Cybersecurity (Security+) and P4 Programmable Switches

Intrusion Detection and Prevention Systems

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 21st, 2023

Intrusion Detection and Prevention Systems

Intrusion Detection/Prevention System (IDS/IPS)

- Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) monitor network traffic to detect and prevent malicious activities
- These systems are either implemented on a dedicated hardware or implemented as applications on a general-purpose server
- IDS and IPS are placed at strategic points in the network to be able to monitor traffic from all devices

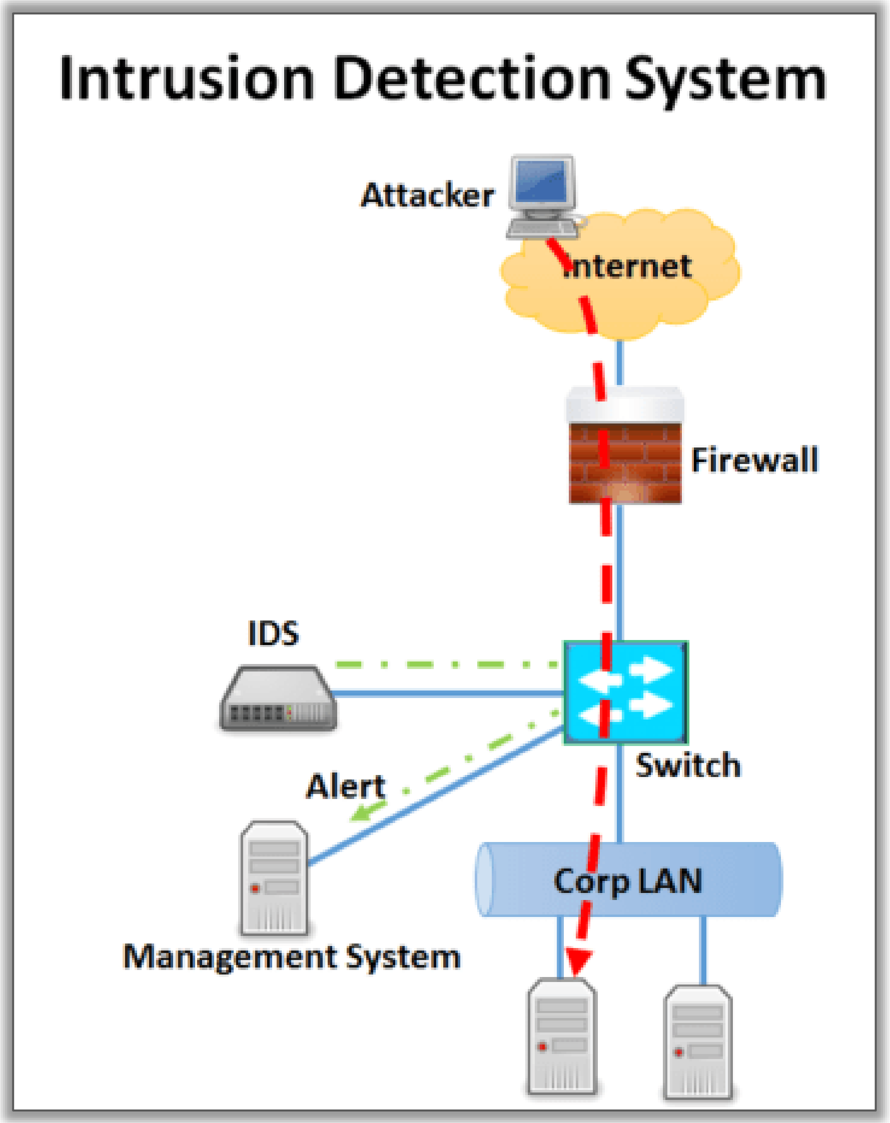
Intrusion Detection/Prevention System (IDS/IPS)

- IDS and IPS leverage a database of attacks’ signatures to detect malicious traffic
- Signature-based IDS/IPS are popular and effective, but cannot detect zero-day attacks
- Machine learning can be leveraged to create a model of the normal of the network
  - Thus, the normal model can be used as a baseline to detect any abnormalities in the network

Intrusion Detection System (IDS)

- An IDS monitors the traffic of a network *passively*
  - ➢ i.e., the IDS is not deployed inline in the topology
- Instead, a network device (e.g., switch, router) duplicates and forwards the traffic to the IDS
- The IDS then analyzes the traffic offline (promiscuous mode) and matches the traffic stream with known malicious signatures
- Advantages of IDS:
  - ➢ It does not negatively impact the performance of the network
  - ➢ It does not affect the network if a problem or misconfiguration of the IDS occurs
- Disadvantages of IDS:
  - ➢ It cannot stop malicious single-packet attacks from reaching the target
  - ➢ It requires assistance from other networking devices to respond to the attack

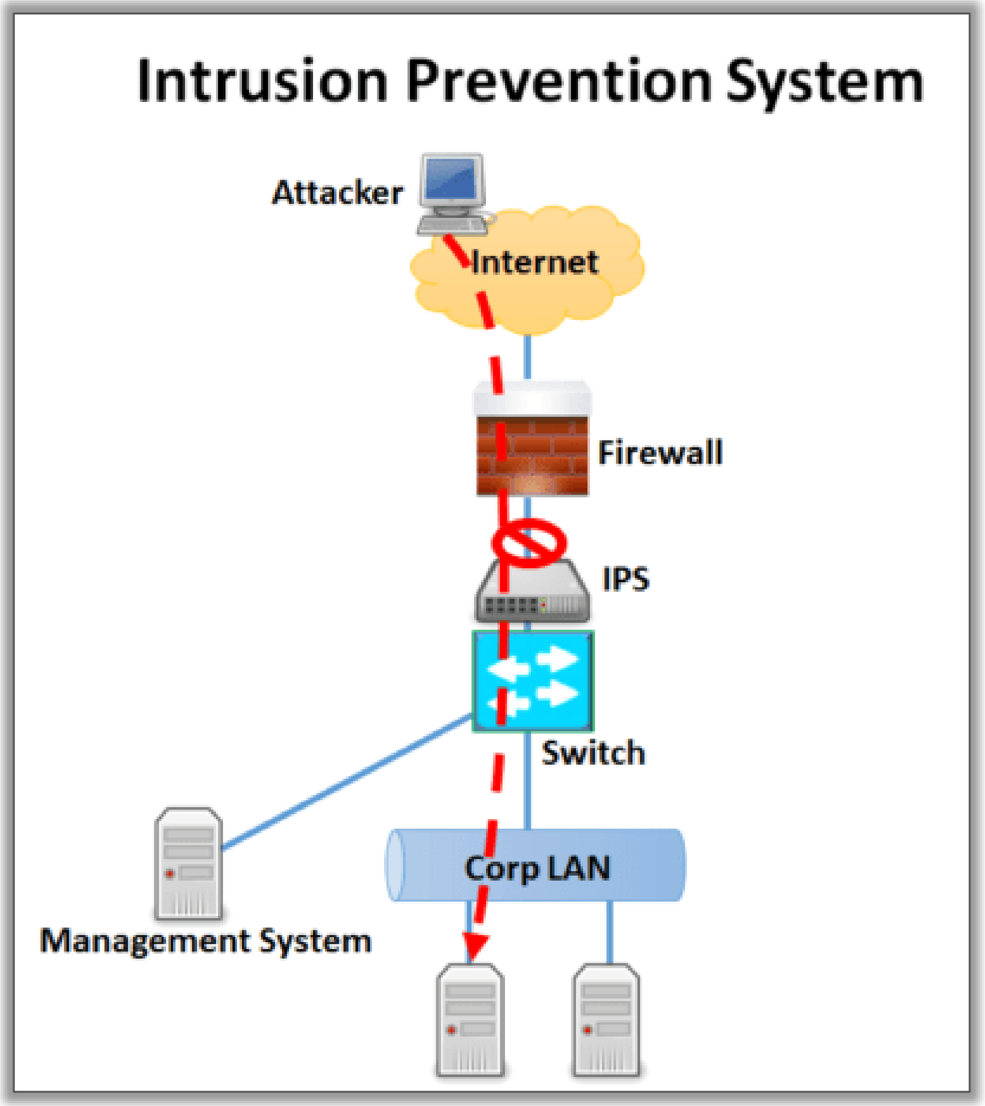
Intrusion Detection System (IDS)



Intrusion Prevention System (IPS)

- An IPS device monitors the network traffic *actively*
  - i.e., the IPS is deployed inline in the topology
- The IPS analyzes traffic online, thus, all ingress and egress traffic must flow through the IPS for processing
- Advantages of IPS:
  - It can stop single packet attacks
- Disadvantages of IPS:
  - It can negatively affect the performance of the network
  - It can disrupt the network if a problem or misconfiguration of the IPS occurs

Intrusion Prevention System (IPS)



Identifying Malicious Traffic on the Network

- Signature-based IPS/IDS
  - ➢ Set of rules looking for some specific pattern in a packet or stream of packets
  - ➢ Most significant method used on today's IPS/IDS
- Policy-based IPS/IDS
  - ➢ Traffic is matched based on the security policy implemented in the network
- Anomaly-based IPS/IDS
  - ➢ A baseline of normal and malicious behavior is modeled and compared to the traffic flowing in the network
- Reputation-based IPS/IDS
  - ➢ A collection of inputs from various sources is gathered, including the reputation of a certain IP address, domain, URL, etc.

IPS/IDS Evasion Techniques

- Traffic fragmentation
  - Malicious traffic is split into multiple parts
- Traffic substitution and insertion
  - Data payload characters are substituted into different formats
- Timing attacks
  - Malicious traffic is sent at slow time intervals
- Encryption and tunneling
  - Malicious traffic is encrypted and cannot be easily inspected
- Resource exhaustion
  - Thousands of alerts are generated

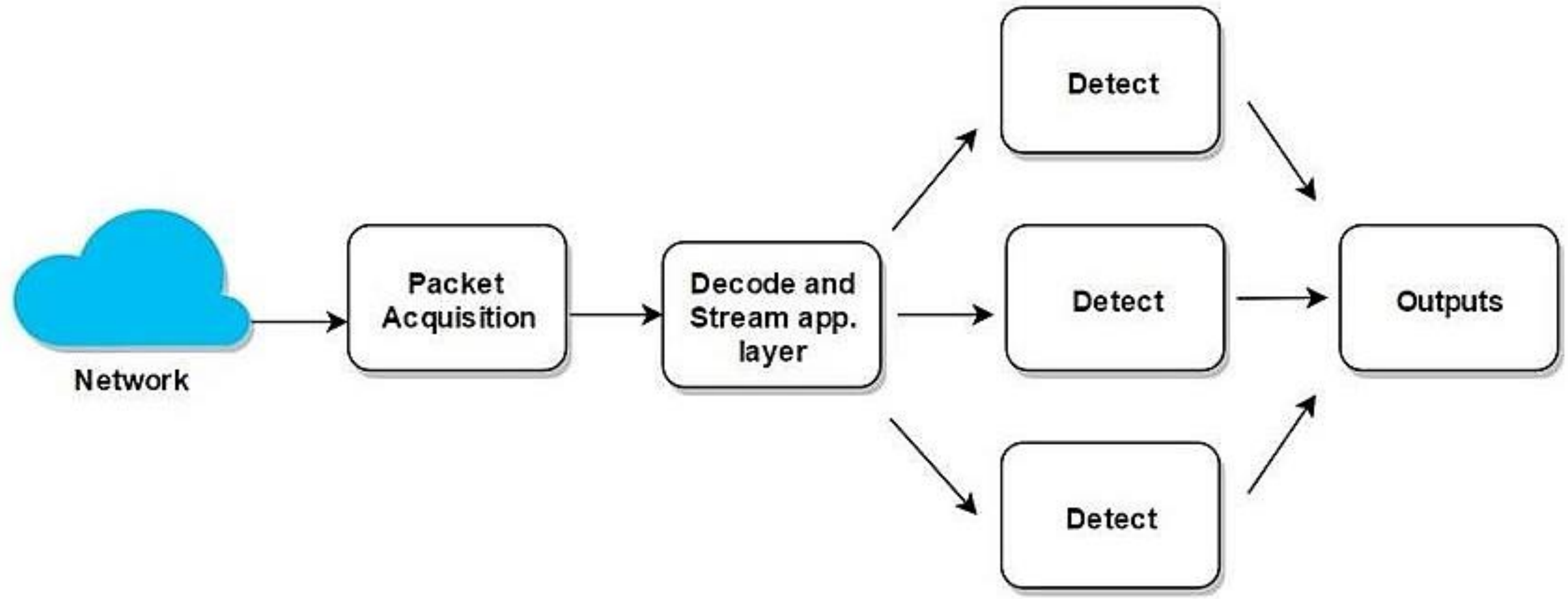
Suricata

Introduction to Suricata

- Suricata is an open-source engine Intrusion Detection System (IDS), Intrusion Prevention System (IPS)
- It is capable of performing Deep Packet Inspection (DPI)
- Suricata has the following properties:
  - Multithreading: multiple cores can be allocated to a single Suricata instance
  - Application ID: Suricata can detect the application type, regardless of the port number
  - Supports logging of events
  - Extensible through a scripting language (Lua)
- Suricata is backed by the Open Information Security Foundation (OISF)

Multi-threading Engine

- Networks today process traffic in the order of tens and hundreds of Gigabytes per second
- Multithreading allows scaling horizontally on a single appliance



Multi-threading Engine